Cours de Troisième Cycle

Année 1986/87.

Université P. et M. Curie (Paris VI)

Institut Henri Poincaré.

QUELQUES ASPECTS TRANSCENDANTS

DE LA THEORIE DES NOMBRES ALGEBRIQUES.

par

Michel WALDSCHMIDT.

SOMMAIRE

CHAPITRE II
REPRESENTATIONS ℓ-ADIQUES.

CHAPITRE III
LA CONJECTURE DE LEOPOLDT.

Le texte qui suit est la rédaction d'un cours de troisième cycle donné à l'Institut Henri Poincaré en 1987. Le but de ce cours était de décrire quelques applications de résultats de la théorie des nombres transcendants. Les énoncés de transcendance eux-mêmes sont formulés (sans démonstration !) dans l'introduction, accompagnés de quelques corollaires qui préfigurent ce qui va suivre.

Dans la première partie, on s'intéresse aux caractères de Hecke. Le second chapitre, qui concerne les représentations ℓ-adiques, est en quelque sorte une traduction ultramétrique de la première. Le dernier thème est la conjecture de Leopoldt sur le rang p-adique du groupe des unités d'un corps de nombres, et l'étude des $\mathbb{Z}_p$-extensions.

La première version de ce texte a été rédigée pour être distribuée aux auditeurs le jour-même où le cours correspondant était donné. Il a ensuite bénéficié de remarques pertinentes et hebdomadaires de François Gramain, qui ont conduit à plusieurs listes d'errata. Quelques mois plus tard, Damien Roy a relu et étudié très soigneusement ce texte, et y apporté de nombreux autres commentaires (une quarantaine de pages) dont la version qui suit tient compte.

Depuis que ce cours a été donné, deux développements nouveaux ont été apportés à ce sujet. D'abord Michel Laurent a obtenu de nouveaux énoncés portant sur la conjecture de Leopoldt, utilisant des outils transcendants. Ensuite Damien Roy a fait progresser considérablement la question de Sansuc considérée au Chapitre 1, §3, grâce à une étude approfondie des sous-groupes de type fini de $\mathbb{R}^n$, denses dans $\mathbb{R}^n$, et minimaux pour cette propriété.

Ces deux développements n'ont pas été inclus ici, mais le présent texte pourra servir d'introduction à ces travaux récents.

Paris, Février 1989.

Michel Waldschmidt.

INTRODUCTION.

Dans ce chapitre introductif, nous présentons les principaux énoncés de transcendance qui seront utilisés, et nous en indiquons quelques corollaires qui préfigurent ce que l'on fera dans le cours.

§1.- Sur la mesure des angles.

Dans l'annexe I de son livre Algèbre linéaire et géométrie élémentaire, (Hermann, 1964), J. Dieudonné traite de la "mesure" des angles. Il commence par énoncer :

Proposition 1.1.- *Il existe des homomorphismes continus du groupe additif* $\mathbb{R}$ *sur le groupe multiplicatif* $\mathbb{U}$ *des nombres complexes de module* 1, *qui sont tous donnés par* $x \longrightarrow e^{i\lambda x}$, *avec* $\lambda \in \mathbb{R}^*$.

Le noyau d'un tel homomorphisme est un sous-groupe fermé de $\mathbb{R}$, isomorphe à $\mathbb{Z}$, et on en déduit un isomorphisme continu de $\mathbb{R}/\mathbb{Z}$ sur $\mathbb{U}$.

Soit maintenant $K=\overline{\mathbb{Q}} \cap \mathbb{R}$ le corps des nombres algébriques réels. Alors, suivant Dieudonné, $K/\mathbb{Z}$ est isomorphe au groupe $\overline{\mathbb{Q}} \cap \mathbb{U}$, mais il n'y a pas de tel isomorphisme qui soit restriction d'un homomorphisme continu en 0. Il en déduit aussi qu'un tel isomorphisme ne peut pas être "localement croissant".

Le point essentiel de la démonstration consiste à dire que si un homomorphisme $x \longrightarrow e^{i\lambda x}$, avec $\lambda \in \mathbb{R}^*$ envoyait K dans $\overline{\mathbb{Q}}=K(i)$, on aurait $e^{i\lambda\alpha} \in \overline{\mathbb{Q}}$ pour tout $\alpha \in K$, ce qui contredirait un résultat de transcendance (voir ci-dessous).

Dans la même direction, Dieudonné signale que les groupes $\overline{\mathbb{Q}} \cap \mathbb{R}_+^*$ et $\overline{\mathbb{Q}} \cap \mathbb{R}$ sont isomorphes (ils tous deux isomorphes (à $\mathbb{Q}^{(\mathbb{N})}$)), mais qu'aucun isomorphisme entre ces deux groupes n'est

- de la forme $x \longrightarrow e^{\lambda x}$,
- localement continu,
- localement croissant.

§2. Enoncés de transcendance.

Nous avons utilisé ci-dessus l'énoncé suivant : soit $t\in\mathbb{C}$; si $e^{t\alpha}\in\overline{\mathbb{Q}}$ pour tout $\alpha\in\overline{\mathbb{Q}}\cap\mathbb{R}$, alors $t=0$.

Il semble nécessaire, pour établir ce résultat, de faire appel à l'arsenal des méthodes transcendantes. En contre-partie, ces méthodes donnent beaucoup mieux : il suffit que l'hypothèse soit vérifiée pour seulement *deux* valeurs de α linéairement indépendantes sur $\mathbb{Q}$:

Théorème 2.1 (Gel'fond-Schneider).- (Première forme): *soient α et β deux nombres algébriques, avec $\alpha\neq 0$, et $\beta\notin\mathbb{Q}$. Soit $\log\alpha$ une détermination non nulle du logarithme de α. Alors le nombre $\alpha^{\beta}=\exp(\beta\log\alpha)$ est transcendant.* (Deuxième forme): *soient α_1 et α_2 deux nombres algébriques non nuls, et $\log\alpha_1$, $\log\alpha_2$ des déterminations de leurs logarithmes. On suppose que les deux nombres $\log\alpha_1$, $\log\alpha_2$ sont $\mathbb{Q}$-linéairement indépendants. Alors $\log\alpha_1$, $\log\alpha_2$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.*

Nous utiliserons aussi la généralisation suivante, due à Baker (Transcendental number theory, Cambridge Univ. Press,1979) :

Théorème 2.2 (Baker).-(Première forme): *soient $\alpha_1,\ldots,\alpha_n$ des nombres algébriques non nuls, $\log\alpha_1,\ldots,\log\alpha_n$ des déterminations non toutes nulles de leurs logarithmes, et $\beta_1,\ldots,\beta_n$ des nombres algébriques $\mathbb{Q}$-linéairement indépendants. Alors*

$$\sum_{i=1}^{n}\beta_i\log\alpha_i \neq 0.$$

(Deuxième forme): *soient* $\alpha_1,\ldots,\alpha_n$ *des nombres algébriques non nuls, et* $\log\alpha_1,\ldots,\log\alpha_n$ *des déterminations de leurs logarithmes ; si* $\log\alpha_1,\ldots,\log\alpha_n$ *sont linéairement indépendants sur* $\mathbb{Q}$, *alors* $\log\alpha_1,\ldots,\log\alpha_n$ *sont linéairement indépendants sur* $\overline{\mathbb{Q}}$.

Ainsi, en désignant par $\mathbf{L}$ le sous-espace vectoriel de $\mathbb{C}$ sur $\mathbb{Q}$ formé des logarithmes de nombres algébriques :

$$\mathbf{L} = \{\ell\in\mathbb{C} \ ; \ e^{\ell}\in\overline{\mathbb{Q}}^*\},$$

le théorème de Baker signifie que pour un hyperplan V de $\mathbb{C}^n$ défini sur $\overline{\mathbb{Q}}$:

$$\beta_1 z_1+\ldots+\beta_n z_n = 0, \quad \text{avec } \beta_1,\ldots,\beta_n \text{ algébriques,}$$

on a $V\cap\mathbf{L}^n=0$ si et seulement si $V\cap\mathbb{Q}^n=0$ (c'est-à-dire si et seulement si $\beta_1,\ldots,\beta_n$ sont $\mathbb{Q}$-linéairement indépendants).

Un autre type d'énoncé sera utile ; on ne suppose plus V défini sur $\overline{\mathbb{Q}}$; on peut caractériser les hyperplans V pour lesquels le $\mathbb{Q}$-espace vectoriel $V\cap\mathbf{L}^n$ est de dimension infinie (cf. M. Emsalem, Places totalement décomposées dans des $\mathbb{Z}_p$-extensions, Crelle J. **382** (1987), 181-198).

Théorème 2.3.- *Soit* V *un hyperplan de* $\mathbb{C}^n$ *d'équation* $\sum_{i=1}^{n} t_i z_i=0$. *Alors la dimension sur* $\mathbb{Q}$ *de* $V\cap\mathbf{L}^n$ *est finie si et seulement si* $V\cap\mathbb{Q}^n = 0$. *Dans ce cas, on a*

$$\dim_{\mathbb{Q}}(V\cap\mathbf{L}^n) \leq n(n-1).$$

Dans le cas $n=2$, on obtient le **théorème des six exponentielles** :

Corollaire 2.4.- (Première forme): *soient* x_1, x_2 *des nombres complexes linéairement indépendants sur* $\mathbb{Q}$, *et* y_1, y_2, y_3 *des nombres complexes linéairement indépendants sur* $\mathbb{Q}$. *Alors un au moins des six nombres*

$$e^{x_i y_j}, \qquad (i=1,2 \ ; \ j=1,2,3)$$

est transcendant.

(Deuxième forme): *soit* $(\log\alpha_{ij})_{1\leq i\leq d, 1\leq j\leq \ell}$ *une matrice* $d\times\ell$ *à coefficients dans* **L**. *On suppose que deux au moins des lignes sont linéairement indépendantes sur* $\mathbb{Q}$, *et que trois au moins des colonnes sont linéairement indépendantes sur* $\mathbb{Q}$. *Alors le rang de la matrice est supérieur ou égal à* 2.

On déduit du théorème des six exponentielles que si t est un nombre complexe tel que 2^t, 3^t et 5^t sont tous trois algébriques, alors t est rationnel. Il est d'ailleurs facile de démontrer (en utilisant les différences finies) que si un nombre réel t est tel que n^t soit un entier rationnel pour tout $n\in\mathbb{Z}$, $n\geq 0$, alors $t\in\mathbb{Z}$. (Question : peut-on démontrer de manière similaire le cas particulier du théorème de Gel'fond-Schneider utilisé par Dieudonné ?).

On ne sait pas s'il existe un nombre réel irrationnel t tel que 2^t et 3^t soient tous deux entiers. Plus généralement, le **problème des 4 exponentielles** consiste à montrer que, dans le théorème des 6 exponentielles, on peut remplacer y_1, y_2, y_3 par y_1, y_2 (première forme), c'est-à-dire qu'il suffit de deux colonnes $\mathbb{Q}$-linéairement indépendantes (deuxième forme).

D'un autre côté, il ne suffit pas de supposer ℓ et d grands, avec toutes les lignes (resp. les colonnes) $\mathbb{Q}$-linéairement indépendantes, pour assurer que le rang de la matrice est au moins 3.

Pour décrire la situation d'un point de vue conjectural, il devrait suffire d'admettre l'énoncé suivant :

Conjecture 2.5.- *soient* $\alpha_1,\ldots,\alpha_n$ *des nombres algébriques non nuls, et* $\log\alpha_1,\ldots,\log\alpha_n$ *des déterminations de leurs logarithmes ; si* $\log\alpha_1,\ldots,\log\alpha_n$ *sont linéairement indépendants sur* $\mathbb{Q}$, *alors* $\log\alpha_1,\ldots,\log\alpha_n$ *sont algébriquement indépendants (sur* $\mathbb{Q}$ *ou sur* $\overline{\mathbb{Q}}$, *cela revient au même).*

Question.- Cette conjecture implique-t-elle que dans la situation du théorème 2.3, on a $\dim_{\mathbb{Q}} V\cap L^n \leq \frac{1}{2}.n(n-1)$? [1]

§3.- Caratères de Hecke.

Le début du cours sera consacré à l'étude des homomorphismes continus de G_1 dans G_2, quand G_1 (resp. G_2) désigne l'un des groupes topologiques $\mathbb{R}$, $\mathbb{R}_+^*$, $\mathbb{U}$, $\mathbb{C}$, et $\mathbb{C}^*$. Par exemple on vérifiera que tout homomorphisme continu $\chi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$ est de la forme

$$z \longrightarrow \left[\frac{z}{|z|}\right]^m . |z|^t,$$

avec $m\in\mathbb{Z}$, et $t\in\mathbb{C}$.

Le théorème des six exponentielles donne alors l'équivalence entre les assertions suivantes :

(i) $t\in\mathbb{Q}$

(ii) $\chi(\mathbb{Q}^*)\subset\overline{\mathbb{Q}}^*$

(iii) pour tout corps de nombres k plongé dans $\mathbb{C}$, on a $\chi(k^*)\subset\overline{\mathbb{Q}}^*$.

Suivant Weil (Tokyo-Nikko 1955), on dit alors que χ est de type (A) (pour : algébrique).

Nous voulons maintenant remplacer dans (iii), le corps $\overline{\mathbb{Q}}$ des nombres algébriques par un corps de nombres E (dépendant de k)

Montrons d'abord que la condition $t\in\mathbb{Z}$ équivaut à dire qu'il existe un corps de nombres E tel que $\chi(\mathbb{Q}^*)\subset E^*$. Cela repose sur le lemme suivant :

---

[1] Cette question a été résolue en 1987 par Damien Roy. La réponse est affirmative.

Lemme 3.1.- *Soit* E *un corps de nombres et soit* ℓ *un nombre premier. Il existe un entier* $n>0$ *tel que l'équation* $x^{\ell}=n$ *n'ait pas de solution* x *dans* E.

Alors, si $t\in\mathbb{Q}$ n'est pas entier, on écrit $t=p/q$, avec $(p,q)=1$, on choisit un diviseur premier ℓ de q, puis un entier $n>0$ qui ne soit pas une puissance ℓ-ième dans E. Si $\alpha:=n^t$ appartenait à E, on aurait

$$n^p=\alpha^q=\beta^{\ell}, \qquad \text{avec } \beta:=\alpha^{q/\ell}\in E ;$$

en écrivant l'identité de Bezout : $ap+b\ell=1$, on trouverait

$$n=n^{ap+b\ell}=(\beta^a n^b)^{\ell},$$

avec $\beta^a n^b\in E$, et n serait une puissance ℓ-ième dans E.

Démonstration du lemme 3.1.-

Si un nombre premier p est une puissance ℓ-ième dans E, alors $(p)=(\alpha)^{\ell}$, et l'idéal (p) est ramifié dans E. Il n'y en a donc qu'un nombre fini.

Revenons au problème consistant à remplacer, dans (iii), le corps $\overline{\mathbb{Q}}$ des nombres algébriques par un corps de nombres E. En prenant $k=\mathbb{Q}(i)$, nous allons montrer qu'il ne suffit pas de supposer $t\in\mathbb{Z}$:

Lemme 3.2.- *Soit* E *un corps de nombres. Il existe* $\alpha\in\mathbb{Z}[i]$ *tel que* $\alpha\bar{\alpha}$ *ne soit pas un carré dans* E.

Démonstration.- On veut trouver a et b dans $\mathbb{Z}$ avec $\sqrt{a^2+b^2}\notin E$. Pour cela, soit p un nombre premier qui se décompose dans $\mathbb{Q}(i)$:

$$p=a^2+b^2, \qquad (a,b)\in\mathbb{Z}^2.$$

Si $\alpha:=a+ib$ vérifie $\alpha\bar{\alpha}=\beta^2$ avec $\beta\in E$, alors p se ramifie dans E, donc divise le discriminant de E. Comme il y a une infinité de nombres premiers congrus à 1 modulo 4, on en déduit le lemme.

Grâce à ce lemme, nous allons démontrer :

Proposition 3.3.- *Soit* $\chi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$ *un homomorphisme continu. Les propriétés suivantes sont équivalentes :*

(i) *Il existe* a *et* b *dans* $\mathbb{Z}$ *tels que*

$$\chi(z) = z^a.\bar{z}^b.$$

(ii) $\chi(\mathbb{Q}(i))\subset\mathbb{Q}(i)^*$.

(iii) *Pour tout corps de nombres* k *plongé dans* $\mathbb{C}$, *il existe un corps de nombres* E *tel que* $\chi(k^*)\subset E^*$.

Définition : suivant Weil, on dira alors que χ est de type (A_0).

Remarque : si on écrit $\chi(z) = \left(\frac{z}{|z|}\right)^m.|z|^t$, alors la condition (i) revient à dire que t est un entier de même parité que m : $t-m\in 2\mathbb{Z}$.

Démonstration de la proposition 3.3.-

Si (i) est vraie, alors dans (iii) on peut prendre pour E le compositum de k et de son image par la conjugaison complexe.

Il reste à démontrer que si $\chi(\mathbb{Q}(i))$ est contenu dans E^* où E est un corps de nombres, alors χ vérifie (i). Quitte à remplacer E par E(i), on peut supposer $E\supset\mathbb{Q}(i)$. L'hypothèse implique en particulier $\chi(\mathbb{Q}^*)\subset E^*$. D'après ce qui précède, on a donc $t\in\mathbb{Z}$:

$$\chi(z) = z^m.|z|^{t-m}.$$

Si $t-m$ n'est pas pair, en posant $t-m=1+2h$ on a

$$\chi(z) = z^{m+h}.\bar{z}^{-h}.(z\bar{z})^{1/2},$$

et $\chi(\alpha)/\ \alpha^{m+h}.\bar{\alpha}^{-h} = (\alpha\bar{\alpha})^{1/2}$ appartient à E^* pour tout $\alpha\in\mathbb{Q}(i)^*$, ce qui contredit le lemme 3.2.

Dans le premier chapitre, consacré aux caractères de Hecke, nous généraliserons les résultats précédents en considérant des homomorphismes de $\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$ dans $\mathbb{C}^*$; nous verrons que, si k est un corps de nombres ayant r_1 plongements réels et $2r_2$ plongements complexes, pour qu'un tel

homomorphisme envoie k^* dans $\overline{\mathbb{Q}}^*$ (resp. dans le groupe multiplicatif E^* d'un corps de nombres E), il faut et il suffit qu'il soit produit de caractères de type (A) (resp. (A_0)).

§4. Nombres p-adiques.

Nous allons remplacer dans l'étude précédente la valeur absolue ordinaire de $\mathbb{Q}$ par une valeur absolue p-adique : $|n|_p=p^{-a_p}$ si $n = \prod_p p^{a_p}$. Nous désignons par $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ l'anneau des entiers p-adiques, par $\mathbb{Q}_p$ le corps des nombres p-adiques, par $\overline{\mathbb{Q}}_p$ la clôture algébrique de $\mathbb{Q}_p$, et par $\mathbb{C}_p$ le complété de $\overline{\mathbb{Q}}_p$. On rappelle que $\mathbb{C}_p$ est algébriquement clos (voir par exemple Y. Amice, les nombres p-adiques, P.U.F., Collection SUP, N°14, 1975 ; L. Washington, Introduction to cyclotomic fields, §5.1 ; J-P. Serre, Cours d'arithmétique, P.U.F., Collection SUP, N°2, 1970, Ch.2 §3).

L'anneau $\mathbb{Z}_p$ est un anneau de valuation discrète, d'idéal maximal $p\mathbb{Z}_p$, de corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Le groupe $\mathbb{Z}_p^*=\mathbb{Z}_p-p\mathbb{Z}_p$ des éléments inversibles de $\mathbb{Z}_p$ se décompose en produit direct $T\times(1+p\mathbb{Z}_p)$, où T est l'ensemble des racines $(p-1)$-ièmes de l'unité dans $\mathbb{Z}_p$ (c'est un sous-groupe discret cyclique d'ordre $p-1$ de $\mathbb{Z}_p^*$), et

$$1+p\mathbb{Z}_p = \{x\in\mathbb{Z}_p \ ; \ |x-1|_p<1\}$$

est un sous-groupe ouvert et fermé de $\mathbb{Z}_p^*$. D'autre part $\mathbb{Q}_p^*=G\times\mathbb{Z}_p^*$, où $G=\{p^n \ ; \ n\in\mathbb{Z}\}$.

Le domaine de convergence de la série

$$\sum_{n\geq 0} z^n/n!$$

dans $\mathbb{C}_p$ est le sous-groupe de $\mathbb{C}_p$:

$$D = \{z\in\mathbb{C}_p \ ; \ |z|_p<p^{-1/(p-1)}\},$$

et cette série définit un homomorphisme continu noté $\exp_p$ (ou plus simplement exp) de D dans $\mathbb{C}_p^*$. L'image de D par $\exp_p$ est $1+D$. D'autre part le domaine de convergence de la série

$$\sum_{n\geq 1} (-1)^{n-1}(z-1)^n/n$$

dans $\mathbb{C}_p$ est le sous-groupe de $\mathbb{C}_p^*$:

$$L = \{z\in\mathbb{C}_p \ ; \ |z-1|_p<1\},$$

et cette série définit un homomorphisme continu $\log_p$ de L dans $\mathbb{C}_p$. L'image $\log_p(L)$ de $\log_p$ est un sous-groupe de $\mathbb{C}_p$ contenant D, et on a, pour $x\in D$ et $y\in 1+D$:

$$\log_p(\exp_p x)=x \quad \text{et} \quad \exp_p(\log_p y)=y.$$

Donc $\exp_p$ et $\log_p$ établissent des isomorphismes réciproques entre D et 1+D. Enfin il existe un unique homomorphisme de $\mathbb{C}_p^*$ dans $\mathbb{C}_p$, qui coïncide avec $\log_p$ sur L, et qui s'annule en p. On notera encore $\log_p$ ce prolongement : $\log_p p=0$.

Les énoncés de transcendance que nous avons vus au §1 peuvent être étendus au cas p-adique, à condition de remplacer $\overline{\mathbb{Q}}$ par la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_p$ (que nous noterons encore $\overline{\mathbb{Q}}$) ; de plus, bien entendu, si on travaille avec la fonction exponentielle, on doit se limiter à son domaine de convergence.

Théorème 4.1 (Baker-Brumer).- *Soient* $\alpha_1,\dots\alpha_n$ *des éléments non nuls de* $\mathbb{C}_p$ *algébriques sur* $\mathbb{Q}$; *si les nombres* $\log_p\alpha_1,\dots,\log_p\alpha_n$ *sont linéairement indépendants sur* $\mathbb{Q}$, *alors ils sont linéairement indépendants sur la clôture algébrique* $\overline{\mathbb{Q}}$ *de* $\mathbb{Q}$ *dans* $\mathbb{C}_p$.

Autrement dit (cf. Th. 2.2, première forme), si nous désignons par $\mathbb{L}_p$ le sous-espace vectoriel de $\mathbb{C}_p$ sur $\mathbb{Q}$ formé des $\log_p\alpha$, pour $\alpha\in\overline{\mathbb{Q}}^*$, pour un hyperplan V de $\mathbb{C}_p^n$ défini sur $\overline{\mathbb{Q}}$, on a $V\cap\mathbb{L}_p^n=0$ si et seulement si $V\cap\mathbb{Q}^n=0$. Voici ce qui se passe si on ne suppose plus V défini sur $\overline{\mathbb{Q}}$ (cf. M. Emsalem, op. cit.).

Theorème 4.2.- *Soit* V *un hyperplan de* $\mathbb{C}_p^n$. *Le* $\mathbb{Q}$*-espace vectoriel* $V\cap L_p^n$ *est de dimension finie si et seulement si* $V\cap\mathbb{Q}^n=0$, *et dans ce cas*

$$\dim_{\mathbb{Q}} V\cap L_p^n \leq n(n-1).$$

On traduit de même en p-adique le théorème des six exponentielles et la conjecture des quatre exponentielles (cf. J.-P. Serre, Dépendance d'exponentielles p-adiques, Sém. Delange-Pisot-Poitou, 7ème année, 1965-66, N°15).

§5.- La conjecture de Leopoldt.

a) Le théorème des unités de Dirichlet.

Soit k un corps de nombres de degré d. Soient $\sigma_1,\ldots,\sigma_{r_1}$ les différents plongements de k dans $\mathbb{R}$, et $\sigma_{r_1+1},\ldots,\sigma_d$ les plongements non réels de k dans $\mathbb{C}$, deux-à-deux conjugués :

$$\sigma_{r_1+j}=\overline{\sigma}_{r_1+r_2+j} , \qquad (1\leq j\leq r_2).$$

Le plongement canonique de k est l'application de k dans $\mathbb{R}^d$ qui envoie α sur

$$(\sigma_1\alpha,\ldots,\sigma_{r_1}\alpha,\ \mathrm{Re}\sigma_{r_1+1}\alpha,\mathrm{Im}\sigma_{r_1+1}\alpha,\ldots,\ \mathrm{Re}\sigma_{r_1+r_2}\alpha,\mathrm{Im}\sigma_{r_1+r_2}\alpha).$$

C'est un homomorphisme injectif, et l'image de l'anneau des entiers $\mathcal{O}=\mathcal{O}_k$ de k est un réseau de $\mathbb{R}^d$ (sous-groupe discret de rang d).

Le plongement logarithmique de k est l'homomorphisme λ du groupe multiplicatif k^* de k dans le groupe additif $\mathbb{R}^{r_1+r_2}$ qui envoie α sur

$$(\log|\sigma_1\alpha|,\ldots,\log|\sigma_{r_1}\alpha|,\ 2\log|\sigma_{r_1+1}\alpha|,\ldots,2\log|\sigma_{r_1+r_2}\alpha|).$$

L'image par λ du groupe des unités $\mathcal{O}_k^*$ de k est évidement contenue dans l'hyperplan H d'équation $\sum_{i=1}^{d} z_i=0$, et le **théorème de Dirichlet** affirme que $\lambda(\mathcal{O}_k^*)$ est un réseau de rang $r=r_1+r_2-1$ dans cet hyperplan. On en déduit que $\mathcal{O}_k^*$ est un groupe de type fini, isomorphe au produit de son sous-groupe de torsion ($\mathcal{O}_{tors}^*$, groupe des racines de l'unité contenues dans k, qui est un

groupe cyclique d'ordre pair), par un groupe abélien libre de type fini (isomorphe à $\mathbb{Z}^r$).

On appelle *système indépendant d'unités* (resp *système fondamental d'unités*) toute famille de r unités qui engendre un sous-groupe d'indice fini de $\mathcal{O}_k^*$ (resp. qui, avec $\mathcal{O}_{tors}^*$, engendre $\mathcal{O}_k^*$).

Quand $\eta_1,\dots,\eta_t$ sont des unités de k, on appelle *matrice régulateur de* $\eta_1,\dots,\eta_t$ la matrice $t\times(r_1+r_2)$ dont les lignes sont $\lambda(\eta_i)$, $(1\leq i\leq t)$. Si $t=r$, comme $\lambda(\mathcal{O}_k^*)$ est contenu dans l'hyperplan H, tous les mineurs $r\times r$ ont la même valeur absolue ; cette valeur absolue est *le régulateur de* $\eta_1,\dots,\eta_r$:

$$R = \left|\det \begin{bmatrix} \log|\sigma_1\eta_1| & \dots & \log|\sigma_{r_1}\eta_1| & 2\log|\sigma_{r_1+1}\eta_1| & \dots 2\log|\sigma_r\eta_1| \\ \vdots & & \vdots & \vdots & \vdots \\ \log|\sigma_1\eta_r| & \dots & \log|\sigma_{r_1}\eta_r| & 2\log|\sigma_{r_1+1}\eta_r| & \dots 2\log|\sigma_r\eta_r| \end{bmatrix}\right|.$$

Un système indépendant d'unités est caractérisé par $R\neq 0$. D'autre part le quotient du régulateur d'un système indépendant $\eta_1,\dots,\eta_r$ par le régulateur d'un système fondamental $\epsilon_1,\dots,\epsilon_r$ est égal à l'indice dans $\mathcal{O}_k^*$ du sous-groupe engendré par $\eta_1,\dots,\eta_r$ et $\mathcal{O}_{tors}^*$. En particulier la valeur minimale du régulateur est atteinte si et seulement si le système d'unités est fondamental ; cette valeur minimale est *le régulateur* R_k *du corps* k.

<u>Exemple</u>. Prenons pour k le corps de décomposition du polynôme X^3-2 sur $\mathbb{Q}$: $k=\mathbb{Q}(j,\sqrt[3]{2})$, avec $j=e^{2i\pi/3}$; on a $d=6$, $r_1=0$, $r_2=3$, $r=2$. Un système indépendant d'unités est $\eta_1=\sqrt[3]{2}-1$, $\eta_2=j\sqrt[3]{2}-1$. Trois plongements non conjugués de k dans $\mathbb{C}$ sont σ_1, σ_2, σ_3, qui envoient $\sqrt[3]{2}$ respectivement sur $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2.\sqrt[3]{2}$, et laissent j invariant. On a $\sigma_1(\eta_1)=\eta_1$, $\sigma_1(\eta_2)=\eta_2$, $\sigma_2(\eta_1)=\eta_2$, et $|\sigma_2(\eta_2)|=|\eta_2|$. Si m désigne l'indice dans $\mathcal{O}_k^*$ du sous-groupe engendré par η_1, η_2, -1 et j, le régulateur de k est donc :

$$R_k = \frac{1}{m}\left|\det \begin{bmatrix} 2\log|\eta_1| & 2\log|\eta_2| \\ 2\log|\eta_2| & 2\log|\eta_2| \end{bmatrix}\right|$$
$$= \frac{4}{m}\,(\log|\eta_2|).(\log|\eta_2|-\log|\eta_1|).$$

On peut calculer $|\eta_2|^2=1+\sqrt[3]{2}+\sqrt[3]{4}$, d'où $mR_k=5,44627715\dots$(et on peut vérifier qu'en fait, $m=1$).

Le régulateur intervient dans la *formule du nombre de classes* : la fonction zêta du corps k a un pôle simple au point 1, de résidu

$$2^{r_1}(2\pi)^{r_2}hR_k/w\sqrt{\Delta},$$

où h est le nombre de classes de k, Δ la valeur absolue du discriminant de k, et w l'ordre de $\mathcal{O}^*_{\text{tors}}$.

b) **Le régulateur p-adique.** (Réf.: Washington, §5.5).

Soient k un corps de nombres et p un nombre premier. On fixe un plongement de $\mathbb{C}_p$ dans $\mathbb{C}$ (un tel plongement existe parce que toute base de transcendance de $\mathbb{C}_p$ sur $\mathbb{Q}$ a la puissance du continu). On peut alors numéroter les plongements de k dans $\mathbb{C}_p$:

$$\sigma_1,\dots,\sigma_{r_1},\ \sigma_{r_1+1},\ \overline{\sigma}_{r_1+1},\dots,\sigma_{r_1+r_2},\overline{\sigma}_{r_1+r_2},$$

où $\sigma_1,\dots,\sigma_{r_1}$ sont réels, et les autres sont complexes. Posons $\delta_i=1$ pour $1\le i\le r_1$, et $\delta_{r_1+i}=2$ pour $1\le i\le r_2$. Si $\epsilon_1,\dots,\epsilon_r$ est un système fondamental d'unités de k, le régulateur p-adique de k est défini par

$$R_p(k) = \det\left[\delta_i \log_p(\sigma_i\epsilon_j)\right]_{1\le i,j\le r}.$$

La définition est donc analogue à celle du régulateur complexe, en remplaçant le logarithme des modules par le logarithme p-adique. Notons que $R_p(k)$ dépend en fait non seulement de k et p, mais aussi du plongement choisi de $\mathbb{C}_p$ dans $\mathbb{C}$, et il change par un facteur ±1 si on permute les σ_i (ou les ϵ_j). Mais nous nous intéressons principalement à savoir s'il est nul ou non, et cela ne dépend pas des différents choix.

Conjecture 5.1 (Leopoldt).- *Pour tout nombre premier* p *et tout corps de nombres* k, *on a* $R_p(k)\neq0$.

Nous verrons que cette conjecture est vraie quand l'extension $k/\mathbb{Q}$ est abélienne. On en déduit que la fonction zêta p-adique d'un tel corps a un pôle simple au point 1, de résidu

$$2^{d-1}\Delta^{-1/2}hR_p \cdot \prod_{\chi\in X}(1-\frac{\chi(p)}{p}),$$

où X est le groupe des caractères de Dirichlet associé à k et cette formule donne le signe de R_p.

La démonstration de la conjecture de Leopoldt dans le cas abélien utilise :

-l'existence d'une unité de Minkowski dans une extension galoisienne de $\mathbb{Q}$, c'est-à-dire d'une unité ϵ qui, avec ses conjugués, engendre un sous-groupe d'indice fini de $\mathcal{O}_k^*$;

-le calcul explicite du déterminant de groupe dans le cas abélien :

$$\det\left[X_{st^{-1}}\right]_{s,t\in G} = \prod_{\chi\in\hat{G}}\sum_{s\in G}\chi(s)X_s \ ;$$

-le théorème 4.1 de Baker-Brumer.

Voici un exemple simple d'extension non abélienne pour laquelle la conjecture de Leopoldt est résolue : prenons pour k le corps de décomposition sur $\mathbb{Q}$ du polynôme X^3-2. Il s'agit de vérifier que le déterminant de la matrice

$$\begin{bmatrix} \log_p\eta_1 & \log_p\eta_2 \\ \log_p\eta_2 & \log_p\eta_3 \end{bmatrix}$$

n'est pas nul, avec $\eta_1=\sqrt[3]{2}-1$, $\eta_2=j\sqrt[3]{2}-1$, et $\eta_3=j^2.\sqrt[3]{2}-1$. (Le quotient η_2/η_3 n'est pas égal à j, donc n'est pas une racine de l'unité, et $\log_p\eta_2\neq\log_p\eta_3$). Mais $\eta_1\eta_2\eta_3=N(\sqrt[3]{2}-1)=1$, et le déterminant ci-dessus est égal à:

$$\begin{vmatrix} a & b \\ b & -a-b \end{vmatrix} = -(a^2+ab+b^2)=-(a-jb)(a-j^2b),$$

avec $a=\log_p\eta_1$, $b=\log_p\eta_2$; ce déterminant est non nul (pour tout p) par le théorème (p-adique) de Gel'fond-Schneider (c'est-à-dire le cas $n=2$ du théorème 4.1).

Plus généralement, la démonstration de Baker-Brumer (méthode d'Ax) permet de résoudre la conjecture de Leopoldt quand le corps k est une extension abélienne d'un corps quadratique imaginaire.

Nous verrons que le théorème des 6 exponentielles p-adiques donne aussi la conjecture de Leopoldt pour certains corps de petit degrés, et la conjecture des 4 exponentielles la donnerait pour quelques autres (voir le problème à la fin).

Pour résoudre la conjecture de Leopoldt dans le cas général, il suffirait d'établir l'analogue p-adique de la conjecture 2.5 sur l'indépendance algébrique de logarithmes de nombres algébriques (le cas homogène suffirait).

Enfin la conjecture de Leopoldt peut s'énoncer en terme de nombre de $\mathbb{Z}_p$-extensions indépendantes d'un corps de nombres : en gros, une $\mathbb{Z}_p$-extension correspond (par la théorie du corps de classes) à une relation sur $\mathbb{Z}_p$ entre les unités, et le problème revient à majorer le nombre de telles extensions. La fin du cours sera consacrée à l'étude des $\mathbb{Z}_p$-extensions et à la décomposition des idéaux premiers.

CHAPITRE I

CARACTERES DE HECKE.

§1.- Quasi-caractères de $\mathbb{R}^*$ et de $\mathbb{C}^*$.

a) Homomorphismes continus entre les groupes $\mathbb{R}$, $\mathbb{R}_+^*$, $\mathbb{R}^*$, $\mathbb{U}$, $\mathbb{C}$ et $\mathbb{C}^*$.

Dans un tableau (p.I.4) nous indiquons tous les homomorphismes continus de G_1 dans G_2, quand G_1 (resp. G_2) désigne l'un des groupes topologiques $\mathbb{R}$, $\mathbb{R}_+^*$, $\mathbb{U}$, $\mathbb{C}$ et $\mathbb{C}^*$ ($\mathbb{U}$ désigne le groupe multiplicatif des nombres complexes de module 1). Nous allons vérifier qu'il n'y en a effectivement pas d'autre. (Voir Bourbaki, Topologie Générale, Chap.5 : groupes à un paramètre).

Lemme 1.1.- *Soit* $f:\mathbb{R} \longrightarrow \mathbb{R}$ *un homomorphisme continu. Il existe* $\lambda\in\mathbb{R}$ *tel que* $f(x)=\lambda x$.

Démonstration.- Soit $\lambda=f(1)$. On a $f(n)=\lambda n$ pour tout $n\in\mathbb{Z}$, donc $qf(p/q)=\lambda p$ pour tout $p/q\in\mathbb{Q}$, ce qui donne $f(p/q)=\lambda p/q$, et par continuité on en déduit $f(x)=\lambda x$ pour tout $x\in\mathbb{R}$.

De même un homomorphisme continu $\mathbb{R} \longrightarrow \mathbb{C}$ est de la forme $x \longrightarrow tx$, avec $t\in\mathbb{C}$.

Corollaire 1.2.- *Soit* $f:\mathbb{R} \longrightarrow \mathbb{R}_+^*$ *un homomorphisme continu. Alors il existe* $\lambda\in\mathbb{R}$ *tel que* $f(x)=e^{\lambda x}$.

Démonstration.- L'application $\exp:\mathbb{R} \longrightarrow \mathbb{R}_+^*$ qui envoie z sur e^z est un isomorphisme continu, d'inverse $\log:\mathbb{R}_+^* \longrightarrow \mathbb{R}$; donc $\log f$ est un homomorphisme continu de $\mathbb{R}$ dans $\mathbb{R}$, et on applique le lemme 1.1, ce qui donne le résultat avec $\lambda=\log f(1)$.

Lemme 1.3.- *Soit* $f:\mathbb{R} \longrightarrow \mathbb{U}$ *un homomorphisme continu. Alors il existe* $\lambda\in\mathbb{R}$ *tel que* $f(x)=e^{i\lambda x}$.

Démonstration.- Comme $\mathbb{R}$ et $\mathbb{U}$ sont connexes, on voit facilement que si $f\neq 1$, alors f est surjective (théorème des valeurs intermédiaires). Comme $\mathbb{R}$ et $\mathbb{U}$ ne sont pas isomorphes ($\mathbb{U}$ est compact, alors que $\mathbb{R}$ ne l'est pas), f n'est pas injective. Alors $\ker f=f^{-1}(1)$ est un sous-groupe fermé de $\mathbb{R}$, distinct de 0 et de $\mathbb{R}$, donc isomorphe à $\mathbb{Z}$. Soit $\omega\in\mathbb{R}^*$ avec $\ker f=\mathbb{Z}\omega$. On va montrer qu'on peut choisir le signe de ω de sorte que $f(x)=e^{2i\pi x/\omega}$. On remarque que $f(\omega/2)=f(-\omega/2)=-1$, puis que $\{f(\omega/4),\ f(-\omega/4)\}=\{i,-i\}$. On choisit le signe de ω de sorte que $f(\omega/4)=i$. On montre alors par récurrence que $f(m\omega/2^n)=e^{2i\pi m/2^n}$ (pour $m=2k-1$, sur le cercle unité, la seule racine 2^{n+1}-ième de l'unité dans l'arc ouvert d'extrémités $e^{2i\pi(k-1)/2^n}$, $e^{2i\pi k/2^n}$ est $e^{2i\pi m/2^{n+1}}$).

Ainsi $f(x)=e^{2i\pi x/\omega}$ pour tous les x dans un sous-ensemble dense de l'intervalle $[0,\omega]$. Par continuité, puis périodicité, on obtient le résultat avec $\lambda=2\pi/\omega$.

On aurait pu aussi écrire $f(x)=e^{ig(x)}$, avec $g : \mathbb{R} \longrightarrow \mathbb{R}$ continue et $g(0)=0$, et appliquer le lemme 1.1 à g.

Corollaire 1.4.- *Soit* $f:\mathbb{R} \longrightarrow \mathbb{C}^*$ *un homomorphisme continu. Alors il existe* $t\in\mathbb{C}$ *tel que* $f(x)=e^{tx}$.

Démonstration.- Le module de f défini un homomorphisme continu $|f|$ de $\mathbb{R}$ dans $\mathbb{R}_+^*$, donc $|f(x)|=e^{\lambda_1 x}$, avec $\lambda_1\in\mathbb{R}$ (corollaire 1.2). Ensuite l'application $f/|f|$ définit un homomorphisme continu de $\mathbb{R}$ dans $\mathbb{U}$, donc $f(x)=|f(x)|.e^{i\lambda_2 x}$, avec $\lambda_2\in\mathbb{R}$ (lemme 1.3). D'où le résultat avec $t=\lambda_1+i\lambda_2$.

Corollaire 1.5.- *Soit* $f:\mathbb{U} \longrightarrow \mathbb{C}^*$ *un homomorphisme continu. Alors il existe* $m\in\mathbb{Z}$ *tel que* $f(u)=u^m$.

En particulier $f(\mathbb{U})\subset\mathbb{U}$. De plus les seuls automorphismes continus de $\mathbb{U}$ sont $u \longrightarrow u^{-1}$ et l'identité.

Démonstration.- Soit $e:\mathbb{R} \longrightarrow \mathbb{U}$ l'application définie par $e(x)=e^{2i\pi x}$. Alors $f\circ e$ est un homomorphisme continu de $\mathbb{R}$ dans $\mathbb{C}^*$, donc (corollaire 1.4) il existe $t\in\mathbb{C}$ tel que $f(e^{2i\pi x})=e^{tx}$. En prenant $x=1$ on trouve $e^t=1$, donc $t\in 2i\pi\mathbb{Z}$. Soit $m=t/2i\pi$; on a $m\in\mathbb{Z}$ et

$$f(e^{2i\pi x})=e^{2i\pi mx} \qquad \text{pour tout } x\in\mathbb{R},$$

c'est-à-dire $f(u)=u^m$ pour tout $u\in\mathbb{U}$.

Lemme 1.6.- *Soit $\chi:\mathbb{R}^* \longrightarrow \mathbb{C}^*$ un homomorphisme continu. Alors il existe $t\in\mathbb{C}$ tel que l'on ait soit $\chi(x)=|x|^t$, soit $\chi(x)=\mathrm{sgn}(x).|x|^t$ (où $\mathrm{sgn}(x)=x/|x|$ désigne le signe de x).*

Démonstration.- L'application $\chi\circ\exp :\mathbb{R} \longrightarrow \mathbb{C}^*$ est un homomorphisme continu. Le corollaire 1.4 permet d'écrire $\chi(e^x)=e^{tx}$, avec $t\in\mathbb{C}$. Donc $\chi(x)=x^t$ pour $x>0$. Mais $\chi(-x)=\chi(-1).\chi(x)$ et $\chi(-1)^2=1$, D'où

$$\chi(x)=|x|^t \qquad \text{si } \chi(-1)=1,$$

et

$$\chi(x)=\mathrm{sgn}(x).|x|^t \qquad \text{si } \chi(-1)=-1.$$

Lemme 1.7.- *Soit $\chi:\mathbb{C}^* \longrightarrow \mathbb{C}^*$ un homomorphisme continu. Alors il existe $m\in\mathbb{Z}$ et $t\in\mathbb{C}$ tel que l'on ait*

$$\chi(z)=(z/|z|)^m.|z|^t, \qquad \textit{pour tout } z\in\mathbb{C}^*.$$

Démonstration.- La restriction de χ à $\mathbb{R}^*$ est de la forme

$$\chi(x)=\mathrm{sgn}(x)^a.|x|^t,$$

avec $a=0$ si $\chi(-1)=1$, et $a=1$ si $\chi(-1)=-1$ (lemme 1.6). L'application g de $\mathbb{C}^*$ dans $\mathbb{C}^*$ définie par $g(z)=\chi(z)|z|^{-t}$ est un homomorphisme continu, dont le noyau contient $\mathbb{R}_+^*$. Elle définit par passage au quotient un homomorphisme continu Ψ de $\mathbb{C}^*/\mathbb{R}_+^*\simeq\mathbb{U}$ dans $\mathbb{C}^*$ avec $g(z)=\Psi(z/|z|)$ pour tout $z\in\mathbb{C}^*$. Le corollaire 1.5 permet de conclure.

Liste des homomorphismes continus $G_1 \longrightarrow G_2$:

G_2 / G_1	$\mathbb{R}$	$\mathbb{R}_+^*$	$\mathbb{R}^*$	$\mathbb{U}$	$\mathbb{C}$	$\mathbb{C}^*$
$\mathbb{R}$	λx	$e^{\lambda x}$	$e^{\lambda x}$	$e^{i\lambda x}$	tx	e^{tx}
$\mathbb{R}_+^*$	$\lambda \log x$	x^{λ}	x^{λ}	$x^{i\lambda}$	$t\log x$	x^{t}
$\mathbb{R}^*$	$\lambda \log \lvert x\rvert$	$\lvert x\rvert^{\lambda}$	$\mathrm{sgn}(x)^{\epsilon}.\lvert x\rvert^{\lambda}$	$\mathrm{sgn}(x)^{\epsilon}.\lvert x\rvert^{i\lambda}$	$t\log \lvert x\rvert$	$\mathrm{sgn}(x)^{\epsilon}\lvert x\rvert^{t}$
$\mathbb{U}$	0	1	1	u^{n}	0	u^{n}
$\mathbb{C}$	$\lambda_1 \mathrm{Re}z+\lambda_2 \mathrm{Im}z$	$e^{\lambda_1 \mathrm{Re}z+\lambda_2 \mathrm{Im}z}$	$e^{\lambda_1 \mathrm{Re}z+\lambda_2 \mathrm{Im}z}$	$e^{i\lambda_1 \mathrm{Re}z+i\lambda_2 \mathrm{Im}z}$	$t_1 z+t_2 \bar{z}$	$e^{t_1 z+t_2 \bar{z}}$
$\mathbb{C}^*$	$\lambda \log \lvert z\rvert$	$\lvert z\rvert^{\lambda}$	$\lvert z\rvert^{\lambda}$	$(z/\lvert z\rvert)^{n}\lvert z\rvert^{i\lambda}$	$t\log \lvert z\rvert$	$(z/\lvert z\rvert)^{n}\lvert z\rvert^{t}$

Notations : $\lambda \in \mathbb{R}$, $t \in \mathbb{C}$, $n \in \mathbb{Z}$, $\epsilon = 0$ ou 1.

Variable $\in G_1$: $x \in \mathbb{R}$, $x \in \mathbb{R}_+^*$, $x \in \mathbb{R}^*$, $u \in \mathbb{U}$, $z \in \mathbb{C}$, $z \in \mathbb{C}^*$.

b) Quasi-caractères de $\mathbb{R}^*$ ou de $\mathbb{C}^*$ de type (A) ou (A_0).

Un *quasi-caractère* de $\mathbb{R}^*$ (resp. de $\mathbb{C}^*$) est un homomorphisme continu de $\mathbb{R}^*$ (resp. de $\mathbb{C}^*$) dans $\mathbb{C}^*$. C'est un *caractère* s'il est à valeurs dans $\mathbb{U}$.

Soit χ un quasi-caractère de $\mathbb{R}^*$ (resp. de $\mathbb{C}^*$). Grâce aux lemmes 1.6 et 1.7, on peut écrire

$$\chi(z)=(z/\lvert z\rvert)^{m}.\lvert z\rvert^{t}$$

pour tout $z \in \mathbb{R}^*$ (resp. $\mathbb{C}^*$). Le couple $(m,t) \in \{0,1\} \times \mathbb{C}$ (resp. $(m,t) \in \mathbb{Z} \times \mathbb{C}$) est le *type* de χ (dans le cas réel, χ est *pair* si $m=0$, et χ est *impair* si $m=1$).

Proposition 1.8.- *Soit* χ *un quasi-caractère de* $\mathbb{R}^*$ *(resp. de* $\mathbb{C}^*$*) ayant pour type* (m,t). *Les propriétés suivantes sont équivalentes :*

(i) $t\in\mathbb{Q}$

(ii) $\chi(\mathbb{Q}^*)\subset\overline{\mathbb{Q}}^*$

(iii) *pour tout corps de nombres* k *plongé dans* $\mathbb{R}$ *(resp.* $\mathbb{C}$*), on a*

$$\chi(k^*)\subset\overline{\mathbb{Q}}^*.$$

On dira qu'un tel caractère est *de type* (A).

La proposition 1.8 est une conséquence immédiate du théorème des six exponentielles (voir Introduction, corollaire 2.4 et début du §3).

Proposition 1.9.- *Soit* χ *un quasi-caractère de* $\mathbb{R}^*$ *ayant pour type* (m,t). *Les propriétés suivantes sont équivalentes :*

(i) $t\in\mathbb{Z}$, *c'est-à-dire* $\chi(x)=\mathrm{sgn}(x)^a.x^b$ *avec* $(a,b)\in\mathbb{Z}^2$

(ii) $\chi(\mathbb{Q}^*)\subset\mathbb{Q}^*$

(iii) *pour tout corps de nombres* k *plongé dans* $\mathbb{R}$, *on a*

$$\chi(k^*)\subset k^*.$$

(iv) *pour tout corps de nombres* k *plongé dans* $\mathbb{R}$, *il existe un corps de nombres* E *tel que*

$$\chi(k^*)\subset E^*.$$

Proposition 1.10.- *Soit* χ *un quasi-caractère de* $\mathbb{C}^*$ *ayant pour type* (m,t). *Les propriétés suivantes sont équivalentes :*

(i) $t-m\in2\mathbb{Z}$, *c'est-à-dire* $\chi(z)=z^{a-b}\bar{z}^b$ *avec* $(a,b)\in\mathbb{Z}^2$

(ii) $\chi(\mathbb{Q}(i)^*)\subset\mathbb{Q}(i)^*$

(iii) *pour tout corps de nombres* k *plongé dans* $\mathbb{C}$, *il existe un corps de nombres* E *tel que*

$$\chi(k^*)\subset E^*.$$

Un quasi-caractère de $\mathbb{R}^*$ (resp. de $\mathbb{C}^*$) vérifiant les propriétés équivalentes de la proposition 1.9 (resp. 1.10) est dit *de type* (A_0).

Les démonstrations des propositions 1.9 et 1.10 ont été données dans l'Introducttion (§3) ; elles utilisent principalement la proposition 1.8 ci-dessus, avec les lemmes 3.1 et 3.2 de l'Introduction.

§2.-Quasi-caractères de type (A) ou (A_0).

a) Définitions et énoncé du théorème.

Soit F un corps. Une F-algèbre A est *diagonalisable* s'il existe un entier $d\geq 0$ tel que A soit isomorphe à F^d. On dit que A est *étale* s'il existe une extension E de F telle que l'algèbre sur E déduite de A par extension des scalaires soit diagonalisable (cf. Bourbaki, Algèbre, Ch.V §6 N°3).

Choisissons une place réelle de F, c'est-à-dire un isomorphisme de F avec un sous-corps de $\mathbb{R}$. Si A est une F-algèbre étale de degré d, alors l'algèbre étendue $A_{\mathbb{R}}=A\otimes_F\mathbb{R}$ est une $\mathbb{R}$-algèbre étale de degré d ; comme toute extension finie de $\mathbb{R}$ est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$, on a $A_{\mathbb{R}}\simeq\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, avec $r_1+2r_2=d$.

Ainsi, quand k est un corps de nombres de degré $d=[k:\mathbb{Q}]$,, on a $k\otimes_{\mathbb{Q}}\mathbb{R}\simeq\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ (voir par exemple R. Godement, Introduction à la théorie des groupes de Lie, Ch.1 §6) ; soient $\sigma_1,\ldots,\sigma_d$ les plongements de k dans $\mathbb{C}$, avec comme d'habitude

$$\sigma_i(k)\subset\mathbb{R} \qquad \text{pour} \quad 1\leq i\leq r_1,$$

et

$$\sigma_{r_1+j}=\overline{\sigma}_{r_1+r_2+j} \qquad \text{pour} \quad 1\leq j\leq r_2.$$

On désigne par $\sigma : k \longrightarrow \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ le plongement canonique donné par $\sigma_1,\ldots,\sigma_n$, avec $n=r_1+r_2$. Ainsi $\sigma(k^*)$ est un sous-groupe de $\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$.

Soit χ un homomorphisme continu de $\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$ dans $\mathbb{C}^*$. Chacune des restrictions de χ à un facteur $\mathbb{R}^*$ ou $\mathbb{C}^*$ est un quasi caractère de $\mathbb{R}^*$ ou $\mathbb{C}^*$ respectivement, donc a un type (m_ν,t_ν), $(1\leq\nu\leq n)$. Danc ce cas, on dit que χ a pour *type* $(m_1,\ldots,m_n,t_1,\ldots,t_n)$; alors pour $z=(z_1,\ldots,z_n)\in\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$ on a

$$\chi(z)=\prod_{\nu=1}^{n}\left[\frac{z_\nu}{|z_\nu|}\right]^{m_\nu}.|z_\nu|^{t_\nu}.$$

On dit que χ est *de type* (A) si $t_\upsilon \in \mathbb{Q}$ pour tout $\upsilon=1,\dots,n$. On dit que χ est *de type* (A_0) si

$$t_\upsilon \in \mathbb{Z} \quad \text{pour} \quad 1 \leq \upsilon \leq r_1$$

et

$$t_\upsilon - m_\upsilon \in 2\mathbb{Z} \quad \text{pour} \quad r_1 < \upsilon \leq n.$$

Nous allons nous intéresser aux valeurs de χ sur $\sigma(k^*)$; on a, pour $\alpha \in k^*$,

$$\chi\circ\sigma(\alpha) = \prod_{\upsilon=1}^{n} \left[\frac{\sigma_\upsilon \alpha}{|\sigma_\upsilon \alpha|}\right]^{m_\upsilon} . |\sigma_\upsilon \alpha|^{t_\upsilon}$$

Il est évident que, si χ est de type (A), alors $\chi\circ\sigma(k^*) \subset \overline{\mathbb{Q}}^*$.

D'autre part, si χ est de type (A_0), on peut écrire

$$\chi\circ\sigma(\alpha) = \prod_{i=1}^{r_1} (\mathrm{sgn}(\sigma_i \alpha))^{a_i} . (\sigma_i \alpha)^{b_i} . \prod_{j=r_1+1}^{n} (\sigma_j \alpha)^{a_j} . (\overline{\sigma}_j \alpha)^{b_j}$$

avec des entiers a_υ, b_υ, $(1 \leq \upsilon \leq n)$. Alors. si E désigne la clôture galoisienne de k dans $\mathbb{C}$, on a $\chi\circ\sigma(k^*) \subset E^*$.

Nous allons voir, inversement, que si $\chi\circ\sigma(k^*) \subset \overline{\mathbb{Q}}^*$, alors χ est de type (A), et s'il existe un corps de nombres E tel que $\chi\circ\sigma(k^*) \subset E^*$ alors χ est de type (A_0).

On aura besoin d'un résultat un peu plus précis :

Théorème 2.1.- *Soient* $\alpha_1,\dots,\alpha_\ell$ *des éléments de* k^*, *avec* $\ell > n(n+1)$, *tels que les nombres* $\sigma_i \alpha_j$ $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$ *soient multiplicativement indépendants. Si* $\chi\circ\sigma(\alpha_j) \in \overline{\mathbb{Q}}^*$ *pour* $1 \leq j \leq \ell$, *alors* χ *est de type* (A).

Proposition 2.2.- *Soient* E *un corps de nombres, et* β *un élément de* k *ayant la propriété suivante : pour tout nombre premier* p, *et tout* $m_1,\dots,m_d$ *dans* $\mathbb{Z}$, *si*

$$\prod_{i=1}^{d} (\sigma_i \beta)^{m_i} = \gamma^p$$

avec $\gamma \in E$, *alors* p *divise tous les* m_i.

Si χ *est de type* (A) *et vérifie* $\chi(\beta) \in E$, *alors* χ *est de type* (A_0).

Nous allons démontrer ces deux énoncés. Au §3 nous construirons des suites (α_j) vérifiant l' hypothèse du théorème 2.1, et des nombres β vérifiant l'hypothèse de la proposition 2.2.

b) Démonstration du théorème 2.1.

L'hypothèse s'écrit

$$\prod_{\upsilon=1}^{n} |\sigma_\upsilon \alpha_j|^{t_\upsilon} \in \overline{\mathbb{Q}} \qquad \text{pour} \quad 1 \leq j \leq \ell,$$

et il faut voir que cela implique $t_\upsilon \in \mathbb{Q}$ pour tout $\upsilon=1,\ldots,n$. Nous allons utiliser le théorème 2.3 de l'Introduction.

Soit $1, \tau_1, \ldots, \tau_s$ une base du $\mathbb{Q}$-espace vectoriel engendré dans $\mathbb{C}$ par $1, t_1, \ldots, t_n$, avec $0 \leq s \leq n$. Nous supposons $s \geq 1$, et nous voulons aboutir à une contradiction. On a par hypothèse

$$\sum_{\upsilon=1}^{n} t_\upsilon \log|\sigma_\upsilon \alpha_j| \in L \qquad \text{pour} \quad 1 \leq j \leq \ell.$$

On peut écrire

$$t_\upsilon = \sum_{i=0}^{s} a_{\upsilon i} \tau_i \qquad (1 \leq \upsilon \leq n),$$

avec $a_{\upsilon i} \in \mathbb{Q}$, et $\tau_0 = 1$. Alors en posant

$$\lambda_i(\alpha) = \sum_{\upsilon=1}^{n} a_{\upsilon i} \log|\sigma_\upsilon \alpha|, \qquad (1 \leq i \leq s),$$

on a $\lambda_i(\alpha_j) \in L$, et

$$\sum_{i=1}^{s} \tau_i \lambda_i(\alpha_j) \in L.$$

Mais $1, \tau_1, \ldots, \tau_s$ sont $\mathbb{Q}$-linéairement indépendants. L'hyperplan $\sum_{i=1}^{s} \tau_i z_i = z_{s+1}$ de $\mathbb{C}^{s+1}$ a donc une intersection avec L^{s+1} de dimension sur $\mathbb{Q}$ au plus $s(s+1)$ (cf. théorème 2.3 de l'Introduction).

On a supposé que les nombres $\sigma_i\alpha_j$ $(1\leq i\leq d,\ 1\leq j\leq \ell)$ sont multiplicativement indépendants ; donc les nombres $\log|\sigma_\nu\alpha_j|$ $(1\leq\nu\leq n,\ 1\leq j\leq\ell)$ sont $\mathbb{Q}$-linéairement indépendants, par conséquent les points $(\lambda_1(\alpha_j),\ldots,\lambda_s(\alpha_j))$, $(1\leq j\leq\ell)$ sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}^s$, et à plus forte raison les points $(\lambda_1(\alpha_j),\ldots,\lambda_s(\alpha_j),\ \sum_{i=1}^{s}\tau_i\lambda_i(\alpha_j))$, $(1\leq j\leq\ell)$ sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}^{s+1}$, d'où la contradiction.

c) Démonstration de la proposition 2.2.

Pour $1\leq\nu\leq r_1$, on a $\sigma_\nu\beta/|\sigma_\nu\beta|\in\{-1,+1\}$. L'hypothèse peut donc s'écrire :

$$\prod_{\nu=1}^{r_1}(\sigma_\nu\beta)^{t_\nu}.\prod_{\nu=r_1+1}^{n}(\sigma_\nu\beta)^{m_\nu}|\sigma_\nu\beta|^{t_\nu-m_\nu}\in E^*.$$

Comme $|\sigma_\nu\beta|^2=\sigma_\nu\beta.\sigma_{r_2+\nu}\beta$ pour $r_1<\nu\leq n$, on peut encore écrire

$$\prod_{i=1}^{d}(\sigma_i\beta)^{s_i}\in E^*,$$

avec

$$s_i=\begin{cases} t_i & \text{pour } 1\leq i\leq r_1\\ (t_i+m_i)/2 & \text{pour } r_1<i\leq n\\ (t_{i-r_2}-m_{i-r_2})/2 & \text{pour } n<i\leq d.\end{cases}$$

Comme χ est de type (A), les nombres $s_1,\ldots,s_d$ sont rationnels, et il s'agit de vérifier qu'il sont entiers. Sinon, il existe un entier N et un nombre premier p tels que les nombres $m_i=Ns_ip$ soient entiers et non tous divisibles par p. Alors

$$\prod_{i=1}^{d}(\sigma_i\beta)^{m_i}\in E^{*p},$$

contrairement à l'hypothèse.

Préliminaires au Chapitre I §3 :

Rappels de théorie algébrique des nombres :

DECOMPOSITION DES NOMBRES PREMIERS DANS UN CORPS DE NOMBRES

a) Indice de ramification, degré résiduel.

Soient k un corps de nombres de degré $d=[k:\mathbb{Q}]$, et $\mathcal{O}_k=\mathcal{O}$ l'anneau des entiers de k (clôture intégrale de $\mathbb{Z}$ dans k). Tout idéal premier non nul de $\mathcal{O}$ est maximal, et tout idéal non nul de $\mathcal{O}$ s'écrit de manière unique sous la forme

$$\prod_{\mathfrak{P}} \mathfrak{P}^{n_{\mathfrak{P}}},$$

où $\mathfrak{P}$ décrit l'ensemble des idéaux premiers non nuls de $\mathcal{O}$, et $n_{\mathfrak{P}}\in\mathbb{Z}$, $n_{\mathfrak{P}}\geq 0$, avec $n_{\mathfrak{P}}=0$ pour tout $\mathfrak{P}$ sauf un nombre fini.

Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}$. Alors $\mathfrak{P}\cap\mathbb{Z}$ est un idéal premier $p\mathbb{Z}$ de $\mathbb{Z}$, et $\mathcal{O}/\mathfrak{P}$ est un corps fini de caractéristique p. Le *degré*, ou *degré résiduel* de $\mathfrak{P}$, est $f(\mathfrak{P})=[\mathcal{O}/\mathfrak{P}:\mathbb{F}_p]$, de sorte que $\mathcal{O}/\mathfrak{P}$ est un corps fini à $p^{f(\mathfrak{P})}$ éléments, et $p^{f(\mathfrak{P})}$ est la norme $N(\mathfrak{P})$ de l'idéal $\mathfrak{P}$. Plus généralement, la *norme* $N(\mathfrak{A})$ d'un idéal $\mathfrak{A}$ de $\mathcal{O}$ est le nombre d'éléments de $\mathcal{O}/\mathfrak{A}$; si

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{n_{\mathfrak{P}}},$$

on a $N(\mathfrak{A}) = \prod_{\mathfrak{P}} N(\mathfrak{P})^{n_{\mathfrak{P}}}$. Pour un idéal principal $\mathcal{O}x$, $x\in\mathcal{O}$, on a

$$N(\mathcal{O}x)=\left|N_{k/\mathbb{Q}}(x)\right|.$$

Soit p un nombre premier ; considérons l'idéal $p\mathcal{O}$; on peut l'écrire

$$p\mathcal{O}=\prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P})},$$

et l'ensemble des $\mathfrak{P}$ tels que $e(\mathfrak{P})>0$ est précisément l'ensemble des idéaux premiers de $\mathcal{O}$ tels que $\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}$ (on dit que $\mathfrak{P}$ est *au-dessus de* p) ; pour un tel idéal $\mathfrak{P}$ l'exposant $e(\mathfrak{P})$ est l'*indice de ramification*, et on a

$$\sum_{\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}} e(\mathfrak{P})f(\mathfrak{P}) = [k:\mathbb{Q}],$$

et

$$\mathcal{O}/p\mathcal{O} \simeq \prod_{\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}} \mathcal{O}/\mathfrak{P}^{e(\mathfrak{P})}.$$

On dit que p est *ramifié* dans $\mathcal{O}$ (ou dans k) si $\max\{e(\mathfrak{P})\}\geq 2$. Il n'y a qu'un nombre fini de premiers p ramifiés dans k : ce sont les diviseurs premiers du discriminant de k sur $\mathbb{Q}$ (la trace définit une forme bilinéaire non dégénérée sur k).

Quand $k\neq\mathbb{Q}$, on dit que p est *totalement ramifié* dans k si l'un des $e(\mathfrak{P})$ vaut $[k:\mathbb{Q}]$; alors tous les autres sont nuls, et $p\mathcal{O}=\mathfrak{P}^d$.

On dit que p est *totalement décomposé* si l'ensemble des $\mathfrak{P}$ tels que $\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}$ comporte d éléments ; alors $p\mathcal{O}=\mathfrak{P}_1\ldots\mathfrak{P}_d$, et $f(\mathfrak{P}_i)=1$ pour tout $i=1,\ldots,d$.

On dit que p est *inerte* dans k si l'un des $f(\mathfrak{P})$ vaut $[k:\mathbb{Q}]$, c'est-à-dire si $p\mathcal{O}$ est un idéal premier de $\mathcal{O}$.

b) Cas galoisien.

Supposons maintenant que l'extension $k/\mathbb{Q}$ est galoisienne, et soit $G=Gal(k/\mathbb{Q})$ son groupe de Galois. Pour chaque nombre premier p, G permute transitivement les $\mathfrak{P}$ tels que $\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}$, et les nombres $e(\mathfrak{P})$, $f(\mathfrak{P})$ dépendent seulement de p ; on les note alors e_p, f_p respectivement. Soit g_p le nombre de $\mathfrak{P}$ tels que $\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}$; on a donc $e_pf_pg_p=d$.

Le *groupe de décomposition* en $\mathfrak{P}$ est $D=D_{\mathfrak{P}}=\{\sigma\in G\ ;\ \sigma\mathfrak{P}=\mathfrak{P}\}$; il est d'ordre e_pf_p ; son corps fixe k_D (extension de $\mathbb{Q}$ de degré g_p), appelé *corps de décomposition* en $\mathfrak{P}$, est le plus grand sous-corps de k dans lequel l'idéal $\mathfrak{P}_D$ de k_D en-dessous de $\mathfrak{P}$ soit totalement décomposé sur $\mathbb{Q}$ (c'est-à-dire non ramifié de degré 1). Le groupe de décomposition de $\sigma\mathfrak{P}$, $(\sigma\in G)$ est $\sigma D_{\mathfrak{P}}\sigma^{-1}$. En particulier dans le cas abélien $D_{\mathfrak{P}}$ ne dépend que de p.

Le *groupe d'inertie* en $\mathfrak{P}$ est $I=I_{\mathfrak{P}}=\{\sigma\in D_{\mathfrak{P}}\ ;\ \sigma x\equiv x \bmod\mathfrak{P}$ pour tout $x\in\mathcal{O}\}$. C'est un sous-groupe normal de $D_{\mathfrak{P}}$ d'ordre e_p ; son corps fixe k_I,

extension cyclique de k_D de degré f_p, est le *corps d'inertie* en $\mathfrak{P}$. C'est le plus grand sous-corps de k dans lequel l'idéal $\mathfrak{P}_I$ de k_I en-dessous de $\mathfrak{P}$ ne soit pas ramifié sur $\mathbb{Q}$.

L'idéal $\mathfrak{P}_D$ est inerte dans l'extension k_I/k_D, et l'idéal $\mathfrak{P}_I$ est totalement ramifié dans l'extension k/k_I. Ainsi p est non ramifié si et seulement si $I=\{1\}$.

$$G\left[\begin{array}{l} D\left[\begin{array}{l} I\left[\begin{array}{l} k \\ | \\ k_I \end{array}\right. \quad \text{Tot. ramifié degré } e_p \\ \quad\quad | \\ \quad k_D \quad \text{Inerte degré } f_p \\ \quad\quad | \\ \quad \mathbb{Q} \quad \text{Tot. décomposé degré } g_p. \end{array}\right. \end{array}\right.$$

c) Anneau local en $\mathfrak{P}$.

Soit $\mathfrak{P}$ un idéal premier d'un corps de nombres k. L'*anneau local* en $\mathfrak{P}$ est

$$A_{\mathfrak{P}}=\{u/v \in k \ ; \ u,v\in\mathcal{O}, \ v\notin\mathfrak{P}\}.$$

C'est l'anneau de fractions $S^{-1}\mathcal{O}$ pour $S=\mathcal{O}-\mathfrak{P}$. Son idéal maximal est

$$\mathcal{M}_{\mathfrak{P}}=\mathfrak{P}A_{\mathfrak{P}}=\{u/v \in A_{\mathfrak{P}} \ ; \ u\in\mathfrak{P}, \ v\notin\mathfrak{P}\},$$

et $\mathcal{M}_{\mathfrak{P}}\cap\mathcal{O}=\mathfrak{P}$. Le corps résiduel $A_{\mathfrak{P}}/\mathcal{M}_{\mathfrak{P}}$ est $\mathcal{O}/\mathfrak{P}$, corps fini à p^f éléments. L'anneau $A_{\mathfrak{P}}$ est un *anneau de valuation discrète* (anneau principal avec un seul idéal premier non nul). Ses idéaux non nuls sont tous de la forme $\mathcal{M}_{\mathfrak{P}}^h$, $h\geq 0$ (avec $\mathcal{M}_{\mathfrak{P}}^0=A_{\mathfrak{P}}$). Un élément π de k est une *uniformisante* en $\mathfrak{P}$ si $\pi\in\mathcal{M}_{\mathfrak{P}}$ et $\pi\notin\mathcal{M}_{\mathfrak{P}}^2$, c'est-à-dire si $\mathcal{M}_{\mathfrak{P}}=\pi A_{\mathfrak{P}}$. Un élément de k est une *unité en* $\mathfrak{P}$ s'il appartient à $A_{\mathfrak{P}}^*=A_{\mathfrak{P}}-\mathcal{M}_{\mathfrak{P}}$.

d) Valeurs absolues.

Une *valeur absolue* sur un corps k est une application $|.|$ de k dans $\mathbb{R}_+$ telle que

- pour $x\in k$, on a $|x|=0$ si et seulement si $x=0$;
- pour x et y dans k, on a $|x.y|=|x|.|y|$;
- pour x et y dans k, on a $|x+y|\leq|x|+|y|$.

La valeur absolue *triviale* est définie par $|x|=1$ pour tout $x\in k^*$. Deux valeurs absolues $|.|_1$, $|.|_2$ sur k sont *équivalentes* si elles définissent la même topologie sur k ; cela revient à dire qu'il existe $\lambda\in\mathbb{R}^*$ tel que $|x|_1=|x|_2^\lambda$ pour tout $x\in k$. Deux valeurs absolues qui ne sont pas équivalentes sont encore appelées *indépendantes*. Une *place* de k est une classe d'équivalence de valeurs absolues non triviales de k.

Soit de nouveau k un corps de nombres, et soit $\mathfrak{P}$ un idéal premier de k. Soit p la *caractéristique résiduelle* (c'est-à-dire le nombre premier tel que $p\mathbb{Z}=\mathfrak{P}\cap\mathbb{Z}$), et soit π une uniformisante en $\mathfrak{P}$. On a $p=\pi^e.u$, où $e=e(\mathfrak{P})$ est l'indice de ramification de $\mathfrak{P}$, et $u\in A_{\mathfrak{P}}^*$. On définit une valeur absolue $|.|_{\mathfrak{P}}$ sur k, qui prolonge la valeur absolue p-adique sur $\mathbb{Q}$, en imposant

$$|x|_{\mathfrak{P}} = 1 \quad \text{pour} \quad x\in A_{\mathfrak{P}}^*,$$

et

$$|\pi|_{\mathfrak{P}} = p^{-1/e}.$$

En notation additive, on définit une *valuation* $v=v_{\mathfrak{P}}$ par $|x|_v=p^{-v(x)}$:

$$v(A_{\mathfrak{P}}^*)=0 \quad \text{et} \quad v(\pi)=1/e.$$

Le groupe des valeurs est $v(k^*)=(1/e)\mathbb{Z}$.

Soit $k_{\mathfrak{P}}=k_v$ le complété de k pour cette valuation ; c'est une extension finie de $\mathbb{Q}_p$ de degré $d_{\mathfrak{P}}=d_v=e(\mathfrak{P})f(\mathfrak{P})$ (degré local en $\mathfrak{P}$). L'*anneau des entiers $\mathfrak{P}$-adiques* est l'adhérence (pour la topologie de k_v) de $\mathcal{O}$ dans k_v :

$$A_v=\{x\in k_v \ ; \ |x|_v\leq 1\} \ ;$$

c'est encore un anneau de valuation discrète, son idéal premier est

$$\mathcal{M}_v=\pi A_v=\{x\in k_v \ ; \ |x|_v<1\} \ ;$$

le groupe des valeurs $v(k_v^*)$ est encore $(1/e)\mathbb{Z}$, et le corps résiduel $A_v/\mathcal{M}_v$ est toujours le corps fini à $N(\mathfrak{P})$ éléments. Le corps k_v est localement compact.

Si k est une extension finie galoisienne de $\mathbb{Q}$, le groupe de Galois $Gal(k/\mathbb{Q})$ opère transitivement sur l'ensemble des places archimédiennes de k, et aussi sur l'ensemble des places de k au-dessus d'un nombre premier p fixé.

Les valeurs absolues (normalisées) de k au-dessus de p s'écrivent $\alpha \longrightarrow |\sigma\alpha|_p$, σ parcourant les plongements de k dans $\mathbb{C}_p$. En particulier, si p est complètement décomposé dans k, on obtient une bijection entre l'ensemble des places au-dessus de p et l'ensemble des plongements de k dans $\mathbb{C}_p$.

e) Formule du produit.

Toute valeur absolue non triviale sur k est équivalente à l'une des valeurs absolues v associées à un idéal premier $\mathfrak{P}$ de k (valeurs absolues ultramétriques), ou à l'une des $n=r_1+r_2$ valeurs absolues archimédiennes déduites d'un plongement de k dans $\mathbb{C}$. Pour ces dernières, le degré local est $d_v=[k_v:\mathbb{R}]$ qui vaut 1 si v est réelle et 2 sinon (le degré résiduel vaut 1 aux places à l'infini). Alors, pour tout $x\in k^*$, l'ensemble des places v de k telles que $|x|_v\neq 1$ est fini, et on a

$$\prod_v |x|_v^{d_v} = 1.$$

Noter que $|\pi|_v^{d_v}=1/q$ si π est une uniformisante en v et $q=p^f$ est le nombre d'éléments du corps résiduel $(=N(\mathfrak{P}):=N(v).)$

Par exemple, pour $k=\mathbb{Q}(i)$ et $x=1+i$, on a $|x|_v=\sqrt{2}$ et $d_v=2$ pour la place à l'infini, $|x|_v=1/\sqrt{2}$, $e=2$, $f=g=1$, $d_v=2$ pour la place associée à l'idéal premier $(1+i)$, et $|x|_v=1$ sinon.

Références.-

Les introductions des chapitres 4 et 10 de D.P. Parent (Exercices de théorie des Nombres, Gauthier-Villars 1978) contiennent un abrégé de ce qu'il faut savoir sur la décomposition des idéaux premiers dans une extension de corps de nombres (à la fin du b) ci-dessus on a dû faire intervenir un corps de base différent de $\mathbb{Q}$).

On pourra consulter par exemple :

P. Samuel, Théorie algébrique des nombres, Coll. Méthodes, Hermann, Paris 1967.

Y. Amice, Les nombres p-adiques, Coll. SUP, P.U.F.,1975.

S. Lang, Algebraic Number Theory, Addison-Wesley 1970.

S. Lang, Algebra, Part II: Field Theory, Second edition, Addison-Wesley, 1984.

J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press 1967 (voir Chap.1, local fields, par Fröhlich, et Chap.2, global fields, par Cassels).

N. Bourbaki, Algèbre Commutative, Ch.5 (entiers) et Ch. 6 (valuations) ; Algèbre, Ch.5 (corps commutatifs).

§3. Théorèmes d'approximation.

Nous allons d'abord vérifier que les hypothèses du théorème 2.1 et du corollaire 2.2 sont toujours satisfaites. L'approximation faible permet de construire des suites $(\alpha_j)_{j\geq 1}$ ou des éléments β dans k vérifiant les conditions requises. L'approximation forte permet d'imposer en plus, par exemple, que ces éléments soient entiers. En procédant différemment on peut faire en sorte que ce soient des S-unités. On utilisera ces résultats pour préciser le fait que k a une image dense dans $k\otimes_{\mathbb{Q}}\mathbb{R}$ par le plongement canonique. Cela permet de donner un raffinement au théorème de la progression arithmétique généralisé de Dirichlet

a) Approximation faible : le théorème d'Artin-Whaples.

Soient $|.|_1,\ldots,|.|_s$ des valeurs absolues non triviales sur un corps k, deux-à-deux indépendantes. Le théorème d'Artin-Whaples dit alors que l'image de k dans le produit des $(k, |.|_i)$ (muni de la topologie produit) est partout dense. Autrement dit, pour tout $\epsilon>0$ et tout $x_1,\ldots,x_s$ dans k, il existe $x\in k$ vérifiant

$$|x-x_i|_i<\epsilon \qquad \text{pour tout } i=1,\ldots,s.$$

Voir par exemple :

- S. Lang, Algebra, 2nd Ed., Chap. 12 §1 p.406 ;
- S. Lang, Algebraic Number Theory, Chap. 2 §1 p.35 ;
- Cassels-Fröhlich, Algebraic Number Theory, Chap.2 §6 p.48.
- N. Bourbaki, Algèbre Commutative, Ch.6 (valuations) §7 (théorème d'approximation).

En voici une première application :

Lemme 3.1.- *Soient* k *un corps de nombres,* p *un nombre premier,* $\mathfrak{p}_1,\ldots,\mathfrak{p}_g$ *des idéaux premiers deux-à-deux distincts de* k *au-dessus de* p. *Il existe* $\alpha\in k$ *tel que* α *soit une uniformisante en* $\mathfrak{p}_1$ *et que* α *soit une unité en* $\mathfrak{p}_i$ *pour* $2\leq i\leq g$.

Démonstration.- Les valeurs absolues $|.|_1,\ldots,|.|_g$ sur k associées aux idéaux $\mathfrak{p}_1,\ldots,\mathfrak{p}_g$ sont deux-à-deux indépendantes. Soit π une uniformisante en $\mathfrak{p}_1$. Par le théorème d'Artin-Whaples, il existe $\alpha\in k$ vérifiant

$$|\alpha-\pi|_1<|\pi|_1 \quad \text{et} \quad |\alpha-1|_i<1 \quad \text{pour} \quad 2\leq i\leq g.$$

Alors α est une uniformisante en $\mathfrak{p}_1$ et une unité en $\mathfrak{p}_i$ pour $2\leq i\leq g$.

Lemme 3.2.- *Soient* k *un corps de nombres de degré* d, p *un nombre premier, et* $\sigma_1,\ldots,\sigma_d$ *les différents plongements de* k *dans* $\mathbb{C}_p$. *On suppose* p *complètement décomposé dans* k. *Alors il existe* $\alpha\in k$ *tel que*

$$|\sigma_1\alpha|_p=1/p \quad \textit{et} \quad |\sigma_i\alpha|_p=1 \quad \textit{pour} \quad 2\leq i\leq d.$$

Démonstration. Si $\mathfrak{p}_1,\ldots,\mathfrak{p}_d$ désignent les d idéaux premiers au-dessus de p dans k, la valeur absolue $|.|_i$ associée à $\mathfrak{p}_i$ est définie par $|\alpha|_i=|\sigma_i\alpha|_p$. Comme $e(\mathfrak{p}_1)=1$, pour une uniformisante en $\mathfrak{p}_1$ on a $|\pi|_1=1/p$. Il suffit donc d'appliquer le lemme 3.1.

On peut encore énoncer le lemme 3.2 sous la forme suivante :

Lemme 3.3.- *Soient* k *un corps de nombres,* $\sigma_1,\ldots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}$, E *un sous-corps de* $\mathbb{C}$ *de degré fini sur* $\mathbb{Q}$ *contenant tous les* $\sigma_i(k)$, p *un nombre premier totalement décomposé dans* k, *et* $\mathfrak{P}$ *un idéal premier de* E *au-dessus de* p. *Alors il existe* $\alpha\in k$ *tel que* $v_{\mathfrak{P}}(\sigma_1\alpha)=1$ *et* $v_{\mathfrak{P}}(\sigma_i\alpha)=0$ *pour* $2\leq i\leq d$.

Démonstration. Il suffit de fixer un plongement de E dans $\mathbb{C}_p$ associé à $\mathfrak{P}$, puis d'appliquer le lemme 3.2. Si p est ramifié dans E, le lemme 3.2 fournit un α tel que $v_{\mathfrak{P}}(\sigma_1\alpha)=1/e$ et $v_{\mathfrak{P}}(\sigma_i\alpha)=0$ pour $2\leq i\leq d$. ; il suffit alors de remplacer α par α^e.

On va en déduire :

Lemme 3.4.- *Soient* k *et* E *deux corps de nombres. Soient* $\sigma_1,\ldots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}$. *On fixe un plongement de* E *dans* $\mathbb{C}$. *Alors il existe* $\beta\in k^*$ *tel que pour tout* ℓ, $m_1,\ldots,m_d$ *dans* $\mathbb{Z}$, *avec* $\ell>0$, *la relation*

$$\prod_{i=1}^{d}(\sigma_i\beta)^{m_i}\in E^{*\ell}$$

implique que ℓ *divise tous les* m_i.

(on a noté $E^{*\ell}$ le sous-groupe de E^* formé des α^ℓ, pour $\alpha\in E^*$).

Démonstration. On peut supposer que E est une extension galoisienne de $\mathbb{Q}$ contenant $\sigma_1(k)$ (donc contenant tous les $\sigma_i(k)$). Soit p un nombre premier totalement décomposé dans l'extension $k/\mathbb{Q}$ et non ramifié dans E ; soit $\mathfrak{P}$ un idéal premier de E au dessus de p. Le lemme 3.3 nous fournit un élément β de k tel que $\sigma_1(\beta)$ soit une uniformisante en $\mathfrak{P}$, tandis que $\sigma_2\beta,\ldots,\sigma_d\beta$ sont des unités en $\mathfrak{P}$. Supposons

$$\prod_{i=1}^{d}(\sigma_i\beta)^{m_i}=\gamma^\ell$$

avec $\gamma\in E^*$. Soit i_o avec $1\leq i_o\leq d$. Il existe $\tau_{i_o}\in Gal(E/\mathbb{Q})$ tel que $\tau_{i_o}\circ\sigma_{i_o}=\sigma_1$. Comme τ_{i_o} permute les σ_i, on a $\tau_{i_o}\sigma_i\beta\neq\sigma_1\beta$ pour $i\neq i_o$, donc

$$v_{\mathfrak{P}}\left(\prod_{i=1}^{d}(\tau_{i_o}\sigma_i\beta)^{m_i}\right)=m_{i_o}\ ;$$

d'autre part comme $e(\mathfrak{P})=1$, $v_{\mathfrak{P}}(\tau_{i_o}\gamma)^\ell$ est un multiple de ℓ ; donc ℓ divise m_{i_o}.

Il reste à voir que pour tout corps de nombres k il existe une infinité de premiers p totalement décomposés dans k. Il suffit de le voir quand $k/\mathbb{Q}$ est une extension galoisienne, et alors cela résulte immédiatement du fait que la fonction zêta du corps k a un pôle au point s=1 ; en effet, la fonction

$$\log\zeta_k(s)-\sum_{f(p)=1}1/Np^s$$

est bornée au voisinage de s=1 (voir par exemple Lang, A.N.T., Chap. VIII §4.), donc il existe une infinité de p tels que $f_p=1$; si un tel p n'est pas ramifié, il est donc totalement décomposé dans l'extension galoisienne $k/\mathbb{Q}$. On notera d'ailleurs que la *densité de Dirichlet* d'un ensemble $\mathcal{E}$

d'idéaux premiers de k , définie par

$$\lim_{s\to 1_+} \frac{\sum_{p\in\mathcal{E}} 1/Np^s}{\log \frac{1}{s-1}}$$

vaut 1 si $\mathcal{E}$ est l'ensemble des idéaux premiers de k qui sont au-dessus d'un nombre premier totalement décomposé dans k (par exemple, pour $k=\mathbb{Q}(i)$, cette densité ignore les idéaux au-dessus d'un nombre premier congru à 3 modulo 4).

Lemme 3.5.- *Soient* k *un corps de nombres et* $\sigma_1,\ldots,\sigma_d$ *les différents plongements de* k *dans* $\mathbb{C}$. *Il existe une suite infinie* $(\alpha_j)_{j\geq 1}$ *d'éléments de* k^* *telle que les nombres* $\sigma_i\alpha_j$, $(1\leq i\leq d,\ j\geq 1)$ *soient multiplicativement indépendants.*

Démonstration.- Soit K la clôture galoisienne de $\sigma_1(k)$ dans $\mathbb{C}$. Soit p_1 un nombre premier totalement décomposé dans k, et soit $\mathcal{P}_1$ un idéal de K au-dessus de p_1. On utilise le lemme 3.3 pour trouver $\alpha_1\in k$ tel que $v_{\mathcal{P}_1}(\sigma_1\alpha_1)>0$ et $v_{\mathcal{P}_1}(\sigma_i\alpha_1)=0$ pour $2\leq i\leq d$.

Une fois construits, par récurrence, $\alpha_1,\ldots,\alpha_{t-1}$, on choisit un nombre premier p_t totalement décomposé dans k, tel que les $\sigma_i\alpha_j$ $(1\leq i\leq d,\ 1\leq j\leq t-1)$ soient des unités en toutes les places de K au-dessus de p_t. Soit $\mathcal{P}_t$ un idéal de K au-dessus de p_t. On utilise le lemme 3.3 pour trouver $\alpha_t\in k$, premier à $\mathcal{P}_j$ pour $1\leq j<t$, et tel que $v_{\mathcal{P}_t}(\sigma_1\alpha_t)>0$ et $v_{\mathcal{P}_t}(\sigma_i\alpha_t)=0$ pour $2\leq i\leq d$.

La suite (α_j) ainsi construite vérifie la propriété requise : partons d'une relation de dépendance multiplicative

$$\prod_{i=1}^{d}\prod_{j=1}^{t}(\sigma_i\alpha_j)^{m_{ij}} = 1,$$

avec des entiers $m_{ij}\in\mathbb{Z}$, pour $1\leq j\leq t$; soit (i_o,j_o) avec $1\leq i_o\leq d$, $1\leq j_o\leq t$; il existe $\tau_{i_o}\in Gal(K/\mathbb{Q})$ tel que $\tau_{i_o}\circ\sigma_{i_o}=\sigma_1$; alors la valeur absolue $\mathcal{P}_{j_o}$-adique de l'image par τ_{i_o} du membre de gauche doit être 1 ; mais

$$|\tau_{i_o}\sigma_i\alpha_j|_{\mathfrak{P}_{j_o}} = 1 \iff (i_o,j_o)\neq(i,j) ;$$

donc $m_{i_oj_o}=0$.

Remarque.- La théorie de Kummer montre que, sous les hypothèses du lemme 3.4, si E_ℓ désigne le corps obtenu en adjoignant à E les racines ℓ-ièmes de l'unité, on a

$$[E_\ell(\sigma_1\beta^{1/\ell},\ldots,\sigma_d\beta^{1/\ell}):E_\ell] = \ell^d.$$

De même, ce qui précède permet de construire une suite $(\alpha_j)_{j\geq 1}$ d'éléments de k^* telle que, pour tout entier $\ell>0$, et pour tout $t\geq 1$, le corps obtenu en adjoignant à E_ℓ les dt nombres $\sigma_i\alpha_j^{1/\ell}$ $(1\leq i\leq d,\ 1\leq j\leq t)$ ait un degré sur E_ℓ égal à ℓ^{dt}. On construit cette suite par récurrence en appliquant le lemme 3.4 au corps obtenu en adjoignant à E_ℓ les $d(t-1)$ nombres $\sigma_i\alpha_j^{1/\ell}$ $(1\leq i\leq d,\ 1\leq j\leq t-1)$.

Le théorème d'approximation faible permet aussi d'imposer un nombre fini de congruences aux α_j. En voici un exemple qui nous sera utile.

Soit $\mathfrak{M}$ un idéal entier non nul de k,

$$\mathfrak{M}=\prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})},$$

on écrit $v_{\mathfrak{p}}(\mathfrak{M})=m(\mathfrak{p})$, et on définit $k^*(\mathfrak{M})$ comme le sous-groupe de k^* formé des α tels que, pour tout $\mathfrak{p}$ divisant $\mathfrak{M}$, $\alpha-1$ appartienne, dans l'anneau local en $\mathfrak{p}$, à la puissance $m(\mathfrak{p})$-ième de l'idéal maximal :

$$k^*(\mathfrak{M})=\{\alpha\in k^* \ ;\ v_{\mathfrak{p}}(\alpha-1)\geq \frac{1}{e_{\mathfrak{p}}}.v_{\mathfrak{p}}(\mathfrak{M}) \text{ pour tout } \mathfrak{p} \text{ tel que } v_{\mathfrak{p}}(\mathfrak{M})>0\}.$$

Noter que l'on a $k^*(\mathfrak{M})\cap\mathcal{O}=1+\mathfrak{M}$.

Au lieu de $\alpha\in k^*(\mathfrak{M})$, on écrit aussi $\alpha\equiv 1 \bmod^*\mathfrak{M}$. De même, pour α et β dans k^*, $\alpha\equiv\beta \bmod^*\mathfrak{M}$ signifie $\alpha/\beta\equiv 1 \bmod^*\mathfrak{M}$.

Si $\alpha\equiv\beta \bmod^*\mathfrak{M}$ et $\alpha'\equiv\beta' \bmod^*\mathfrak{M}$, alors $\alpha\alpha'\equiv\beta\beta' \bmod^*\mathfrak{M}$.

Par exemple pour $k=\mathbb{Q}$, $m=\prod p^{m(p)}$, deux nombres rationnels non nuls a et b vérifient $a\equiv b \bmod^* m$ si et seulement si on peut écrire $a=b(1+m.\frac{u}{v})$, avec u et v entiers, et $(v,m)=1$.

D'autre part un élément $\alpha \in k^*$ est dit *totalement positif*, et on écrit $\alpha >> 0$, si son image par tout plongement de k dans $\mathbb{R}$ est positive. Par exemple pour tout $\gamma \in k^*$, on a évidemment $\gamma^2 >> 0$. On note $k_+^*(\mathfrak{R})$ le sous-groupe de $k^*(\mathfrak{R})$ formé des $\alpha >> 0$.

(Pour tout ceci, voir par exemple S. Lang, A.N.T., Chap.VI §1, p. 124).

Lemme 3.6.- *Soit* $\mathfrak{R}$ *un idéal entier de* k. *Il existe une suite infinie* $(\alpha_j)_{j\geq 1}$ *d'éléments de* $k_+^*(\mathfrak{R})$ *telle que les nombres* $\sigma_i \alpha_j$, $(1 \leq i \leq d,\ j \geq 1)$ *soient multiplicativement indépendants. De plus, si* E *est un corps de nombres, il existe* $\beta \in k_+^*(\mathfrak{R})$ *tel que pour tout nombre entier* $\ell > 0$, *et pour tout* $(m_1, \ldots, m_d)$ *dans* $\mathbb{Z}^d$, *la relation*

$$\prod_{j=1}^{d} (\sigma_i \beta)^{m_i} \in E^{*\ell}$$

implique que ℓ *divise tous les* m_i.

La démonstration est essentiellement la même que celles des lemmes 3.4 et 3.5 : comme ℓ peut être pair, au lieu d'élever β au carré pour passer de $k^*(\mathfrak{R})$ à $k_+^*(\mathfrak{R})$, on utilise Artin-Whaples pour assurer $|\beta - 1| < 1$ en les places à l'infini.

b) Le théorème d'approximation forte.

Le théorème d'approximation forte est le résultat suivant (Cassels et Fröhlich, Chap.II §15 p.67 ; O.T.O'Meara, Introduction to quadratic forms, §36.G).

Proposition 3.7.- *Soient* k *un corps de nombres,* S *un ensemble fini de places de* k, *et* v_0 *une place de* k, *avec* $v_0 \notin S$. *Pour chaque* $v \in S$, *soit* x_v *un élément de* k_v. *Enfin soit* $\epsilon > 0$.

Alors il existe $\alpha \in k^*$ *tel que*

$$|\alpha - x_v|_v < \epsilon \qquad \textit{pour tout} \quad v \in S$$

et

$$|\alpha|_v \leq 1 \qquad \textit{pour tout} \quad v \notin S,\ v \neq v_0.$$

Pour illustrer ce résultat, nous en déduisons le théorème des restes chinois : *soient* $m_1,\dots,m_t$ *des entiers premiers entre eux deux-à-deux, et* $a_1,\dots,a_t$ *des entiers rationnels ; alors il existe* $n\in\mathbb{Z}$ *tel que*

$$n\equiv a_i \bmod m_i \quad \textit{pour tout} \quad i=1,\dots,t.$$

On choisit pour cela $k=\mathbb{Q}$, v_o est la valeur absolue usuelle (archimédienne), et, en désignant par S_i l'ensemble des diviseurs premiers de m_i, on prend pour S la réunion (disjointe) des S_i. Ecrivons

$$m_i = \prod_{p\in S_i} p^{v(p)} \ ;$$

pour $p\in S$, soit $i(p)$ l'indice i, $1\leq i\leq t$, tel que $p\in S_i$; la proposition 3.6 montre qu'il existe $x\in\mathbb{Q}$ vérifiant

$$|x-a_{i(p)}|_p \leq p^{-v(p)} \quad \text{pour tout} \quad p\in S,$$

et

$$|x|_p \leq 1 \quad \text{pour tout} \quad p\notin S,\ p \text{ premier}.$$

Alors $|x|_p\leq 1$ pour tout premier p, donc $x\in\mathbb{Z}$.

Du théorème d'approximation forte on déduit immédiatement, comme précédemment :

Lemme 3.8.– *Soient* k *un corps de nombres,* p *un nombre premier totalement décomposé dans* k, $\mathfrak{p}_1,\dots,\mathfrak{p}_d$ *les idéaux de* k *au-dessus de* p, $\mathfrak{R}$ *un idéal entier de* k, *premier à* p. *Il existe* $\alpha\in 1+\mathfrak{R}$ *tel que* α *soit une uniformisante en* $\mathfrak{p}_1$ *et que* α *soit une unité en* $\mathfrak{p}_i$ *pour* $2\leq i\leq d$.

Par conséquent dans les lemmes 3.1, 3.2, 3.3, (resp. 3.4, 3.5 et 3.6), on peut ajouter la condition $\alpha\in 1+\mathfrak{R}$ (resp. $\beta\in 1+\mathfrak{R}$, $\alpha_j\in 1+\mathfrak{R}$). En particulier on voit que ces éléments sont entiers. On peut ajouter d'autres conditions du même type, pourvu qu'elles ne fassent intervenir qu'un nombre fini de places. Si on veut une solution dans $\mathcal{O}$, il suffit qu'il y ait une place archimédienne en laquelle on n'impose aucune condition.

c) S-unités.

Commençons par une variante du lemme 3.1.

Lemme 3.9.- *Soit* $\mathfrak{p}$ *un idéal premier de* k. *Il existe* $\gamma\in k^*$ *tel que* $v_{\mathfrak{p}}(\gamma)>0$, *et que* γ *soit une unité en toute place finie de* k *différente de* $\mathfrak{p}$.

Démonstration.- Soit h le nombre de classes de k. L'idéal $\mathfrak{p}^h$ est principal, et il suffit de prendre pour γ un générateur.

Définition. Soit S un ensemble de places de k. Un élément α de k est une S-*unité* si $v(\alpha)=0$ pour toute place finie v n'appartenant pas à S. Les S-unités forment un sous-groupe k_S^* de k^*.

Par exemple, si $k=\mathbb{Q}$, pour $S=\{p_1,\dots,p_\ell\}$, on a

$$\mathbb{Q}_S^*=\{\ \pm p_1^{\alpha_1}\dots p_\ell^{\alpha_\ell}\ ;\ \alpha_j\in\mathbb{Z},\ 1\le j\le\ell\ \}.$$

Si $S=\{v_1,\dots,v_\ell\}$ où $v_1,\dots,v_\ell$ sont ℓ places finies deux-à-deux distinctes, alors le groupe quotient $k_S^*/\mathcal{O}_k^*$ est de rang ℓ sur $\mathbb{Z}$. Plus précisément, si $\mathfrak{P}_i$ est l'idéal premier de k associé à v_i, et si α_i est un générateur de l'idéal principal $\mathfrak{P}_i^h$ (où h est le nombre de classes de k), alors $\alpha_1,\dots,\alpha_\ell$ et $\mathcal{O}_k^*$ engendrent un sous-groupe d'indice fini de k_S^*. En effet, pour tout élément α de k_S^* on peut écrire $(\alpha)=\mathfrak{P}_1^{a_1}\dots\mathfrak{p}_\ell^{a_\ell}$, et alors $\alpha^h/(\alpha_1^{a_1}\dots\alpha_\ell^{a_\ell})^h$ est une unité de $\mathcal{O}_k$.

Lemme 3.10.- *Soient* k *un corps de nombres,* $\sigma_1,\dots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}$, $p_1,\dots,p_\ell$ *des nombres premiers complètement décomposés dans* k, *et, pour* $1\le j\le\ell$, v_j *une place de* k *au-dessus de* p_j. *Posons* $S=\{v_1,\dots,v_\ell\}$. *Il existe des éléments* $\alpha_1,\dots,\alpha_\ell$ *de* k_S^* *tels que les* $d\ell$ *nombres* $\sigma_i\alpha_j$, $(1\le i\le d,\ 1\le j\le\ell)$ *soient multiplicativement indépendants.*

Démonstration.

Désignons par K la clôture galoisienne du corps $k_1=\sigma_1(k)$ dans $\mathbb{C}$, et posons $G=Gal(K/\mathbb{Q})$, $H=Gal(K/k_1)$. Soient p un nombre premier complètement décomposé dans k, v une place de k au-dessus de p, v_1 la place de k_1 qui lui est associée via σ_1, et w une place de K au-dessus de v_1 : ainsi $w(\sigma_1(\alpha))=v(\alpha)$ pour tout $\alpha\in k^*$.

Comme p est complétement décomposé dans k, il l'est aussi dans $\sigma_i(k)$ pour $i=1,\dots,d$. Le corps de décomposition de w contient donc chacun des $\sigma_i(k)$, et par suite c'est K, ce qui signifie que w est complétement décomposée dans K, et que les places τw, $\tau\in G$ sont deux-à-deux distinctes.

Soit $\mathfrak{P}$ l'idéal premier de K associé à la place w, et soit γ un générateur de $\mathfrak{P}^h$, où h est le nombre de classes de K. La seule place de K pour laquelle γ ne soit pas une unité est w. On définit $\alpha\in k$ par $\sigma_1\alpha=N_{K/k_1}\gamma$, et, pour $1\le i\le d$, on choisit $\tau_i\in G$ tel que $\sigma_i=\tau_i\circ\sigma_1$. Alors les places $(\tau_i\circ\sigma)w$, $\sigma\in H$ sont les seules places de K pour lesquelles le nombre

$$\sigma_i(\alpha)=\prod_{\sigma\in H}\tau_i\circ\sigma(\gamma)$$

ne soit pas une unité. Les ensembles $\tau_i Hw$, $(1\le i\le d)$ sont des ensembles deux-à-deux disjoints de places de K au-dessus de p. Enfin, comme les places σw, $\sigma\in H$ sont toutes au-dessus de v_1, α est une v-unité.

Le lemme 3.10 résulte alors de la remarque suivante : soient $\beta_1,\dots,\beta_m$ des éléments de k^* ; pour $1\le j\le m$, désignons par S_j l'ensemble des places de k en lesquelles β_j n'est pas une unité. Si $S_1,\dots,S_m$ sont non vides et deux-à-deux disjoints, alors $\beta_1,\dots,\beta_m$ sont multiplicativement indépendants.

Soient de nouveau k un corps de nombres, S un ensemble de places de k, et $\mathfrak{R}$ un idéal entier non nul de k. On notera

$$k_S^*(\mathfrak{R})=k_S^*\cap k^*(\mathfrak{R}) \quad\text{et}\quad k_S^*(\mathfrak{R})_+=k_S^*\cap k_+^*(\mathfrak{R}).$$

Ecrivons

$$\mathfrak{M} = \prod_{i=1}^{t} \mathfrak{p}_i^{m_i} ,$$

avec $m_i>0$, et supposons $\mathfrak{M}$ et S étrangers (c'est-à-dire qu'aucune des places associées à $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ n'est dans S). Montrons que dans ce cas il existe un entier $a\geq 1$ tel que

$$k_S^{*a} \subset k_S^*(\mathfrak{M})_+ ,$$

où $k_S^{*a}=\{\alpha^a \ ; \ \alpha\in k_S^*\}$. Quitte à prendre a pair, il suffit de vérifier

$$k_S^{*a} \subset k_S^*(\mathfrak{M}) \ ;$$

autrement dit, si $\mathfrak{p}$ est un idéal premier de k et m un entier positif, il existe un entier $a\geq 1$ tel que, pour tout $\alpha\in k^*$ unité en $\mathfrak{p}$, on ait

$$\alpha^a \in 1+\mathfrak{p}^m A_{\mathfrak{p}}$$

(cela suffit : si a vérifie cette propriété, alors tout multiple de a la vérifie encore). Pour $m=1$ on peut prendre $a=N(\mathfrak{p})-1$, car $(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})^*$ est un groupe d'ordre $N(\mathfrak{p})-1$. En général, on peut prendre $a=(N(\mathfrak{p})-1).N(\mathfrak{p})^{m-1}$, car si $\beta\in 1+\mathfrak{p}^m A_{\mathfrak{p}}$, alors $\beta^{N(\mathfrak{p})}\in 1+\mathfrak{p}^{m+1}A_{\mathfrak{p}}$.

Par exemple, pour $k=\mathbb{Q}$, on a

$$\mathbb{Q}^*(m)=\{1+m\frac{u}{v} \ ; \ u\in\mathbb{Z}, \ v\in\mathbb{Z}, \ (v,m)=1\},$$

et ce que l'on vient de faire généralise le fait suivant : si n est un entier positif, il existe un entier $a\geq 1$ tel que $p^a\equiv 1 \bmod n$ pour tout nombre premier p ne divisant pas n (il suffit de prendre pour a un multiple de l'indicatrice d'Euler $\varphi(n)$).

On déduit de ces remarques que dans le lemme 3.10, on peut remplacer k_S^* par $k_S^*(\mathfrak{M})_+$, à condition que S et $\mathfrak{M}$ soient étrangers.

Corollaire 3.11.- *Soient* k *un corps de nombres,* $\sigma_1,\ldots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}$, $\mathfrak{p}_1,\ldots,\mathfrak{p}_\ell$ *des nombres premiers complètement décomposés dans* k, *et, pour* $1\leq j\leq \ell$, v_j *une place de* k *au-dessus de* $\mathfrak{p}_j$. *Soit* $S=\{v_1,\ldots,v_\ell\}$ *et soit* $\mathfrak{M}$ *un idéal entier de* k *étranger à* S. *Il existe* ℓ *éléments* $\alpha_1,\ldots,\alpha_\ell$ *de* $k_S^*(\mathfrak{M})_+$ *tels que les* $d\ell$ *nombres* $\sigma_i\alpha_j$, $(1\leq i\leq d, \ 1\leq j\leq \ell)$ *soient multiplicativement indépendants.*

d) Un critère de densité.

Rappelons que le *rang* d'un groupe abélien (c'est-à-dire d'un $\mathbb{Z}$-module) A est le nombre maximum d'éléments de A linéairement indépendants sur $\mathbb{Z}$ (c'est la dimension du $\mathbb{Q}$-espace vectoriel $A\otimes_{\mathbb{Z}}\mathbb{Q}$). On note rgA ou $rg_{\mathbb{Z}}A$ ce nombre. Par exemple $rg_{\mathbb{Z}}\mathbb{Q}=1$. Si A est de type fini, alors $A\simeq T\times\mathbb{Z}^r$, où T est un groupe fini, et $r=rg_{\mathbb{Z}}A$. Si A est libre, alors A est de rang fini sur $\mathbb{Z}$ si et seulement si A est de type fini (alors $A\simeq\mathbb{Z}^r$).

Rappelons aussi (cf. par exemple Bourbaki, Topologie Générale, chap.7 §1) que si G est un sous-groupe fermé de $\mathbb{R}^n$ de rang r, $0\leq r\leq n$, il existe un plus grand sous-espace vectoriel V de $\mathbb{R}^n$ contenu dans G ; pour tout supplémentaire W de V, le groupe $W\cap G$ est discret dans $\mathbb{R}^n$, et G est somme directe de V et de $W\cap G$.

Enfin le **théorème de Kronecker** (cf. par exemple Bourbaki, op. cit., n°3, prop.7, ou Hardy and Wright, An introduction to the theory of numbers, Chap.23) montre que pour $x_1,\ldots,x_n$ dans $\mathbb{R}$, le sous-groupe

$$\mathbb{Z}^n+\mathbb{Z}(x_1,\ldots,x_n) = \{(h_1+h_0x_1,\ldots,h_n+h_0x_n) \ ; \ (h_0,h_1,\ldots,h_n)\in\mathbb{Z}^n\}$$

de $\mathbb{R}^n$ est dense dans $\mathbb{R}^n$ si et seulement si les nombres $1,x_1,\ldots,x_n$ sont linéairement indépendants sur $\mathbb{Z}$.

Voici d'abord un critère pour qu'un sous-groupe G de $\mathbb{R}^n$ possède un sous-groupe de type fini qui soit dense dans $\mathbb{R}^n$. Si G lui-même est de type fini, cela donne un critère pour que G soit dense dans $\mathbb{R}^n$.

Le cas $n=1$ est facile : d'après le théorème de Kronecker (par exemple), un sous-groupe de type fini de $\mathbb{R}$ est dense dans $\mathbb{R}$ si et seulement si son rang est ≥ 2. Par exemple, pour x_1 et x_2 réels, $\mathbb{Z}x_1+\mathbb{Z}x_2$ est dense dans $\mathbb{R}$ si et seulement si x_1 et x_2 sont linéairement indépendants sur $\mathbb{Z}$. Donc un sous-groupe G de $\mathbb{R}$ possède un sous-groupe de type fini dense dans $\mathbb{R}$ si et seulement si $rg_{\mathbb{Z}}G\geq 2$.

Lemme 3.12.- *Soit* G *un sous-groupe de* $\mathbb{R}^n$. *Les assertions suivantes sont équivalentes :*

(i) *Il existe un sous-groupe de type fini de* G *qui soit dense dans* $\mathbb{R}^n$.

(ii) *Pour tout hyperplan* H *de* $\mathbb{R}^n$, *on a* $rg_{\mathbb{Z}}(G/G\cap H)\geq 2$.

(iii) *Pour tout sous-espace vectoriel* V *de* $\mathbb{R}^n$, $V\neq\mathbb{R}^n$, *on a*

$$rg_{\mathbb{Z}}(G/G\cap V)>\dim_{\mathbb{R}}(\mathbb{R}^n/V).$$

Démonstration.

(i)⇒(ii) Soit Γ un sous-groupe de type fini de G dense dans $\mathbb{R}^n$. Soit H un hyperplan de $\mathbb{R}^n$, et soit $s:\mathbb{R}^n\longrightarrow\mathbb{R}^n/H$ la surjection canonique. Comme Γ est dense dans $\mathbb{R}^n$, $s(\Gamma)$ est dense dans $\mathbb{R}^n/H$, donc $rg_{\mathbb{Z}}s(\Gamma)\geq 2$. Or $s(\Gamma)=\Gamma/\Gamma\cap H\subset G/G\cap H$, d'où le résultat.

(ii)⇒(iii) Commençons par le cas $V=0$. Il s'agit de vérifier que si G est un sous-groupe de $\mathbb{R}^n$ de rang $\leq n$, il existe un hyperplan H de $\mathbb{R}^n$ tel que $rg_{\mathbb{Z}}G/G\cap H\leq 1$. Soit $e_1,\ldots,e_r$ un sous-ensemble maximal $\mathbb{Z}$-linéairement indépendant d'éléments de G, avec $r=rg_{\mathbb{Z}}G$. Alors G est contenu dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}e_1+\ldots+\mathbb{Q}e_r$. Si $\mathbb{R}e_1+\ldots+\mathbb{R}e_r\neq\mathbb{R}^n$, alors pour tout hyperplan H contenant $\mathbb{R}e_1+\ldots+\mathbb{R}e_r$ on a $G=G\cap H$, et $rg_{\mathbb{Z}}G/G\cap H=0$. Si $r=n$ et si $e_1,\ldots,e_n$ est une base de $\mathbb{R}^n$, alors en prenant par exemple $H=\mathbb{R}e_1+\ldots+\mathbb{R}e_{n-1}$ on a $rg_{\mathbb{Z}}G/G\cap H=1$.

Dans le cas général, si V est un sous-espace de $\mathbb{R}^n$ tel que $rg_{\mathbb{Z}}G/G\cap V\leq\dim_{\mathbb{R}}\mathbb{R}^n/V$, d'après le cas particulier qui précède appliqué à $G/G\cap V$ il existe un hyperplan H de $\mathbb{R}^n$ contenant V tel que $rg_{\mathbb{Z}}(G/G\cap V)/(G\cap H/G\cap V)\leq 1$. Or $(G/G\cap V)/(G\cap H/G\cap V)=G/G\cap H$

(iii)⇒(i) Montrons d'abord que si G est un sous-groupe de $\mathbb{R}^n$ qui n'est pas dense dans $\mathbb{R}^n$, alors il existe un sous-espace vectoriel V de $\mathbb{R}^n$ tel que $rg_{\mathbb{Z}}G/G\cap V\leq\dim_{\mathbb{R}}\mathbb{R}^n/V$. Pour cela, soit $\overline{G}$ l'adhérence de G dans $\mathbb{R}^n$, soit V le sous-espace vectoriel maximal de $\mathbb{R}^n$ contenu dans $\overline{G}$, et soit W un supplémentaire de V. Comme $\overline{G}$ est somme directe de V et de $\overline{G}\cap W$, et que $\overline{G}\cap W$ est discret dans W, on a $rg_{\mathbb{Z}}\overline{G}\cap W\leq\dim W$. Or $\overline{G}\cap W\simeq\overline{G}/\overline{G}\cap V\supset G/G\cap V$, et $W\simeq\mathbb{R}^n/V$, donc $rg_{\mathbb{Z}}G/G\cap V\leq\dim_{\mathbb{R}}\mathbb{R}^n/V$.

On peut démontrer ce résultat plus rapidement en utilisant la dualité des groupes abéliens localement compacts (voir ci-dessous §4c). Du lemme 1.3 on déduit que $\mathbb{R}^n$ est en dualité avec lui-même par $(x,y) \longrightarrow e^{2i\pi\langle x,y\rangle}$, où $\langle x,y\rangle = \sum_{i=1}^{n} x_i y_i$. Si G n'est pas dense dans $\mathbb{R}^n$, il existe un caractère non trivial χ de $\mathbb{R}^n$ tel que $\chi(G)=1$; donc il existe $x\in\mathbb{R}^n$, $x\neq 0$, tel que $\langle x,y\rangle\in\mathbb{Z}$ pour tout $y\in G$. On prend alors pour V l'hyperplan $\{z\in\mathbb{R}^n$; $\langle x,z\rangle=0\}$. Cela démontre donc (ii)⇒(i) quand G est de type fini (et (iii)⇒(ii) est trivial).

Il reste à traiter le cas où G n'est pas de type fini. On suppose donc que G est un sous-groupe de $\mathbb{R}^n$ tel que, pour tout sous-groupe de type fini Γ, il existe un sous-espace vectoriel V_Γ de $\mathbb{R}^n$, $V_\Gamma\neq\mathbb{R}^n$ vérifiant

$$\mathrm{rg}_{\mathbb{Z}}\Gamma/\Gamma\cap V_\Gamma \leq \dim_{\mathbb{R}}\mathbb{R}^n/V_\Gamma \ ;$$

on veut montrer qu'il existe un sous-espace vectoriel V de $\mathbb{R}^n$, $V\neq\mathbb{R}^n$, tel que

$$\mathrm{rg}_{\mathbb{Z}}G/G\cap V \leq \dim_{\mathbb{R}}\mathbb{R}^n/V \ .$$

Bien entendu, si G est de rang fini, et si $\gamma_1,\ldots,\gamma_s$ est une famille maximale d'éléments de G linéairement indépendants sur $\mathbb{Z}$, il suffit de prendre $V=V_\Gamma$ où Γ est le sous-groupe de G engendré par $\gamma_1,\ldots,\gamma_s$. On supposera donc $\mathrm{rg}_{\mathbb{Z}}G>n^2$.

On démontre le résultat annoncé par récurrence sur n, le cas $n=1$ étant banal. Soit Γ_o un sous-groupe de type fini de G de rang $>n^2$, et soit V_o l'intersection de tous les V_Γ pour Γ sous-groupe de type fini de G contenant Γ_o. On peut évidemment écrire

$$V_o = V_{\Gamma_1}\cap\ldots\cap V_{\Gamma_s} \ ,$$

avec $s\leq n$. La suite exacte

$$0 \longrightarrow \Gamma_o\cap V_1/\Gamma_o\cap V_1\cap V_2 \longrightarrow \Gamma_o/\Gamma_o\cap V_1\cap V_2 \longrightarrow \Gamma_o/\Gamma_o\cap V_1 \longrightarrow 0$$

et l'inégalité

$$\mathrm{rg}_{\mathbb{Z}}\ \Gamma_o\cap V_1/\Gamma_o\cap V_1\cap V_2 \leq \mathrm{rg}\ \Gamma_o/\Gamma_o\cap V_2$$

montrent que l'on a $\mathrm{rg}_{\mathbb{Z}}\Gamma_o/\Gamma_o\cap V_1\cap V_2 \leq \mathrm{rg}_{\mathbb{Z}}\Gamma_o/\Gamma_o\cap V_1 + \mathrm{rg}_{\mathbb{Z}}\Gamma_o/\Gamma_o\cap V_2$.

d'où

$$rg_{\mathbb{Z}}\Gamma_o/\Gamma_o\cap V_o \leq \sum_{i=1}^{s} rg_{\mathbb{Z}}\Gamma_o/\Gamma_o\cap V_{\Gamma_i} \leq sn \leq n^2,$$

donc $V_o\neq 0$. On va montrer que $H=G/G\cap V_o$ vérifie l'hypothèse de récurrence dans $\mathbb{R}^n/V_o$. Pour cela soit H' un sous-groupe de type fini de H ; on peut écrire $H'=\Gamma''/\Gamma''\cap V_o$, où Γ'' est un sous-groupe de type fini de G. Soit $\Gamma'=\Gamma_o+\Gamma''$. Alors Γ' est un sous-groupe de type fini de G contenant Γ_o, donc $V_{\Gamma'}$ contient V_o. Soit $W'=V_{\Gamma'}/V_o$. On a

$$rg_{\mathbb{Z}}(H'/H'\cap W')\leq rg_{\mathbb{Z}}(\Gamma'/\Gamma'\cap V_{\Gamma'})\leq \dim(\mathbb{R}^n/V_{\Gamma'})=\dim((\mathbb{R}^n/V_o)/W').$$

On peut donc utiliser l'hypothèse de récurrence : il existe un sous-espace vectoriel V de $\mathbb{R}^n$, contenant V_o, tel que $W=V/V_o$ vérifie

$$rg_{\mathbb{Z}}(H/H\cap W)\leq \dim((\mathbb{R}^n/V_o)/W) ;$$

mais $H/H\cap W=G/G\cap V$ et $(\mathbb{R}^n/V_o)/W=\mathbb{R}^n/V$, d'où le résultat.

Ceci termine la démonstration du lemme 3.12.

e) Un énoncé de transcendance.

Pour pouvoir vérifier la condition (iii) du lemme 3.12, on utilisera le corollaire suivant du théorème 2.3 de l'Introduction) :

Proposition 3.13.- *Soient* $y_1,\ldots,y_\ell$ *des éléments de* $\mathbf{L}^d$, *avec* $y_j=(y_{1j},\ldots,y_{dj})$, $1\leq j\leq \ell$. *On suppose que les* ℓd *nombres* y_{ij} *sont linéairement indépendants sur* $\mathbb{Z}$. *Soit* $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$, *et soit* H *un hyperplan de* $\mathbb{C}^d$. *Alors*

$$rg_{\mathbb{Z}}Y\cap H\leq d(d-1).$$

Démonstration.- On sait par le théorème 2.3 de l'Introduction que la conclusion est satisfaite si H ne contient pas de sous-espace de $\mathbb{C}^d$ rationnel sur $\mathbb{Q}$. On va se ramener à cette situation.

On écrit une équation de H :

$$x_1z_1+\ldots+x_dz_d=0.$$

Soit $\xi_1,\ldots,\xi_n$ une base du $\mathbb{Q}$-espace vectoriel engendré par $x_1,\ldots,x_d$; écrivons

$$x_i = \sum_{s=1}^{n} a_{is}\xi_s,$$

avec $a_{is} \in \mathbb{Q}$. Soit $p:\mathbb{C}^d \longrightarrow \mathbb{C}^n$ définie par

$$p(z_1,\ldots,z_d) = \Big(\sum_{i=1}^{d} a_{i1}z_i, \ldots, \sum_{i=1}^{d} a_{in}z_i\Big).$$

Le noyau de p est un sous-espace vectoriel de $\mathbb{C}^d$, rationnel sur $\mathbb{Q}$ (c'est-à-dire qu'il est le noyau de formes linéaires à coefficients dans $\mathbb{Q}$, ce qui équivaut à dire qu'il est engendré par des éléments de $\mathbb{Q}^d$). L'hypothèse sur l'indépendance linéaire des y_{ij} implique aussitôt $Y \cap \mathrm{Ker}p = 0$, donc $\mathrm{rg}_{\mathbb{Z}} p(Y \cap H) = \mathrm{rg}_{\mathbb{Z}} Y \cap H$. Soit Z l'hyperplan de $\mathbb{C}^n$ d'équation $t_1\xi_1 + \ldots + t_n\xi_n = 0$, (où $t_1,\ldots,t_n$ sont les variables de $\mathbb{C}^n$). Alors $p(H) \subset Z$, donc $p(Y \cap H) \subset p(Y) \cap Z \subset \mathbf{L}^n \cap Z$. Comme $\xi_1,\ldots,\xi_n$ sont linéairement indépendants sur $\mathbb{Z}$, on a (théorème 2.3 de l'Introduction) $\mathrm{rg}_{\mathbb{Z}} \mathbf{L}^n \cap Z \leq n(n-1)$, d'où le résultat.

On utilisera la version "réelle" suivante de la proposition 3.13, qui s'en déduit immédiatement en complexifiant.

Corollaire 3.14.- *Soient* $y_1,\ldots,y_\ell$ *des éléments de* $(\mathbf{L} \cap \mathbb{R})^d$, *avec* $y_j = (y_{1j},\ldots,y_{dj})$, $1 \leq j \leq \ell$. *On suppose que les* ℓd *nombres* y_{ij} *sont linéairement indépendants sur* $\mathbb{Z}$. *Soit* $Y = \mathbb{Z}y_1 + \ldots + \mathbb{Z}y_\ell$, *et soit* H *un hyperplan de* $\mathbb{R}^d$. *Alors*

$$\mathrm{rg}_{\mathbb{Z}} Y \cap H \leq d(d-1).$$

Si on admet la conjecture 2.5 (la version homogène suffit) de l'Introduction sur l'indépendance algébrique de logarithmes, alors on peut remplacer, dans la conclusion des propositions 3.13 et 3.14, la borne $d(d-1)$ par $d-1$ (ce qui est évidemment le meilleur possible). En effet, si

$$\eta_s = \sum_{j=1}^{\ell} a_{sj}y_j, \qquad (1 \leq s \leq d)$$

étaient des éléments $\mathbb{Z}$-linéairement indépendants de $Y \cap H$, la matrice $d \times d$:

$$\Big[\sum_{j=1}^{\ell} a_{sj}y_{ij}\Big]_{1 \leq s,i \leq d}$$

aurait un rang strictement inférieur à d. Or la matrice $(a_{sj})_{1\leq s\leq d, 1\leq j\leq \ell}$ a pour rang d, donc il existe des matrices rationnelles $(b_{ij})_{1\leq i\leq d, 1\leq j\leq \ell}$ telles que la matrice

$$\left(\sum_{j=1}^{\ell} a_{sj}b_{ij}\right)_{1\leq s,i\leq d}$$

ait pour rang d ; à plus forte raison, la matrice $(y_{ij})_{1\leq i\leq d, 1\leq j\leq \ell}$ dont les coefficients sont algébriquement indépendants sur $\mathbb{Q}$ (si on en croit la conjecture 2.5 de l'Introduction), satisfait cette propriété, ce qui donne une contradiction.

Le cas le plus simple où on ne sait pas démontrer la borne $d-1$ est $d=2$, et le problème n'est autre que celui des 4 exponentielles (deuxième forme ; cf. Introduction, §2).

Si, dans la proposition 3.13 ou 3.14, on suppose que l'hyperplan H est défini sur le corps $\overline{\mathbb{Q}}$ des nombres algébriques, alors le théorème de Baker (Introduction, th. 2.2) montre immédiatement que l'on a $Y\cap H=0$.

f) Image de k^* par le plongement canonique.

Grâce au théorème d'Artin-Whaples, on voit que l'image de k dans $k\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ par le plongement canonique σ est dense. On en déduit facilement que l'image de k^* dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^*=\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$ par σ est aussi dense. Nous allons préciser cet énoncé en montrant qu'il existe un sous-groupe de type fini de k^* dont l'image dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$ est encore dense.

Commençons par le cas facile $k=\mathbb{Q}$. Si a et b sont deux nombres rationnels positifs, une condition nécessaire et suffisante pour que le sous-groupe de $\mathbb{R}^*$ engendré par a et b :

$$\{a^m b^n \ ; \ (m,n)\in\mathbb{Z}^2\}$$

soit dense dans $\mathbb{R}_+^*$ est que a et b soient multiplicativement indépendants, c'est-à-dire que $\log a$ et $\log b$ soient $\mathbb{Q}$-linéairement indépendants. On en déduit que, si p et p' sont deux nombres premiers distincts, et m un entier non divisible par p ni par p', alors pour $S=\{p,p'\}$, le groupe $\mathbb{Q}_S^*(m)$ est dense dans $\mathbb{R}^*$. En effet, comme nous l'avons

vu plus haut, il existe un entier $t\geq 1$ tel que $p^t\equiv 1 \bmod^* m$ et $p'^t\equiv 1 \bmod^* m$, et alors p^t et p'^t engendrent un sous-groupe de $\mathbb{Q}_S^*(m)_+$ de rang ≥ 2 sur $\mathbb{Z}$, donc dense dans $\mathbb{R}_+^*$.

Nous étendrons cet énoncé aux corps de nombres.

L'application exponentielle associée à un corps de nombres k est définie par :

$$\exp : \quad k\otimes_{\mathbb{Q}}\mathbb{R} \longrightarrow (k\otimes_{\mathbb{Q}}\mathbb{R})^*$$
$$(z_1,\ldots,z_n) \longrightarrow (e^{z_1},\ldots e^{z_n})$$

Son noyau est un sous-groupe de type fini de $k\otimes_{\mathbb{Q}}\mathbb{R}$, isomorphe à $(2i\pi\mathbb{Z})^{r_2}$:

$$\ker\exp = \{\ (0,\ldots,0,2i\pi h_1,\ldots 2i\pi h_{r_2})\in\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\ ;\ (h_1,\ldots,h_{r_2})\in\mathbb{Z}^{r_2}\ \}.$$

Son conoyau est un groupe fini, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{r_1}$: le noyau de la surjection

$$\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{r_1}$$
$$(z_1,\ldots,z_n) \longrightarrow (\mathrm{sgn}z_1,\ldots,\mathrm{sgn}z_{r_1})$$

est $\mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2}=\mathrm{Im}\ \exp$, qui est la composante connexe de l'élément neutre de $\mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2}$. Autrement dit on a la *suite exacte exponentielle* :

$$0 \longrightarrow (2i\pi\mathbb{Z})^{r_2} \longrightarrow k\otimes_{\mathbb{Q}}\mathbb{R} \longrightarrow (k\otimes_{\mathbb{Q}}\mathbb{R})^* \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{r_1} \longrightarrow 1.$$

Si Γ est un sous-groupe de type fini de $k\otimes_{\mathbb{Q}}\mathbb{R}$ dense dans $k\otimes_{\mathbb{Q}}\mathbb{R}$, alors $\exp\Gamma$ est un sous-groupe de type fini de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$, dense dans la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

Soit σ le plongement canonique de k dans $k\otimes_{\mathbb{Q}}\mathbb{R}$; $\sigma(k^*)$ est un sous-groupe de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$, et on désigne par G l'image inverse de $\sigma(k^*)$ dans $k\otimes_{\mathbb{Q}}\mathbb{R}$ par exp :

$$G=\{(z_1,\ldots,z_n)\in\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\ ;\ \exists\alpha\in k^*,\ e^{z_i}=\sigma_i(\alpha)\ \text{ pour }\ 1\leq i\leq n\}.$$

Un élément $\sigma(\alpha)$ de $\sigma(k^*)$ appartient à l'image de exp si et seulement si $\alpha>>0$. On peut donc écrire :

$$G=\{(\log\sigma_1\alpha,\ldots,\log\sigma_n\alpha)\ ;\ \alpha\in k^*,\ \alpha>>0\},$$

où on choisit la détermination principale pour $1\leq i\leq r_1$, et n'importe quelle détermination pour $r_1<i\leq n$. On notera que G est contenu dans $\mathbf{L}_{\mathbb{R}}^{r_1}\times\mathbf{L}^{r_2}$.

On est donc amené à regarder si G contient un sous-groupe de type fini dense dans $k\otimes_{\mathbb{Q}}\mathbb{R}$. Le lemme 3.12 nous conseille de regarder le rang de $G/G\cap H$, quand H est un hyperplan réel de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$.

Proposition 3.15.- *Soit H un hyperplan réel de $k\otimes_{\mathbb{Q}}\mathbb{R}$. Alors $G/G\cap H$ est de rang infini sur $\mathbb{Z}$.*

Démonstration. Le lemme 3.5 nous fournit une suite $(\alpha_j)_{j\geq 1}$ d'éléments de k telle que les nombres $\sigma_i\alpha_j$ $(1\leq i\leq d,\ j\geq 1)$ soient multiplicativement indépendants. Quitte à les remplacer par leur carré, on peut supposer de plus qu'ils sont totalement positifs. Pour $j\geq 1$, soit $y_j\in G$ tel que $\exp(y_j)=\sigma(\alpha_j)$, et soit $Y=\sum_{j\geq 1}\mathbb{Z}y_j$. Autrement dit $y_j=(\log\sigma_1\alpha_j,\ldots,\log\sigma_n\alpha_j)$, où on choisit la détermination principale pour $1\leq i\leq r_1$, et n'importe quelle détermination pour $r_1<i\leq n$. Alors (théorème de Gel'fond-Schneider) les nombres $\log\sigma_1\alpha_j,\ldots,\log\sigma_{r_1}\alpha_j$, $\mathrm{Re}\log\sigma_{r_1+1}\alpha_j,\ldots,\mathrm{Re}\log\sigma_n\alpha_j,\mathrm{Im}\log\sigma_{r_1+1}\alpha_j,\ldots,\mathrm{Im}\log\sigma_n\alpha_j$ $(j\geq 1)$ sont linéairement indépendants sur $\mathbb{Z}$, et le corollaire 3.14 montre que pour tout hyperplan réel H de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, on a $\mathrm{rg}_{\mathbb{Z}}Y\cap H\leq d(d-1)$. La proposition 3.15 en résulte.

En combinant ce qui précède avec le lemme 3.9, nous obtenons le résultat annoncé :

Corollaire 3.16.- *Il existe un sous-groupe de type fini de k^* dont l'image par σ est dense dans $\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$.*

Démonstration. La proposition 3.15 et le lemme 3.12 montrent que G contient un sous-groupe de type fini Γ dense dans $k\otimes_{\mathbb{Q}}\mathbb{R}$. Donc $\exp\Gamma$ est un sous-groupe de type fini de $\sigma(k^*)$ dense dans la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$. Pour chaque $e=(e_1,\ldots,e_{r_1})\in(\mathbb{Z}/2\mathbb{Z})^{r_1}$, le théorème d'approximation faible permet de trouver $\gamma_e\in k^*$ tel que $\mathrm{sgn}\sigma_i\gamma_e=e_i$, $(1\leq i\leq r_1)$. Alors le sous-groupe de $\sigma(k^*)$ engendré par $\exp\Gamma$ et les $\sigma(\gamma_e)$ est dense dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

On en déduit que *tout homomorphisme continu* $\chi : (k\otimes_{\mathbb{Q}}\mathbb{R})^* \longrightarrow \mathbb{C}^*$ *qui envoie* $\sigma(k^*)$ *dans le sous-groupe de torsion de* $\mathbb{C}^*$ (groupe des racines de l'unité, isomorphe à $\mathbb{Q}/\mathbb{Z}$) *est d'ordre fini*. En effet, sur un sous-groupe de type fini, un tel homomorphisme χ est d'ordre fini, et par continuité il en est de même sur l'adhérence. Il est facile de déterminer ces caractères χ : ce sont ceux de la forme $z \longrightarrow \prod_{i=1}^{r_1} (z_i/|z_i|)^{a_i}$, avec $a_i=0$ ou 1. Il y en a donc 2^{r_1}.

On peut préciser le corollaire 3.16. Voici la généralisation promise de ce que nous avons vu tout à l'heure pour $\mathbb{Q}$.

Corollaire 3.17.- *Soient* k *un corps de nombres,* $\sigma_1,\ldots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}$, $p_1,\ldots,p_\ell$ *des nombres premiers complètement décomposés dans* k, *et, pour* $1\leq j\leq \ell$, v_j *une place de* k *au-dessus de* p_j. *Soit* $S=\{v_1,\ldots,v_\ell\}$ *et soit* $\mathfrak{M}$ *un idéal entier de* k *étranger à* S. *Si* $\ell>d^2-d+1$, *alors le groupe* $k_S^*(\mathfrak{M})_+$ *est dense dans la composante neutre de* $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

Démonstration.(cf. Sansuc, Sém. TdN, p.262).- On prend $\alpha_1,\ldots,\alpha_\ell$ dans $k_S^*(\mathfrak{M})_+$ tels que les $d\ell$ nombres $\sigma_i\alpha_j$, $(1\leq i\leq d,\ 1\leq j\leq \ell)$ soient multiplicativement indépendants. On prend ensuite $y_1,\ldots,y_\ell$ dans $k\otimes_{\mathbb{Q}}\mathbb{R}$ tels que $\exp y_j=\sigma\alpha_j$ $(1\leq j\leq \ell)$. Soit Y le sous-groupe de $k\otimes_{\mathbb{Q}}\mathbb{R}$ engendré par $y_1,\ldots,y_\ell$. Le corollaire 3.14 montre que pour tout hyperplan réel de $k\otimes_{\mathbb{Q}}\mathbb{R}$, on a $\mathrm{rg}_{\mathbb{Z}} Y/Y\cap H\geq \ell-d^2+d>1$. Le lemme 3.12 permet de conclure que Y est dense dans $k\otimes_{\mathbb{Q}}\mathbb{R}$. Donc le sous-groupe engendré par les $\sigma(\alpha_j)$ est dense dans $\mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2}$, qui est la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

Sansuc (op. cit., p. 264) demande quel est le rang minimum d'un sous-groupe de type fini de k^* dont l'image par σ est dense dans la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$. Notons $s(k)$ ce rang minimum. On a évidemment $s(k)\geq r_1+r_2+1$. Le groupe $k_S^*(\mathfrak{M})_+$ du corollaire 3.17 étant de rang ℓ sur $\mathbb{Z}$, on a $s(k)\leq d^2-d+2$. Comme le remarque Sansuc (resp. Roy), la démonstration, par Lenstra (Sém. TdN, p. 143-147) du corollaire 3.14 dans le cas particulier

d'une extension $k/\mathbb{Q}$ abélienne (ou plus généralement d'une extension galoisienne de groupe de Galois G tel que tout idéal à gauche de $\mathbb{Q}[G]$ soit bilatère), qui n'utilise pas de résultat de transcendance, donne la majoration $s(k)\leq 2d$ (resp. $s(k)\leq d+n$). Voici une autre démonstration de cette majoration $s(k)\leq 2d$ dans le cas où k est une extension abélienne de $\mathbb{Q}$, utilisant le théorème de Baker (l'argument est dû à Brylinski ; cf. l'exposé de Lenstra, p.143; les détails sont dûs à D.Roy).

Lemme 3.18.- *Soit* k *une extension abélienne de* $\mathbb{Q}$ *de degré* d. *Soient* α_1, α_2 *deux éléments de* k^* *tels que les* $2d$ *nombres* $\sigma_i\alpha_j$ $(1\leq i\leq d,\ j=1,2)$ *soient multiplicativement indépendants. Alors le sous-groupe de* k^* *engendré par ces* $2d$ *nombres a une image par* ϖ *dense dans la composante neutre de* $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

Démonstration. Considérons d'abord un corps de nombres k quelconque. Notons $\sigma_{\mathbb{R}}$ le plongement canonique $(\sigma_1,\ldots,\sigma_n)$ (noté précédemment $\boldsymbol{\sigma}$) de k dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, et $\sigma_{\mathbb{C}}$ le plongement $(\sigma_1,\ldots,\sigma_d)$ de k dans $\mathbb{C}^d$. Ils sont liés par $\sigma_{\mathbb{C}}=\theta\circ\sigma_{\mathbb{R}}$, où θ est l'application de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ dans $\mathbb{C}^d$ donnée par

$$\theta(x_1,\ldots,x_{r_1},z_1,\ldots,z_{r_2})=(x_1,\ldots,x_{r_1},z_1,\ldots,z_{r_2},\overline{z}_1,\ldots,\overline{z}_{r_2}).$$

Comme θ est $\mathbb{R}$-linéaire et applique une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ sur une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}^d$, il en résulte que, si $V_{\mathbb{R}}$ est un $\mathbb{R}$ sous-espace vectoriel de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, alors le sous-espace vectoriel $V_{\mathbb{C}}$ de $\mathbb{C}^d$ engendré par $\theta(V_{\mathbb{R}})$ vérifie

$$\dim_{\mathbb{R}}V_{\mathbb{R}}=\dim_{\mathbb{C}}V_{\mathbb{C}} \quad\text{et}\quad \theta(V_{\mathbb{R}})=\theta(\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})\cap V_{\mathbb{C}}.$$

On a aussi un diagramme commutatif

$$\begin{array}{ccc} \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} & \xrightarrow{\exp_{\mathbb{R}}} & \mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2} \\ \theta\downarrow & & \downarrow\theta \\ \mathbb{C}^d & \xrightarrow{\exp_{\mathbb{C}}} & \mathbb{C}^{*d}. \end{array}$$

Supposons maintenant k contenu dans $\mathbb{C}$ et galoisien sur $\mathbb{Q}$. On identifie son groupe de Galois G à l'ensemble $\{\sigma_1,\ldots,\sigma_d\}$ des plongements de k dans $\mathbb{C}$, et on définit une action de G sur $\mathbb{C}^d$ par

$$\sigma(z_1,\ldots,z_d)=(z_{i_1},\ldots,z_{i_d}),$$

où $(i_1,\ldots,i_d)$ est la permutation de $(1,\ldots,d)$ donnée par $\sigma_s\circ\sigma=\sigma_{i_s}$ pour $s=1,\ldots,d$. De cette manière on a

$$\sigma\circ\sigma_{\mathbb{C}}(\alpha)=\sigma_{\mathbb{C}}(\sigma\alpha) \quad \text{pour tout } \alpha\in k \text{ et } \sigma\in G,$$

$$\sigma\circ\exp_{\mathbb{C}}=\exp_{\mathbb{C}}\circ\sigma \quad \text{pour tout } \sigma\in G,$$

et $\mathbb{C}^d$ devient un $\mathbb{C}[G]$-module libre de rang 1 engendré par $(1,0,\ldots,0)$.

Enfin on vérifie que $\theta(\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})$ est invariant par G, donc on peut définir une action de G sur $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ par

$$\theta\circ\sigma=\sigma\circ\theta \quad \text{pour tout } \sigma\in G.$$

Comme θ est $\mathbb{R}$-linéaire, cela fait de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ un $\mathbb{R}[G]$-module. Cette action vérifie aussi

$$\sigma\circ\sigma_{\mathbb{R}}(\alpha)=\sigma_{\mathbb{R}}(\sigma\alpha) \quad \text{pour tout } \alpha\in k \text{ et } \sigma\in G,$$

$$\sigma\circ\exp_{\mathbb{R}}=\exp_{\mathbb{R}}\circ\sigma \quad \text{pour tout } \sigma\in G,$$

Dans le cas présent, G est abélien. En notant $\hat{G}$ le dual de G, $\mathbb{C}^d$ admet la décomposition suivante en somme directe de sous-modules irréductibles

$$\mathbb{C}^d=\bigoplus_{\chi\in\hat{G}}\mathbb{C}v_\chi \quad \text{avec} \quad v_\chi=(\chi(\sigma_1),\ldots,\chi(\sigma_d)),$$

et $\mathbb{C}v_\chi$ est le sous-espace sur lequel chaque $\sigma\in G$ agit via $\chi(\sigma)$: $\sigma v_\chi=\chi(\sigma)v_\chi$. Dans la base des v_χ, un élément $(z_1,\ldots,z_d)$ de $\mathbb{C}^d$ s'écrit

$$(z_1,\ldots,z_d)=\sum_{\chi\in\hat{G}}a_\chi v_\chi \quad \text{avec} \quad a_\chi=\frac{1}{d}\sum_{i=1}^{d}\overline{\chi(\sigma_i)}.z_i.$$

Revenons à la démonstration du lemme 3.18. Soit Γ le sous-groupe de k^* engendré par α_1, α_2 et par leurs conjugués. Il s'agit de montrer que $\sigma_{\mathbb{R}}\Gamma$ est dense dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. Quitte à remplacer α_1 et α_2 par leurs carrés, on peut les supposer totalement positifs. Alors $\sigma_{\mathbb{R}}(\alpha_1)$ et $\sigma_{\mathbb{R}}(\alpha_2)$ admettent des pré-images z_1 et z_2 sous $\exp_{\mathbb{R}}$. Soit Z_i le $\mathbb{Z}[G]$-sous-module de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ engendré par z_i. Comme $\sigma_{\mathbb{R}}\Gamma=\exp_{\mathbb{R}}(Z_1+Z_2)$, il suffit de montrer que Z_1+Z_2 est dense dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$.

Si ce n'est pas le cas, il existe une fonctionnelle linéaire non nulle $\Psi_{\mathbb{R}}$ de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ qui applique Z_1+Z_2 dans $\mathbb{Z}$. Soit $Y_i=\theta(Z_i)$ le $\mathbb{Z}[G]$-sous-module de $\mathbb{C}^d$ engendré par $y_i=\theta(z_i)$. La fonctionnelle linéaire $\Psi_{\mathbb{R}}$ de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ détermine une fonctionnelle linéaire $\Psi_{\mathbb{C}}$ de $\mathbb{C}^d$ par la condition $\Psi_{\mathbb{R}}=\Psi_{\mathbb{C}}\circ\theta$, et cette dernière applique Y_1+Y_2 dans $\mathbb{Z}$. On peut choisir des déterminations des logarithmes telles que

$$y_i=(\log\sigma_1\alpha_i,\ldots,\log\sigma_d\alpha_i),\quad i=1,2.$$

Dans la base des v_χ, $(\chi\in\hat{G})$, y_1 et y_2 s'écrivent

$$y_1=\sum_{\chi\in\hat{G}} a_\chi v_\chi \quad\text{et}\quad y_2=\sum_{\chi\in\hat{G}} b_\chi v_\chi,$$

avec

$$a_\chi=\frac{1}{d}\sum_{\chi\in\hat{G}}\overline{\chi(\sigma)}\log\sigma\alpha_1,\quad\text{et}\quad b_\chi=\frac{1}{d}\sum_{\chi\in\hat{G}}\overline{\chi(\sigma)}\log\sigma\alpha_2.$$

Pour chaque $\chi\in\hat{G}$, posons $t_\chi=\Psi_{\mathbb{C}}(v_\chi)$. Le fait que $\Psi_{\mathbb{C}}$ applique Y_1+Y_2 dans $\mathbb{Z}$ se traduit par

$$\Psi_{\mathbb{C}}(\sigma y_1)=\sum_{\chi\in\hat{G}} a_\chi\chi(\sigma)t_\chi=m_\sigma\in\mathbb{Z}$$
$$\Psi_{\mathbb{C}}(\sigma y_2)=\sum_{\chi\in\hat{G}} b_\chi\chi(\sigma)t_\chi=n_\sigma\in\mathbb{Z}.$$

Par dualité on en déduit

$$\sum_{\sigma\in G} m_\sigma\overline{\chi(\sigma)}=da_\chi t_\chi\quad\text{et}\quad\sum_{\sigma\in G} n_\sigma\overline{\chi(\sigma)}=db_\chi t_\chi$$

pour tout $\chi\in\hat{G}$. Par le théorème de Baker, aucun des a_χ n'est nul, donc les m_σ ne sont pas tous nuls. Des relations

$$\Big(\sum_{\sigma\in G} m_\sigma\overline{\chi(\sigma)}\Big)b_\chi=\Big(\sum_{\sigma\in G} n_\sigma\overline{\chi(\sigma)}\Big)a_\chi$$

on déduit

$$\sum_{\sigma\in G}\sum_{\tau\in G} m_\sigma\overline{\chi(\sigma\tau)}\log\tau\alpha_2=\sum_{\sigma\in G}\sum_{\tau\in G} n_\sigma\overline{\chi(\sigma\tau)}\log\tau\alpha_1,$$

pour tout $\chi\in\hat{G}$, et en sommant ces égalités sur $\chi\in\hat{G}$ on trouve

$$\sum_{\sigma\in G} m_\sigma\log\sigma^{-1}\alpha_2=\sum_{\sigma\in G} n_\sigma\log\sigma^{-1}\alpha_1$$

en contradiction avec le choix de α_1 et α_2.

Ceci termine la démonstration du lemme 3.18.

Enfin, quand k est totalement réel, la conjecture 2.5 de l'Introduction (version homogène) sur l'indépendance algébrique de logarithmes implique s(k)=d+1. Plus précisément, il résulte de ce que nous avons vu que si $\alpha_1,\ldots,\alpha_{d+1}$ sont tels que les d(d+1) nombres $\sigma_i\alpha_j$ sont multiplicativement indépendants, alors, sous la conjecture en question, le sous-groupe de k^* engendré par $\alpha_1,\ldots,\alpha_{d+1}$ a une image par σ dense dans $\mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2}$. La solution du problème des 4 exponentielles permettrait d'obtenir ce résultat pour d=2.[1]

g) Image de k^* par le plongement logarithmique.

Considérons maintenant le plongement logarithmique λ de k^* dans $\mathbb{R}^n$ (avec $n=r_1+r_2$) :

$$\lambda(\alpha) = (\delta_i \log|\sigma_i\alpha|)_{1\leq i\leq n} \in \mathbb{R}^n$$

avec $\delta_i=1$ pour $1\leq i\leq r_1$, $\delta_i=2$ pour $r_1<i\leq n$ (les δ_i sont les degrés locaux en les places infinies). On a pour $\alpha\in k^*$:

$$\exp\circ\lambda(\alpha)=(|\sigma_1\alpha|^{\delta_1},\ldots,|\sigma_n\alpha|^{\delta_n}),$$

ce qui donne un diagramme commutatif

$$\begin{array}{ccc} k^* & \xrightarrow{\sigma} & (k\otimes_{\mathbb{Q}}\mathbb{R})^*. \\ \lambda\downarrow & & \downarrow\varphi \\ \mathbb{R}^n & \xrightarrow{\exp} & \mathbb{R}_+^{*n} \end{array}$$

où $\varphi(z_1,\ldots,z_n)=(|z_1|^{\delta_1},\ldots,|z_n|^{\delta_n})$. Soit $\psi: k\otimes_{\mathbb{Q}}\mathbb{R}\longrightarrow\mathbb{R}^n$ définie par

$$\psi(z_1,\ldots,z_n) = (z_1,\ldots,z_{r_1},2\mathrm{Re}z_{r_1+1},\ldots 2\mathrm{Re}z_n).$$

Alors $\psi(G)$ est l'image par λ du sous-groupe k_+^* de k^* formé par les éléments totalement positifs.

De la proposition 3.15 on déduit :

---

[1] Damien Roy a montré que l'on a toujours $s(k)=d+1$ pour $d\leq 4$ et $s(k)<\frac{3}{2}d$ pour $d\geq 5$. (Mai 1988).

Corollaire 3.19.- *Si* H *est un hyperplan de* $\mathbb{R}^n$, *le rang sur* $\mathbb{Z}$ *de* $\lambda(k^*)/\lambda(k^*)\cap H$ *est infini*

Démonstration. Comme $\psi(G)=\lambda(k_+^*)$, on a :

$$G/G\cap\psi^{-1}(H)\simeq\lambda(k_+^*)/\lambda(k_+^*)\cap H\subset\lambda(k^*)/\lambda(k^*)\cap H.$$

Mais la codimension sur $\mathbb{R}$ de $\psi^{-1}(H)$ dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ est ≥ 1 ; la proposition 3.15 donne donc le résultat.

Par conséquent il existe un sous-groupe de type fini de k^* dont l'image par λ est dense dans $\mathbb{R}^n$, et on peut préciser cet énoncé comme dans la partie f) ci-dessus.

h) Le théorème de la progression arithmétique.

Commençons par un cas particulier élémentaire. *Soient* p', p'' *deux nombres premiers distincts,* m *un entier premier à* $p'.p''$, a_0 *un nombre rationnel non nul,* x *un nombre réel, et* $\epsilon>0$. *Il existe une infinité de nombres premiers* p *ayant la propriété suivante :*

pour chacun de ces p, *il existe* $a\in\mathbb{Q}^*$ *vérifiant*

(i) $a\equiv a_0 \bmod^* m$

(ii) $|a-x|\leq\epsilon$

(iii) $a=pb$, *où* b *est une* SUS' *unité, avec* $S'=\{p',p''\}$, *et* S *est l'ensemble des diviseurs premiers de* m.

Démonstration.- Quitte à changer a_0 en $-a_0$, il n'y a pas de restriction à supposer $x>0$. On écrit $a_0=a_0'a_0''$, avec $a_0'\in\mathbb{Q}^*$ premier à m (c'est-à-dire $a_0'=u/v$, avec u et v dans $\mathbb{Z}$ premiers à m), et $a_0''\in\mathbb{Q}_S^*$, $a_0''>0$. Le théorème de la progression arithmétique de Dirichlet permet de trouver une infinité de nombres premiers p vérifiant $p\equiv a_0' \bmod^* m$ (on écrit $vv'+mm'=1$, et on prend $p\equiv uv' \bmod m$). Prenons un tel p, et notons $a'=a_0''p$. On a

$$a'\equiv a_0 \bmod^* m$$

car $(a_0',m)=1$.

Nous avons vu que $\mathbb{Q}_{S'}^*(m)_+$ est dense dans $\mathbb{R}_+^*$. On peut donc choisir

$b' \in \mathbb{Q}_S^*, (m)_+$ vérifiant

$$|b' - \frac{x}{a'}| \leq \frac{\epsilon}{a'}.$$

On pose $a=a'b'$, et on vérifie immédiatement les propriétés annoncées avec $b=a_0''b'$.

En quelque sorte, par rapport au théorème de Dirichlet, on perd de l'information en deux places finies (en autorisant des facteurs p' et p''), mais on gagne de l'information à la place à l'infini.

Grâce au corollaire 3.17, ce résultat se généralise aux corps de nombres.

Corollaire 3.20.- *Soient* k *un corps de nombres de degré* d, S *un ensemble fini de* ℓ *places de* k *au-dessus de* ℓ *nombres premiers totalement décomposés dans la clôture galoisienne de* k, *avec* $\ell > d^2-d+1$, ϵ *un nombre réel* >0, $\mathfrak{R}$ *un idéal entier de* k *étranger à* S, α_0 *un élément de* k^*, *et, pour chaque place archimédienne* v, *soit* $\alpha_v \in k_v$. *Soit* S' *l'ensemble des idéaux premiers divisant* $\mathfrak{R}$.

Il existe alors un ensemble infini d'idéaux premiers de k, *de degré* 1, *étrangers à* $\mathfrak{R}$ *et* S, *avec la propriété suivante : pour chaque idéal* $\mathfrak{p}$ *dans cet ensemble, il existe* $\alpha \in k^*$, *vérifiant*

(i) $\alpha \equiv \alpha_0 \bmod \mathfrak{R}$;

(ii) $|\alpha - \alpha_v|_v < \epsilon$ *pour toute place archimédienne* v ;

(iii) $(\alpha) = \mathfrak{p}.\mathfrak{D}$, *où* $\mathfrak{D}$ *est un idéal fractionnaire de* k *dont la décomposition en idéaux premiers ne fait intervenir que des éléments de* SUS'.

Schéma de la démonstration.(Réf.: J.J. Sansuc, op. cit., corollaire 4.4 p.264). On utilise le théorème de Dirichlet généralisé (cf. S. Lang, A.N.T., Chap.VIII §4 p. 166) pour résoudre (i) et (iii), puis le corollaire 3.17 pour vérifier (ii).

Dans l'exposé de Sansuc est donnée une application de ce résultat à l'étude du principe de Hasse pour des intersections de quadriques.

§4. Etude locale p-adique.

Cette section concerne l'analogue p-adique du §1 : nous déterminons les homomorphismes continus de K ou K^* dans $\mathbb{C}^*$, quand K est un corps valué ultramétrique localement compact. La solution repose sur l'existence d'un caractère non trivial de $\mathbb{Q}_p$; on peut ensuite soit expliciter tous les homomorphismes, soit utiliser la dualité dans les groupes abéliens localement compacts.

a) Groupes topologiques.

Un *groupe topologique* est un groupe muni d'une topologie pour laquelle l'application $(x,y) \longrightarrow xy^{-1}$ est continue. Les translations $x \longrightarrow ax$ et $x \longrightarrow xa$ sont alors des homéomorphismes de G sur G. Si H est un sous-groupe ouvert de G, alors H est fermé dans G (puisque le complémentaire de H dans G est réunion des classes aH, qui sont ouvertes). Si H est un sous-groupe fermé d'indice fini, alors H est ouvert dans G.

Un groupe topologique est *localement compact* si et seulement si l'élément neutre possède un voisinage compact.

Si H est un sous-groupe fermé d'un groupe localement compact, il est clair que H est alors localement compact. Si H est un sous-groupe localement compact d'un groupe topologique G, alors H est fermé dans G.

Un groupe topologique G est *totalement discontinu* (ce qui veut dire que les seules parties connexes sont les points) si et seulement s'il existe un système fondamental de voisinages ouverts de l'élément neutre formé de sous-groupes de G.

Lemme 4.1.- *Soit* G *un groupe localement compact totalement discontinu, et soit* χ *un quasi-caractère de* G *(homomorphisme continu de* G *dans* $\mathbb{C}^*$*). Alors* χ *est localement constant.*

De plus, si G *est compact, alors* χ *est un caractère de* G *(homomorphisme continu à valeurs dans* $\mathbb{U}$*) d'ordre fini.*

Démonstration.- Comme χ est continu, il existe un sous-groupe ouvert H de G tel que $\chi(H)$ soit contenu dans un demi-plan $Re(z)>\eta$ avec $0<\eta<1$ (qui est un voisinage de 1 dans $\mathbb{C}^*$). Mais $\{Re(z)>\eta\}$ ne contient pas de sous-groupe de $\mathbb{C}^*$ autre que $\{1\}$. Donc la restriction de χ à H est constante.

Si maintenant G est compact, alors tout sous-groupe ouvert de G est d'indice fini dans G. Puisque H est un sous-groupe ouvert de G sur lequel χ est constant, alors χ sera constant sur chaque classe modulo H, donc χ sera d'ordre fini.

b) Corps valués ultramétriques.

Soient K un corps, et v une *valuation* sur K, c'est-à-dire une application de K dans $\mathbb{R}\cup\{\infty\}$ vérifiant

$v(x)=\infty \Leftrightarrow x=0$

$v(xy)=v(x)+v(y)$

$v(x+y)\geq\min\{v(x),v(y)\}$.

Le corps K est alors un *corps valué ultramétrique*. En notation exponentielle, on obtient une *valeur absolue ultramétrique*, et K est un espace topologique totalement discontinu, les boules $\{|x-a|\leq r\}$ et $\{|x-a|<r\}$ étant, pour $r>0$, à la fois ouvertes et fermées. Le *groupe de valuation* $v(K^*)$ est un sous-groupe de $\mathbb{R}$, et la valuation est *discrète* (resp. *dense*) si ce sous-groupe l'est dans $\mathbb{R}$. Dans la suite, on suppose v discrète.

L'*anneau de valuation* :

$$A=\{x\in K\ ;\ v(x)\geq 0\}$$

est un anneau de valuation discrète, de corps des fractions K ; son unique

idéal maximal est l'*idéal de valuation* :

$$\mathcal{M}=\{x\in K \ ; \ v(x)>0\},$$

qui est principal ; le groupe des unités de A (groupe multiplicatif des éléments inversibles) est $U=A^*=A-\mathcal{M}$, et le *corps résiduel* est $A/\mathcal{M}$. La *caractéristique résiduelle* est la caractéristique du corps résiduel. Une *uniformisante* est un générateur de l'idéal $\mathcal{M}$.

Si K' est le complété d'un corps valué K, alors K' a le même groupe de valuation et le même corps résiduel que K.

Si K est un corps valué complet, K est localement compact si et seulement si la valuation est discrète et le corps résiduel fini. Nous supposerons désormais que K est un tel corps de caractéristique 0, et nous désignerons par q le nombre d'éléments du corps résiduel. Si p désigne la caractéristique résiduelle de K, alors K est (isomorphe à) une extension finie de $\mathbb{Q}_p$ (voir par exemple Weil, B.N.T., Ch.I §3 Th.5).

L'anneau de valuation A est un voisinage compact de 0 dans K. Soit S un sous-ensemble de A ayant q éléments formant un système de représentants des classes modulo $\mathcal{M}$, et soit π une uniformisante. Alors tout élément de A s'écrit de manière unique sous la forme d'une série convergente (développement de Hensel) :

$$\sum_{j\geq 0} a_j \pi^j,$$

avec $a_j\in S$ pour tout $j\geq 0$, et bien sûr tout élément de K s'écrit $\pi^n\alpha$, avec $n\in\mathbb{Z}$ et $\alpha\in A$.

D'autre part

$$1+\mathcal{M}=\{u\in U \ ; \ v(u-1)>0\}$$

est un sous-groupe ouvert et fermé de U, le groupe de torsion de A^* contient un groupe cyclique T d'ordre $q-1$, et tout élément de U s'écrit de manière unique comme un produit d'une racine $q-1$ ième de l'unité par un élément de $1+\mathcal{M}$: $U=T\times(1+\mathcal{M})$. De plus $K^*\simeq\mathbb{Z}\times T\times(1+\mathcal{M})$ (la projection sur le premier facteur étant donnée par la valuation qui est supposée discrète). Nous étudierons plus en détail la structure multiplicative de $1+\mathcal{M}$ au début du

Chapitre 2 (cf. A. Weil, Basic Number Theory, Chap. II §3).

Si on pose, pour $m\geq 1$,

$$U^{(m)}=\{x\in K \ ; \ v(x-1)\geq mv(\pi)\}=1+\mathcal{M}^m,$$

alors on a une filtration

$$U\supset U^{(1)}\supset U^{(2)}\supset\ldots\supset U^{(m)}\supset\ldots$$

où chaque terme est un sous-groupe compact ouvert de K^*. On a $U\simeq T\times U^{(1)}$; donc $U/U^{(1)}$ est isomorphe au groupe multiplicatif $(A/\mathcal{M})^*$, tandis que pour $m\geq 1$, $U^{(m)}/U^{(m+1)}$ est isomorphe au groupe additif du corps résiduel $A/\mathcal{M}$. Ainsi l'indice de $U^{(m)}$ dans U est $q^{m-1}(q-1)$.

Si L est une extension finie de K de degré n, alors

$$w(x)=\frac{1}{n}.v(N_{L/K}(x)), \qquad (x\in L)$$

définit l'unique valuation sur L qui prolonge v. La topologie définie par w coïncide avec celle sur le K-espace vectoriel K^n identifié à L par le choix d'une base, et L est complet. Le groupe des valeurs $w(L^*)$ contient $v(K^*)$ comme sous-groupe d'indice fini, et cet indice e est l'*indice de ramification* de L sur K. Le *degré résiduel* f de L sur K est le degré de l'extension $[A_L/\mathcal{M}_L : A_K/\mathcal{M}_K]$:

$$\begin{array}{ccc} A_K & \longrightarrow & A_L \\ \downarrow & & \downarrow \\ A_K/\mathcal{M}_K & \longrightarrow & A_L/\mathcal{M}_L \end{array}$$

où A_K (resp. A_L) est l'anneau de valuation de K (resp. L) et $\mathcal{M}_K$ (resp. $\mathcal{M}_L$) son idéal de valuation. Enfin on a $n=ef$.

Signalons aussi que le groupe additif de K est localement isomorphe au groupe multiplicatif K^* par l'exponentielle et le logarithme (définis par des séries entières convergeant au voisinage de 0 et de 1 respectivement). Donc K^* est localement isomorphe à $\mathbb{Z}_p^n$, avec $n=[K:\mathbb{Q}_p]$.

Le théorème de structure des sous-espaces vectoriels fermés de $\mathbb{R}^n$ que nous avons vu au §3 a un analogue p-adique (cf. Bourbaki, Topologie Générale, Ch. VII §1 Ex.17) : pour tout sous-groupe fermé G de $\mathbb{Q}_p^n$, il existe un plus grand sous-espace vectoriel V de $\mathbb{Q}_p^n$ sur $\mathbb{Q}_p$ contenu dans G, et pour tout

supplémentaire W de V dans $\mathbb{Q}_p^n$, $W \cap G$ est compact, et G est la somme directe de V et de $G \cap W$.

c) Quasi caractères additifs.

Soit $n=p_1^{\alpha_1}\dots p_s^{\alpha_s} \in \mathbb{Z}$ un entier non nul. Comme les nombres $n/p_i^{\alpha_i}$, $1 \leq i \leq s$, sont premiers entre eux dans leur ensemble, il existe des entiers $q_1,\dots,q_s$ tels que $\sum_{i=1}^{s} q_i n p_i^{-\alpha_i}=1$, c'est-à-dire $1/n=\sum_{i=1}^{s} q_i p_i^{-\alpha_i}$ (décomposition en éléments simples). On en déduit que tout nombre rationnel x admet une décomposition

$$x=a+\sum_{p}\sum_{h\geq 1} r_{ph}p^{-h},$$

où $a \in \mathbb{Z}$ (ce n'est pas en général la partie entière de x), $r_{ph} \in \mathbb{Z}$, $0 \leq r_{ph} < p$ pour tout $h \geq 1$ et tout p premier, les r_{ph} étant tous nuls sauf un nombre fini. Cette décomposition est unique. C'est la décomposition du $\mathbb{Z}$-module de torsion $\mathbb{Q}/\mathbb{Z}$ en somme directe des $(\mathbb{Q}/\mathbb{Z})_p$, où p parcourt l'ensemble des nombres premiers, où $(\mathbb{Q}/\mathbb{Z})_p$ est l'ensemble des éléments de $\mathbb{Q}/\mathbb{Z}$ annulés par une puissance de p.

Le groupe $(\mathbb{Q}/\mathbb{Z})_p$ est isomorphe au quotient $\mathbb{Z}[1/p]/\mathbb{Z}$, où $\mathbb{Z}[1/p]$ (encore noté $\mathbb{Z}_{(p)}$) est l'anneau de fractions de $\mathbb{Z}$ par la partie multiplicative $\{p^n ; n \geq 0\}$:

$$\mathbb{Z}[1/p]=\{a/p^h ; a \in \mathbb{Z}, h \geq 0\} \subset \mathbb{Q}.$$

Comme $\mathbb{Z}_p \cap \mathbb{Z}[1/p]=\mathbb{Z}$ et que $\mathbb{Q}_p=\mathbb{Z}_p+\mathbb{Z}[1/p]$, le groupe $\mathbb{Q}_p/\mathbb{Z}_p$ est isomorphe au sous-groupe $(\mathbb{Q}/\mathbb{Z})_p$ de $\mathbb{Q}/\mathbb{Z}$; l'homomorphisme φ_p composé :

$$\mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow (\mathbb{Q}/\mathbb{Z})_p$$

est décrit de la manière suivante : tout $x \in \mathbb{Q}_p$ peut s'écrire sous la forme $x=r+z$, avec $r \in \mathbb{Z}[1/p]$, et $z \in \mathbb{Z}_p$ (r est unique modulo $\mathbb{Z}$) ; l'image de x par $\varphi_p : \mathbb{Q}_p \longrightarrow (\mathbb{Q}/\mathbb{Z})_p$ est la classe modulo 1 de r. Autrement dit pour

$$x=\sum_{n=-k}^{\infty} a_n p^n$$

avec $0 \leq a_n < p$, $(n \geq 0)$, $\varphi_p(x)$ est la classe modulo 1 de

$$\sum_{n=-k}^{-1} a_n p^n = \frac{a_{-k}}{p^k} + \frac{a_{-k+1}}{p^{k-1}} + \ldots + \frac{a_{-1}}{p} .$$

La décomposition en éléments simples montre que la surjection canonique $\mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z}$ est donnée par $\sum_p \varphi_p$.

Il est clair que φ_p est un homomorphisme de groupes additifs de noyau $\mathbb{Z}_p$. Ainsi φ_p est constant sur les ouverts $|x-x_0|<1$, et définit un homomorphisme localement constant, donc continu, de $\mathbb{Q}_p$ dans $\mathbb{R}/\mathbb{Z}$. Soit $e:\mathbb{R}/\mathbb{Z} \longrightarrow \mathbb{U}$ l'isomorphisme obtenu par passage au quotient à partir de $x \longrightarrow e^{2i\pi x}$. Pour tout $a\in\mathbb{Q}_p^*$, l'application $x \longrightarrow e(\varphi_p(ax))$ est donc un homomorphisme continu de $\mathbb{Q}_p$ dans $\mathbb{C}^*$. Nous allons voir qu'il n'y en a pas d'autre.

Lemme 4.2.- *Soit* $f:\mathbb{Q}_p \longrightarrow \mathbb{C}^*$ *un homomorphisme continu. Alors il existe* $a\in\mathbb{Q}_p$, *unique, tel que* $f(x)=e\circ\varphi_p(ax)$ *pour tout* $x\in\mathbb{Q}_p$.

Démonstration. Commençons par l'unicité. Si $a=\sum_{i=-h}^{\infty} a_i p^i$ est le développement de Hensel de $a\in\mathbb{Q}_p$, avec $0\leq a_i<p$, on a, pour tout $n\in\mathbb{Z}$, $\varphi_p(ap^{-n})=\sum_{i=-h}^{n-1} a_i/p^{n-i}$ dans $\mathbb{Q}/\mathbb{Z}$; or nous avons vu que pour $0\leq b_i<p$ l'égalité

$$\sum_{i=-h}^{n-1} a_i/p^{n-i} = \sum_{i=-h}^{n-1} b_i/p^{n-i}$$

implique $a_i=b_i$ pour $-h\leq i\leq n-1$.

Passons maintenant à l'existence de a. Montrons d'abord qu'il existe un entier $\ell\in\mathbb{Z}$ tel que $f(x)=1$ pour $v(x)\geq\ell$. C'est une conséquence immédiate du lemme 4.1 : les ouverts $p^n\mathbb{Z}_p$, $n\geq 0$, forment une base des voisinages de 0 dans $\mathbb{Z}_p$, et f est localement constant.

On peut aussi voir directement l'existence de ℓ de la manière suivante. Par continuité il suffit de vérifier $f(p^n)=1$ pour n suffisamment grand. Or pour tout $x\in\mathbb{Q}_p$, la suite des nombres $f(p^n x)=f(x)^{p^n}$, $n\geq 1$, tend vers $f(\lim_n p^n x)=f(0)=1$ quand n tend vers l'infini. Il reste à vérifier que si $z\in\mathbb{C}^*$ est tel que z^{p^n} tend vers 1 pour n tendant vers l'infini, alors z

est une racine de l'unité d'ordre une puissance de p. D'abord on a évidemment $|z|=1$. Ensuite si, pour un entier $n\geq 1$, on a

$$0<|z^{p^n}-1|<|e^{i\pi/p}-1|,$$

alors

$$|z^{p^n}-1|<|z^{p^{n+1}}-1|.$$

Or si z^{p^n} tend vers 1, on a pour une infinité de n

$$|z^{p^{n+1}}-1|\leq|z^{p^n}-1|<|e^{i\pi/p}-1|,$$

ce qui n'est possible que si $z^{p^n}=1$ pour tout n suffisamment grand.

Donc pour tout $x\in\mathbb{Q}_p^*$ il existe $s\in\mathbb{Z}$ tel que $f(p^s x)=1$. En particulier l'image de f est contenue dans le groupe des racines de l'unité, qui est isomorphe à $\mathbb{Q}/\mathbb{Z}$. Soit $\psi:\mathbb{Q}_p\longrightarrow\mathbb{Q}/\mathbb{Z}$ l'homomorphisme obtenu en composant f avec l'inverse de e, c'est-à-dire tel que $e\circ\psi(x)=f(x)$; ψ est un homomorphisme localement constant, puisque $\psi(x)=0$ pour $v_p(x)\geq\ell$.

On peut écrire $\psi(p^{\ell-1})=a_{-\ell}/p$, avec $0\leq\ell<p$, puisque $p.\psi(p^{\ell})=1$. De même $p\psi(p^{\ell-2})=\psi(p^{\ell-1})$, donc

$$\psi(p^{\ell-2})=\frac{a_{-\ell}}{p^2}+\frac{a_{-\ell+1}}{p}.$$

Plus généralement, pour $m\in\mathbb{Z}$, $m<\ell$, on a $p\psi(p^m)=\psi(p^{m+1})$, donc si

$$\psi(p^{m+1})=\frac{a_{-\ell}}{p^{\ell-m-1}}+\ldots+\frac{a_{-m-2}}{p},$$

avec $0\leq a_i<p$, $(-\ell\leq i\leq -m-2)$, on peut définir un entier a_{-m-1} dans l'intervalle $0\leq a_{-m-1}<p$ par

$$\psi(p^m)=\frac{a_{-\ell}}{p^{\ell-m}}+\ldots+\frac{a_{-m-2}}{p^2}+\frac{a_{-m-1}}{p}.$$

On définit $a\in\mathbb{Q}_p$ par $a=\sum_{i\geq\ell}a_i p^i$. Alors $\psi(p^m)=\varphi_p(ap^m)$ pour tout $m\in\mathbb{Z}$ (si $m>\ell$, les deux membres sont nuls). Finalement par continuité on a $\psi(x)=\varphi_p(ax)$ pour tout $x\in\mathbb{Q}_p$.

Remarque.- Si $f:\mathbb{Q}_p\longrightarrow\mathbb{R}$ est un homomorphisme continu, alors $f(p^n x)=p^n f(x)$ doit tendre vers $f(0)=0$ quand n tend vers l'infini, donc $f(x)=0$ pour

tout $x\in\mathbb{Q}_p$. Le fait qu'il n'y ait pas d'homomorphisme continu non nul de $\mathbb{Q}_p$ dans $\mathbb{R}$ se déduit aussi du lemme 4.2, puisque le groupe topologique $\mathbb{R}$ est isomorphe à $\mathbb{R}_+^*$, qui est lui-même un sous-groupe de $\mathbb{C}^*$.

Nous aurons aussi besoin de connaître les homomorphismes continus de $\mathbb{Z}_p$ dans $\mathbb{C}^*$. Si f est un tel homomorphisme, alors f se prolonge (d'une infinité de façons) en un homomorphisme continu ψ de $\mathbb{Q}_p$ dans $\mathbb{C}^*$: on définit par récurrence $\psi(1/p^k)$, $k\geq 1$, en choisissant une racine p-ième de $\psi(1/p^{k-1})$, et on pose

$$\psi(a_0+\sum_{i=-h}^{-1} a_i p^i)= f(a_0)+\sum_{i=-h}^{-1} a_i\psi(p^i), \qquad (a_0\in\mathbb{Z}_p,\ a_i\in\mathbb{Z},\ 0\leq a_i<p,\ -h\leq i\leq -1).$$

Alors pour $x=(p-1)(p^{-k}+\ldots+p^{-k-s})$ on a

$$\psi(x+p^{-k-s})=\psi(p^{-k+1})=\psi(x).\psi(p^{-k-s}),$$

ce qui permet de vérifier que ψ est un homomorphisme continu. Le lemme 4.2 dit qu'il existe $a\in\mathbb{Q}_p$ tel que $f(x)=e\circ\varphi_p(ax)$ pour tout $x\in\mathbb{Z}_p$.

Si $a'\in\mathbb{Q}_p$ est tel que $a-a'\in\mathbb{Z}_p$, alors $ax-a'x\in\mathbb{Z}_p$ pour tout $x\in\mathbb{Z}_p$, donc $\varphi_p(ax)=\varphi_p(a'x)$ pour tout $x\in\mathbb{Z}_p$. Comme $\mathbb{Q}_p/\mathbb{Z}_p\simeq\mathbb{Z}[1/p]/\mathbb{Z}$, f est déterminé par un élément de la forme m/p^ℓ, avec $(\ell,m)\in\mathbb{Z}^2$, $\ell\geq 0$, $0\leq m<p^\ell$, $(m,p)=1$. Pour $x\in\mathbb{Z}_p$ donné par son développement de Hensel :

$$x=\sum_{i\geq 0} x_i p^i,$$

on trouve

$$f(x)=e\left(\frac{m}{p^\ell}\,(x_0+x_1p+\ldots+x_{\ell-1}p^{\ell-1})\right).$$

On peut retrouver ce résultat d'une autre manière : comme dans le début de la démonstration du lemme 4.2, on a $f(p^n\mathbb{Z}_p)=1$ pour n suffisamment grand. Soit ℓ le plus petit entier tel que $f(p^\ell\mathbb{Z}_p)=1$. Le noyau de f est un sous-groupe de $\mathbb{Z}_p$: c'est $p^\ell\mathbb{Z}_p$; alors f définit par passage au quotient un homomorphisme de $\mathbb{Z}_p/p^\ell\mathbb{Z}_p\simeq\mathbb{Z}/p^\ell\mathbb{Z}$ dans $\mathbb{C}^*$, c'est-à-dire un caractère du groupe cyclique $\mathbb{Z}/p^\ell\mathbb{Z}$, et on retrouve bien le résultat.

Soit maintenant K un corps valué complet localement compact de caractéristique nulle et de caractéristique résiduelle p ; cela revient à dire que K est une extension finie de $\mathbb{Q}_p$. Si $\mathcal{L}$ est une application $\mathbb{Q}_p$-linéaire de K dans $\mathbb{Q}_p$, alors $e\circ\varphi_p\circ\mathcal{L}$ est un homomorphisme continu de K dans $\mathbb{C}^*$. On les obtient tous ainsi : c'est vrai pour $K=\mathbb{Q}_p$ par le lemme 4.2 ; en général, le groupe topologique additif K est isomorphe à $\mathbb{Q}_p^n$ avec $n=[K:\mathbb{Q}_p]$; pour $f:\mathbb{Q}_p^n \longrightarrow \mathbb{C}^*$ homomorphisme continu, on définit $(a_1,\ldots,a_n)\in\mathbb{Q}_p^n$ par

$$f(0,\ldots,0,x_\nu,0,\ldots,0)=e\circ\varphi_p(a_\nu x_\nu), \qquad (1\leq\nu\leq n).$$

Si $\mathcal{L}(x_1,\ldots,x_n)=a_1x_1+\ldots+a_nx_n$, on a bien $f=e\circ\varphi_p\circ\mathcal{L}$.

Comme toute application linéaire $\mathcal{L}$ de K dans $\mathbb{Q}_p$ peut s'écrire sous la forme $\mathcal{L}(x)=\mathrm{Tr}_{K/\mathbb{Q}_p}(\eta x)$, avec $\eta\in K$, on peut énoncer :

Lemme 4.3.- *Soit $f:K \longrightarrow \mathbb{C}^*$ un homomorphisme continu. Alors il existe $\eta\in K$, unique, tel que $f(x)=e\circ\varphi_p(\mathrm{Tr}_{K/\mathbb{Q}_p}(\eta x))$ pour tout $x\in K$.*

L'unicité provient du fait que la trace est une application surjective : pour tout $x\in\mathbb{Q}_p$, on a $\mathrm{Tr}(x/n)=x$ quand $n=[K:\mathbb{Q}_p]$. Le caractère $\chi=e\circ\varphi_p\circ\mathrm{Tr}$ n'étant pas trivial, si $\chi(\eta x)=1$ pour tout $x\in K$, alors $\eta.K\neq K$, donc $\eta=0$.

Ce résultat fait partie des préliminaires de la thèse de Tate (Cassels et Fröhlich, Chap. XV). Pour le démontrer Tate utilise la dualité des groupes abéliens localement compacts. Voici ce dont il s'agit.

Soit G un groupe abélien localement compact. On munit le groupe $\hat{G}$ des caractères de G d'une topologie (qui en fait un groupe topologique localement compact : le *dual* du groupe G) en prenant pour base de voisinages de l'unité dans $\hat{G}$ les ensembles $W(C,U)$ suivants : pour C fermé compact dans G, et U voisinage de 1 dans $\mathbb{U}$, $W(C,U)$ désigne l'ensemble des caractères χ de G vérifiant $\chi(x)\in U$ pour tout $x\in C$.

Un élément x de G définit un caractère $y \longrightarrow y(x)$ de $\hat{G}$, et ceci définit un isomorphisme entre G et le dual de $\hat{G}$. Si H est un sous-groupe

fermé de G, alors l'annulateur de H :

$$H^{\perp}=\{y\in\hat{G} \ ; \ y(x)=1 \quad \text{pour tout} \quad x\in H\}$$

est un sous-groupe fermé de $\hat{G}$, et $(H^{\perp})^{\perp}=H$ (en identifiant G et son bidual). On a de plus les isomorphismes de groupes topologiques :

$$\hat{G}\simeq\hat{G}/H^{\perp} \quad \text{et} \quad (G/H)\hat{}\simeq H^{\perp}.$$

Le groupe G est compact si et seulement si $\hat{G}$ est discret.

Soient G et G' deux groupes abéliens localement compact, et soit Ψ une application continue de $G\times G'$ dans $\mathbb{U}$. On suppose

(i) pour tout $x\in G$, l'application $x' \longrightarrow \Psi(x,x')$ est un caractère de G', et pour tout $x'\in G'$, l'application $x \longrightarrow \Psi(x,x')$ est un caractère de G.

(ii) les noyaux à droite et à gauche sont triviaux : pour $x\in G$, la condition $\Psi(x,x')=1$ pour tout $x'\in G'$ implique $x=1$, et pour $x'\in G'$, la condition $\Psi(x,x')=1$ pour tout $x\in G$ implique $x'=1$.

Pour chaque $x'\in G'$, on définit un élément $\chi_{x'}$ de $\hat{G}$ par $\chi_{x'}(x)=\Psi(x,x')$.

Lemme 4.4.- *L'application* $\theta:x' \longrightarrow \chi_{x'}$ *est un homomorphisme injectif de* G' *dans* $\hat{G}$, *dont l'image est dense dans* $\hat{G}$.

Démonstration. Le fait que θ soit un homomorphisme injectif résulte immédiatement des propriétés (i) et (ii). Soit $W(C,U)$ un voisinage de 1 dans $\hat{G}$, avec C compact de G, et U voisinage ouvert de 1 dans $\mathbb{U}$. Soit $x\in C$. Comme Ψ est continue, et que $\Psi(x,1)=1\in\hat{G}$, il existe un voisinage V_x de x dans G et un voisinage V' de 1 dans G', tels que

$$\Psi(V_x \ , \ V')\subset U.$$

Etant donné que C est compact, on peut le recouvrir par un nombre fini de V_{x_i}, avec $x_i\in C$; pour chacun de ces x_i, il existe un V'_i tel que

$$\Psi(V_{x_i} \ , \ V'_i)\subset U.$$

Soit W l'intersection de ces V'_i ; on a

$$\Psi(C, \ W)\subset U,$$

donc $\theta(W)\subset W(C,U)$. Donc θ est continue.

Il reste à voir que l'image est dense. Soit H l'adhérence de l'image dans $\hat{G}$. Le quotient est un groupe abélien localement compact. S'il n'est pas trivial, alors $(\hat{G}/H)^{\wedge}$ non plus, et il existe un caractère $\lambda\neq 1$ de $\hat{G}$ qui vaut 1 sur H. Donc il existe $x\in G$, $x\neq 1$, tel que $\lambda(y)=y(x)=1$ pour tout $y\in H$; cela est vrai en particulier pour $y\in\theta(G)$: on a donc $\chi_{x'}(x)=1$ pour tout $x'\in G'$, sans que x soit égal à 1, ce qui contredit l'hypothèse (ii). D'où le lemme.

On dit que Ψ *met* G *et* G' *en dualité* quand θ est surjectif ; alors θ est un isomorphisme topologique de G' sur $\hat{G}$.

Par exemple l'application $(x,y)\longrightarrow e(xy)=e^{2i\pi xy}$ met $\mathbb{R}$ en dualité avec lui-même (lemme 1.3), l'application $(x,y)\longrightarrow e\circ\varphi_p(xy)$ met $\mathbb{Q}_p$ en dualité avec lui-même (lemme 4.2), et l'application $(x,\eta)\longrightarrow e\circ\varphi_p\circ Tr_{K/\mathbb{Q}_p}(x\eta)$ met K en dualité avec lui-même (lemme 4.3). Aussi $\mathbb{Z}$ et $\mathbb{U}$ sont en dualité par $(n,u)\longrightarrow u^n$ (corollaire 1.5), ce qui revient à dire que $\mathbb{Z}$ et $\mathbb{R}/\mathbb{Z}$ sont en dualité par $(n,x)\longrightarrow e(nx)$; enfin nous avons vu ci-dessus que $\mathbb{Z}_p$ et $\mathbb{Q}_p/\mathbb{Z}_p$ étaient en dualité par l'application $(z,\bar{t})\longrightarrow e\circ\varphi_p(zt)$, où $\bar{t}$ est la classe de $t\in\mathbb{Q}_p$ modulo $\mathbb{Z}_p$.

Montrons que si K est un corps localement compact non discret, et si χ est un caractère additif non trivial de K, alors l'application $(x,y)\longrightarrow\chi(xy)$ met le groupe additif de K en dualité avec lui-même.

Avec les notations précédentes (pour $G=G'=K$, $\hat{G}=\hat{K}$), il s'agit de voir que l'application θ, définie par $\theta(y)=\chi_y$, où $\chi_y(x)=\chi(xy)$, est surjective. On a vu que l'image de θ était dense, il suffit de montrer qu'elle est fermée. Montrons que l'injection θ est bicontinue. Soit $|.|$ la valeur absolue sur K définissant la topologie. Soit $\epsilon>0$. On choisit $x_0\in K$ tel que $\chi(x_0)\neq 1$, et on prend un compact $C=\{x\in K\ ;\ |x|\leq M\}$ dans K avec $M\geq|x_0|/\epsilon$; soit U le voisinage de 1 dans $\mathbb{U}$ défini par $U=\{u\in\mathbb{U}\ ;\ |u-1|<|\chi(x_0)-1|\ \}$. Si $\theta(y)\in W(C,U)$, alors $\chi_y(C)\subset U$, donc $|\chi(xy)-1|<|\chi(x_0)-1|$ pour tout $x\in C$, ce

qui implique $x_o/y \notin C$, c'est-à-dire $|y|<|x_o|/M\leq\epsilon$.

On en déduit que $\theta(K)$ est isomorphe à K, donc $\theta(K)$ est un sous-groupe localement compact de $\hat{K}$, et par conséquent il est fermé dans $\hat{K}$.

Voir à ce sujet Bourbaki, Théories spectrales, Chap. II ; S. Iyanaga, The theory of numbers, Chap. III ; A. Weil, Basic Number Theory, Chap. II, et la thèse de Tate déjà mentionnée (Cassels-Fröhlich, Chap. XV), E.Hewitt and K.A.Ross, Abstract Harmonic Analysis I, p.404, 435 et 451.

d) Quasi-caractères multiplicatifs.

Commençons par étudier les homomorphismes continus de $\mathbb{Q}_p^*$ dans $\mathbb{C}^*$. Tout $z\in\mathbb{Q}_p^*$ s'écrit de manière unique $z=p^m u$, avec $u\in\mathbb{Z}_p^*$, et $m\in\mathbb{Z}$, de sorte que $|z|=p^{-m}$. Ainsi $\mathbb{Q}_p^*\simeq\mathbb{Z}\times\mathbb{Z}_p^*$. Soit χ un homomorphisme continu de $\mathbb{Q}_p^*$ dans $\mathbb{C}^*$. La restriction de χ au premier facteur $\mathbb{Z}$ donne un homomorphisme de $\mathbb{Z}$ dans $\mathbb{C}^*$, donc de la forme $p^m \longrightarrow p^{tm}$, et la restriction $\tilde{\chi}$ de χ au second facteur est un homomorphisme continu de $\mathbb{Z}_p^*$ dans $\mathbb{C}^*$.

Maintenant $\mathbb{Z}_p^*\simeq T\times(1+p\mathbb{Z}_p)$ où T est cyclique d'ordre $p-1$: tout $u\in\mathbb{Z}_p^*$ s'écrit de manière unique $u=\zeta.(1+px)$, avec ζ racine de l'unité : $\zeta^{p-1}=1$, et $x\in\mathbb{Z}_p$. La restriction de $\tilde{\chi}$ au facteur T est simplement un caractère du groupe cyclique T ; on peut fixer un isomorphisme entre T et le groupe des racines $(p-1)$-ièmes de l'unité dans $\mathbb{C}$ (cela revient à choisir une place au dessus de p dans le corps cyclotomique ; comme p est totalement décomposé dans ce corps, il y a $p-1$ choix distincts), on peut écrire $\tilde{\chi}(\zeta)=\zeta^b$, avec $b\in\mathbb{Z}$, $0\leq b<p$. Enfin, l'application $\log_p$ établit un isomorphisme entre les groupes topologiques $1+p\mathbb{Z}_p$ et $\mathbb{Z}_p$ si $p>2$, et entre $1+2\mathbb{Z}_2$ et $\{\pm1\}\times\mathbb{Z}_2$ si $p=2$; or nous avons vu ci-dessus que tout homomorphisme continu de $\mathbb{Z}_p$ dans $\mathbb{C}^*$ est un caractère d'ordre fini, qui provient d'un caractère d'un groupe fini $\mathbb{Z}/p^\ell\mathbb{Z}$, $\ell\geq0$. En particulier $\tilde{\chi}$ est un caractère de $\mathbb{Z}_p^*$. On a donc démontré :

Lemme 4.5.- *Soit* $\chi:\mathbb{Q}_p^* \longrightarrow \mathbb{C}^*$ *un homomorphisme continu. Il existe un nombre complexe* t *et un caractère d'ordre fini* $\tilde{\chi}$ *de* $\mathbb{Z}_p^*$, *déterminés de manière unique, tels que, pour* $z=p^m u$ *avec* $u\in\mathbb{Z}_p^*$, *on ait*

$$\chi(z)=\tilde{\chi}(u).|z|^t.$$

Soit maintenant K une extension finie de $\mathbb{Q}_p$. On désigne par $\mathcal{M}$ l'idéal de valuation, par U le groupe des unités, et par $U^{(m)}$, $m\geq 0$ le système fondamental de voisinages de 1 dans U donné par $U^{(m)}=1+\mathcal{M}^m$, $(m\geq 1)$, et $U^{(0)}=U$. Soit $\chi:K^* \longrightarrow \mathbb{C}^*$ un homomorphisme continu. Comme U est compact, la restriction de χ à U est un caractère de U (lemme 4.1). De plus χ est localement constant (lemme 4.1), donc χ doit être constant sur $U^{(m)}$ pour m suffisamment grand. Le plus petit entier ℓ tel que $\chi(U^{(\ell)})=1$ est appelé le *degré de ramification* de χ, l'idéal $\mathcal{F}=\mathcal{M}^\ell$ est le *conducteur* de χ, et on dit que χ est *non ramifié* si $\ell=0$, c'est-à-dire si $\chi(U)=1$.

Par exemple, pour $K=\mathbb{Q}_p$, et χ donné par le lemme 4.5, on étend $\tilde{\chi}$ à $\mathbb{Q}_p^*$ par $\tilde{\chi}(p)=1$, et on considère le caractère $\psi:\mathbb{Q}_p^* \longrightarrow \mathbb{C}^*$ qui coïncide avec χ sur $U^{(1)}$, et qui vérifie $\psi(p)=\psi(\zeta)=1$. Si $\ell(\chi)$, $\ell(\tilde{\chi})$ et $\ell(\psi)$ sont les conducteurs de χ, $\tilde{\chi}$ et ψ respectivement, on a

$$\ell(\chi)=\ell(\tilde{\chi})=\begin{cases} 1 & \text{si } \ell(\psi)=0 \text{ et } b\neq 0 \\ \ell(\psi) & \text{sinon.}\end{cases}$$

Lemme 4.6.- *Soit* $\chi:K^* \longrightarrow \mathbb{C}^*$ *un homomorphisme continu non ramifié. Alors il existe* $t\in\mathbb{C}$ *tel que* $\chi(x)=|x|^t$ *pour tout* $x\in K^*$. *Ce nombre complexe* t *est unique modulo* $2i\pi e/\log p$ *où* e *est l'indice de ramification.*

Démonstration. Soit π une uniformisante (à ne pas confondre avec le π de $2i\pi$). Soit $t\in\mathbb{C}$ tel que $\chi(\pi)=|\pi|^t$. L'isomorphisme $K^*\simeq U\times\mathbb{Z}$ permet d'écrire tout $x\in K^*$ de manière unique sous la forme $x=u\pi^m$, avec $u\in U$ et $m\in\mathbb{Z}$. Par hypothèse $\chi(u)=1$, donc $\chi(x)=\chi(\pi^m)=|\pi|^{tm}=|x|^t$. Comme $|\pi|=p^{-1/e}$, on a $|\pi|^t=|\pi|^{t'}$ si et seulement si $t-t'\in(2i\pi e/\log p)\mathbb{Z}$.

Si on écrit $\chi(x)=\|x\|^{\lambda}$, avec $\|x\|=|x|^{d}$ où d=ef est le degré local, et $\lambda=t/d$, alors λ est défini modulo $2i\pi/\log N(v)$, puisque $N(v)=p^{f}$.

Lemme 4.7.- *Soit* $\chi:K^{*}\longrightarrow\mathbb{C}^{*}$ *un homomorphisme continu. Alors il existe un caractère* $\tilde{\chi}$ *de* U, *uniquement déterminé par* χ, *et il existe* $t\in\mathbb{C}$, *tels que, pour* $x=a\pi^{m}\in K^{*}$ *avec* $a\in U$ *et* $m\in\mathbb{Z}$, *on ait* $\chi(x)=\tilde{\chi}(a).|a|^{t}$.

Démonstration. On a $K^{*}\simeq U\times\mathbb{Z}$, c'est-à-dire que tout $x\in K^{*}$ s'écrit de manière unique $x=a\pi^{m}$ avec $a\in U$ et $m\in\mathbb{Z}$. On prend (et on n'a pas le choix) pour $\tilde{\chi}$ la restriction de χ à U.

On voit ainsi que χ est un caractère de K^{*} si et seulement si l'*exposant* t est nul.

Il reste à déterminer les caractères de U. Un tel caractère $\tilde{\chi}$ est trivial sur $U^{(\ell)}$ où ℓ est le conducteur, donc $\tilde{\chi}$ s'identifie à un caractère du groupe fini $U/U^{(\ell)}=U/(1+\mathcal{P})$.

Références :

J. Tate, Fourier Analysis in Number Fields and Hecke's Zeta Functions, Chap. XV de : J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press 1967.

A. Weil, Basic Number Theory, Grundlehren der Math. 144, Springer Verlag 1985 ; voir notamment Chap. II §5 et Chap VII §3.

S. Iyanaga, The Theory of Numbers, North Holland 1975 (Chap. III).

§5. Idèles.

Pour étudier simultanément tous les complétés d'un corps de nombres en les différentes places, on introduit l'anneau $\mathbb{A}_k$ des adèles et le groupe $\mathfrak{I}_k$ des idèles. Nous étudierons les homomorphismes continus de $\mathfrak{I}_k$ dans $\mathbb{C}^*$, puis, parmi eux, ceux qui s'annulent sur k^*.

a) Produit direct restreint ; adèles, idèles.

Soit I un ensemble non vide. Pour chaque $i\in I$, soit G_i un groupe topologique localement compact. Pour chaque $i\in I$ sauf peut-être un nombre fini, soit H_i un sous-groupe ouvert compact de G_i. Le *produit direct restreint* des G_i relativement aux H_i est le sous-ensemble du produit $\prod_{i\in I} G_i$ constitué des (x_i) tels que $x_i\in H_i$ pour tout i sauf au plus un nombre fini. On munit ce groupe G d'une topologie qui en fait un groupe topologique localement compact de la manière suivante : soit J un sous-ensemble fini de I tel que pour tout $i\notin J$, H_i soit défini ; on pose

$$G^J = \prod_{i\notin J} H_i \cdot \prod_{i\in J} G_i,$$

et on munit G^J de la topologie produit ; on prend comme système fondamental de voisinages de 1 dans G un système fondamental de voisinages de 1 dans G^J, et la topologie ainsi définie ne dépend pas du choix de J. Comme $\prod_{i\notin J} H_i$ est compact, le groupe G^J est localement compact, et G aussi.

Un système fondamental de voisinages de 1 dans G est donné par les parallélotopes : $V=\prod_{i\in I} V_i$, où V_i est un voisinage compact de 1 dans G_i pour tout i, et $V_i=H_i$ pour tout i sauf au plus un nombre fini. Un sous-ensemble de G est relativement compact (i.e. d'adhérence compacte) si et seulement s'il est contenu dans un tel parallélotope.

L'injection naturelle de G_i dans G est un isomorphisme topologique de G_i sur un sous-groupe fermé de G, et la projection de G sur G_i est un homomorphisme continu ouvert.

L'annulateur $H_i^\perp$ de H_i dans le dual $\hat{G}_i$ est un groupe compact, isomorphe au dual de G_i/H_i, et le quotient de $\hat{G}_i$ par $H_i^\perp$ est discret, isomorphe à $\hat{H}_i$. On peut donc former le produit restreint des groupes localement compacts $\hat{G}_i$ relativement aux $H_i^\perp$, et on trouve un groupe topologiquement isomorphe au dual $\hat{G}$ de G.

Soit k un corps de nombres. Pour chaque place v de k, soit k_v le complété de k. Si v est finie, on désigne par A_v l'anneau de valuation de k_v, par U_v le groupe des unités de A_v, et par $\mathfrak{M}_v$ l'idéal maximal de A_v.

Le produit direct restreint des groupes additifs k_v relatif aux ouverts compacts A_v est donc un groupe additif $\mathbb{A}_k$ localement compact. Les éléments de $\mathbb{A}_k$ s'appellent les *adèles* de k ; ils s'écrivent $\mathbf{x}=(x_v)$, où v décrit l'ensemble des places de k, $x_v \in k_v$ pour tout v, et $x_v \in A_v$ pour toute place finie v, sauf au plus un nombre fini d'entre elles : $\mathbb{A}_k$ est la réunion des

$$\Big(\prod_{v\in S} k_v\Big)\times\Big(\prod_{v\notin S} A_v\Big),$$

où S décrit les ensembles finis de places contenant les places archimédiennes. L'élément neutre est (0_v) où 0_v est l'élément neutre de k_v. Comme groupe topologique, $\mathbb{A}_k$ est isomorphe à $\mathbb{A}_{\mathbb{Q}}^n$, où $n=[k:\mathbb{Q}]$.

On munit $\mathbb{A}_k$ d'une structure d'anneau topologique localement compact en définissant le produit $(x_v).(y_v)=(x_v y_v)$; on vérifie en effet que cette multiplication est continue. L'élément neutre est (1_v).

Un système fondamental de voisinages de 0 dans $\mathbb{A}_k$ est donné par les ensembles

$$\{(x_v)\in\mathbb{A}_k \ ; \ |x_v|_v \leq c_v \ \text{ pour tout } \ v\}$$

avec $c_v \in \mathbb{R}$, $c_v>0$ pour tout v, et $c_v=1$ pour tout v sauf au plus un nombre fini.

Chaque k_v est isomorphe à un sous-anneau de $\mathbb{A}_k$, et $\mathbb{A}_k \simeq \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} k$ est aussi le produit direct restreint des $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{v|p} k_v$, (p premier ou $p=\infty$) relativement aux $\mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \prod_{v|p} A_v$, (p premier).

D'autre part k se plonge diagonalement dans $\mathbb{A}_k$ (ce plongement n'est pas celui obtenu en plongeant k dans k_v, puis k_v dans $\mathbb{A}_k$). On identifie k à un sous-anneau de $\mathbb{A}_k$ par le plongement diagonal ; k est discret dans $\mathbb{A}_k$, et $\mathbb{A}_k/k$ est compact. Le groupe topologique $\mathbb{A}_k$ est en dualité avec lui-même par l'application

$$(x,y) \longrightarrow \prod_{v \text{ finie}} e^{\circ}\varphi_p{}^{\circ}\mathrm{Tr}_{k_v/\mathbb{Q}_p}(x_v y_v) . \prod_{v \text{ infinie}} \exp(-2i\pi . \mathrm{Tr}_{k_v/\mathbb{R}}(x_v y_v)) .$$

Pour la topologie induite par $\mathbb{A}_k$, l'application $\mathbf{x} \longrightarrow \mathbf{x}^{-1}$, définie sur le groupe des éléments inversibles de $\mathbb{A}_k$, n'est pas continue : en effet, prenons $k=\mathbb{Q}$, désignons par p_n le n-ième nombre premier, et définissons la suite $\mathbf{x}^{(n)}$ d'éléments de $\mathbb{A}_k$ par

$$x_v^{(n)} = \begin{cases} 1 & \text{pour } p=\infty \text{ ou pour } v=v_p,\ p \neq p_n \ , \\ p & \text{pour } v=v_p,\ p=p_n \ ; \end{cases}$$

alors $\mathbf{x}^{(n)}$ est inversible dans $\mathbb{A}_k$, son inverse $\mathbf{y}^{(n)}=(y_v^{(n)})$ est

$$y_v^{(n)} = \begin{cases} 1 & \text{pour } p=\infty \text{ ou pour } v=v_p,\ p \neq p_n \ , \\ p^{-1} & \text{pour } v=v_p,\ p=p_n \ ; \end{cases}$$

la suite $(\mathbf{x}^{(n)})$ tend vers 1 dans $\mathbb{A}_k$, mais la suite $(\mathbf{y}^{(n)})$ ne tend pas vers 1 dans $\mathbb{A}_k$ (il n'y a pas d'ensemble fini S, indépendant de n, tel que $y_p^{(n)} \in \mathbb{Z}_p$ pour $p \notin S$).

On définit le *groupe des idèles* $\mathcal{J}_k$ comme le produit direct restreint des k_v^* relativement aux U_v. Un *idèle* de k est un élément inversible de l'anneau $\mathbb{A}_k$; un idèle s'écrit (x_v), où $x_v \in k_v^*$ pour tout v, et $x_v \in U_v$ pour tout v sauf peut-être un nombre fini. Autrement dit $\mathcal{J}_k$ est la réunion des

$$\mathcal{J}_k(S) = (\prod_{v \in S} k_v^*) \times (\prod_{v \notin S} U_v),$$

quand S décrit les ensembles finis de places contenant les places archimédiennes.

La topologie que nous avons définie sur $\mathfrak{I}_k$ est plus fine que celle induite par $\mathbb{A}_k$. Elle fait de $\mathfrak{I}_k$ un groupe topologique localement compact.

Une base de voisinages de 1 dans $\mathfrak{I}_k$ est donnée par $\prod_v U_v$, où U_v est un voisinage de 1 pour tout v, et $U_v=A_v^*$ pour tout v sauf un nombre fini. Autrement dit une base de voisinages de 1 est donnée par

$$\prod_{\substack{v \text{ finie} \\ v\notin T}} A_v^* \cdot \prod_{v\in T} (1+\mathfrak{M}_v^{a_v}) \cdot \prod_{v\in S_\infty} U_v,$$

où T est un ensemble fini de places ultramétriques de k, pour chaque $v\in T$, a_v est un entier ≥ 0, et pour $v\in S_\infty$, U_v est un voisinage de 1 dans k_v^* (avec $k_v^*=\mathbb{R}^*$ ou $\mathbb{C}^*$).

Chaque k_v^* se plonge dans $\mathfrak{I}_k$ comme sous-groupe fermé. D'autre part k^* se plonge diagonalement dans $\mathfrak{I}_k$, et l'image (que nous écrivons k^*) est un sous-groupe discret (donc fermé). Le quotient $\mathbf{C}_k=\mathfrak{I}_k/k^*$ est le *groupe des classes d'idèles*.

Le volume d'un idèle $\mathbf{x}=(x_v)$ est défini par $\|\mathbf{x}\|=\prod_v \|x_v\|_v$, où $\|.\|_v=|.|_v^{d_v}$ (de sorte que la formule du produit sur k^* s'écrive $\prod_v \|\alpha\|_v=1$). L'homomorphisme $\mathbf{x}\longrightarrow \log\|\mathbf{x}\|$ de $\mathfrak{I}_k$ dans $\mathbb{R}$ a pour noyau le groupe $\mathfrak{I}_k^0$ des idèles de volume 1 ; le quotient $\mathfrak{I}_k/\mathfrak{I}_k^0$ est isomorphe à $\mathbb{R}$. De plus $\mathfrak{I}_k^0$ contient k^*, et le quotient $\mathfrak{I}_k^0/k^*$ est compact.

Références : la thèse de Tate, §3 ; Iyanaga, Chap. III, §4 ; Weil, Chap.IV ; Lang, A.N.T, Chap VII ; Neukirch, Chap. IV, §2.

b) Quasi-caractères du groupe des idèles.

Soient k un corps de nombres, et $\chi : \mathfrak{I}_k \longrightarrow \mathbb{C}^*$ un homomorphisme continu. Pour chaque place v, la restriction χ_v de χ à k_v^* est un quasi-caractère de k_v^*.

Si v est une place archimédienne, on peut écrire

$$\chi_v(z)=(z/|z|)^{m_v}.|z|^{t_v} \qquad \text{pour tout } z\in k_v^*,$$

avec $m_v\in\mathbb{Z}$, $t_v\in\mathbb{C}$.

La partie à l'infini du groupe des idèles est $(k\otimes_{\mathbb{Q}}\mathbb{R})^*=\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$, et la restriction ψ de χ à ce sous-groupe est

$$\psi(z)=\prod_{v=1}^{n}(z_v/|z_v|)^{m_v}.|z_v|^{t_v}$$

pour $z=(z_1,\ldots,z_n)\in\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}$, avec comme précédemment $n=r_1+r_2$.

On dira que χ est de type (A) si les t_v sont tous rationnels, et qu'il est de type (A_0) si $t_v\in\mathbb{Z}$ pour $1\le v\le r_1$ et $t_v-m_v\in 2\mathbb{Z}$ pour $r_1<v\le n$. Autrement dit χ est de type (A) ou (A_0) s'il en est de même de chacun des χ_v pour v infinie.

Grâce au lemme 3.6, le théorème 2.1 et la proposition 2.2 permettent d'énoncer :

Corollaire 5.1.- *Soit $\mathcal{M}$ un idéal entier de* k. *Alors χ est de type* (A) *si et seulement si les nombres $\psi\circ\sigma(\alpha)$, $(\alpha\in k_+^*(\mathcal{M}))$ sont tous algébriques ; il est de type (A_0) si et seulement s'ils appartiennent tous à un même corps de nombres* E.

Si v est une place finie, correspondant à un idéal premier $\mathfrak{p}_v$ de k, on désigne par ℓ_v l'indice de ramification de χ_v, et par $\mathfrak{p}_v^{\ell_v}=\mathfrak{F}_v$ le conducteur en v.

Tout voisinage de 1 dans $\mathfrak{C}_k$ contient un sous-groupe compact de la forme

$$\Big(\prod_{v\in P}\{1\}\Big)\times\Big(\prod_{v\notin P}U_v\Big),$$

où P est un ensemble fini de places contenant les places archimédiennes. Comme χ est continu, il existe un tel voisinage dont l'image par χ est contenue dans un ouvert $\{z\in\mathbb{C}\ ;\ \mathrm{Re}z>\eta\}$, avec $0<\eta<1$. Mais $\{1\}$ est le seul sous-groupe de $\mathbb{C}^*$ qui soit contenu dans cet ouvert. Donc χ est trivial sur un tel voisinage, ce qui signifie que χ n'est ramifié qu'en un nombre fini

de places. L'idéal entier $\mathfrak{f}=\prod \mathfrak{f}_v$ (où le produit est étendu aux places finies ramifiées) est le *conducteur* de χ. Pour $\alpha\in k^*(\mathfrak{f})$, on a $\chi_v(\alpha)=1$ pour toute place v ramifiée. On appliquera le corollaire 5.1 à un idéal $\mathfrak{M}$ contenant le conducteur $\mathfrak{f}$.

Pour $\mathbf{x}=(x_v)\in\mathfrak{I}_k$, l'ensemble des v telles que $\chi_v(x_v)\neq 1$ est fini, et on a $\chi(\mathbf{x})=\prod_v \chi_v(x_v)$.

c) Quasi-caractères du groupe des classes d'idèles.

Soit $\chi:\mathbf{C}_k \longrightarrow \mathbb{C}^*$ un homomorphisme continu du groupe des classes d'idèles de k. En composant avec la surjection $\mathfrak{I}_k \longrightarrow \mathbf{C}_k$, on identifie χ avec un quasi-caractère de $\mathfrak{I}_k$, trivial sur k^*.

Montrons qu'il existe $s\in\mathbb{R}$ tel que $\mathrm{Re}(t_j)=\delta_j s$ pour $1\leq j\leq n$. Pour cela, choisissons une place infinie v_o, et notons ρ l'homomorphisme de $\mathfrak{I}_k$ sur $\mathfrak{I}_k^o$ qui envoie $\mathbf{x}=(x_v)$ sur $\mathbf{y}=(y_v)$, avec

$$y_v=\begin{cases} x_v & \text{pour } v\neq v_o \\ x_{v_o}/\|\mathbf{x}\|^{1/d_{v_o}} & \text{pour } v=v_o. \end{cases}$$

Le noyau de ρ est isomorphe à $\mathbb{R}$. La restriction de χ à $\mathfrak{I}_k^o/k^*$ est un caractère χ_o de ce groupe compact. On définit un caractère χ_1 de $\mathfrak{I}_k$ par $\chi_1(\mathbf{x})=\chi\circ\rho(\mathbf{x})$. Alors l'homomorphisme χ/χ_1 est trivial sur $\mathfrak{I}_k^o$, donc définit un homomorphisme continu de $\mathfrak{I}_k/\mathfrak{I}_k^o\simeq\mathbb{R}$ dans $\mathbb{C}^*$, et le corollaire 1.4 montre qu'il existe $s_1\in\mathbb{C}$ tel que

$$\chi(\mathbf{x})=\chi_1(\mathbf{x}).\|\mathbf{x}\|^{s_1}.$$

Soit ψ_1 la restriction de χ_1 à $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$. Les valeurs de ψ_1 étant dans $\mathbb{U}$, on peut écrire

$$\psi_1(z)=\prod_{j=1}^{n}(z_j/|z_j|)^{m_j}.|z_j|^{i\sigma_j},$$

avec $\sigma_j\in\mathbb{R}$, $(1\leq j\leq n)$. Or

$$\psi(z)=\psi_1(z).\prod_{j=1}^{n}|z_j|^{\delta_j s_1},$$

donc

$$\psi(z)=\prod_{j=1}^{n}(z_j/|z_j|)^{m_j}.|z_j|^{\delta_j s_1+i\sigma_j},$$

ce qui démontre ce que nous voulions avec $s=\mathrm{Re}(s_1)$.

Montrons que les caractères de Dirichlet sont des cas particuliers de caractères d'un groupe des classes d'idèles de type (A_0). Le groupe des idèles de $\mathbb{Q}$ admet une décomposition en produit direct $\mathfrak{I}_{\mathbb{Q}}=\mathbb{Q}^*\times\mathbb{R}_+^*\times\prod_p \mathbb{Z}_p^*$ avec la topologie discrète sur $\mathbb{Q}^*$: en effet, si, pour $x\in\mathfrak{I}_{\mathbb{Q}}$, on pose

$$r(x)=(\mathrm{sgn}(x_\infty)).\prod_p |x_p|_p^{-1}\in\mathbb{Q}^*,$$

alors on a $x/r(x)\in\mathbb{R}_+^*\times\prod_p \mathbb{Z}_p^*$. Comme $\prod_p \mathbb{Z}_p^*$ est un groupe topologique compact totalement discontinu, ses caractères sont tous d'ordre fini. Soit $m\geq 1$; on projette $\mathfrak{I}_{\mathbb{Q}}$ sur $\prod_p \mathbb{Z}_p^*$ (avec noyau $\mathbb{Q}^*\times\mathbb{R}_+^*$), puis chaque $\mathbb{Z}_p^*$ sur $(\mathbb{Z}/p^{v_p(m)}.\mathbb{Z})^*$ (homomorphisme canonique provenant de $\mathbb{Z}_p\longrightarrow\mathbb{Z}_p/p^{v_p(m)}.\mathbb{Z}_p$). On obtient ainsi un homomorphisme f de $\mathfrak{I}_{\mathbb{Q}}$ sur $(\mathbb{Z}/m\mathbb{Z})^*$; alors l'application $\psi\longrightarrow\psi\circ f$ établit une bijection entre le groupe des caractères de $(\mathbb{Z}/m\mathbb{Z})^*$ et le groupe des caractères continus de $\mathfrak{I}_{\mathbb{Q}}$ qui sont triviaux sur

$$\mathbb{Q}^*\times\mathbb{R}_+^*\times\prod_{(p,m)=1}\mathbb{Z}_p^*\times\prod_{p|m}(1+p^{v_p(m)}\mathbb{Z}_p).$$

Les quasi-caractères du groupe des classes d'idèles, notamment ceux de type (A_0), jouent un rôle important dans la théorie du corps de classes global (voir par exemple Lang, A.N.T., ou Cassels et Fröhlich, ou Weil, B.N.T., ou Neukirch, ou Iyanaga).

§6. Grössencharaktere et séries L.

a) Grössencharaktere.

Explicitons d'abord le fait que les idèles généralisent la notion d'idéal. Soit S un ensemble fini de places de k, contenant l'ensemble S_∞ des places archimédiennes. Notons I_k^S le groupe des idéaux fractionnaires non nuls de k premiers à S ; par exemple $I_k := I_k^{S_\infty}$ est le groupe des idéaux fractionnaires non nuls de k.

A chaque idèle $\mathbf{x}=(x_v)\in\mathfrak{I}_k$ on associe un idéal $(\mathbf{x})^S\in I_k^S$ défini par

$$(\mathbf{x})^S = \prod_{v\notin S} \mathfrak{p}_v^{v(x_v)}.$$

Par exemple pour $\alpha\in k^*$, l'idéal $(\alpha)^S$ est

$$(\alpha)^S = \prod_{v\notin S} \mathfrak{p}_v^{v(\alpha)} ;$$

en particulier, pour $S=S_\infty$, $(\alpha)^{S_\infty}$ est l'idéal principal (α).

Pour $\mathbf{x}\in\mathfrak{I}_k$, l'idéal $(\mathbf{x})^S$ ne dépend que de la projection $\mathbf{x}^S$ de $\mathbf{x}$ sur le sous-groupe

$$\mathfrak{I}_k^S = \{\mathbf{x}=(x_v)\in\mathfrak{I}_k \ ; \ x_v=1 \ \text{ pour tout } \ v\in S\}.$$

Cette projection $\mathbf{x}^S$ est évidemment définie par $x_v^S = x_v$ pour $v\notin S$, et $x_v^S = 1$ pour $v\in S$.

Alors l'application $\mathbf{x} \longrightarrow (\mathbf{x})^S$ de $\mathfrak{I}_k^S$ dans I_k^S est un homomorphisme surjectif dont le noyau

$$U^S = \{\mathbf{x}\in\mathfrak{I}_k^S \ ; \ x_v\in U_v \ \text{ pour toute place finie } \ v\}$$

est un voisinage compact de 1 dans $\mathfrak{I}_k^S$.

Un quasi-caractère du groupe des classes d'idèles peut s'interpréter comme un homomorphisme d'un groupe I_k^S dans $\mathbb{C}^*$ de la manière suivante.

Si χ est un quasi-caractère de $\mathfrak{I}_k$ non ramifié en dehors des places finies de S, alors χ est trivial sur U^S, donc définit (par restriction à $\mathfrak{I}_k^S$, puis passage au quotient par U^S) un homomorphisme $\tilde{\chi}$ de I_k^S dans $\mathbb{C}^*$.

Concrètement, pour $v\notin S$, si π_v est une uniformisante en v, on a

$$\tilde{\chi}(\mathfrak{p}_v)=\chi_v(\pi_v)$$

(rappelons que χ_v est la restriction de χ à k_v^*).

Nous allons voir quels sont les homomorphismes de I_k^S dans $\mathbb{C}^*$ qui sont de la forme $\tilde{\chi}$, pour χ quasi-caractère du groupe des classes d'idèles (c'est-à-dire trivial sur k^*). [Voir à ce sujet : A. Weil, Tokyo-Nikko, et Basic Number Theory, Chap. VII §8 ; Cassels et Fröhlich, p.168-170 et 204-209 ; J-P. Serre, McGill, Chap.II §2.1 ; P. Deligne, SGA.4½.]

Lemme 6.1.- *Soient* k *un corps de nombres de degré* d, S *un ensemble fini de places de* k *contenant les places archimédiennes, et* Φ *un homomorphisme de* I_k^S *dans* $\mathbb{C}^*$. *Les assertions suivantes sont équivalentes.*

(i) *Il existe un quasi-caractère* χ *du groupe des classes d'idèles de* k, *non ramifié en dehors de* S, *tel que* $\Phi=\tilde{\chi}$.

(ii) *Il existe un idéal entier* $\mathfrak{M}$ *de* k, *dont le support est la partie finie de* S, *il existe des entiers* $e_1,\dots,e_d$, *et des nombres complexes* $s_1,\dots,s_d$, *tels que, pour tout* $\alpha\in k^*(\mathfrak{M})$, *on ait*

$$\Phi((\alpha)) = \prod_{i=1}^{d} (\sigma_i\alpha)^{e_i}.|\sigma_i\alpha|^{s_i}.$$

(iii) *Pour tout* $\epsilon>0$, *il existe* $\eta>0$ *tel que, pour tout* $\alpha\in k^*$ *satisfaisant :* $|\alpha-1|_v<\eta$ *pour tout* $v\in S$, *on ait* $|\Phi((\alpha)^S)-1|<\epsilon$.

Démonstration.

(i)⇒(ii). Prenons

$$\mathfrak{M}= \prod_v \mathfrak{p}_v^{\max\{1,\ell_v\}},$$

où v décrit l'ensemble des places finies de S, et ℓ_v est le degré de ramification de χ en v. Pour $\alpha\in k^*(\mathfrak{M})$, on a $\alpha\in U_v$ pour tout $v\in S$, donc $(\alpha)^S=(\alpha)$. Soit ψ la restriction de χ à $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$; comme χ est trivial sur k^*, on a

$$1=\chi(\alpha)=\psi\circ\sigma(\alpha).\prod_v \chi_v(\alpha)$$

où le produit sur v est étendu aux places finies de k. Pour $v\in S$, on a

$\chi_v(\alpha)=1$, car $\alpha\in 1+\mathfrak{M}_v^{\ell_v}$, et χ_v est trivial sur $1+\mathfrak{M}_v^{\ell_v}$ par définition de ℓ_v. Pour $v\notin S$, on peut écrire $\alpha=\pi_v^{v(\alpha)}.u_v$, où π_v est une uniformisante en la place v, et $u_v\in U_v$. Alors

$$\chi_v(\alpha)=\chi(\pi_v)^{v(\alpha)}=\tilde{\chi}(\mathfrak{p}_v^{v(\alpha)}) \ ;$$

la définition de $\tilde{\chi}$ permet donc d'écrire :

$$\Phi((\alpha))=\Phi((\alpha)^S)=\tilde{\chi}((\alpha)^S)=\prod_{v\notin S}\chi_v(\alpha)=1/\psi\circ\sigma(\alpha),$$

ce qui démontre (ii).

(i)$\Rightarrow$(iii). Pour $\mathbf{x}\in\mathfrak{I}_k^S$, d'après (i) on a : $\Phi((\mathbf{x})^S)=\chi(\mathbf{x})$. Pour $\alpha\in k^*$, soit α^S sa projection sur $\mathfrak{I}_k^S$; dans le groupe des idèles α^S et α ont les mêmes composantes en toutes les places qui ne sont pas dans S, et on a $\chi(\alpha^S)=\Phi((\alpha)^S)$.

Par continuité de χ il existe un voisinage W de 1 dans $\mathfrak{I}_k$ tel que pour $\mathbf{x}\in W$, on ait $|\chi(\mathbf{x})-1|<\epsilon$. On peut choisir W de la forme $\prod_v W_v$, où W_v est un voisinage compact de 1 dans k_v pour tout v, et $W_v=A_v^*$ pour presque tout v. On choisit $\eta<1$ de sorte que, pour $v\in S$, la condition $|x_v-1|_v<\eta$ assure $x_v\in W_v$. Si, pour tout $v\in S$, on a $|\alpha-1|_v<\eta/2$, alors on a aussi $|\alpha^{-1}-1|_v<\eta$, et donc $\alpha^S/\alpha\in W$; d'où $|\chi(\alpha^S)-\chi(\alpha)|<\epsilon.|\chi(\alpha)|$; enfin $\chi(\alpha)=1$.

(ii)$\Rightarrow$(i). Ecrivons $\mathfrak{m}=\prod_{v\in S}\mathfrak{p}_v^{m_v}$. Soit $\mathbf{x}\in\mathfrak{I}_k$. Par le théorème d'approximation faible, il existe $\alpha\in k^*$ tel que $\mathbf{y}=\alpha\mathbf{x}$ vérifie $y_v\in 1+\mathfrak{p}_v^{m_v}$ pour tout $v\in S$ fini. Nous allons voir que le nombre complexe

$$\Phi((\mathbf{y})^S).\prod_{i=1}^{d} y_i^{-e_i}.|y_i|^{-s_i}$$

ne dépend pas du choix d'un tel α ; nous prendrons alors pour $\chi(\mathbf{x})$ cette valeur, et nous vérifierons que χ définit bien un quasi-caractère du groupe des classes d'idèles tel que $\tilde{\chi}=\Phi$.

Si $\beta\in k^*$ vérifie aussi $\beta x_v\in 1+\mathfrak{p}_v^{m_v}$ pour tout $v\in S$, alors $\alpha/\beta\in 1+\mathfrak{p}_v^{m_v}$ pour tout $v\in S$, c'est-à-dire $\alpha\equiv\beta \bmod^* \mathfrak{m}$. Dans ce cas, en posant $\mathbf{z}=\beta\mathbf{x}$, on a

$$\Phi((\mathbf{y})^S).\prod_{i=1}^{d} y_i^{-e_i}.|y_i|^{-s_i}/\Phi((\mathbf{z})^S).\prod_{i=1}^{d} z_i^{-e_i}.|z_i|^{-s_i}=$$

$$\Phi((\alpha/\beta)^S).\prod_{i=1}^{d}(\sigma_i(\beta/\alpha))^{e_i}.|\sigma_i(\beta/\alpha)|^{s_i}=1,$$

par l'hypothèse (ii).

L'application χ est donc bien définie, et elle vaut 1 sur k^* (pour $\mathbf{x}\in k^*$, prendre $\alpha=1/x$). Si $\mathbf{y}=\alpha\mathbf{x}$ et $\mathbf{y}'=\alpha'\mathbf{x}'$ vérifient $|y_v-1|_v<c_v$ et $|y'_v-1|_v<c_v$ pour tout $v\in S$ fini, alors $\mathbf{z}=\mathbf{y}\mathbf{y}'$ vérifie $|z_v-1|_v<c_v$, et il s'ensuit facilement que χ est un homomorphisme. De plus χ est continue : sur un voisinage de 1 dans $\mathfrak{I}_k$ formé des $\mathbf{z}$ tels que

$$|z_v-1|_v<\eta \qquad \text{pour } v \text{ archimédienne,}$$

$$z_v\in 1+\mathfrak{p}_v^{m_v} \qquad \text{pour } v \text{ finie } \in S,$$

$$z_v\in A_v^* \qquad \text{pour } v \text{ finie } \notin S,$$

on a $\Phi((\mathbf{z})^S)=1$, et $\chi(\mathbf{z})=\prod_{i=1}^{d} z_i^{-e_i}.|z_i|^{-s_i}$, donc $|\chi(\mathbf{z})-1|<\epsilon$.

Enfin, si $\mathbf{x}\in\mathfrak{I}_k^S$, on peut prendre $\alpha=1$; on a $y_i=1$ pour $1\leq i\leq d$, d'où $\Phi((\mathbf{x})^S)=\tilde{\chi}((\mathbf{x})^S)$.

(iii)⇒(i) Pour $\mathbf{x}\in\mathfrak{I}_k$, notons $\mathbf{x}'$ l'idèle $\mathbf{x}.(\mathbf{x}^S)^{-1}$:

$$x'_v=\begin{cases}1 & \text{pour } v\notin S\\ x_v & \text{pour } v\in S.\end{cases}$$

On veut trouver χ tel que, pour tout $\alpha\in k^*$, en posant $\mathbf{y}=\alpha\mathbf{x}$, on ait

$$\chi(\mathbf{x})=\chi(\mathbf{y})=\chi(\mathbf{y}').\chi(\mathbf{y}^S),$$

avec $\chi(\mathbf{y}^S)=\Phi((\mathbf{y})^S)$. Or $k^*.\mathfrak{I}_k^S$ est dense dans $\mathfrak{I}_k$ par le théorème d'approximation faible : il existe une suite d'éléments α_n de k^* qui convergent vers x_v^{-1} en toutes les places v de S ; on aura alors, pour $\mathbf{y}_n=\alpha_n\mathbf{x}$,

$$\mathbf{y}'_n\longrightarrow 1 \text{ dans } \mathfrak{I}_k, \text{ donc } \chi(\mathbf{y}'_n)\longrightarrow 1,$$

et

$$\Phi((\mathbf{y}_n)^S)\longrightarrow\chi(\mathbf{x}) \quad \text{pour } n\longrightarrow\infty.$$

On choisit donc une suite α_n comme ci-dessus, et on définit

$$\chi(\mathbf{x})=\lim_{n\longrightarrow\infty}\Phi((\alpha_n\mathbf{x})^S).$$

La limite existe car $\mathbb{C}^*$ est complet : l'hypothèse (iii) montre en effet que pour n et m tendant vers l'infini,

$$\frac{\Phi((\alpha_n \mathbf{x})^S)}{\Phi((\alpha_m \mathbf{x})^S)} = \Phi((\alpha_n/\alpha_m)^S)$$

tend vers 1 car α_n/α_m tend vers 1 en toutes les places de S.

Si (β_n) est une autre suite d'éléments de k^* telle que $\lim_{n \to \infty} |\beta_n - x_v^{-1}|_v = 0$ pour tout $v \in S$, alors

$$\frac{\Phi((\alpha_n \mathbf{x})^S)}{\Phi((\beta_n \mathbf{x})^S)} = \Phi((\alpha_n/\beta_n)^S)$$

tend vers 1 pour $n \to \infty$ car α_n/β_n tend vers 1 en toutes les places de S.

Il est clair que χ est un homomorphisme. Montrons qu'il est continu. Si $|x_v - 1|_v < \eta/2$ pour $v \in S$, alors $|\alpha_n - 1|_v < \eta$ pour $v \in S$ et n suffisamment grand, donc $|\Phi((\alpha_n)^S) - 1| < \epsilon$ d'après (iii). Si, de plus, $x_v \in U_v$ pour $v \notin S$, alors $(\alpha_n \mathbf{x})^S = (\alpha_n)^S$, et

$$\chi(\mathbf{x}) = \lim_{n \to \infty} \Phi((\alpha_n)^S).$$

Donc χ est continu. Enfin il est banal de vérifier que $\chi(k^*) = 1$ (pour $\mathbf{x} \in k^*$, prendre $\alpha_n = 1/\mathbf{x} \in k^*$), et que $\chi(\mathbf{x}) = \Phi((\mathbf{x})^S)$ pour $\mathbf{x} \in \mathfrak{S}_k^S$.

Définition. Un *Grössencharakter* est une application Φ de I_k^S dans $\mathbb{C}^*$ vérifiant les propriétés du lemme 6.1.

Deux Grössencharaktere sont dits *équivalents* si leurs valeurs coïncident en tous les idéaux pour lesquels ils sont tous deux définis ; les classes d'équivalence sont donc en bijection avec les quasi-caractères χ du groupe des classes d'idèles, et l'intersection des ensembles S pour tous les Grössencharaktere dans une classe est le support S du conducteur de χ ; le Grössencharakter $\tilde{\chi}$ est appelé Grössencharakter *primitif* de conducteur S.

Du corollaire 3.16, on déduit qu'un Grössencharakter dont les valeurs sont toutes des racines de l'unité est d'ordre fini. D'autre part du corollaire 5.1 nous allons déduire :

Corollaire 6.2.- *Soit* χ *un quasi-caractère du groupe des classes d'idèles* C_k, *et soit* S *un ensemble fini de places en dehors duquel* χ *n'est pas ramifié. Alors* χ *est de type* (A) *si et seulement si les nombres* $\tilde{\chi}(\mathfrak{A})$, $(\mathfrak{A}\in I_k^S)$, *sont tous algébriques. Il est de type* (A_0) *si et seulement s'il existe un corps de nombres* E *tel que* $\tilde{\chi}(\mathfrak{A})\in E$ *pour tout* $\mathfrak{A}\in I_k^S$.

Démonstration. Soit $\mathfrak{F}$ le conducteur de χ. Comme nous l'avons vu, pour $\alpha\in k^*(\mathfrak{F})$, on a

$$\tilde{\chi}((\alpha)).\psi\circ\sigma(\alpha)=1,$$

où ψ est la restriction de χ à $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$. Soit $\mathfrak{M}$ un idéal entier multiple de $\mathfrak{F}$, de support la partie finie de S. L'application de $k^*(\mathfrak{M})$ dans I_k^S qui envoie α sur l'idéal principal (α) a pour noyau le groupe $E(\mathfrak{M})$ des unités ϵ qui appartiennent à $1+\mathfrak{M}$, et $E(\mathfrak{M})$ est d'indice fini dans le groupe des unités de k (cf. fasc.4, p.9) ; l'image de $k^*(\mathfrak{M})$ dans I_k^S est d'indice fini (cf. par exemple S. Lang, A.N.T. Chap.6 §1), et on peut appliquer le corollaire 5.1.

Remarque. Si S est un ensemble fini de places de k, contenant les places archimédiennes, le sous-groupe

$$\mathfrak{I}_k(S)=\prod_{v\in S} k_v^* \cdot \prod_{v\notin S} U_v$$

de $\mathfrak{I}_k$ est appelé *groupe des S-idèles* de k. Le groupe k_S^* des S-unités de k n'est autre que $\mathfrak{I}_k(S)\cap k^*$. L'homomorphisme $\mathfrak{I}_k \longrightarrow I_k$ que nous avons considéré ci-dessus est surjectif, de noyau $\mathfrak{I}_k(S_\infty)=(k\otimes_{\mathbb{Q}}\mathbb{R})^*\times \prod_v U_v$, où S_∞ est l'ensemble des places archimédiennes de k, et le produit sur v est étendu aux places finies de k. Donc $\mathfrak{I}_k/\mathfrak{I}_k(S_\infty)$ est isomorphe au groupe I_k des idéaux fractionnaires de k, et $\mathfrak{I}_k/k^*.\mathfrak{I}_k(S_\infty)$ est isomorphe au groupe des classes d'idéaux de k (quotient de I_k par le sous-groupe des idéaux fractionnaires principaux).

On peut montrer aussi qu'il existe un ensemble fini S_o de places de k, contenant S_∞, tel que pour tout $S \supset S_o$, on ait $\mathfrak{I}_k = k^* . \mathfrak{I}_k(S)$ (on choisit un idéal $\mathfrak{a}_i$ de k dans chaque classe, et on prend pour S_o l'ensemble des places archimédiennes, et des places finies v pour lesquelles l'un des $v(\mathfrak{a}_i)$ est non nul).

(Voir à ce sujet l'article de Knapowski dans le Journal of Number Theory, **1** (1969), 235-251).

b) Série L attachée à un Grössencharakter.

Soit χ un quasi-caractère du groupe des classes d'idèles de k. On définit la série L attachée au Grössencharakter $\tilde{\chi}$ par

$$L(s,\tilde{\chi}) = \sum_{\mathfrak{A}} \tilde{\chi}(\mathfrak{A}) . N(\mathfrak{A})^{-s},$$

où $\mathfrak{A}$ décrit l'ensemble $G(\mathfrak{f})$ des idéaux entiers premiers à $\mathfrak{f}$ (noter que $G(\mathfrak{f})$ est l'ensemble des idéaux entiers dans I_k^S, quand S est l'ensemble des places de k où χ est ramifié). Si χ est le caractère trivial, $L(s,\tilde{\chi})$ est la fonction zêta de Dedekind du corps k. Si $k=\mathbb{Q}$ et si χ est un caractère de Dirichlet, $L(s,\tilde{\chi})$ est la fonction L de Dirichlet associée à ce caractère.

Cette série de Dirichlet converge pour $\mathrm{Re}(s)$ suffisamment grand, et admet un produit eulérien :

$$L(s,\tilde{\chi}) = \prod_{\mathfrak{p}} (1-\tilde{\chi}(\mathfrak{p}).(N(\mathfrak{p}))^{-s})^{-1}.$$

Nous allons nous intéresser aux coefficients a_n de la série L :

$$L(s,\tilde{\chi}) = \sum_{n\geq 1} a_n n^{-s} \quad \text{avec} \quad a_n = \sum_{N(\mathfrak{A})=n} \tilde{\chi}(\mathfrak{A}).$$

Lemme 6.3.- *Si* $a_n \in \overline{\mathbb{Q}}$ *pour tout* $n\in\mathbb{Z}$, $n\geq 1$, *alors* $\tilde{\chi}(\mathfrak{A}) \in \overline{\mathbb{Q}}$ *pour tout* $\mathfrak{A} \in G(\mathfrak{f})$.

Démonstration. Posons $\tilde{\chi}(\mathfrak{A})=0$ pour $\mathfrak{A}$ non premier à $\mathfrak{f}$. Pour chaque nombre premier $\mathfrak{p}$, on définit une fraction rationnelle

$$A_{\mathfrak{p}}(T) = \prod_{\mathfrak{p}|\mathfrak{p}} (1-\tilde{\chi}(\mathfrak{p}).T^{\deg \mathfrak{p}})^{-1}.$$

Montrons que son développement de Taylor à l'origine est

$$A_p(T) = \sum_{k\geq 0} a_{p^k} T^k.$$

En effet, on a, pour $\mathfrak{p}|p$,

$$(1-\tilde{\chi}(\mathfrak{p}).T^{\deg\mathfrak{p}})^{-1} = \sum_{n\geq 0} \tilde{\chi}(\mathfrak{p}^n).T^{n\deg(\mathfrak{p})}$$

et on fait le produit de ces relations pour $\mathfrak{p}|p$, en utilisant le fait que $\tilde{\chi}$ est multiplicatif : pour $\deg\mathfrak{p}_i=f_i$ on a $N\mathfrak{p}_i=p^{f_i}$ et

$$N(\mathfrak{p}_1^{a_1}\ldots\mathfrak{p}_g^{a_g})=p^{a_1f_1+\ldots+a_gf_g}$$

donc

$$\sum_{N(\mathfrak{A})=p^k} \tilde{\chi}(\mathfrak{A}) = \sum_{a_1f_1+\ldots+a_gf_g=k} \tilde{\chi}(\mathfrak{p}_1^{a_1}\ldots\mathfrak{p}_g^{a_g}).$$

Ainsi l'hypothèse entraîne que $A_p\in\overline{\mathbb{Q}}(T)$; alors ses pôles sont algébriques sur $\mathbb{Q}$, et la relation $\tilde{\chi}(\mathfrak{p})\in\overline{\mathbb{Q}}$ pour tout $\mathfrak{p}$ entraîne par multiplicativité $\tilde{\chi}(\mathfrak{A})\in\overline{\mathbb{Q}}$ pour tout idéal entier $\mathfrak{A}$.

Par conséquent *les trois assertions suivantes sont équivalentes :*

(i) *le quasi-caractère* χ *est de type* (A) ;

(ii) *les nombres* a_n, $(n\geq 1)$ *sont tous algébriques ;*

(iii) *les nombres* $\tilde{\chi}(\mathfrak{A})$, $(\mathfrak{A}\in G(\mathfrak{F}))$ *sont tous algébriques.*

De même, si le corps obtenu en adjoignant à $\mathbb{Q}$ les coefficients a_n, $(n\geq 0)$, est une extension finie E de $\mathbb{Q}$, alors $\tilde{\chi}(\mathfrak{A})\in E$ pour tout $\mathfrak{A}$ de la forme $\mathfrak{p}_1^{n_1}\ldots\mathfrak{p}_d^{n_d}$, où $\mathfrak{p}_1,\ldots,\mathfrak{p}_d$ sont les idéaux premiers de k au dessus d'un nombre premier p totalement décomposé dans k. En combinant le théorème 2.1 et le corollaire 3.11, on conclut que *les trois assertions suivantes sont équivalentes :*

(i) *le quasi-caractère* χ *est de type* (A_0) ;

(ii) *il existe un corps de nombres* E *tel que les nombres* a_n, $(n\geq 1)$ *appartiennent tous à* E ;

(iii) *il existe un corps de nombres* E *tel que* $\tilde{\chi}(\mathfrak{A})\in E$ *pour tout* $\mathfrak{A}\in G(\mathfrak{F})$.

c) Note historique et compléments.

L'existence d'un prolongement analytique et d'une équation fonctionnelle pour les fonctions zêta (de Dedekind) d'un corps de nombres est due à Hecke, qui étendit ensuite (vers 1920) ce résultat à des fonctions zêta et des séries L plus générales, associées aux Grössencharaktere qu'il définit à cette occasion.

Les idèles ont été introduits par Chevalley il y a cinquante ans comme une généralisation de la notion d'idéal, afin de donner un traitement algébrique de la théorie du corps de classes. Peu après, Weil introduisit les adèles pour donner une démonstration adélique du théorème de Riemann-Roch. Les "vecteurs valuations" d'Artin-Whaples (1945) correspondent aux adèles. La thèse de Tate utilise l'analyse de Fourier sur le groupe des idèles pour établir le prolongement analytique et l'équation fonctionnelle de fonctions zêta généralisant celles de Hecke.

A chaque courbe elliptique E (resp. chaque variété algébrique non singulière) définie sur un corps de nombres, on associe une fonction L (dite de Hasse-Weil), qui s'exprime comme un produit infini sur les nombres premiers p , où pour chaque p le facteur correspondant dépend du nombre de points de la réduction de la courbe (resp. de la variété) modulo p. Hasse (resp. Weil) avait conjecturé que cette fonction, définie pour Re(s) suffisamment grand, admettait un prolongement analytique. Dans le cas elliptique, cela a été démontré dans certains cas par Weil, puis, plus généralement par Deuring pour toutes les courbes admettant des multiplications complexes. La démonstration consiste à montrer que la fonction L de Hasse-Weil coïncide avec une fonction L de Hecke, attachée à un Grössencharakter. Ces fonctions L jouent un rôle fondamental dans l'étude de l'arithmétique des courbes elliptiques ; ce sont elles qui interviennent notamment dans la conjecture de Birch et Swinnerton-Dyer. (Voir pour un exemple : Ireland-Rosen, Chap.18 ;

pour le cas général : S. Lang, Elliptic Functions). La généralisation aux variétés abéliennes a été faite par Shimura et Taniyama (voir par exemple Lang, Complex multiplication ; G. Shimura, Arithmetic theory of automorphic functions).

Les quasi-caractères qui interviennent dans ces travaux sont tous de type (A_0) (on dit aussi que ce sont des quasi-caractères de Hecke *algébriques*). Si on veut obtenir tous les caractères de type (A_0), les variétés abéliennes ne suffisent pas, mais les motifs de Grothendieck suffisent. Les principaux travaux dans ce domaine sont dus à P. Deligne, G. Anderson, N. Schappacher (voir le texte de Schappacher, L.N. 1301).

Pour les sommes de Jacobi vues comme Grössencharaktere (sujet initié par Weil dans son étude de courbes algébriques sur $\mathbb{Q}$ dont le nombre de points modulo p peut être calculé par des sommes trigonométriques), voir, outre le Lecture Notes de Schappacher, le §1.4 de S.Lang : Cyclotomic fields.

Enfin, pour toutes les questions que nous avons plus spécialement traitées ici, voir A. Weil, Tokyo-Nikko, 1955.

Références du chapitre I.

J.W.S. CASSELS and A. FROHLICH.- Algebraic number theory ; Academic Press 1967.

S. IYANAGA.- The theory of numbers ; North Holland, 1975.

S. LANG.- Algebraic number theory ; Addison Wesley, 1970.

H.W. LENSTRA Jr.- On a question of Colliot-Thélène ; Séminaire de théorie des nombres, Paris 1980-81, (Séminaire Delange-Pisot-Poitou), Progress in Math., **22**, Birkhäuser Verlag 1982, 143-147.

J. NEUKIRCH.- Class field theory ; Grund. der Math. Wiss., **280**, Springer-Verlag 1986.

J.-J. SANSUC.- Descente et principe de Hasse pour certaines variétés rationnelles ; Séminaire de théorie des nombres, Paris 1980-81, (Séminaire Delange-Pisot-Poitou), Progress in Math., **22**, Birkhäuser Verlag 1982, 253-271.

M. WALDSCHMIDT.- Sur certains caractères du groupe des classes d'idèles d'un corps de nombres ; Séminaire de théorie des nombres, Paris 1980-81, (Séminaire Delange-Pisot-Poitou), Progress in Math., **22**, Birkhäuser Verlag 1982, 323-335.

A. WEIL.- On a certain type of characters of the idèle class group of an algebraic number field ; Proc. Intern. Symp. Alg. Geom., Tokyo-Nikko 1955, Tokyo 1956, 7p. ; Oeuvres Scientifiques (Springer Verlag, 1980), Vol.II, 255-261 (1955c).

A. WEIL.- Basic number theory ; Grund. der Math. Wiss., **144**, Springer-Verlag 1974.

Voir aussi :

H. COHN.- A classical invitation to algebraic numbers and class fields ; Springer Verlag, Universitext, 1978 (en particulier : §19.c : Hecke L functions).

K. IRELAND and M. ROSEN.- A classical introduction to modern number theory ; Graduate texts in Math., **84**, Springer Verlag 1982 (spécialement §18.5 : Hecke L-functions).

S. LANG.- Elliptic functions ; Addison Wesley, 1973 (notamment : Chap.8 §4 : summary of class field theory ; chap. 10 : complex multiplication).

S. LANG.- Cyclotomic fields ; Graduate texts in Math., **59**, Springer Verlag 1978 (entre autres §1.4 : Jacobi sums as Hecke characters).

S. LANG.- Complex multiplication ; Grund. der Math. Wiss., **255**, Springer-Verlag 1983 (voir §4.1 : the second main theorem of complex multiplication).

J. OESTERLE.- Corps de classes : théorie locale et globale ; Cours de troisième cycle, Univ. P. et M. Curie, 1985-86 (Notes par Alain Faisant et Georges Philibert).

N. SCHAPPACHER.-Periods of Hecke characters ; Lecture Notes in Math., **1301** (1988), Springer Verlag.

Y. TANIYAMA.- L-functions of number fields and zeta functions of abelian varieties ; J. Math. Soc. Japan, **9** (1957), 330-366.

CHAPITRE II

REPRESENTATIONS ℓ-ADIQUES.

§1. Caractères ℓ-adiques.

Dans tout ce chapitre, les lettres ℓ et p désignent des nombres premiers. Quand G est un groupe topologique, nous appellerons *caractère ℓ-adique* de G tout homomorphisme continu de G dans $\mathbb{C}_\ell^*$.

Nous étudions ici les caractères ℓ-adiques du groupe multiplicatif d'un corps local. Nous démontrons d'abord, dans les cas qui nous intéressent, l'énoncé suivant (Bourbaki, Groupes et Algèbres de Lie, Chap.III §8 N°2 Prop.1) : *soient G et G' deux groupes topologiques, et f:G $\longrightarrow$ G' un homomorphisme continu ; on suppose que l'on est dans l'un des trois cas suivants :*

a) G *est un groupe de Lie réel, et* G' *un groupe de Lie ℓ-adique*

b) G *est un groupe de Lie ℓ-adique, et* G' *un groupe de Lie réel*

c) G *est un groupe de Lie* p*-adique, et* G' *un groupe de Lie ℓ-adique, avec $\ell \neq p$.*

Alors f *est localement constant*

Par exemple, pour a), il nous suffit de savoir qu'un homomorphisme continu $\mathbb{C}^* \longrightarrow \mathbb{C}_\ell^*$ est constant, de même qu'un homomorphisme continu $\mathbb{R}_+^* \longrightarrow \mathbb{C}_\ell^*$; cela résulte du fait que l'image est un sous-groupe connexe de $\mathbb{C}_\ell^*$, donc égal à $\{1\}$ puisque $\mathbb{C}_\ell^*$ est un espace totalement discontinu. Ainsi un

homomorphisme continu $\mathbb{R}^* \longrightarrow \mathbb{C}_\ell^*$ est soit constant, soit de la forme $x \longrightarrow \mathrm{sgn}(x)$.

Pour b), nous avons déjà vu (au Chap.1, §4) ce dont nous avions besoin. Nous allons donc étudier les homomorphismes continus de K^* dans $\mathbb{C}_\ell^*$, quand K est une extension finie de $\mathbb{Q}_p$, d'abord quand $p \neq \ell$, puis quand $p=\ell$. Enfin nous étudierons les caractères ℓ-adiques du groupe des idèles d'un corps de nombres.

a) Préliminaires.

Nous allons démontrer quelques lemmes concernant la structure du groupe multiplicatif du corps $\mathbb{C}_\ell$, puis d'un corps local. Un rôle important sera joué par le logarithme ℓ-adique, qui fournit un isomorphisme local entre le groupe multiplicatif et le groupe additif d'un tel corps.

Pour $x \in \mathbb{C}_\ell^*$ vérifiant $|x-1|_\ell < 1$, on a défini (dans l'introduction) $\log_\ell x$. Soit de plus $t \in \mathbb{C}_\ell$ avec $|t.\log_\ell x|_\ell < \ell^{-1/(\ell-1)}$. On peut maintenant définir $\exp(t.\log_\ell x)$. Ces hypothèses ne suffisent pas à assurer que, si $t \in \mathbb{Z}$, alors $\exp(t.\log_\ell x) = x^t$; par exemple pour $t=1$ et $x \neq 1$ racine ℓ-ième de l'unité, on a $|x-1|_\ell < 1$ (puisque $x-1$ est une racine non nulle du polynôme $(X+1)^\ell - 1$ dont tous les coefficients sauf un sont des entiers divisibles par ℓ), et $\log_\ell x = 0$, donc $\exp(\log_\ell x) \neq x$.

Supposons maintenant $|x-1|_\ell < \ell^{-1/(\ell-1)}$, c'est-à-dire $x-1 \in D$, où D est le domaine de convergence de la série exponentielle. Rappelons (Introduction, §4) que exp et $\log_\ell$ définissent des isomorphismes réciproques entre le groupe additif D et le groupe multiplicatif $1+D$. Alors, si $t \in \mathbb{Z}$, on a d'abord $x^t \in 1+D$, ensuite $t.\log_\ell x = \log_\ell(x^t)$, car $\log_\ell$ est un homomorphisme de groupes, et enfin, $\exp(\log_\ell(x^t)) = x^t$.

Nous poserons donc

$$x^t = \exp(t.\log_\ell x)$$

pour $x \in \mathbb{C}_\ell^*$ et $t \in \mathbb{C}_\ell$ vérifiant $|x-1|_\ell < \ell^{-1/(\ell-1)}$ et $|t.\log_\ell x|_\ell < \ell^{-1/(\ell-1)}$. Pour chaque $t \in \mathbb{C}_\ell$, il existe un voisinage U de 1 dans $\mathbb{C}_\ell^*$ tel que x^t

soit défini pour tout $x\in U$; en effet, $\log_\ell x$ tend vers 0 quand x tend vers 1. Voir à ce sujet par exemple : N. Koblitz, p-adic numbers, p-adic analysis and zeta functions, Ch.IV §1.

Lemme 1.1.- *Soit* η *un nombre réel,* $0<\eta<1$. *Il existe une constante* $C=C(\eta)>0$ *telle que pour tout* $a\in\mathbb{Z}$ *et tout* $z\in\mathbb{C}_\ell$ *vérifiant* $|z|_\ell\leq\eta$, *on ait*

$$|(1+z)^a-1|_\ell\leq C.\,|az|_\ell.$$

Démonstration.- Comme $|1+z|_\ell=1$, quitte à remplacer a par -a et z par $-z/(1+z)$, on peut supposer $a>0$. On écrit

$$(1+z)^a-1 = az\Big(1+\sum_{i=2}^{a}\binom{a-1}{i-1}.\frac{z^{i-1}}{i}\Big),$$

et on choisit $C=\max_{i\geq 2}\{|i|_\ell^{-1}.\eta^{i-1}\}$; ainsi $C\leq\max_{i\geq 2}\{i\eta^{i-1}\}$ est finie, et $|z|_\ell^{i-1}\leq C|i|_\ell$ pour $|z|_\ell\leq\eta$ et pour tout $i\geq 2$. L'inégalité annoncée en résulte.

On peut étendre le lemme 1.1 aux éléments a de $\mathbb{Z}_\ell$ grâce au fait que $\mathbb{Z}$ est dense dans $\mathbb{Z}_\ell$.

Dans l'étude complexe faite au chapitre 1, nous avons utilisé le fait que $\mathbb{C}^*$ ne possédait pas de sous-groupe non trivial dans un voisinage ouvert du point 1 (par exemple $\mathrm{Re}(z)>\eta$ pour $0<\eta<1$). Le groupe multiplicatif d'un corps ℓ-adique, qui est totalement discontinu, possède une base de voisinages de l'élément neutre formée de sous-groupes. Néanmoins le résultat complexe admet un analogue ℓ-adique si on se restreint aux sous-groupes *finis*.

Lemme 1.2.- *Il existe un voisinage ouvert* V *de* 1 *dans* $\mathbb{C}_\ell$ *tel que le seul sous-groupe fini de* $\mathbb{C}_\ell^*$ *contenu dans* V *soit* $\{1\}$.

Démonstration. Remarquons d'abord que toute racine ζ de l'unité dans $\mathbb{C}_\ell$, différente de 1, d'ordre m premier à ℓ, vérifie $|\zeta-1|_\ell=1$. En effet, si on avait $|\zeta-1|_\ell<1$, en écrivant la relation de Bézout $am+b\ell=1$, on aurait

$$\zeta=\zeta^{b\ell}=\ldots=\zeta^{b^n\ell^n}$$

pour tout $n\geq 1$; or le lemme 1.1 montre que si $|\zeta-1|_\ell<1$, alors $\zeta^{b^n\ell^n}$ tend vers 1 quand n tend vers l'infini.

Soit ζ_ℓ une racine primitive ℓ-ième de l'unité ; on choisit

$$V=\{z\in\mathbb{C}_\ell \ ; \ |z-1|_\ell<|\zeta_\ell-1|_\ell\}.$$

Si ℓ divise l'ordre de ζ, en divisant $\zeta_\ell-1$ par $\zeta-1$ on obtient $|\zeta-1|_\ell\geq|\zeta_\ell-1|_\ell$, et par suite $\zeta\notin V$. D'où le lemme 1.2.

Le groupe $\mathbb{C}_\ell^*$ se décompose en produit direct $\mathbb{Q}\times W\times U_1$, où la projection sur la première composante est donnée par la valuation, où W est le groupe des racines de l'unité d'ordre premier à ℓ, et $U_1=\{z\in\mathbb{C}_\ell \ ; \ |z-1|_\ell<1\}$ est le domaine de convergence de $\log_\ell$ (voir par exemple L. Washington, Introduction to cyclotomic fields, §5.1 ; cela sert à montrer l'unicité de l'extension de la fonction $\log_\ell$ en un homomorphisme de $\mathbb{C}_\ell^*$ dans $\mathbb{C}_\ell$ nul au point ℓ).

Soit maintenant K une extension finie de $\mathbb{Q}_\ell$, de degré d. On note A l'anneau de valuation de K, A^* le groupe des unités, $\mathcal{M}$ l'idéal de valuation, e l'indice de ramification, et f le degré résiduel.

Lemme 1.3.- *Il existe un entier $v_0>0$ tel que pour tout $v\geq v_0$ et tout entier n premier à ℓ, l'application $x\longrightarrow x^n$ soit un automorphisme du groupe $1+\mathcal{M}^v$.*

Démonstration.- Prenons $v_0>e/(\ell-1)$, de sorte que, pour $x\in 1+\mathcal{M}^v$ avec $v\geq v_0$, on ait $|x-1|_\ell<\ell^{-1/(\ell-1)}$. Alors comme $1/n\in\mathbb{Z}_\ell$ on peut définir $x^{1/n}=\exp(\frac{1}{n}.\log_\ell x)$, on a $x^{1/n}\in 1+\mathcal{M}^v$, et $(x^{1/n})^n=x$.

Remarque. On peut montrer que dans l'énoncé du lemme 1.3, on peut remplacer v_0 par 1. Pour cela on montre que l'homomorphisme $n\longrightarrow x^n$ de $\mathbb{Z}$ dans $1+\mathcal{M}$ se prolonge en un homomorphisme continu de $\mathbb{Z}_\ell$ dans $1+\mathcal{M}$, puis que l'application $(n,x)\longrightarrow x^n$ de $\mathbb{Z}_\ell\times(1+\mathcal{M})$ dans $1+\mathcal{M}$ est continue, ce qui donne une structure de $\mathbb{Z}_\ell$-module à $1+\mathcal{M}$; alors pour $n\in\mathbb{Z}_\ell^*$, l'application

$x \longrightarrow x^n$ est un automorphisme de $1+\mathcal{M}$.

Pour avoir plus d'informations sur la structure de $1+\mathcal{M}$, consulter par exemple : A. Weil, B.N.T., Chap.II §3.

b) Caractéristiques résiduelles différentes.

Soient ℓ et p deux nombres premiers différents. On désigne par K une extension finie de $\mathbb{Q}_p$ de degré d ; comme précédemment A, $\mathcal{M}$ désignent l'anneau et l'idéal de valuation de K.

Lemme 1.4.- *Soit* $f:K^* \longrightarrow \mathbb{C}_\ell^*$ *un homomorphisme continu. Alors* f *est localement constant.*

Démonstration.- Soit $\eta<1$. Comme f est continu, il existe un voisinage U de 1 dans K^* tel que $|f(x)-1|_\ell \leq \eta$ pour tout $x\in U$. Soit s un entier positif suffisamment grand $(s\geq v_0)$ tel que $1+\mathcal{M}^s \subset U$, et soit $x_0 \in 1+\mathcal{M}^s$. D'après le lemme 1.3, pour tout entier $h\geq 0$ l'application $x \longrightarrow x^{\ell^h}$ est un automorphisme de $1+\mathcal{M}^s$; donc il existe $x_h \in 1+\mathcal{M}^s$ tel que $x_0=x_h^{\ell^h}$. Alors

$$f(x_0)=f(x_h^{\ell^h})=f(x_h)^{\ell^h};$$

mais le lemme 1.1 montre que

$$|f(x_h)^{\ell^h}-1|_\ell \leq C\eta\ell^{-h},$$

donc $f(x_h)^{\ell^h}$ tend vers 1 quand h tend vers l'infini. D'où $f(x_0)=1$ pour $x_0 \in 1+\mathcal{M}^s$.

Corollaire 1.5.- *Sous les hypothèses du lemme* 1.4, $f(A^*)$ *est un sous-groupe fini de* $\mathbb{C}_\ell^*$.

Démonstration. Soit $s\geq 1$ tel que $f(1+\mathcal{M}^s)=1$; alors f définit un caractère du groupe fini $A^*/(1+\mathcal{M}^s)$, donc la restriction de f à A^* est un caractère d'ordre fini de A^*.

Sous les hypothèses du lemme 1.4, on notera $\mathfrak{f}$ le plus petit entier tel que $f(1+\mathfrak{M}^{\mathfrak{f}})=1$, et on dira que $\mathfrak{f}$ est le *degré de ramification* de f. L'idéal $\mathfrak{M}^{\mathfrak{f}}$ est le *conducteur* du caractère f. On dit que f est *non ramifié* si $\mathfrak{f}=0$, c'est-à-dire si $f(A^*)=1$.

c) Mêmes caractéristiques résiduelles.

Commençons par regarder les homomorphismes continus de $\mathbb{Z}_\ell$ dans $\mathbb{C}_\ell$ ou dans $\mathbb{C}_\ell^*$.

Tout homomorphisme continu de $\mathbb{Z}_\ell$ dans $\mathbb{C}_\ell$ est une homothétie. En effet, si f est un tel homomorphisme, en posant $\lambda=f(1)$, on a

$$f(\sum_{i=0}^{n} a_i \ell^i)=(\sum_{i=0}^{n} a_i \ell^i).f(1),$$

donc $f(x)=\lambda x$ pour tout $x\in\mathbb{Z}$, et par continuité $f(x)=\lambda x$ pour tout $x\in\mathbb{Z}_p$.

Soit maintenant f un homomorphisme continu de $\mathbb{Z}_\ell$ dans $\mathbb{C}_\ell^*$. Montrons qu'il existe $t\in\mathbb{C}_\ell$ et $m\in\mathbb{Z}$, $m\geq 0$, tels que

$$f(x)=\exp(tx) \qquad \text{pour tout } x\in\ell^m\mathbb{Z}_\ell.$$

Pour cela choisissons m tel que l'image de $\ell^m\mathbb{Z}_\ell$ soit contenue dans $1+D$ (où D est le domaine de convergence de la série exponentielle ℓ-adique). Alors l'application $y \longrightarrow \log(f(\ell^m y))$ de $\mathbb{Z}_\ell$ dans $\mathbb{C}_\ell$ est un homomorphisme continu, donc de la forme $y \longrightarrow \lambda y$, avec $\lambda\in\mathbb{C}_\ell$. Mais pour $z\in 1+D$ on a $\exp\circ\log(z)=z$, donc $f(\ell^m y)=\exp(\lambda y)$ pour tout $y\in\mathbb{Z}_\ell$. On prend alors $t=\lambda\ell^{-m}$.

Dans Les nombres p-adiques (Exercices 3, 5 et 6 p.104-105), Y. Amice esquisse l'étude du dual p-adique de $\mathbb{Z}_p$ ainsi que de celui de $\mathbb{Q}_p$.

Nous désignons maintenant par K une extension finie de $\mathbb{Q}_\ell$. Regardons déjà quels sont les homomorphismes de K dans $\mathbb{C}_\ell$.

Lemme 1.6.- *Les homomorphismes continus de* K *dans* $\mathbb{C}_\ell$ *sont les applications* $\mathbb{Q}_\ell$*-linéaires de* K *dans* $\mathbb{C}_\ell$. *Ils forment donc un* $\mathbb{C}_\ell$*-espace vectoriel de dimension* $d=[K:\mathbb{Q}_\ell]$. *De plus, si* V *est un sous-groupe ouvert de* K *et* f *un homomorphisme continu de* V *dans* $\mathbb{C}_\ell$, *alors* f *se prolonge de manière unique en un homomorphisme continu de* K *dans* $\mathbb{C}_\ell$.

Démonstration.- Toute application $\mathbb{Q}_\ell$-linéaire de K dans $\mathbb{C}_\ell$ est continue. La réciproque va découler de la deuxième partie du lemme (avec $V=K$) que nous établissons maintenant.

Soit $\alpha_1,\ldots,\alpha_d$ une base de K sur $\mathbb{Q}_\ell$. Pour $1\leq j\leq d$, soit f_j la restriction de f au sous-groupe $V\cap(\mathbb{Q}_\ell.\alpha_j)$ de K. D'après ce qui précède il existe un voisinage U_j de 0 dans $\mathbb{Q}_\ell$ tel que la restriction de f_j à $U_j\alpha_j$ soit de la forme $z\alpha_j \longrightarrow \lambda_j z$. Alors pour $z=z_1\alpha_1+\ldots+z_d\alpha_d$ dans un voisinage de 0 dans V, on a

$$f(z)=\sum_{j=1}^{d} f_j(z_j\alpha_j)=\sum_{j=1}^{d}\lambda_j z_j=F(z),$$

où F désigne l'application $\mathbb{Q}_\ell$-linéaire de K dans $\mathbb{C}_\ell$ qui envoie α_j sur λ_j pour $1\leq j\leq d$. Or pour tout $z\in V$, il existe un entier $n\geq 0$ tel que $\ell^n z$ appartienne à ce voisinage de 0. On en déduit $\ell^n f(z)=f(\ell^n z)=F(\ell^n z)=\ell^n F(z)$, donc $f(z)=F(z)$. Ainsi f est la restriction de F à V. Il est clair que F est la seule application $\mathbb{Q}_\ell$-linéaire de K dans $\mathbb{C}_\ell$ à posséder cette propriété.

Ainsi les d homomorphismes $z=z_1\alpha_1+\ldots+z_d\alpha_d \longrightarrow z_j$, $(1\leq j\leq d)$ forment une base du $\mathbb{C}_\ell$-espace vectoriel des homomorphismes continus de K dans $\mathbb{C}_\ell$, et on a des isomorphismes

$$\mathrm{Hom}_{\mathrm{cont}}(K,\mathbb{C}_\ell) \simeq \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_\ell^d,\mathbb{C}_\ell) \simeq (\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_\ell,\mathbb{C}_\ell))^d \simeq \mathbb{C}_\ell^d.$$

On appellera *plongement* de K dans $\mathbb{C}_\ell$ tout isomorphisme $\mathbb{Q}_\ell$-linéaire de K dans $\mathbb{C}_\ell$.

Comme l'extension $K/\mathbb{Q}_\ell$ est séparable et que $\mathbb{C}_\ell$ est algébriquement clos, il existe d plongements σ_i, $(1\leq i\leq d)$ de K dans $\mathbb{C}_\ell$. L'unicité de l'extension de la valeur absolue de $\mathbb{Q}_\ell$ à K (car $\mathbb{Q}_\ell$ est complet) montre que $|\sigma_i\alpha|_\ell=|\alpha|_\ell$ pour $1\leq i\leq d$ et $\alpha\in K$; en particulier les σ_i sont continus. Enfin le lemme d'Artin sur l'indépendance linéaire des caractères (cf. par exemple S. Lang, Algebra, 2ème éd., chap.VIII §4) assure que $\sigma_1,\ldots,\sigma_d$ sont linéairement indépendants sur $\mathbb{C}_\ell$.

Corollaire 1.7.- *Tout homomorphisme continu* f *de* K *dans* $\mathbb{C}_\ell$ *s'écrit de manière unique*

$$z \longrightarrow \sum_{i=1}^{d} t_i\sigma_i(z),$$

avec $(t_1,\ldots,t_d)\in\mathbb{C}_\ell$.

Passons maintenant aux caractères ℓ-adiques. D'abord le cas additif.

Corollaire 1.8.- *Soient* U_o *un sous-groupe ouvert de* K *et* $f:U_o\longrightarrow\mathbb{C}_\ell^*$ *un homomorphisme continu. Il existe* $t_1,\ldots,t_d$ *dans* $\mathbb{C}_\ell$, *et il existe un voisinage* U *de* 0 *contenu dans* U_o, *tels que pour* $z\in U$ *on ait*

$$f(z)=\exp\left(\sum_{i=1}^{d} t_i\sigma_i z\right).$$

Démonstration.- Soit $U\subset U_o$ un sous-groupe ouvert de K tel que $f(z)\in 1+D$ pour tout $z\in U$. Alors $\log\circ f$ est un homomorphisme continu de U dans $\mathbb{C}_\ell$, donc de la forme $z\longrightarrow\sum_{i=1}^{d} t_i\sigma_i z$, d'après les lemmes 1.6 et 1.7.

Voici enfin le cas multiplicatif.

Lemme 1.9.- *Soient* V_0 *un sous-groupe ouvert de* K^* *et* $f:V_0 \longrightarrow \mathbb{C}_\ell^*$ *un homomorphisme continu. Il existe un unique* d-*uplet* $(t_1,\dots,t_d)\in\mathbb{C}_\ell^d$, *et il existe un voisinage* V *de* 1 *contenu dans* V_0, *tels que pour* $z\in V$ *on ait*

$$f(z)=\prod_{i=1}^{d}(\sigma_i z)^{t_i}.$$

Démonstration.- Notons D_1 le domaine de convergence de la série exponentielle dans K (pour tout plongement de K dans $\mathbb{C}_\ell$, D_1 est l'intersection de D avec K). L'application $f\circ\exp$ est un homomorphisme continu de $U_0=D_1\cap\exp^{-1}V_0$ dans $\mathbb{C}_\ell^*$. Le corollaire 1.8 montre que l'on peut écrire

$$f\circ\exp(u)=\exp\left(\sum_{i=1}^{d}t_i\sigma_i u\right)$$

pour u dans un certain voisinage U de 0 contenu dans U_0. Soit $V=\exp(U)$. Pour $z\in V$ on pose $u=\log_\ell z$ et on a $\sigma_i u=\log_\ell\sigma_i z$ grâce à la continuité des σ_i ; d'où

$$f(z)=\exp\left(\sum_{i=1}^{d}t_i\log_\ell\sigma_i z\right)$$

pour tout $z\in V$, ce qui donne le résultat annoncé.

d) Caractères du groupe des idèles.

Soient k un corps de nombres, $\mathfrak{I}_k$ le groupe des idèles de k, et χ un homomorphisme continu de $\mathfrak{I}_k$ dans $\mathbb{C}_\ell^*$. Pour chaque place v de k, désignons par χ_v la restriction de χ à k_v^*. D'après le lemme 1.4 ci-dessus, pour chaque place finie v ne divisant pas ℓ, χ_v est localement constant sur k_v^*. Nous avons vu qu'il en est de même pour v archimédienne.

Pour chaque place finie v de k, nous désignons par A_v^* le groupe des unités v-adiques.

Lemme 1.10.- *L'ensemble des places finies* v *de* k *telles que* $\chi_v(A_v^*)\neq 1$ *est fini.*

Démonstration.- Choisissons, en utilisant le lemme 1.2, un voisinage V de 1 dans $\mathbb{C}_\ell^*$ qui ne contienne pas de sous-groupe fini non trivial de $\mathbb{C}_\ell^*$. Par continuité de χ, il existe un voisinage ouvert W de 1 dans $\mathfrak{I}_k$ tel que $\chi(W)\subset V$. D'après la topologie de $\mathfrak{I}_k$, l'ensemble des v tels que W ne contienne pas A_v^* est fini. D'autre part, si W contient A_v^* pour v finie ne divisant pas ℓ, le corollaire 1.5 nous dit que $\chi_v(A_v^*)$ est un sous-groupe fini de $\mathbb{C}_\ell^*$. On a $\chi_v(A_v^*)\subset V$, ce qui permet de conclure $\chi_v(A_v^*)=1$.

On dira que χ est *ramifié* en une place finie v ne divisant pas ℓ si $\chi_v(A_v^*)\neq 1$. Pour chaque place finie v de k ne divisant pas ℓ, soit f_v le conducteur de χ_v, c'est-à-dire le plus petit entier tel que $\chi_v(1+\mathcal{M}_v^{f_v})=1$. L'idéal $\prod_v \mathfrak{p}_v^{f_v} = \mathfrak{F}$ est le *conducteur* de χ (le produit sur v est étendu aux places finies de k ne divisant pas ℓ, et $\mathfrak{p}_v$ est l'idéal premier de k correspondant à la place v ; si χ n'est pas ramifié en v, alors on a $f_v=0$, $1+\mathcal{M}_v^{f_v}=A_v^*$, et $\mathfrak{p}_v^{f_v}=\mathcal{O}_k$).

Pour nous, la partie la plus intéressante de χ est sa restriction à la ℓ-partie de $\mathfrak{I}_k$, c'est-à-dire à $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^* = \prod_{\lambda|\ell} k_\lambda^*$. Chaque k_λ, $(\lambda|\ell)$, est une extension finie de $\mathbb{Q}_\ell$, et si $d_\lambda=[k_\lambda:\mathbb{Q}_\ell]$ désigne son degré, on a $\sum_{\lambda|\ell} d_\lambda=[k:\mathbb{Q}]$. Désignons par $\sigma_1,\dots,\sigma_d$ les différents plongements de k dans $\mathbb{C}_\ell$, avec $d=[k:\mathbb{Q}]$.

Lemme 1.11.- *Soit χ_ℓ la restriction de χ à $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^* = \prod_{\lambda|\ell} k_\lambda^*$. Il existe un unique d-uplet $(t_1,\dots,t_d)\in\mathbb{C}_\ell^d$, et il existe un voisinage V de 1 dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^*$, tels que pour $\alpha\in k$ vérifiant $\sigma(\alpha)\in V$ on ait*

$$\chi_\ell\circ\sigma(\alpha)=\prod_{i=1}^{d}(\sigma_i\alpha)^{t_i}.$$

Démonstration.- Rappelons d'abord (cf. S. Lang, A.N.T., Chap.II §1 Th.2) que deux plongements σ et τ de k dans $\mathbb{C}_\ell$ donnent la même valeur absolue sur k si et seulement s'ils sont conjugués sur $\mathbb{Q}_\ell$, c'est-à-dire si et seulement s'il existe un $\mathbb{Q}_\ell$-automorphisme υ de $\mathbb{C}_\ell$ tel que $\tau=\upsilon\circ\sigma$.

Pour chaque place λ de k au dessus de ℓ, désignons par $\sigma_{\lambda j}$, $(1\leq j\leq d_\lambda)$ les plongements de k_λ dans $\mathbb{C}_\ell$, et par i_λ l'injection de k dans k_λ. Alors, pour $\lambda|\ell$ et $1\leq j\leq d_\lambda$, $\sigma_{\lambda j}\circ i_\lambda$ est un plongement de k dans $\mathbb{C}_\ell$. Montrons que ces plongements sont deux-à-deux distincts. En effet, les $\sigma_{\lambda j}\circ i_\lambda$ sont des isométries de k_λ dans $\mathbb{C}_\ell$, donc la valeur absolue sur k déterminée par $|\alpha|=|\sigma_{\lambda j}\circ i_\lambda|_\ell$ est $|.|_\lambda$. Par conséquent une égalité $\sigma_{\lambda_1 j_1}\circ i_{\lambda_1}=\sigma_{\lambda_2 j_2}\circ i_{\lambda_2}$ implique $\lambda_1=\lambda_2$. Ensuite, comme k est dense dans k_λ, une égalité $\sigma_{\lambda j_1}\circ i_\lambda=\sigma_{\lambda j_2}\circ i_\lambda$ implique $j_1=j_2$.

Comme $d=\sum_{\lambda|\ell} d_\lambda$, on en déduit

$$\{\sigma_{\lambda j}\circ i_\lambda \ ; \ 1\leq j\leq d_\lambda,\ \lambda|\ell\} = \{\sigma_1,\ldots,\sigma_d\}.$$

Pour conclure, il suffit d'utiliser le lemme 1.9, avec le fait que χ_ℓ est le produit des χ_λ pour $\lambda|\ell$. D'où le lemme 1.11.

§2. Caractères ℓ-adiques de type (A) ou (A_0).

Le but principal de ce paragraphe est d'établir les analogues ℓ-adiques d'abord des théorèmes 2.1 et 2.2 du chapitre 1, puis des résultats du §3 a,b,c du chapitre 1.

a) Définitions.

Soient k un corps de nombres, ℓ un nombre premier, et χ un homomorphisme continu de $\mathfrak{S}_k$ dans $\mathbb{C}_\ell^*$. Nous avons vu au lemme 1.11 que la restriction χ_ℓ de χ à la ℓ-partie de $\mathfrak{S}_k$ était localement (au voisinage de 1) de la forme $z=(z_\lambda) \longrightarrow \prod_{\lambda|\ell} \prod_{1\leq i\leq d_\lambda} (\sigma_{\lambda i} z_\lambda)^{t_{\lambda i}}$, où $\sigma_{\lambda i}$ désignent les plongements de k_λ dans $\mathbb{C}_\ell$. Nous dirons que χ est *de type* (A) (resp. (A_0)) si les nombres complexes $t_{\lambda i}$ sont tous rationnels (resp. entiers rationnels). Les caractères de type (A_0) sont encore appelés caractères *algébriques*.

b) Théorèmes de transcendance.

Notons $\sigma=(\sigma_1,\ldots,\sigma_d)$ l'application de k dans $\mathfrak{S}_k$, composée du plongement canonique σ_ℓ de k dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$, et de l'injection de $k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ dans $\mathfrak{S}_k$; l'image de σ a pour adhérence $k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$. Soit χ un caractère ℓ-adique de $\mathfrak{S}_k$. On voudrait pouvoir déterminer, à partir de la nature arithmétique de l'image de $\chi\circ\sigma$, si χ est de type (A) (resp. (A_0)). Montrons d'abord, sur un exemple, qu'une telle caractérisation ne peut être que locale.

Prenons $k=\mathbb{Q}$, choisissons s nombres premiers distincts $\ell_1,\ldots,\ell_s$ (l'un d'eux peut être ℓ), ainsi que des éléments $\theta_1,\ldots,\theta_s$ de $\mathbb{C}_\ell^*$. Prenons alors pour χ le caractère de $\mathfrak{S}_\mathbb{Q}$ trivial sur toutes les composantes $\mathbb{R}^*$ et $\mathbb{Q}_p^*$, $p\notin\{\ell_1,\ldots,\ell_s\}$, tandis que, pour $1\leq i\leq s$, la restriction de χ à $\mathbb{Q}_{\ell_i}^*$

envoie $\ell_i^a.u$ (avec $a\in\mathbb{Z}$, $u\in\mathbb{Z}_{\ell_i}^*$) sur θ_i^a. Alors χ est un caractère ℓ-adique algébrique, et pourtant, si l'un des θ_i est transcendant, $\chi\circ\sigma(\mathbb{Q}^*)$ n'est pas contenu dans $\bar{\mathbb{Q}}^*$ (où $\bar{\mathbb{Q}}$ désigne la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_\ell$). Néanmoins les valeurs de $\chi\circ\sigma$ sur

$$\{u/v\ ;\ u\in\mathbb{Z},\ v\in\mathbb{Z},\ v>0,\ u\neq 0,\ (v,\ell_i)=(u,\ell_i)=1 \text{ pour } 1\leq i\leq s\}$$

sont rationnelles.

Revenons au cas général. Montrons que *si* χ *est de type* (A), *alors il existe un ensemble* S *de places de* k, *contenant toutes les places archimédiennes de* k, *et toutes les places ultramétriques sauf peut-être un nombre fini, tel que* $\chi\circ\sigma(k_S^*)$ *soit contenu dans* $\bar{\mathbb{Q}}^*$.

En effet, il existe un voisinage V de {1} dans $\mathfrak{S}_k$ tel que, pour $\alpha\in k^*$ vérifiant $\sigma(\alpha)\in\sigma(k^*)\cap V$, on ait

$$\chi\circ\sigma(\alpha) = \prod_{i=1}^{d} (\sigma_i\alpha)^{t_i},$$

où $t_1,\ldots,t_d$ sont des nombres rationnels. D'autre part il existe un idéal entier $\mathfrak{M}$ de k, de support contenu dans l'ensemble des places de k au dessus de ℓ, tel que $\sigma(k^*(\mathfrak{M}))\subset V$. Enfin (Chap.I, §3c), en désignant par S l'ensemble des places infinies de k et des places ultramétriques v de k telles que $v(\mathfrak{M})=0$ (autrement dit S est le complémentaire du support de $\mathfrak{M}$), il existe un entier rationnel positif a tel que $k_S^{*a}\subset k^*(\mathfrak{M})$. Donc $\chi\circ\sigma(\alpha)^a$ est algébrique sur $\mathbb{Q}$ pour tout $\alpha\in k_S^*$, ce qui démontre $\chi\circ\sigma(k_S^*)\subset\bar{\mathbb{Q}}^*$.

De même, *si* χ *est de type* (A_0), *alors il existe un idéal entier* $\mathfrak{M}$ *de* k *tel que* $\chi\circ\sigma(k^*(\mathfrak{M}))$ *soit contenu dans une extension finie de* $\mathbb{Q}$ (le compositum des $\sigma_i(k)$ dans $\mathbb{C}_\ell$). Nous allons voir que la réciproque est vraie. C'est l'analogue ℓ-adique du théorème 2.1 du chapitre I.

Théorème 2.1.- *Soit* χ *un caractère* ℓ*-adique de* $\mathfrak{S}_k$, *et soient* $\alpha_1,\ldots,\alpha_m$ *des éléments de* k^*, *avec* $m>d(d+1)$, *tels que les nombres* $\sigma_i\alpha_j$, $(1\leq i\leq d,\ 1\leq j\leq m)$ *soient multiplicativement indépendants dans* $\mathbb{C}_\ell^*$ *et vérifient* $|\sigma_i\alpha_j-1|_\ell<1$. *On suppose que les nombres* $\chi\circ\sigma(\alpha_j)$, $(1\leq j\leq m)$ *sont algébriques sur* $\mathbb{Q}$. *Alors* χ *est de type* (A).

Démonstration. Pour n entier tendant vers l'infini, $(\sigma_i\alpha_j)^{\ell^n}$ tend vers 1 dans $\mathbb{C}_\ell$ d'après le lemme 1.1. Donc pour n suffisamment grand, en posant $\alpha'_j=\alpha_j^{\ell^n}$, on a

$$\chi\circ\sigma(\alpha'_j) = \prod_{i=1}^{d} (\sigma_i\alpha'_j)^{t_i} \qquad \text{pour } 1\le j\le m.$$

et il faut voir que cela implique $t_i\in\mathbb{Q}$ pour tout $i=1,\dots,d$. Nous reprenons la démonstration du théorème 2.1 du chapitre 1. Rappelons que L_ℓ désigne l'ensemble des $\log_\ell\alpha$, pour $\alpha\in\mathbb{C}_\ell^*$ algébrique sur $\mathbb{Q}$.

Soit $1, \tau_1,\dots,\tau_n$ une base du $\mathbb{Q}$-espace vectoriel engendré dans $\mathbb{C}_\ell$ par $1, t_1,\dots,t_d$. On a par hypothèse

$$\sum_{i=1}^{d} t_i \log_\ell\sigma_i\alpha_j \in L_\ell \qquad \text{pour } 1\le j\le m.$$

On écrit

$$t_i = \sum_{\nu=0}^{n} a_{i\nu}\tau_\nu \qquad (1\le i\le d),$$

avec $a_{i\nu}\in\mathbb{Q}$, et $\tau_0=1$. Alors en posant

$$\lambda_\nu(\alpha_j)= \sum_{i=1}^{d} a_{i\nu}\log_\ell\sigma_i\alpha_j, \qquad (1\le\nu\le n,\ 1\le j\le m),$$

on a $\lambda_\nu(\alpha_j)\in L_\ell$, et

$$\sum_{\nu=1}^{n} \tau_\nu\lambda_\nu(\alpha_j) \in L_\ell, \qquad (1\le j\le m).$$

Le théorème 4.2 de l'Introduction donne alors $n=0$, donc $t_1,\dots,t_d$ sont tous rationnels.

Voici maintenant l'analogue ℓ-adique de la proposition 2.2 du Chapitre I.

Proposition 2.2.- *Soit E un corps de nombres, et soit $\beta\in k^*$ ayant la propriété suivante : pour tout nombre premier p, et tout $(h_1,\dots,h_d)\in\mathbb{Z}^d$, la condition*

$$\prod_{i=1}^{d} (\sigma_i\beta)^{h_i}\in K^{*p}$$

implique que p divise chacun des nombres $h_1,\dots,h_d$.

Soit χ *un caractère* ℓ*-adique de* $\mathfrak{S}_k$ *de type* (A). *On suppose que* $\sigma\beta$ *appartient à un voisinage de* 1 *dans* $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^*$ *dans lequel*

$$\chi(z)=\prod_{\lambda\mid\ell}\prod_{1\le i\le d_\lambda}(\sigma_{\lambda i}z_\lambda)^{t_{\lambda i}}.$$

On suppose aussi $\chi\circ\sigma(\beta)\in E$. *Alors* χ *est de type* (A_0).

Démonstration. L'hypothèse peut s'écrire :

$$\prod_{i=1}^{d}(\sigma_i\beta)^{t_i}\in E^*,$$

avec $t_1,\dots,t_d$ rationnels, et il s'agit de vérifier que ces nombres sont en fait entiers. Sinon, il existe un entier N et un nombre premier p tels que les nombres $m_i=Nt_ip$ soient entiers et non tous divisibles par p. Alors

$$\prod_{i=1}^{d}(\sigma_i\beta)^{m_i}\in E^{*p},$$

contrairement à l'hypothèse.

c) Construction des α_j et de β.

Dans les résultats des parties a,b,c du ch.1 §3, on peut remplacer $\mathbb{C}$ par $\mathbb{C}_\ell$, c'est-à-dire, en désignant par $\sigma_1,\dots,\sigma_d$ les plongements de k dans $\mathbb{C}_\ell$, construire des suites (α_j) d'éléments de k^* telles que les $\sigma_i\alpha_j$ soient multiplicativement indépendants, et construire un nombre $\beta\in k^*$ tel que $\prod_{i=1}^{d}(\sigma_i\beta)^{h_i}$ ne soit une puissance p-ième dans un corps de nombres donné E que si p divise tous les h_i.

Lemme 2.3.- *Soient* k *un corps de nombres,* $\sigma_1,\dots,\sigma_d$ *les plongements de* k *dans* $\mathbb{C}_\ell$, $p_1,\dots,p_m$ *des nombres premiers complètement décomposés dans* k, *et, pour* $1\le j\le m$, v_j *une place de* k *au-dessus de* p_j. *Soit* $S=\{v_1,\dots,v_m\}$ *et soit* $\mathfrak{M}$ *un idéal entier de* k *étranger à* S. *Il existe* m *éléments* $\alpha_1,\dots,\alpha_m$ *de* $k_S^*(\mathfrak{M})_+$ *tels que les* dm *nombres* $\sigma_i\alpha_j$, $(1\le i\le d,\ 1\le j\le m)$ *soient multiplicativement indépendants.*

La démonstration est la même que celle du corollaire 3.11 au Chap. I. Noter que si on prend pour $\mathfrak{m}$ un multiple de ℓ, alors on aura $\alpha_i \equiv 1 \bmod^* \ell$, donc $|\sigma_i \alpha_j - 1|_\ell < 1$ pour tout i,j.

Lemme 2.4.- *Soient* $\mathfrak{m}$ *un idéal entier de* k, *et* E *un corps de nombres ; il existe* $\beta \in k^*(\mathfrak{m})$ *tel que pour tout nombre premier* p, *et pour tout* $m_1, \ldots, m_d$ *dans* $\mathbb{Z}$, *la relation*

$$\prod_{j=1}^{d} (\sigma_i \beta)^{m_i} \in E^{*p}$$

implique que p *divise tous les* m_i.

La démonstration est la même que celle du lemme 3.6 du Chapitre I. Notons, pour l'application à la proposition 2.2, que si l'on prend pour $\mathfrak{m}$ un multiple suffisant de ℓ, on peut rendre $|\sigma_i \beta - 1|_\ell$ aussi petit que l'on veut.

d) Caractères ℓ-adiques du groupe des classes d'idèles.

Soit χ un homomorphisme continu de $\mathfrak{S}_k$ dans $\mathbb{C}_\ell^*$, trivial sur k^*. Soit S un ensemble fini de places de k, contenant les places de k au-dessus de ℓ et les places archimédiennes, en dehors duquel χ est non ramifié. On définit

$$U^S = \{x \in \mathfrak{S}_k \ ; \ x_v = 1 \text{ pour } v \in S, \text{ et } x_v \in A_v^* \text{ pour toute place finie } v\}.$$

Comme χ est trivial sur le sous-groupe

$$\{x \in U^S \ ; \ x_v = 1 \text{ pour tout } v \text{ en dehors d'un ensemble fini}\},$$

dont l'adhérence est U^S, on a $U^S \subset \ker\chi$, et χ définit un homomorphisme $\tilde{\chi}$ du groupe I_k^S des idéaux fractionnaires premiers à S à valeurs dans $\mathbb{C}_\ell^*$.

Voici l'analogue ℓ-adique du corollaire 6.2 du Chapitre I ; la démonstration est essentiellement la même, en remplaçant le théorème 2.1 du Chapitre I par le théorème 2.1 de ce Chapitre II.

Corollaire 2.5.- *Soit* χ *un caractère* ℓ*-adique du groupe des classes d'idèles* $\mathbf{C}_k$, *et soit* S *un ensemble fini de places de* k, *contenant les places de* k *au-dessus de* ℓ *et les places archimédiennes, et en dehors duquel* χ *n'est pas ramifié.*

Alors χ *est de type* (A) *si et seulement si les nombres* $\tilde{\chi}(\mathfrak{A})$, $(\mathfrak{A}\in I_k^S)$, *sont tous algébriques. Il est de type* (A_0) *si et seulement s'il existe un corps de nombres* E *tel que* $\tilde{\chi}(\mathfrak{A})\in E$ *pour tout* $\mathfrak{A}\in I_k^S$.

Les énoncés précédents fournissent des traductions ℓ-adiques de résultats du Chapitre I. Voici maintenant une autre conséquence du théorème 2.1, de la proposition 2.2, et des lemmes 2.3, 2.4, qui nous sera utile dans l'étude des représentations ℓ-adiques.

Corollaire 2.6.- *Soient* k *et* E *deux corps de nombres,* S *un ensemble fini de places de* k *contenant les places archimédiennes ainsi que les places au-dessus de* ℓ, *et* χ *un caractère* ℓ*-adique du groupe des classes d'idèles de* k, *non ramifié en dehors de* S. *On suppose* $\chi(\mathfrak{I}_k^S)\subset\overline{\mathbb{Q}}$ *(resp.* $\chi(\mathfrak{I}_k^S)\subset E$*). Alors* χ *est de type* (A) *(resp.* (A_0)*).*

Démonstration.- Rappelons que $\mathfrak{I}_k^S$ est le sous-groupe de $\mathfrak{I}_k$ formé des idèles dont les composantes valent 1 aux places de S. Soit $\mathfrak{M}$ un idéal entier non nul de k tel que, pour toute place finie $v\in S$ ne divisant pas ℓ, et tout $z\in k_v^*$ vérifiant $v(z-1)\geq v(\mathfrak{M})$, on ait $\chi_v(z)=1$. Soit S' un ensemble fini de places de k au-dessus de nombres premiers complètement décomposés dans k, S' étant disjoint de S, et ayant au moins d^2+d+1 éléments. Pour chaque $\alpha\in k_S^*,(\mathfrak{M})_+$, on décompose l'idèle $\boldsymbol{\alpha}$ (image de $\alpha\in k^*$ dans $\mathfrak{I}_k$) en

$$\boldsymbol{\alpha}=\boldsymbol{\sigma}_\infty\alpha.\boldsymbol{\sigma}_\ell\alpha.\boldsymbol{\alpha}_S.\alpha^S,$$

où $\boldsymbol{\sigma}_\infty$ (resp. $\boldsymbol{\sigma}_\ell$) est le plongement canonique complexe (resp. ℓ-adique), et $\boldsymbol{\alpha}_S\in\prod k_v^*$ où le produit est étendu aux places finies de S qui ne sont pas

au-dessus de ℓ, tandis que $\alpha^S \in \mathfrak{S}_k^S$. D'abord χ est trivial sur k^*, donc $\chi(\alpha)=1$. Ensuite $\sigma_\omega \alpha$ appartient à la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$, d'où $\chi(\sigma_\omega \alpha)=1$. Comme $\alpha \equiv 1 \bmod^* \mathfrak{M}$, on a $\chi(\alpha_S)=1$. Enfin $\alpha^S \in \mathfrak{S}_k^S$, ce qui donne $\chi(\alpha^S)\in\overline{\mathbb{Q}}$. Par conséquent $\chi\circ\sigma_\ell(\alpha)\in\overline{\mathbb{Q}}$ pour tout $\alpha \in k_S^*,(\mathfrak{M})_+$. Le théorème 2.1 joint au lemme 2.3 entraîne que χ est de type (A).

Si, de plus, $\chi(\mathfrak{S}_k^S)\subset E$, on prend $\beta\in k^*(\mathfrak{M})$ comme dans le lemme 2.4 ; on a comme ci-dessus $\chi\circ\sigma_\ell(\beta)=\pm(\chi(\beta^S))^{-1}\in E$, et la proposition 2.2 montre que χ est de type (A_0).

e) Densité.

Pour terminer la traduction ℓ-adique des résultats du chapitre 1, il reste à considérer les énoncés du Chapitre I §3 concernant l'image de k^* par le plongement canonique de k dans $k\otimes_{\mathbb{Q}}\mathbb{R}$.

La partie "transcendante" (Chapitre I §3 proposition 3.13 et corollaire 3.14) ne pose pas de problème :

Proposition 2.7.- *Soient* $y_1,\ldots,y_m$ *des éléments de* $\mathbf{L}_\ell^d$, *avec* $y_j=(y_{1j},\ldots,y_{dj})$, $1\le j\le m$. *On suppose que les* md *nombres* y_{ij} *sont linéairement indépendants sur* $\mathbb{Z}$. *Soit* $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_m$, *et soit* H *un hyperplan de* $\mathbb{C}_\ell^d$. *Alors*

$$\mathrm{rg}_{\mathbb{Z}} Y\cap H\le d(d-1).$$

Corollaire 2.8.- *Soient* $y_1,\ldots,y_m$ *des éléments de* $(\mathbf{L}_\ell\cap\mathfrak{M}_\ell)^d$, *avec* $y_j=(y_{1j},\ldots,y_{dj})$, $1\le j\le m$. *On suppose que les* md *nombres* y_{ij} *sont linéairement indépendants sur* $\mathbb{Z}$. *Soit* $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_m$, *et soit* H *un hyperplan de* $\mathfrak{M}_\ell^d$. *Alors*

$$\mathrm{rg}_{\mathbb{Z}} Y\cap H\le d(d-1).$$

Les questions de densité se posent de manière différente dans les domaines ultramétriques. D'abord $\mathbb{Z}$ lui-même est dense dans $\mathbb{Z}_\ell$. Ensuite aucun sous-groupe de type fini n'est dense dans $\mathbb{Q}_\ell$.

Comme k est dense dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ (par le théorème d'approximation faible), il en résulte que k^* est dense dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^*$. Mais aucun sous-groupe de type fini de k^* n'est partout dense dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^*$. On peut chercher un sous-groupe de type fini de k^* qui soit dense dans un voisinage de 1 dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^*$; il suffit pour cela de prendre d éléments de k^* (avec $d=[k:\mathbb{Q}]$), au voisinage de 1, dont les images par $\log_\ell$ sont $\mathbb{Q}_\ell$-linéairement indépendantes dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$.

Le critère de densité (Chapitre I, lemme 3.12) reposait sur le théorème de Kronecker. L'analogue ℓ-adique de celui-ci a été étudié par E. Lutz en 1951, et l'analogue idélique par D. Cantor en 1965 (Illinois J. Math., **9** (1951), 677-700) ; il en déduit le théorème d'approximation forte.

On peut aussi étudier, du point de vue de la densité, l'image de k^* dans $\mathfrak{I}_k$. Rappelons (Chap.I, §6a) que si S est un ensemble fini de places de k contenant les places archimédiennes, alors $k^*\mathfrak{I}_k^S$ est dense dans $\mathfrak{I}_k$, où $\mathfrak{I}_k^S=\{x\in\mathfrak{I}_k \ ; \ x_v=1 \ \text{ pour tout } \ v\in S\}$.

Un autre problème de densité, en liaison avec les représentations ℓ-adiques, a été posé par J.-P.Serre (Dépendance d'exponentielles p-adiques, Sém. DPP, **7** (1965/66), N°15).

§3. Groupes de Galois et corps de classes.

Soit L/k une extension algébrique (finie ou non) galoisienne. On munit le groupe de Galois $G=G(L/k)$ de la topologie de Krull, qui en fait un groupe profini (compact totalement discontinu). Soient E un corps de nombres, λ une place de E, et $\rho : G \longrightarrow E_\lambda^*$ un homomorphisme continu de G dans le groupe multiplicatif du complété de E en λ. En supposant L/k abélienne, on montre que ρ est "localement algébrique" sur E si et seulement si les valeurs de ρ en les Frobenius aux places non ramifiées sont dans une extension finie de E. Ce résultat se démontre en utilisant ce que nous avons vu au §2d sur les caractères du groupe des classes d'idèles, grâce à l'application de réciprocité d'Artin (théorie du corps de classes global).

Nous commençons par des généralités sur les extensions algébriques infinies de corps de nombres. Parmi la nombreuse littérature sur ce sujet, mentionnons les ouvrages de Cassels et Fröhlich, de Iyanaga, et de Neukirch.

a) Groupes profinis.

Soient G un groupe et $\mathcal{F}$ une famille non vide de sous-groupes normaux. On suppose

1) pour tout H_1 et H_2 dans $\mathcal{F}$, il existe $H_3 \in \mathcal{F}$ tel que $H_3 \subset H_1 \cap H_2$

et

2) $\bigcap_{H \in \mathcal{F}} H = \{1\}$.

Pour $H \in \mathcal{F}$, notons $\varphi_H : G \longrightarrow G/H$ la surjection canonique. Pour $H_1 \subset H_2$ dans $\mathcal{F}$, on note $\varphi_{H_1 H_2}$ l'homomorphisme surjectif rendant commutatif le diagramme :

$$\begin{array}{ccc} & & G \\ & \overset{\varphi_{H_2}}{\nearrow} & \\ G & & \downarrow \varphi_{H_1} \\ & \underset{\varphi_{H_1}}{\searrow} & \\ & & G/H_1 \end{array} \qquad \begin{array}{ccc} & & G/H_2 \\ & \overset{\varphi_{H_1 H_2}}{\nearrow} & \\ G/H_2 & & \downarrow \\ & \searrow & \\ & & G/H_1 \end{array} .$$

Dans le produit $\prod_{H\in\mathcal{J}} G/H$, l'ensemble des $(x_H)_{H\in\mathcal{J}}$ vérifiant

$$\varphi_{H_1H_2}(x_{H_1})=x_{H_2} \quad \text{pour tout } (H_1,H_2)\in\mathcal{J}^2,\ H_1\subset H_2,$$

est un sous-groupe noté $\varprojlim_{H\in\mathcal{J}} G/H$ (*limite projective*). Soit Γ ce groupe, et soit Φ l'homomorphisme de G dans Γ qui envoie x sur $(\varphi_H(x))_{H\in\mathcal{J}}$. L'hypothèse 2) revient à dire que Φ est injectif.

On munit G d'une structure de groupe topologique en prenant comme base de voisinages de $x\in G$ les ensembles Hx, $H\in\mathcal{J}$. Rappelons que H est normal dans G, donc que $Hx=xH$. La condition 2) ci-dessus assure que la topologie est séparée. La topologie quotient sur chaque G/H est la topologie discrète, et les applications $\varphi_{H_1H_2}$ sont continues. On munit Γ de la topologie limite projective qui est induite par la topologie produit sur $\prod_{H\in\mathcal{J}} G/H$: une base de voisinages de l'élément neutre dans Γ est formée des $\ker \pi_H$, $H\in\mathcal{J}$, où π_H est la surjection canonique de Γ sur G/H (restriction à Γ de la projection de $\prod_{H\in\mathcal{J}} G/H$ sur le facteur G/H considéré). Alors l'homomorphisme Φ est continu, et $\Phi(G)$ est dense dans Γ (chaque φ_H est surjectif). Enfin Φ est un homéomorphisme de G dans $\Phi(G)$.

Nous supposons maintenant que chaque sous-groupe $H\in\mathcal{J}$ est d'indice fini dans G. Alors Φ *est un isomorphisme de* G *sur* Γ *si et seulement si* G *est compact*. En effet, si G est compact, son image par Φ est fermée, et comme elle est dense, Φ est surjectif. Inversement, comme Γ est compact (il est fermé dans le produit $\prod_{H\in\mathcal{J}} G/H$, et ce produit est compact), si Φ est surjectif, alors G est compact.

Définition. On dit qu'un groupe topologique est *profini* s'il est compact et possède une base de voisinages ouverts de l'élément neutre formée de sous-groupes normaux d'indice fini. En d'autres termes G est profini s'il existe un ensemble $\mathcal{J}$ de sous-groupes d'indices finis tel que la topologie soit définie (comme ci-dessus) par $\mathcal{J}$ et que l'application Φ associée soit surjective. Ou encore : un groupe profini est un groupe topologique qui est compact et totalement discontinu.

Exemples.

0) Le groupe $\Gamma = \varprojlim_{H\in\mathcal{F}} G/H$ que nous venons de construire est un groupe profini.

1) On prend pour $\mathcal{F}$ l'ensemble de tous les sous-groupes normaux de G d'indice fini ; le groupe $\Gamma = \varprojlim_{H\in\mathcal{F}} G/H$ est la *complétion profinie* de G, que l'on note $\hat{G}$ (à ne pas confondre avec le dual). Par exemple $\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$; ce groupe $\hat{\mathbb{Z}}$ est muni d'une structure naturelle d'anneau topologique (*anneau de Prüfer*).

2) Soit p un nombre premier. On prend pour $\mathcal{F}$ l'ensemble de tous les sous-groupes normaux de G d'indice une puissance de p. Le groupe $\varprojlim_{H\in\mathcal{F}} G/H$ ainsi obtenu est appelé un pro-p-groupe. Par exemple $\mathbb{Z}_p = \varprojlim_{h\in\mathbb{Z}} \mathbb{Z}/p^h\mathbb{Z}$ est un pro-p-groupe. Comme, pour $n=\prod p^{\alpha_p}$, on a $\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p^{\alpha_p}\mathbb{Z}$ (théorème des restes chinois), on voit que $\hat{\mathbb{Z}}$ est isomorphe (comme groupe topologique, et aussi comme anneau topologique) à $\prod_p \mathbb{Z}_p$. Pour le groupe des éléments inversibles on a aussi un isomorphisme de groupes topologiques $\hat{\mathbb{Z}}^* \simeq \prod_p \mathbb{Z}_p^*$.

On dit qu'un groupe profini G est *procyclique* s'il existe $\sigma\in G$ tel que G soit l'adhérence du groupe engendré par σ ; on dit alors que σ est un *générateur topologique* de G. Par exemple $\mathbb{Z}$ est dense dans $\hat{\mathbb{Z}}$ et dans $\mathbb{Z}_p$, donc $\hat{\mathbb{Z}}$ et $\mathbb{Z}_p$ sont des groupes procycliques.

b) Topologie de Krull.

Soit L/K une extension galoisienne (i.e. algébrique, normale et séparable), finie ou non (cf. par exemple S. Lang, Algebra, 2nd Ed., Chap.VIII). On désigne par $G=G(L/K)$ le groupe des K-automorphismes de L. Dans le cas où L est la clôture séparable de K, le groupe G est appelé *groupe de Galois absolu* de K et noté G_K. L'étude du groupe de Galois absolu de $\mathbb{Q}$ est un des problèmes d'arithmétique actuellement les plus importants.

On aimerait savoir en particulier si tout groupe fini est un quotient de $G_{\mathbb{Q}}=G(\overline{\mathbb{Q}}/\mathbb{Q})$, c'est-à-dire si tout groupe fini peut se réaliser comme groupe de Galois d'une extension finie de $\mathbb{Q}$ (*problème inverse de la théorie de Galois*).

Si F est un sous-corps de L contenant K, alors L/F est une extension galoisienne ; de plus l'extension F/K est galoisienne si et seulement si $G(L/F)$ est un sous-groupe normal de G, et alors $G(F/K)\cong G/G(L/F)$.

$$\begin{array}{l} L \\ | \\ F \\ | \\ K \end{array} \qquad G$$

On munit G de la *topologie de Krull* en prenant pour système fondamental de voisinages de l'élément neutre l'ensemble des $G(L/F)$, pour F extension galoisienne finie de K contenue dans L. On vérifie en effet que si F_1 et F_2 sont des extensions galoisiennes finies de K contenues dans L, alors $F=K(F_1 \cup F_2)$ l'est aussi :

$$\begin{array}{ccc} & L & \\ & | & \\ & F & \\ / & & \backslash \\ F_1 & & F_2 \\ \backslash & & / \\ & K & \end{array}$$

$$G(L/F)=G(L/F_1)\cap G(L/F_2).$$

Alors le groupe $G=G(L/K)$ est compact. C'est donc un groupe profini. Si H est un sous-groupe de G, le corps des invariants :

$$L^H=\{x\in L \ ; \ \sigma x=x \ \text{ pour tout } \ \sigma\in H\}$$

de H est le même que le corps des invariants de l'adhérence $\overline{H}$ de H dans G.

Le théorème fondamental de la théorie de Galois énonce que l'application $H \longrightarrow L^H$ établit une bijection entre l'ensemble des sous-groupes fermés de G et l'ensemble des sous-corps de L contenant K. La bijection réciproque est $F \longrightarrow G(L/F)$.

Enfin, G étant compact, un sous-groupe fermé H de G est ouvert dans G si et seulement s'il est d'indice fini dans G.

Exemple : le groupe de Galois absolu de $\mathbb{F}_p$.

Soit p un nombre premier, et soit $\overline{\mathbb{F}}_p$ une clôture algébrique du corps fini $\mathbb{F}_p$. Pour chaque entier $n\geq 1$, $\overline{\mathbb{F}}_p$ possède un sous-corps unique $\mathbb{F}_{p^n}$ ayant p^n éléments, et l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est cyclique d'ordre n. On définit le *Frobenius* $\varphi_p\in G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ par

$$\varphi_p(x)=x^p \qquad \text{pour tout } x\in\overline{\mathbb{F}}_p.$$

Alors pour chaque $n\geq 1$, $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est engendré par la restriction de φ_p à $\mathbb{F}_{p^n}$. L'application de $\mathbb{Z}$ dans $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ qui envoie h sur φ_p^h est donc un homomorphisme surjectif de noyau $n\mathbb{Z}$, et en passant à la limite projective on obtient un isomorphisme entre $\hat{\mathbb{Z}}$ et $G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Ainsi φ_p est un générateur topologique de $G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

On dit qu'une extension galoisienne est *une* $\hat{\mathbb{Z}}$- (resp. *une* $\mathbb{Z}_p$-) *extension* si son groupe de Galois est isomorphe (comme groupe topologique) à $\hat{\mathbb{Z}}$ (resp. à $\mathbb{Z}_p$).

c) Extension abélienne maximale.

Quand G est un groupe, on désigne par G' le sous-groupe *dérivé* de G, c'est-à-dire le sous-groupe engendré par les *commutateurs* :

$$aba^{-1}b^{-1} \ ; \ (a,b)\in G^2.$$

C'est un sous-groupe normal de G, et le quotient G/G' est abélien. Tout homomorphisme de G dans un groupe abélien a un noyau qui contient G', donc il se factorise par $G \longrightarrow G/G'$; ainsi G' est le plus petit sous-groupe normal de G tel que le quotient soit abélien. Le groupe G/G' est l'*abélianisé* de G.

Soient E/K une extension galoisienne, et $G=G(E/K)$ son groupe de Galois, muni de la topologie de Krull. On désigne par G^c l'adhérence topologique dans G de G', par G^{ab} le quotient G/G^c, et par K^{ab} le sous-corps de E fixé par G^c (ou par G', c'est le même). Alors K^{ab} est l'extension abélienne maximale de K contenue dans E (autrement dit K^{ab} est la réunion des sous-corps F de E abéliens finis sur K), et le groupe de Galois de K^{ab} sur K est bien entendu G^{ab}. Quand E est la clôture séparable de K, le corps K^{ab} est l'*extension abélienne maximale* de K.

L'étude du groupe des caractères de G^{ab} fait l'objet du Chap.IV §6.2 de Iyanaga.

Exemples.

1) Si K est un corps fini, l'extension abélienne maximale de K est la clôture algébrique $\bar{K}$ de K.

2) L'extension abélienne maximale $\mathbb{Q}^{ab}$ de $\mathbb{Q}$ est le corps obtenu en adjoignant à $\mathbb{Q}$ toutes les racines de l'unité (théorème de Kronecker-Weber). Pour chaque entier $n\geq 1$, soit ζ_n une racine primitive n-ième de l'unité. On a $\mathbb{Q}^{ab}=\bigcup_{n\geq 1}\mathbb{Q}(\zeta_n)$ et $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})\simeq(\mathbb{Z}/n\mathbb{Z})^*$, et on trouve que $G(\mathbb{Q}^{ab}/\mathbb{Q})$ est isomorphe au groupe $\prod_p \mathbb{Z}_p^* \simeq \hat{\mathbb{Z}}^*$.

Le problème inverse de la théorie de Galois dans le cas abélien est donc résolu : tout groupe abélien fini est isomorphe à un quotient de $\hat{\mathbb{Z}}$.

d) Frobenius arithmétique.

Soient k un corps de nombres, L une extension algébrique de k, et v une place de k. Si w est une place de L prolongeant v (on écrit $w|v$), alors pour chaque corps de nombres K contenant k et contenu dans L, la restriction de w à K est une place de K prolongeant v. Pour chaque corps de nombres K on désigne par Σ_K l'ensemble des places de K. On désigne aussi (c'est compatible) par Σ_L la limite projective des Σ_K, pour K extension finie de k contenue dans L, avec les applications de restriction $\Sigma_{K_1}\longrightarrow\Sigma_{K_2}$ pour $K_1\supset K_2$.

Supposons l'extension L/k galoisienne. Le groupe de Galois $G=G(L/k)$ opère sur Σ_L : en terme de valuations sur L, pour $w\in\Sigma_L$ et $\sigma\in G$, σw est l'élément de Σ_L défini par $(\sigma w)x=w(\sigma^{-1}x)$ pour $x\in L$. Soit $w\in\Sigma_L$. On définit le *groupe de décomposition*

$$D_w=\{\sigma\in G\ ;\ \sigma w=w\}.$$

C'est un sous-groupe fermé de G. Pour $\tau\in G$, on a $D_{\tau w}=\tau D_w\tau^{-1}$, donc la classe de conjugaison de D_w ne dépend que de v. Soient k_v le complété de k en v, L_w la réunion des complétés F_w pour F extension finie de K contenue dans L, et k_v^o, L_w^o les corps résiduels. L'extension L_w/k_v est galoisienne, de groupe de Galois (isomorphe à) D_w, et on a un homomorphisme

surjectif canonique de D_w sur $G(L_w^o/k_v^o)$, dont le noyau est le *groupe d'inertie* I_w en w.

Supposons maintenant que la place v est finie. L'extension L/k est *non ramifiée en* w si $I_w=\{1\}$. Comme k_v^o est un corps fini, le groupe de Galois $G(L_w^o/k_v^o)$ est procyclique, engendré topologiquement par le Frobenius ; donc le quotient D_w/I_w est un groupe procyclique (cyclique s'il est fini), et possède un générateur topologique, le *Frobenius arithmétique* F_w, caractérisé par :

$$F_w(x)\equiv x^{N(v)} \mod \mathcal{M}_w \quad \text{pour tout } x\in A_w,$$

où A_w (resp. $\mathcal{M}_w$) est l'anneau de valuation (resp. l'idéal de valuation) de L_w.

Si v n'est pas ramifiée dans l'extension L/k, pour $\tau\in G$ on a $F_{\tau w}=\tau F_w \tau^{-1}$, donc la classe de conjugaison de F_w dans G ne dépend que de v ; on la note F_v :

$$F_v=\{F_w \ ; \ w|v\}\subset G.$$

Si l'extension L/k est abélienne, alors D_w, I_w et F_w ne dépendent que de v ; on les note D_v, I_v et F_v, ce qui est compatible avec ce qui précède.

e) Théorie du corps de classes.

La théorie du corps de classes global pour un corps de nombres k établit un isomorphisme continu entre d'une part le quotient $\mathbf{C}_k/\mathbf{D}_k$ du groupe des classes d'idèles $\mathbf{C}_k$ de k par la composante neutre de l'origine $\mathbf{D}_k$, et d'autre part le groupe de Galois $G(k^{ab}/k)$ de l'extension abélienne maximale de k.

L'homomorphisme surjectif continu $\Psi : \mathbf{C}_k \longrightarrow G(k^{ab}/k)$ de noyau $\mathbf{D}_k$ correspondant est l'*application de réciprocité d'Artin*. Pour décrire cette application, il suffit de dire, pour chaque extension abélienne finie K/k, quel est l'homomorphisme $\Psi_K : \mathbf{C}_k \longrightarrow G(K/k)$ correspondant (on passe ensuite à la limite projective). Cet homomorphisme Ψ_K est caractérisé par la propriété

suivante : pour toute place finie v_o de k non ramifiée dans K, l'image par ψ_K de l'idèle $\mathbf{x}=(x_v)$ avec

$$x_v=\begin{cases} 1 & \text{pour } v\neq v_o, \\ \pi_{v_o} & \text{pour } v=v_o, \end{cases}$$

(où π_{v_o} est une uniformisante en v_o) est le Frobenius F_{v_o} de K/k en v_o.

On connait la composante connexe neutre $\mathfrak{I}_k^o$ de $\mathfrak{I}_k$: c'est la composante connexe de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$, elle est donc isomorphe à $\mathbb{R}_+^{*r_1}\times\mathbb{C}^{*r_2}$. La composante connexe $\mathbf{D}_k$ de l'élément neutre dans $\mathbf{C}_k$ est l'adhérence de l'image de $\mathfrak{I}_k^o$ dans $\mathbf{C}_k$. Et $\mathbf{C}_k/\mathbf{D}_k$ est aussi le quotient de $\mathfrak{I}_k$ par l'adhérence de $k^*\mathfrak{I}_k^o$. (Pour avoir plus de détails sur la structure de $\mathbf{D}_k$, voir Artin-Tate, Class field theory, Chap.9.)

Exemple.- Partons de $k=\mathbb{Q}$. On a $\mathfrak{I}_{\mathbb{Q}}\simeq\mathbb{Q}^*\times\mathbb{R}_+^*\times\prod_p\mathbb{Z}_p^*$, $\mathbf{C}_{\mathbb{Q}}\simeq\mathbb{R}_+^*\times\prod_p\mathbb{Z}_p^*$, $\mathbf{D}_{\mathbb{Q}}\simeq\mathbb{R}_+^*$, et $\mathbf{C}_{\mathbb{Q}}/\mathbf{D}_{\mathbb{Q}}\simeq\prod_p\mathbb{Z}_p^*$. Soient $n\geq 1$ un entier rationnel, ζ_n une racine primitive n-ième de l'unité, et $K=\mathbb{Q}(\zeta_n)$. Soit p_o un nombre premier ne divisant pas n, c'est-à-dire non ramifié dans K. L'idèle $\mathbf{x}\in\mathfrak{I}_{\mathbb{Q}}$ de composantes

$$x_v=\begin{cases} 1 & \text{pour } v\neq p_o, \\ p_o & \text{pour } v=p_o, \end{cases}$$

a pour image dans $\mathbb{Q}^*\times\mathbb{R}_+^*\times\prod_p\mathbb{Z}_p^*$ le triplet $(p_o\ ;\ 1/p_o\ ;\ (u_p))$, où

$$u_p=\begin{cases} 1/p_o & \text{pour } p\neq p_o, \\ 1 & \text{pour } p=p_o. \end{cases}$$

Son image dans $\mathbf{C}_{\mathbb{Q}}/\mathbf{D}_{\mathbb{Q}}\simeq\prod_p\mathbb{Z}_p^*$ est donc $\mathbf{u}=(u_p)$.

Comme $\mathbb{Q}(\zeta_n)$ est un sous-corps de $\mathbb{Q}^{ab}$, le groupe $G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est un quotient de $G(\mathbb{Q}^{ab}/\mathbb{Q})$, et on a le diagramme commutatif

$$\begin{array}{ccc} G(\mathbb{Q}^{ab}/\mathbb{Q}) & \longrightarrow & G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \downarrow & & \downarrow \\ \prod_p\mathbb{Z}_p^* & \xrightarrow[f_n]{} & (\mathbb{Z}/n\mathbb{Z})^* \end{array}$$

où les flèches verticales sont des isomorphismes. Soit $s:\mathbb{Z}\longrightarrow\mathbb{Z}/n\mathbb{Z}$ la surjection canonique. On a alors $f_n(\mathbf{u})=s(a)$, quand $a\in\mathbb{Z}$ vérifie

$$p_o a\equiv 1 \mod n\ .$$

D'autre part, par définition de Ψ, l'élément $\sigma=\Psi_K(\mathfrak{x})$ de $G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfait

$$\sigma\zeta=\zeta^{Po} ;$$

donc

$$\sigma\zeta=\zeta^{u^{-1}},$$

où, pour $u=(u_p)\in\prod_p \mathbb{Z}_p^*$ et $\zeta=\prod_p \zeta_p$, on pose $\zeta^u=\prod_p \zeta_p^{u_p}$.

Revenons au cas général, et supposons l'extension L/k abélienne. Pour chaque place finie v de k, on plonge k_v^* dans $\mathfrak{I}_k$, et on note Ψ_v la restriction de Ψ à k_v^*. Alors $\Psi_v(A_v^*)$ est le sous-groupe d'inertie I_v, donc v est non ramifiée dans l'extension L/k si et seulement si $\Psi_v(A_v^*)=\{1\}$ (on peut aussi décrire l'image par Ψ_v des sous-groupes $1+\mathfrak{M}_v^n$; cf. Cassels et Fröhlich, Chap.VI, §4.1).

f) Caractères du groupe de Galois.

Soient k et E deux corps de nombres, λ une place de E, E_λ le complété, $G=G(k^{ab}/k)$ le groupe de Galois de l'extension abélienne maximale de k, et $\rho:G\longrightarrow E_\lambda^*$ un homomorphisme continu.

On désigne par χ_ρ l'homomorphisme composé de ρ et de l'application d'Artin $\mathbf{C}_k\longrightarrow G$. Ainsi χ_ρ est un homomorphisme continu de $\mathbf{C}_k$ dans E_λ^*, trivial sur la composante connexe neutre $\mathbf{D}_k$.

Inversement, si χ est un homomorphisme continu de $\mathbf{C}_k$ dans E_λ^*, et si λ est une place *finie* de E, alors χ est trivial sur $\mathbf{D}_k$ (puisque E_λ est un espace totalement discontinu), donc il existe $\rho:G\longrightarrow E_\lambda^*$ tel que $\chi=\chi_\rho$; c'est là la différence principale entre le cas archimédien et le cas ultramétrique : les caractères de Hecke à valeurs complexes qui ne sont pas triviaux sur $\mathbf{D}_k$ ne correspondent pas à des représentations galoisiennes.

Quand v est une place finie de k, on dira que ρ est *non ramifié* en v si χ_ρ est non ramifié en v. Cela signifie $\chi_{\rho v}(A_v^*)=\{1\}$, et comme l'image de A_v^* par l'application d'Artin est le groupe d'inertie I_v en v, ρ est

non ramifié en v si et seulement si $\rho(I_v)=\{1\}$. D'autre part le lemme 1.10 montre que l'ensemble des places v de k où ρ est ramifié est fini.

Soit v une place de k où ρ n'est pas ramifié, et soit $F_v \in D_v/I_v$ le Frobenius en une place quelconque w de k^{ab} au dessus de v (F_v ne dépend que de v). On note $F_{v\rho}$ l'image de F_v par ρ, et on dit que ρ est *rationnel sur* E si $F_{v\rho} \in E^*$ pour toute place finie v où ρ n'est pas ramifié.

Enfin on dit que ρ est *localement algébrique* si le caractère χ_ρ est de type (A_0).

Exemple.- Prenons $k=\mathbb{Q}$. Soit ℓ un nombre premier. Le caractère fondamental donnant l'action de $G_{\mathbb{Q}}=G(\mathbb{Q}^{ab}/\mathbb{Q})$ sur les racines de l'unité d'ordre ℓ est un homomorphisme de $G_{\mathbb{Q}}$ dans $\mathbb{F}_\ell^*$ qui envoie $\sigma \in G_{\mathbb{Q}}$ sur la classe de $b_1(\sigma)\in\mathbb{Z}$ modulo ℓ avec

$$\sigma(\zeta)=\zeta^{b_1(\sigma)} \qquad \text{pour tout } \zeta\in\overline{\mathbb{Q}} \text{ vérifiant } \zeta^{\ell}=1.$$

Plus généralement, étant donné $\sigma\in G_{\mathbb{Q}}$, pour chaque $n\geq 1$, on peut trouver $b_n(\sigma)\in(\mathbb{Z}/\ell^n\mathbb{Z})^*$ tel que

$$\sigma(\zeta)=\zeta^{b_n(\sigma)} \qquad \text{pour tout } \zeta\in\overline{\mathbb{Q}} \text{ vérifiant } \zeta^{\ell^n}=1.$$

Pour chaque $\sigma\in G_{\mathbb{Q}}$, la suite $(b_n(\sigma))$ définit un élément $b(\sigma)\in\mathbb{Z}_\ell^*$. D'autre part, pour $\zeta\in\overline{\mathbb{Q}}$ racine de l'unité d'ordre une puissance de ℓ, disons ζ^{ℓ^m}, et pour $b=\sum_{i\geq 0} a_i \ell^i \in \mathbb{Z}_\ell$ (développement de Hensel), on définit

$$\zeta^b=\prod_{i=0}^{m-1} \zeta^{a_i \ell^i}.$$

Ainsi $\mathbb{Z}_\ell^*$ opère continuement sur le groupe des racines de l'unité d'ordre une puissance de ℓ muni de la topologie discrète, et l'action de $G_{\mathbb{Q}}$ est donnée par l'homomorphisme $\rho_\ell : \sigma \longrightarrow b(\sigma)$ de $G_{\mathbb{Q}}$ dans $\mathbb{Z}_\ell^*$

Montrons que ρ_ℓ est continu : étant donné un voisinage V de 1 dans $\mathbb{Z}_\ell$, on peut trouver un voisinage W de 1 dans $G_{\mathbb{Q}}$ tel que $\sigma\in W \Rightarrow b(\sigma)\in V$. En effet, V contient un sous-groupe $1+\ell^m\mathbb{Z}_\ell$, avec $m\in\mathbb{Z}$, et on prend pour W

le voisinage $G(\overline{\mathbb{Q}}/K)$, où K est le corps cyclotomique des racines de l'unité d'ordre ℓ^m.

On obtient ainsi un caractère <u>rationnel</u> ρ_ℓ de $G_{\mathbb{Q}}$ dans $\mathbb{Q}_\ell^*$: pour p premier différent de ℓ, l'image par ρ_ℓ du Frobenius en p est $p \in \mathbb{Q} \cap \mathbb{Z}_\ell^*$. Aussi ρ_ℓ est <u>localement algébrique</u> : si on compose ρ_ℓ avec l'injection de $\mathbb{Z}_\ell^*$ dans $G_{\mathbb{Q}}$ (via l'injection de $\mathbb{Q}_\ell^*$ dans $\mathfrak{I}_{\mathbb{Q}}$), l'homomorphisme $\mathbb{Z}_\ell^* \longrightarrow \mathbb{Z}_\ell^*$ obtenu envoie u sur u^{-1}.

Cet homomorphisme ρ_ℓ se décrit aussi grâce à l'application d'Artin : $\mathfrak{I}_{\mathbb{Q}}/(\mathbb{Q}^* \times \mathbb{R}_+^*)$ est isomorphe à $G_{\mathbb{Q}}$, et aussi à $\prod_p \mathbb{Z}_p^*$, et on obtient ρ_ℓ en projetant $\prod_p \mathbb{Z}_p^*$ sur $\mathbb{Z}_\ell^*$ par $(u_p) \longrightarrow u_\ell^{-1}$.

Il est facile de voir que si ρ est localement algébrique, alors ρ est rationnel sur une extension finie de E. Voici la réciproque.

Théorème 3.1.- *Si ρ est rationnel sur E, alors ρ est localement algébrique.*

<u>Démonstration</u>.- Soit S un ensemble fini de places de k contenant les places archimédiennes et les places finies où ρ est ramifié. De plus, si λ est une place finie de k au-dessus de ℓ, on demande que S contienne toutes les places de k au-dessus de ℓ. Dire que ρ est rationnel revient à dire que $\chi_\rho(\mathbf{x}) \in E^*$ pour tout $\mathbf{x} \in \mathfrak{I}_k$ de la forme $\mathbf{x}=(x_v)$ avec

$$x_v = \begin{cases} 1 & \text{pour } v \neq v_o, \\ \pi_{v_o} & \text{pour } v = v_o, \end{cases}$$

chaque fois que $v_o \notin S$, et que π_{v_o} est une uniformisante en v_o. Mais χ_ρ n'est pas ramifié en v_o, donc cette condition entraîne que $\chi_{\rho v_o}(k_{v_o}^*) \subset E^*$ pour tout $v_o \notin S$. L'adhérence du sous-groupe de $\mathfrak{I}_k$ engendré par les $k_{v_o}^*$, $v_o \notin S$ est $\mathfrak{I}_k^S$; donc ρ est rationnel sur E si et seulement si $\chi_\rho(\mathfrak{I}_k^S) \subset E^*$.

Il suffit alors d'appliquer le corollaire 2.6 si λ est une place finie de E ; si λ est une place archimédienne, χ est de type (A_o) car son noyau contient $\mathfrak{I}_k^o = \mathbb{R}_+^{*r_1} \times \mathbb{C}^{*r_2}$.

Nous allons voir maintenant un peu plus précisément ce que signifie la condition que ρ est localement algébrique.

g) Homomorphismes algébriques.

Soient k un corps de nombres, E un corps de caractéristique 0, et $f:k^* \longrightarrow E^*$ un homomorphisme. On choisit une base $\{e_1,\dots,e_d\}$ de k sur $\mathbb{Q}$, avec $d=[k:\mathbb{Q}]$, on désigne par $\sigma_1,\dots,\sigma_d$ les plongements de k dans une clôture algébrique de E, et on suppose que E contient les $\sigma_i(k)$, $(1\leq i\leq d)$.

Lemme 3.2.- *Les deux assertions suivantes sont équivalentes :*

(i) *Il existe une fraction rationnelle* $A\in E(X_1,\dots,X_d)$ *telle que, pour tout* $(x_1,\dots,x_d)\in\mathbb{Q}^d$, $(x_1,\dots,x_d)\neq(0,\dots,0)$, *la valeur* $A(x_1,\dots,x_d)$ *soit bien définie, et que l'on ait*

$$f(x_1e_1+\dots+x_de_d)=A(x_1,\dots,x_d).$$

(ii) *Il existe des entiers* $n_1,\dots,n_d$ *dans* $\mathbb{Z}$ *tels que, pour tout* $\alpha\in k^*$, *on ait*

$$f(\alpha)=\prod_{i=1}^{d}(\sigma_i\alpha)^{n_i}.$$

Démonstration.- L'implication (ii)$\Rightarrow$(i) est banale : on prend

$$A(X_1,\dots,X_d)=\prod_{i=1}^{d}\Big(\sum_{j=1}^{d}X_j.\sigma_ie_j\Big)^{n_i}.$$

Démontrons (i)$\Rightarrow$(ii). On change de variables : en posant

$$Z_i=\sum_{j=1}^{d}X_j.\sigma_ie_j, \qquad (1\leq i\leq d),$$

on définit $B\in E(Z_1,\dots,Z_d)$ par la condition

$$B\Big(\sum_{j=1}^{d}X_j.\sigma_1e_j,\dots,\sum_{j=1}^{d}X_j.\sigma_de_j\Big)=A(X_1,\dots,X_d).$$

Ainsi

$$f(\alpha)=B(\sigma_1\alpha,\dots,\sigma_d\alpha) \qquad \text{pour tout } \alpha\in k^*.$$

La fraction rationnelle

$$\frac{B(Z_1W_1,\dots,Z_dW_d)}{B(Z_1,\dots,Z_d).B(W_1,\dots,W_d)}-1$$

dans le corps $E(Z_1,\dots,Z_d,\ W_1,\dots,W_d)$, est identiquement nulle sur

$$\{(\sigma_1\alpha_1,\ldots,\sigma_d\alpha_1,\ \sigma_1\alpha_2,\ldots,\sigma_d\alpha_2)\ ;\ (\alpha_1,\alpha_2)\in k^*\times k^*\},$$

qui est l'image de $k^*\times k^*$ dans $E^{*d}\times E^{*d}$ par le plongement $\sigma\times\sigma$. Or l'image de k^* par le plongement σ est dense pour la topologie de Zariski dans E^{*d} (c'est-à-dire que si un polynôme en d variables à coefficients dans E s'annule sur σk^*, alors ce polynôme est identiquement nul : il suffit de repasser à la base $e_1,\ldots,e_d$ pour le voir). On en déduit

$$B(Z_1W_1,\ldots,Z_dW_d)=B(Z_1,\ldots,Z_d).B(W_1,\ldots,W_d).$$

Pour $1\leq i\leq d$, soit $R_i\in E(T)$ la fraction rationnelle définie par

$$R_i(T)=B(1,\ldots,1,T,1,\ldots,1),$$

où T se trouve à la i-ème place. On a donc

$$B(Z_1,\ldots,Z_d)=\prod_{i=1}^{d} R_i(Z_i),$$

et

$$R_i(T.T')=R_i(T).R_i(T'),\qquad (1\leq i\leq d).$$

Il est facile de résoudre cette équation fonctionnelle : les seuls zéros et pôles de R_i sont 0 et ∞, donc il existe $n_i\in\mathbb{Z}$ tel que $R_i(T)=T^{n_i}$.

Définition. Un homomorphisme $f:k^*\longrightarrow E^*$ vérifiant les propriétés équivalentes du lemme 3.2 est dit *algébrique*.

Soit maintenant χ un homomorphisme continu du groupe C_k des classes d'idèles de k dans $\mathbb{C}_\ell^*$. Soit $\mathfrak{M}$ un idéal entier de k, multiple du conducteur $\mathfrak{F}$ de χ. Rappelons que pour chaque place archimédienne v de k, χ est trivial sur la composante connexe neutre k_v^{*o} ($=\mathbb{R}_+^*$ ou $\mathbb{C}^*$) de k_v^*. Soit S l'ensemble formé des places archimédiennes de k, et des places finies v de k distinctes de ℓ, telles que $v(\mathfrak{M})>0$. Le noyau de χ contient donc le sous-groupe suivant de $\mathfrak{I}_k$:

$$U_{\mathfrak{M}}=\prod_{v\neq\ell} U_{\mathfrak{M}v},$$

où

$$U_{\mathfrak{M}v}=\begin{cases} k_v^{*o} & \text{pour } v \text{ infinie,} \\ \{u\in A_v^* \ ; \ v(u-1)\geq v(\mathfrak{M})\} & \text{pour } v\in S,\ v \text{ finie,} \\ A_v^* & \text{pour } v\notin S,\ v\neq \ell. \end{cases}$$

On a défini (cf §2.d) un homomorphisme $\tilde{\chi}$ de I_k^S dans $\mathbb{C}_\ell^*$, où I_k^S est le groupe des idéaux fractionnaires premiers à S :

$$\begin{array}{ccc} \mathfrak{I}_k^S & \xrightarrow{\ \chi\ } & \mathbb{C}_\ell^* \\ \downarrow & & \uparrow \tilde{\chi} \\ \mathfrak{I}_k^S/U^S & \xrightarrow{\ \sim\ } & I_k^S \end{array}$$

(U^S est contenu dans $U_{\mathfrak{M}}$). On définit donc un homomorphisme f de $k_+^*(\mathfrak{M})$ dans $\mathbb{C}_\ell^*$ par $f(\alpha)=\tilde{\chi}((\alpha))$.

Il est alors clair que f *s'étend en un homomorphisme algébrique de* k^* *dans* $\mathbb{C}_\ell^*$ *si et seulement si* χ *est de type* (A_o). On dit encore que le caractère de Hecke ℓ-adique $\tilde{\chi}$ est *algébrique*.

h) Classes d'idéaux généralisées.

Soit E le groupe des unités de k, et soit $E_{\mathfrak{M}}=E\cap U_{\mathfrak{M}}$. On a une suite exacte

$$1 \longrightarrow k^*/E_{\mathfrak{M}} \longrightarrow \mathfrak{I}_k/U_{\mathfrak{M}} \longrightarrow C_{\mathfrak{M}} \longrightarrow 1,$$

où $C_{\mathfrak{M}}=\mathfrak{I}_k/k^*U_{\mathfrak{M}}$ ($C_{\mathfrak{M}}$ est aussi le quotient de $\mathbf{C}_k$ par l'image de $U_{\mathfrak{M}}$ dans $\mathbf{C}_k$). Le groupe $C_{\mathfrak{M}}$ est fini : il est isomorphe au groupe des classes d'idéaux modulo $\mathfrak{M}$.

D'autre part les ouverts $U_{\mathfrak{M}}/\mathfrak{I}_k^o$ forment un système fondamental de voisinage de 1 dans $\mathfrak{I}_k/\mathfrak{I}_k^o$; le sous-groupe $k^*U_{\mathfrak{M}}$ de $\mathfrak{I}_k$ est le groupe de rayon $\mathfrak{M}$; le corps de rayon $\mathfrak{M}$ est son corps fixe $k_{\mathfrak{M}}$ -extension abélienne de k associée par la théorie de Galois et la théorie du corps de classes-.

Voir à ce sujet : S. Lang, A.N.T., Chap.VII ; J-P. Serre, McGill, p.II.8. On pourra consulter aussi le §5 : *caractères de Hecke* du Chapitre *Aplications de la formule des traces aux sommes trigonométriques* par P. Deligne dans S.G.A.4½. Pour l'analogue complexe, voir A. Weil, Tokyo-Nikko.

§4. Représentations λ-adiques.

Soient G le groupe de Galois de l'extension abélienne maximale d'un corps de nombres k, et ρ un homomorphisme continu de G dans GL(V), où V est un espace vectoriel de dimension finie sur un corps E_λ, complété en une place λ d'un corps de nombres E. Nous montrons que, quand ρ est semi-simple, ρ est "localement algébrique" sur E si et seulement si les valeurs propres de l'image par ρ des Frobenius aux places finies non ramifiées sont dans une extension finie de E. Cela résulte immédiatement du théorème 3.1, une fois que les objets considérés ont été définis.

Les références sont : J-P. Serre, Abelian ℓ-adic representations and elliptic curves, et G. Henniart, Sém. T.d.N. 1980-81.

a) Représentations linéaires de groupes compacts.

Soit K un corps local de caractéristique nulle : K sera $\mathbb{R}$, $\mathbb{C}$, ou bien une extension finie d'un corps $\mathbb{Q}_\ell$, avec ℓ premier. Soit V un espace vectoriel de dimension finie sur K. On désigne par λ la valuation de K. On considère le groupe GL(V) des automorphismes K-linéaires de V ; on le munit de la topologie λ-adique induite par celle des endomorphismes K-linéaires de V.

Soit G un groupe compact. Une *représentation λ-adique* est un homomorphisme continu de G dans GL(V) ; autrement dit c'est une application $\rho : G \longrightarrow GL(V)$ telle que

1) $\rho_{st}=\rho_s \circ \rho_t$, $\rho_1=1$, $\rho_{s^{-1}}=\rho_s^{-1}$ pour tout $(s,t)\in G^2$;

2) l'application $G\times V \longrightarrow V$ qui envoie (s,x) sur $\rho_s(x)$ est continue.

Le *degré* de la représentation ρ est la dimension du K- espace vectoriel V. Ainsi une représentation de degré 1 n'est autre qu'un *caractère* de G, c'est-à-dire un homomorphisme continu de G dans K^*.

Un sous-espace vectoriel W de V est dit *stable* si $\rho_s(W)\subset W$ pour tout $s\in G$. Alors la restriction ρ_s^W de ρ_s à W est un élément de $GL(W)$, et $\rho^W: G \longrightarrow GL(W)$ est une représentation λ-adique de G dans W, appelée *sous-représentation* de ρ (ou de V).

La représentation ρ est *irréductible* si $V\neq 0$ et si les seuls sous-espaces stables par ρ sont 0 et V.

Pour une représentation linéaire ρ, les conditions suivantes sont équivalentes :

(i) V est somme directe de sous-espaces stables irréductibles ;

(ii) tout sous-espace W stable par ρ admet un supplémentaire dans V stable par ρ.

Si ces conditions sont satisfaites, on dira que ρ est *semi-simple*. Quand $K=\mathbb{C}$, toute représentation d'un groupe compact est semi-simple (cf. J-P. Serre, Représentations linéaires des groupes finis, Chap.I §4). Mais la représentation de $\mathbb{Z}_\ell$ dans $V=\mathbb{Q}_\ell^2$ donnée sous-forme matricielle par

$$x \longrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

n'est pas semi-simple : la droite $\mathbb{Q}_\ell\times 0$ est stable, mais n'admet pas de supplémentaire stable.

On dit que ρ est une représentation *abélienne* si l'image de ρ est un sous-groupe abélien de $GL(V)$. Cela équivaut à dire que ρ se factorise en une représentation du groupe abélien $G^{ab}=G/G^c$ (où G^c est l'adhérence du groupe des commutateurs) dans V.

Sur un corps algébriquement clos, toute représentation abélienne irréductible est de degré 1. Plus précisément, quand K' est une extension de K et V' le K'-espace vectoriel obtenu par extension des scalaires de K à K', à une représentation ρ de G dans V on associe de manière naturelle une représentation ρ' de G dans V' ; alors si ρ est une représentation λ-adique abélienne semi-simple de dimension n, en prenant pour K' une extension de K dans laquelle le polynôme caractéristique de ρ se décompose complétement, le lemme de Schur montre qu'il existe une base de V dans

laquelle ρ' est donnée par n caractères continus $\rho_1,\ldots,\rho_n$ à valeurs dans K'^*. En particulier ρ' est encore semi-simple.

b) Représentations galoisiennes.

Les représentations λ-adiques qui nous intéresseront seront celles des groupes de Galois absolus d'un corps de nombres k, munis de la topologie de Krull. Nous les supposerons abéliennes, ce qui équivaut à dire qu'elles se factorisent par $G(k^{ab}/k)$.

Soit v une place finie de k ; on dit que ρ est *non ramifiée* en v si $\rho(I_v)=\{1\}$, où I_v est le groupe d'inertie en v (c'est-à-dire en n'importe quelle place de k^{ab} au dessus de v).

Soit $H=\mathrm{Ker}\rho$; c'est un sous-groupe fermé de G ; soit L son corps fixe, extension abélienne de k. Alors ρ est non ramifiée en v si et seulement si la place v n'est pas ramifiée dans l'extension L/k. En effet, v est non ramifiée dans L/K si et seulement si le groupe d'inertie I_v de L/k est trivial. Mais ρ induit une injection de $G/H\simeq G(L/k)$ dans K^*, donc $\rho(I_v)=\{1\}$ si et seulement si $I_v=\{1\}$.

Si ρ est non ramifiée en v, alors la restriction de ρ au sous-groupe de décomposition D_v induit un homomorphisme $D_v/I_v \longrightarrow GL(V)$. L'image $F_{v\rho}=\rho(F_v)$ du Frobenius F_v est le *Frobenius de* ρ *en* v. On définit

$$P_{v\rho}(T)=\det(1-F_{v\rho}T) \in E_\lambda[T].$$

c) Représentations rationnelles.

Soient k et E deux corps de nombres, G_k le groupe de Galois absolu de k, λ une place de E, et E_λ le complété de E en λ.

Nous appellerons *représentation* E_λ*-adique* de G_k tout homomorphisme continu de G_k dans GL(V), quand V est un E_λ-espace vectoriel de dimension finie.

On dit que ρ est *rationnelle* sur E s'il existe un ensemble fini S de places finies de k tel que pour toute place finie v de k n'appartenant pas à S, ρ soit non ramifiée en v, et que $P_{v\rho} \in E[T]$.

d) Représentations localement algébriques.

Soient k un corps de nombres, $\rho : G(\overline{k}/k)^{ab} \longrightarrow GL(V)$ une représentation abélienne λ-adique semi-simple de k. Sur $\mathbb{C}_\ell$, ρ est diagonalisable, et est donnée par une somme directe de caractères continus $\psi_1, \ldots, \psi_h$ de $G = G(\overline{k}/k)^{ab}$ dans $\mathbb{C}_\ell^*$.

On dira que ρ est *localement algébrique* si chacun de ces caractères ψ_i est localement algébrique. Cela signifie donc que pour chaque i, si on compose ψ_i avec l'application de réciprocité et le plongement de $\prod_{v|\ell} k_v^*$ dans $\mathfrak{I}_k$, l'homomorphisme continu $\prod_{v|\ell} k_v^* \longrightarrow \mathbb{C}_\ell^*$ ainsi obtenu est de type (A_0) (cf. §2.a). Comme E_λ est un $\mathbb{Q}_\ell$-espace vectoriel de dimension finie, toute représentation E_λ-adique peut aussi être considérée comme une représentation $\mathbb{Q}_\ell$-adique. Alors ρ est localement algébrique comme représentation λ-adique si et seulement si ρ est localement algébrique comme représentation ℓ-adique.

Théorème 4.1.- *Soit ρ une représentation E_λ-adique abélienne semi-simple rationnelle sur E. Alors ρ est localement algébrique.*

Démonstration.- (D'après G.Henniart, Sém.DPP ; ici encore les détails ont été écrits par D.Roy).

Plongeons les corps k, E et E_λ dans $\mathbb{C}_\ell$, et notons ρ' la composée

$$G(k^{ab}/k) \xrightarrow{\rho} GL(V) \longrightarrow GL(V \otimes_{E_\lambda} \mathbb{C}_\ell).$$

Comme ρ' est semi-simple, il existe une base $\mathcal{B}$ de $V \otimes_{E_\lambda} \mathbb{C}_\ell$ telle que

$$[\rho'(\sigma)]_{\mathcal{B}} = \mathrm{diag}(\Psi_1(\sigma), \ldots, \Psi_m(\sigma)),$$

où $\Psi_1, \ldots, \Psi_m$ sont des caractères continus de $G(k^{ab}/k)$ dans $\mathbb{C}_\ell^*$. En composant les Ψ_i avec l'application d'Artin, on obtient des homomorphismes

continus $\chi_1,\dots,\chi_m$ de C_k à valeurs dans $\mathbb{C}_\ell^*$. Dire que ρ n'est pas ramifié en une place finie v de k qui ne divise pas ℓ revient à dire qu'aucun des χ_i n'est ramifié en v. Pour une telle place on obtient

$$[\rho'(F_v)]_{\mathcal{B}} = \mathrm{diag}(\tilde{\chi}_1(\mathfrak{p}_v),\dots,\tilde{\chi}_m(\mathfrak{p}_v)),$$

où $\tilde{\chi}_i$ désigne le Grössencharakter de k associé à χ_i, et $\mathfrak{p}_v$ l'idéal de k associé à v. Si ρ est rationnelle sur E, il existe un ensemble fini S de places de k contenant les places archimédiennes, celles au-dessus de ℓ, et celles en lesquelles ρ se ramifie, tel que

$$\det(XI-\rho(F_v))=\prod_{i=1}^{n}(X-\tilde{\chi}_i(\mathfrak{p}_v))\in E[X]$$

pour toute place v en dehors de S. Alors les valeurs des $\tilde{\chi}_i$ sur I_k^S sont algébriques. Par le corollaire 2.5, cela implique que les χ_i sont de type (A). Il existe donc un entier $N\geq 1$, des entiers n_{ij}, et un idéal entier $\mathfrak{M}$ de k divisible par $\ell^{2+v_\ell(N)}$, dont le support contient S, tels que

$$\tilde{\chi}_i((\alpha))=\prod_{j=1}^{n}\sigma_j(\alpha)^{n_{ij}/N}\quad\text{pour tout}\quad \alpha\in k_+^*(\mathfrak{M}),$$

où $\sigma_1,\dots,\sigma_n$ désignent les isomorphismes de k dans $\mathbb{C}_\ell$. On va montrer que N divise chacun des n_{ij}, ce qui entraînera que les χ_i sont de type (A_0), et que ρ est localement algébrique.

Supposons au contraire que N ne divise pas tous les n_{ij}. Soit K la fermeture galoisienne du compositum kE dans $\mathbb{C}_\ell$. Par le théorème de la progression arithmétique, il existe $\gamma\in K_+^*(\mathfrak{M})$ tel que l'idéal engendré par γ soit premier, de degré 1 et d'ordre 1 sur $\mathbb{Q}$, et ne divise aucun des idéaux $\mathfrak{p}_v$, $v\in S$. Alors le nombre $\beta=N_{K/k}(\gamma)$ appartient à $k_+^*(\mathfrak{M})$, et l'idéal de k qu'il engendre s'écrit $(\beta)=\mathfrak{p}_v$, où v est une place de k n'appartenant pas à S. Comme les conjugués de γ sont multiplicativement indépendants, et que le quotient de K^* par le sous-groupe qu'ils engendrent est sans torsion, les nombres $\sigma_1(\beta),\dots,\sigma_n(\beta)$ sont aussi multiplicativement indépendants, et le quotient de K^* par le sous-groupe qu'ils engendrent est aussi sans torsion. En vertu de l'hypothèse que N ne divise pas tous les n_{ij}, cela implique que les $\tilde{\chi}_i((\beta))$ n'appartiennent pas tous à K^*. Quitte à permuter les χ_i, on

peut supposer $\tilde{\chi}_1((\beta))\notin K^{*}$. Alors le nombre $\tilde{\chi}_1((\beta))=\tilde{\chi}_1(\mathfrak{p}_v)$ admet un autre conjugué sur K, qui est de la forme $\tilde{\chi}_i((\beta))=\tilde{\chi}_i(\mathfrak{p}_v)$, pour un certain indice i. Comme $\tilde{\chi}_1((\beta))^N\in K$, on doit avoir $\tilde{\chi}_1((\beta))^N=\tilde{\chi}_i((\beta))^N$. Cela implique $n_{1j}=n_{ij}$ pour $1\leq j\leq n$, et par suite $\tilde{\chi}_1((\beta))=\tilde{\chi}_i((\beta))$, ce qui donne la contradiction.

Références du chapitre II.

J.-P. SERRE.- Abelian ℓ-adic representations and elliptic curves ; Benjamin, 1968 (McGill University Lecture Notes).

G. HENNIART.- Représentations ℓ-adiques abéliennes ; Séminaire de théorie des nombres, Paris 1980-81, (Séminaire Delange-Pisot-Poitou), Progress in Math., 22, Birkhäuser Verlag 1982, 107-126.

La littérature concernant les représentations ℓ-adiques est assez abondante. Voir en particulier le chapitre G15 de : W.J. LeVeque, Reviews in Number Theory, A.M.S. 1974, vol.2 ; et les chapitres F32 et G15 de R. Guy, Reviews in Number Theory 1973-83, A.M.S. 1984, vol.2.

CHAPITRE III

LA CONJECTURE DE LEOPOLDT.

§1. Unités d'un corps de nombres.

Dans ce premier paragraphe nous présentons quelques résultats classiques concernant les unités d'un corps de nombres : théorèmes de Dirichlet, de Minkowski, formule du nombre de classes pour des corps abéliens sur $\mathbb{Q}$, unités des corps C.M.. Les nombres p-adiques n'interviendront que dans les paragraphes suivants.

a) Le théorème des unités de Dirichlet.

Soient k un corps de nombres, $\mathcal{O}=\mathcal{O}_k$ l'anneau des entiers de k, et $E=\mathcal{O}^*$ le groupe multiplicatif des éléments inversibles de $\mathcal{O}$. Par abus de langage, les éléments de E sont appelés *unités* de k.

Le sous-groupe de torsion de k^* (ou de E, c'est le même) est formé des racines de l'unité qui appartiennent à k. On le notera $W=W_k$

Il est facile de voir que W est un groupe fini : une racine d-ième de l'unité engendre un corps de degré $\varphi(d)$, où φ est l'indicatrice d'Euler, et $\varphi(d)$ tend vers l'infini quand d tend vers l'infini. On en déduit que W est un groupe cyclique (pour tout corps K, tout sous-groupe fini de K^* est cyclique). On notera $w=w_k$ son ordre. Remarquons déjà que w est pair, puisque $-1\in W$.

Notons comme d'habitude $\sigma=(\sigma_1,\ldots,\sigma_{r_1+r_2})$ le plongement canonique de k^* dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. Rappelons que l'image $\sigma(\mathcal{O})$ de $\mathcal{O}$ est un sous-groupe discret de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. Cela résulte simplement du fait qu'un ensemble d'éléments de $\mathcal{O}$ dont on borne toutes les valeurs absolues des conjugués est fini. De plus, comme $\sigma(\mathcal{O})$ est de rang maximal $d=r_1+2r_2$, c'est un réseau de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$.

Le plongement logarithmique est l'homomorphisme λ de k^* dans $\mathbb{R}^{r_1+r_2}$ qui envoie $\alpha\in k^*$ sur

$$(\delta_i \log|\sigma_i\alpha|)_{1\le i\le r_1+r_2},$$

où $\delta_i=1$ pour $1\le i\le r_1$ (c'est-à-dire pour σ_i réelle) et $\delta_i=2$ pour $r_1<i\le r_1+r_2$ (c'est-à-dire pour σ_i complexe).

Montrons que $\mathcal{O}\cap\mathrm{Ker}\lambda=W$. Pour $\zeta\in W$ on a évidemment $\lambda(\zeta)=0$; inversement, si $\xi\in\mathcal{O}$, $\xi\neq 0$ est tel que $|\sigma_i\xi|\le 1$ pour $1\le i\le r_1+r_2$, alors le sous-groupe engendré par ξ est fini (son image par σ est bornée), donc $\xi\in W$.

En particulier quand u et v sont des unités de k, la condition $\lambda(u)=\lambda(v)$ équivaut à $u/v\in W$.

L'image de E par λ est contenue dans l'hyperplan H d'équation

$$x_1+\ldots+x_{r_1+r_2}=0$$

de $\mathbb{R}^{r_1+r_2}$, et le fait que tout sous-ensemble borné de E soit fini montre que $\lambda(E)$ est un sous-groupe discret de H. En particulier $\lambda(E)$ est un $\mathbb{Z}$-module libre de rang $\le r$, avec $r=r_1+r_2-1$. Ce nombre r est le *nombre de Dirichlet* de k. Comme $\lambda(E)$ est discret, son rang est la dimension du sous-espace vectoriel de $\mathbb{R}^{r_1+r_2}$ qu'il engendre.

Théorème 1.1.(Dirichlet).- *Le rang de* $\lambda(E)$ *est* r.

Autrement dit l'espace vectoriel engendré par $\lambda(E)$ est H. Voici un schéma de démonstration. On utilisera le lemme facile suivant :

Lemme 1.2.- *Soient* V *un sous-espace vectoriel de* $\mathbb{R}^n$, *et* G *un sous-groupe de* V. *Alors* G *engendre* V *sur* $\mathbb{R}$ *si et seulement s'il existe une partie bornée* B *de* V *telle que* $V=\bigcup_{g\in G}(B+g)$.

On désigne par Δ la valeur absolue du discriminant de k, et on pose $\kappa=(2/\pi)^{r_2}\Delta^{1/2}$. Le point intéressant n'est pas la valeur explicite de κ, mais le

fait qu'il existe une constante ne dépendant que du corps k vérifiant le lemme 1.3 ci-dessous.

Le théorème de Minkowski (cf. par exemple Samuel, Théorie algébrique des nombres, §4.1) va nous permettre de montrer :

Lemme 1.3.- *Soient* $t_1,\dots,t_d$ *des nombres réels positifs vérifiant*

$$t_1\dots t_d=\kappa \qquad \text{et} \qquad t_{r_1+r_2+j}=t_{r_1+j}, \qquad (1\le j\le r_2).$$

Alors ils existe $\alpha\in\mathcal{O}$, $\alpha\neq 0$, *tel que*

$$|\sigma_i\alpha|\le t_i \qquad \text{pour} \quad 1\le i\le d.$$

Démonstration.-Soit $\mathcal{C}$ le compact de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ défini par

$$|x_i|\le t_i \quad \text{pour} \quad 1\le i\le r_1 \qquad \text{et} \qquad |z_j|\le t_j \quad \text{pour } r_1<j\le r_1+r_2.$$

Sa mesure de Lebesgue est

$$\mu(\mathcal{C}) = \prod_{i=1}^{r_1}(2t_i).\prod_{i=r_1+1}^{r_1+r_2}(\pi t_i^2) = 2^{r_1}\pi^{r_2}\kappa = 2^{r_1+r_2}\Delta^{1/2}.$$

Mais le volume $v(\mathcal{O})$ du quotient de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ par $\sigma(\mathcal{O})$ (c'est-à-dire la mesure de Lebesgue d'une maille fondamentale de $\sigma(\mathcal{O})$) est $2^{-r_2}\Delta^{1/2}$ (cf. Samuel, op. cit., §4.2). L'inégalité $\mu(\mathcal{C})\ge 2^d v(\mathcal{O})$ assure $\mathcal{C}\cap\sigma(\mathcal{O})\neq\{0\}$ (théorème de Minkowski). Il suffit alors de prendre $\alpha\in\mathcal{O}$, $\alpha\neq 0$, tel que $\sigma\alpha\in\mathcal{C}$.

Remarquons que l'élément α ainsi obtenu vérifie : $1\le N\alpha\le\kappa$, où $N=N_{k/\mathbb{Q}}$ désigne la norme de k sur $\mathbb{Q}$.

Pour terminer la démonstration du théorème de Dirichlet, on prend $x=(x_1,\dots,x_{r_1+r_2})\in H$, on pose $x_{r_2+i}=x_i$ pour $r_1+1\le i\le r_1+r_2$, et on utilise le lemme 1.3 avec

$$t_i=\kappa^{1/d}e^{x_i}, \qquad (1\le i\le r_1),$$

$$t_i=\kappa^{1/d}e^{x_i/2}, \qquad (r_1<i\le d).$$

En écrivant $|N\alpha|\ge 1$, on obtient une minoration des $\sigma_i\alpha$:

$$|\sigma_i\alpha|\ge \frac{1}{\kappa'}.e^{x_i}, \qquad (1\le i\le r_1),$$

$$|\sigma_i\alpha|\ge \frac{1}{\kappa'}.e^{x_i/2}, \qquad (r_1<i\le d),$$

avec $\kappa'=\kappa^{1-1/d}$. Ainsi

$$|x_i-\delta_i \log|\sigma_i\alpha||\leq\kappa'', \qquad (1\leq i\leq r_1+r_2)$$

avec $\kappa''=2\log\kappa'$. Mais il n'y a qu'un nombre fini d'idéaux (α) de norme $\leq\kappa$. On peut donc écrire $\alpha=\epsilon\gamma$, avec $\epsilon\in E$ et $\gamma\in\mathcal{G}$, où $\mathcal{G}$ est un sous-ensemble fini de k^*, indépendant de $x\in H$.

Posons $R=\kappa''+\max_{\gamma\in\mathcal{G}}\|\lambda(\gamma)\|$, où, pour $x=(x_1,\ldots,x_{r_1+r_2})\in\mathbb{R}^{r_1+r_2}$, on pose $\|x\|=\max_{1\leq i\leq r_1+r_2}|x_i|$. Soit B l'intersection de H avec la boule $\|x\|\leq R$ de $\mathbb{R}^{r_1+r_2}$. On a montré

$$H=\bigcup_{\epsilon\in E}(B+\lambda(\epsilon)),$$

et le lemme 1.2 permet de conclure.

Nous avons défini dans l'introduction ce qu'est un système indépendant d'unités, et un système fondamental d'unités de k. Nous noterons $R(\eta_1,\ldots,\eta_r)=R_k(\eta_1,\ldots,\eta_r)$ le régulateur d'un système indépendant d'unités $\eta_1,\ldots,\eta_r$ (avec $r=r_1+r_2-1$).

Montrons que si E' est le sous-groupe de E engendré par $\eta_1,\ldots,\eta_r$ et W, et si $\epsilon_1,\ldots,\epsilon_r$ est un système fondamental d'unités, alors le quotient des régulateurs $R(\eta_1,\ldots,\eta_r)/R(\epsilon_1,\ldots,\epsilon_r)$ est égal à l'indice $[E:E']$ de E' dans E.

On écrit

$$\eta_i=\zeta_i\cdot\prod_{j=1}^{r}\epsilon_j^{a_{ij}}, \qquad (1\leq i\leq r),$$

avec $\zeta_i\in W$ et $a_{ij}\in\mathbb{Z}$. On a

$$R(\eta_1,\ldots,\eta_r)/R(\epsilon_1,\ldots,\epsilon_r)=|\det(a_{ij})|\ ;$$

soient P et Q deux matrices $r\times r$ à coefficients dans $\mathbb{Z}$ de déterminant ±1 telles que $P.(a_{ij}).Q$ soit diagonale, et soit $(d_1,\ldots,d_r)$ la diagonale. On a $|\det(a_{ij})|=|d_1\ldots d_r|$; mais $E/E'\simeq\mathbb{Z}/d_1\mathbb{Z}\times\ldots\times\mathbb{Z}/d_r\mathbb{Z}$, d'où le résultat.

Comme $\delta_1+\ldots+\delta_{r_1+r_2}=d$ et que

$$\sum_{i=1}^{r_1+r_2}\delta_i\log|\sigma_i\epsilon|=0 \quad \text{pour tout } \epsilon\in E,$$

on voit que si $\eta_1,\ldots,\eta_r$ est un système indépendant d'unités, alors pour tout entier rationnel $\eta_{r+1}>1$, on a

$$R_k(\eta_1,\dots,\eta_r)=(d.\log\eta_{r+1})^{-1}.\left|\det\left(\delta_i\log|\sigma_i\eta_j|\right)_{1\le i,j\le r+1}\right|.$$

D'autre part soit $\rho : E\oplus\mathbb{Z} \longrightarrow \mathbb{R}^{r_1+r_2}$ l'application définie par

$$\rho(\epsilon,n)=\lambda(\epsilon)+(n,\dots,n).$$

L'image de ρ est un réseau de $\mathbb{R}^{r_1+r_2}$ (sous-groupe libre de type fini de rang $r_1+r_2=r+1$). Pour un système fondamental d'unités $\epsilon_1,\dots,\epsilon_r$ de k, la valeur absolue du déterminant $|a_{ij}|_{1\le i,j\le r+1}$ avec

$$a_{ij}=\delta_j\log|\sigma_j\epsilon_i| \qquad \text{pour } 1\le i\le r+1,\ 1\le j\le r$$

$$a_{i,r+1}=1 \qquad \text{pour } 1\le i\le r+1$$

est $(r_1+r_2).R_k$, donc le volume du quotient de $\mathbb{R}^{r_1+r_2}$ par $\rho(E\oplus\mathbb{Z})$ est $(r_1+r_2).R_k$.

Pour en savoir plus sur les régulateurs (supérieurs), voir l'exposé n°644 de C. Soulé au Séminaire Bourbaki, Astérisque 133-134, p.237-253.

Si $k=\mathbb{Q}$ ou si k est un corps quadratique imaginaire, on a $r=0$ et $R_k=1$. Dans tous les autres cas il est vraisemblable que le régulateur R_k est un nombre transcendant : cela résulterait de la conjecture 2.5 de l'introduction sur l'indépendance algébrique de logarithmes de nombres algébriques.

b) Unités de Minkowski.

Du théorème de Dirichlet on déduit :

Lemme 1.4.- *Supposons* $k\neq\mathbb{Q}$ *et aussi que* k *n'est pas un corps quadratique imaginaire. Soit* τ *un plongement de* k *dans* $\mathbb{C}$ *(éventuellement dans* $\mathbb{R}$*). Alors il existe une unité* $\epsilon\in E$ *telle que* $|\tau\epsilon|>1$ *et* $|\sigma_i\epsilon|<1$ *pour tout* i, $1\le i\le d$, *tel que* σ_i *soit différent de* τ *et de* $\overline{\tau}$.

Démonstration.- L'hypothèse sur k signifie que le groupe des unités de k est infini. Soit i_0, $1\le i_0\le r_1+r_2$, tel que σ_{i_0} soit égal à τ ou à $\overline{\tau}$. On sait que l'hyperplan H est réunion des $B+\lambda(\epsilon)$, pour $\epsilon\in E$, où B est l'intersection de H et d'une boule $\|x\|\le R$ (on l'a vu dans la démonstration du théorème de Dirichlet, mais cela résulte aussi du théorème de Dirichlet

combiné avec le lemme 1.2). On choisit un point $x=(x_1,\ldots,x_{r_1+r_2})\in H$ avec $x_i<-R$ pour $1\leq i\leq r_1+r_2$, $i\neq i_0$. Alors il existe $\epsilon\in E$ vérifiant

$$|x_i-\delta_i\log|\sigma_i\epsilon||\leq R \qquad \text{pour } 1\leq i\leq r_1+r_2.$$

On en déduit $\log|\sigma_i\epsilon|<0$ pour $1\leq i\leq r_1+r_2$, $i\neq i_0$. Mais $N\epsilon=1$, donc $\log|\sigma_{i_0}\epsilon|>0$.

Proposition 1.5. (Minkowski)- *Supposons* k *galoisien sur* $\mathbb{Q}$, *et notons* $G=G(k/\mathbb{Q})$. *Il existe une unité* $\epsilon\in E$ *telle que* $\{\sigma\epsilon\ ;\ \sigma\in G\}$ *engendre un sous-groupe d'indice fini de* E.

Démonstration.- Si le groupe des unités est fini, on prend $\epsilon=1$. Sinon, on fixe un plongement de k dans $\mathbb{C}$, ce qui permet d'identifier G avec l'ensemble des plongements de k dans $\mathbb{C}$, et on choisit ϵ comme dans le lemme 1.4 : $|\epsilon|>1$, et $|\sigma\epsilon|<1$ pour σ différent de l'identité et de la conjugaison complexe.

Si k est totalement réel, on a $r=d-1$, $\delta_1=\ldots=\delta_{r+1}=1$, et on pose $\{\sigma_1,\ldots,\sigma_r\}=G-\{1\}$, $\delta=1$, et $\sigma_{r+1}=1$.

Si k est totalement imaginaire, on a $r=\frac{d}{2}-1$, $\delta_1=\ldots=\delta_{r+1}=2$, on pose $\delta=2$, et on prend pour $\{\sigma_1,\ldots,\sigma_{r+1}\}$ des représentants des classes $\neq\{1\}$ de $G/\{1,\tau\}$, avec $\sigma_{r+1}=1$, et τ est la conjugaison complexe. On va vérifier que $R(\sigma_1^{-1}\epsilon,\ldots,\sigma_r^{-1}\epsilon)$ n'est pas nul. Mais

$$R(\sigma_1^{-1}\epsilon,\ldots,\sigma_r^{-1}\epsilon)=\left|\det(a_{ij})_{1\leq i,j\leq r}\right|$$

où

$$a_{ij}=\delta\log|\sigma_i\circ\sigma_j^{-1}(\epsilon)|,\quad (1\leq i\leq r,\ 1\leq j\leq r).$$

On a $a_{ii}=\delta\log|\epsilon|>0$, $(1\leq i\leq r)$, et $a_{ij}<0$ pour $i\neq j$. De plus, comme $\sum_{j=1}^{r} a_{ij}=-\delta\log|\sigma_i^{-1}\epsilon|>0$ pour $1\leq j\leq r$, il ne reste plus qu'à appliquer le lemme suivant :

Lemme 1.6.- *Soit* (a_{ij}) *une matrice* $r\times r$ *à coefficients réels satisfaisant*

$$a_{ii}>0, \qquad 1\leq i\leq r,$$

$$a_{ij}<0, \qquad 1\leq i\neq j\leq r,$$

et

$$\sum_{j=1}^{r} a_{ij}>0, \quad 1\leq i\leq r.$$

Alors $\det(a_{ij})\neq 0$.

Démonstration (Artin).- Supposons le déterminant nul. Soit $\mathbf{x}=(x_1,\ldots,x_r)\in\mathbb{R}^r$, $\mathbf{x}\neq 0$, tel que $\sum_{j=1}^{r} a_{ij}x_j=0$ pour $1\leq j\leq r$. Soit i un indice, $1\leq i\leq r$, tel que $|x_i|=\max_{1\leq j\leq r}|x_j|$. Quitte à remplacer $\mathbf{x}$ par $-\mathbf{x}$, on peut supposer $x_i>0$. On écrit

$$a_{ii}x_i + \sum_{j\neq i} a_{ij}x_j=0,$$

et on majore x_j par x_i, $(1\leq j\leq r,\ j\neq i)$; en tenant compte du fait que $a_{ij}<0$ pour $j\neq i$, on trouve :

$$x_i(a_{ii} + \sum_{j\neq i} a_{ij})\leq 0,$$

ce qui donne la contradiction.

On appelle *unité de Minkowski* d'un corps de nombres galoisien sur $\mathbb{Q}$ toute unité qui engendre avec ses conjugués un sous-groupe d'indice fini du groupe des unités (voir Hasse, Klassenkörpertheorie, pour une autre démonstration de la proposition 1.5).

c) Fonctions L et formule analytique du nombre de classes.

La fonction zêta (de Dedekind) d'un corps de nombres k est définie, pour $\mathrm{Re}(s)>1$, par

$$\zeta_k(s) = \prod_{\mathfrak{p}}(1-N\mathfrak{p}^{-s})^{-1} = \sum_{\mathfrak{A}} N\mathfrak{A}^{-s},$$

où $\mathfrak{p}$ (resp. $\mathfrak{A}$) décrit l'ensemble des idéaux premiers (resp. des idéaux entiers) de k.

Cette fonction se prolonge en une fonction méromorphe dans le demi-plan $\mathrm{Re}(s)>1-\frac{1}{d}$, avec un seul pôle, au point $s=1$, et ce pôle est simple. Le résidu est

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{\Delta}} .$$

Rappelons que $R=R_k$ est le régulateur de k, Δ la valeur absolue du discriminant, w l'ordre de W (sous-groupe de torsion de k^*) ; enfin h est le nombre de classes de k (cf. Lang, A.N.T., Chap.8 §2).

Un *caractère de Dirichlet* est une application χ de $\mathbb{Z}$ dans $\mathbb{C}$ telle qu'il existe un entier $n\in\mathbb{Z}$, $n\neq 0$, (on dira que χ est un caractère *modulo* n) vérifiant, pour tout $a\in\mathbb{Z}$:

$\chi(a)$ ne dépend que de la classe de a modulo n ;

$\chi(a)\neq 0$ si et seulement si $(a,n)=1$;

$\chi(a.b)=\chi(a).\chi(b)$ pour tout $(a,b)\in\mathbb{Z}^2$.

Autrement dit, pour $|n|\geq 2$, on part d'un homomorphisme $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, et on le remonte à $\mathbb{Z}$ en le prolongeant par 0 (tandis que pour $n=\pm 1$, χ est l'application constante égale à 1).

Si m est un multiple de n, un caractère χ modulo n *induit* un caractère χ' modulo m défini par

$$\chi'(a)= \chi(a) \qquad \text{si} \quad (a,m)=1,$$

$$\chi'(a)= 0 \qquad \text{si} \quad (a,m)\neq 1.$$

Cela revient à composer l'homomorphisme $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ avec la surjection canonique $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

Un caractère modulo n est dit *primitif* s'il n'est pas induit par un caractère modulo un diviseur de n ; on dit alors que n est le *conducteur* de χ. Quand χ_1 et χ_2 sont deux caractères primitifs, de conducteurs f_1 et f_2 respectivement, il existe un unique caractère primitif χ, de conducteur f divisant f_1f_2, tel que $\chi(a)=\chi_1(a).\chi_2(a)$ pour tout a premier à f_1f_2. On le note $\chi_1.\chi_2$. On forme ainsi le groupe abélien des caractères primitifs ; l'élément neutre est le caractère trivial χ^0 (seul caractère primitif de

conducteur 1), qui vérifie $\chi^o(a)=1$ pour tout $a\in\mathbb{Z}$ avec $a\neq 0$. L'inverse du caractère primitif χ est le caractère $\overline{\chi}$ (où $\overline{\ }$ est la conjugaison complexe), qui a le même conducteur que χ.

A un caractère de Dirichlet χ on associe une série L :

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s},$$

qui converge absolument pour $Re(s)>1$.

Pour $Re(s)>1$, la fonction L admet un produit eulérien

$$L(s,\chi)=\prod_{p}(1-\chi(p).p^{-s})^{-1}\ ;$$

en particulier $L(s,\chi)\neq 0$ pour $Re(s)>1$.

Pour $\chi\neq\chi^o$, on peut prolonger $L(s,\chi)$ en une fonction entière dans $\mathbb{C}$, alors que la fonction zêta de Riemann $L(s,\chi^o)=\zeta(s)=\zeta_{\mathbb{Q}}(s)$ se prolonge en une fonction méromorphe dans $\mathbb{C}$, avec un seul pôle ; comme nous le savons déjà, ce pôle est le point $s=1$, il est simple, et le résidu vaut 1.

Les valeurs de $L(s,\chi)$ au point $s=1$ (pour $\chi\neq\chi^o$) sont particulièrement intéressantes : on trouve

$$L(1,\chi)=-\frac{\tau(\chi)}{f}.\sum_{\substack{a=1\\(a,f)=1}}^{f}\overline{\chi}(a)\log|1-\zeta^a| \qquad \text{si } \chi(-1)=1,\ \chi\neq\chi^o$$

et

$$L(1,\chi)=-\frac{\tau(\chi)}{f}.\frac{\pi}{if}.\sum_{a=1}^{f}\overline{\chi}(a).a \qquad \text{si } \chi(-1)=-1,$$

où f est le conducteur de χ, $\zeta=e^{2i\pi/f}$, et $\tau(\chi)=\sum_{a=1}^{f}\chi(a)\zeta^a$ (*somme de Gauss*).

Un des arguments essentiels du théorème de la progression arithmétique de Dirichlet consiste à montrer $L(1,\chi)\neq 0$ pour tout $\chi\neq\chi^o$. On peut le voir ainsi : un caractère de Dirichlet Ψ modulo n peut être considéré comme un homomorphisme de $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ dans $\mathbb{C}^*$, où ζ est une racine primitive n-ième de l'unité. Soit k le corps fixé par le noyau de Ψ, et soit X le groupe engendré par Ψ. Alors

$$\zeta_k(s)=\chi\prod_{\chi\in X}L(s,\chi).$$

Comme les fonctions $\zeta_k(s)$ et $\zeta(s)=L(s,\chi^o)$ ont chacune un pôle simple au point $s=1$, il en résulte $L(1,\chi)\neq 0$ pour $\chi\neq\chi^o$, et la *formule analytique du nombre de classes* s'écrit

$$\prod_{\chi\neq\chi^o} L(1,\chi)= \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{\Delta}} .$$

Quand χ est pair ($\chi(-1)=1$, $\chi\neq\chi^o$), le fait que $L(1,\chi)$ ne soit pas nul doit pouvoir se déduire du théorème de Baker (Introduction, théorème 2.2), mais cela n'est pas immédiat car les $\log|1-\zeta^a|$, $(1\leq a\leq f, (a,f)=1)$ ne sont pas toujours linéairement indépendants sur $\mathbb{Q}$. Ils le sont quand f est une puissance d'un nombre premier (cf. Lang, Cyclotomic fields, Ch.3 §5 ; Washington, Introduction to cyclotomic fields, §8.1).

Notons que le nombre $L(1,\chi)$ est transcendant pour tout $\chi\neq\chi^o$; si χ est impair, cela résulte du théorème de Lindemann sur la transcendance de π, et si χ est pair, cela résulte du théorème de Baker.

Références : K. Iwasawa, Lectures on p-adic L-functions ; H. Hasse, Uber die Klassenzahl abelscher Zahlkörper ; L.C. Washington, Introduction to cyclotomic fields ; S. Lang, Cyclotomic fields.

d) Corps C.M..

Quand k est un corps de nombres, on note k^+ le sous-corps totalement réel maximal de k.

On appelle *corps* C.M. ("complex multiplication") tout corps de nombres k totalement imaginaire tel que $[k:k^+]=2$. Par exemple un corps cyclotomique $\mathbb{Q}(\zeta)$ (où ζ est une racine de l'unité) est un corps C.M., avec $\mathbb{Q}(\zeta)^+=\mathbb{Q}(\zeta+\zeta^{-1})$.

Si k est un corps de nombres abélien sur $\mathbb{Q}$, alors k est soit un corps totalement réel, soit un corps C.M. : en effet, si σ est un plongement de k dans $\mathbb{C}$ et si $\sigma(k)$ n'est pas contenu dans $\mathbb{R}$, alors le sous-corps de k fixé par la conjugaison complexe, c'est-à-dire par $\tau=\sigma^{-1}\circ\bar{\sigma}$, est totalement réel, donc c'est k^+, et comme τ est d'ordre 2, on a bien $[k:k^+]=2$.

Lemme 1.7.- *Soit* k *un corps* C.M. ; *il existe un automorphisme* τ *de* k *tel que pour tout plongement* σ *de* k *dans* $\mathbb{C}$, *on ait* $\sigma(\tau\alpha)=\overline{\sigma\alpha}$ *pour tout* $\alpha\in k$.

Démonstration.- On choisit un plongement $\sigma_0 : k \longrightarrow \mathbb{C}$. Comme k^+ est totalement réel, le corps $\sigma_0 k^+$ est fixé par la conjugaison complexe. Mais k/k^+ est quadratique, donc normale ; par conséquent $\sigma_0 k=\overline{\sigma}_0 k$, et $\tau=\sigma_0^{-1}\circ\overline{\sigma}_0$ est un automorphisme non trivial de k, fixant k^+. Puisque $G(k/k^+)$ est d'ordre 2, un tel τ est unique, donc $\tau=\sigma^{-1}\circ\overline{\sigma}$ pour tout $\sigma : k \longrightarrow \mathbb{C}$.

Ainsi la conjugaison complexe induit un automorphisme τ de k indépendant du plongement de k dans $\mathbb{C}$; pour $\alpha\in k$, *on notera* $\overline{\alpha}$ au lieu de $\tau\alpha$.

Notons E^+ le groupe des unités de k^+, et W le sous-groupe de torsion de k^*. Comme le nombre de Dirichlet de k^+ est le même que celui de k, E^+ est d'indice fini dans E.

Lemme 1.8.- *L'indice de* WE^+ *dans* E *est égal à* 1 *ou à* 2.

Démonstration.- Soit $\epsilon\in E$; pour tout plongement de k dans $\mathbb{C}$, l'image de $\epsilon/\overline{\epsilon}$ a pour module 1 ; comme $E\cap\mathrm{Ker}\lambda=W$, il en résulte que $\epsilon/\overline{\epsilon}\in W$. L'application $\Phi:E \longrightarrow W$ qui envoie ϵ sur $\epsilon/\overline{\epsilon}$ est un homomorphisme ; son image contient W^2 : en effet, pour $\zeta\in W$, on a $\Phi(\zeta)=\zeta/\overline{\zeta}=\zeta^2$. Mais W est cyclique d'ordre pair, donc W^2 est d'indice 2 dans W, ce qui montre que $\Phi(E)$ est soit W, soit W^2.

Soit $s:W \longrightarrow W/W^2$ la surjection canonique, et soit $\Psi=s\circ\Phi$. Il reste à voir que $\ker\Psi=W.E^+$. Or d'une part si $\zeta\in W$ et $\epsilon\in E^+$ alors $\Phi(\zeta\epsilon)=\zeta^2\in W^2$; d'autre part si $\Phi(\epsilon)=\zeta^2\in W^2$ alors $\epsilon/\overline{\epsilon}=\zeta^2$, donc $\epsilon/\zeta=\overline{\epsilon}/\overline{\zeta}$ est réel, et appartient donc à E^+.

Lemme 1.9.- *Soit* k *un corps* C.M. *de degré* d *sur* $\mathbb{Q}$. *Soit* $r=\frac{d}{2}-1$ *son nombre de Dirichlet. Alors*

$$R_k/R_{k^+} = \begin{cases} 2^r & \text{si } E=WE^+ \\ 2^{r-1} & \text{si } [E:WE^+]=2. \end{cases}$$

Démonstration.- Soit $\epsilon_1,\ldots,\epsilon_r$ un système fondamental d'unités de k^+. Ainsi $R_{k^+}=R_{k^+}(\epsilon_1,\ldots,\epsilon_r)$. D'autre part $R_k/R_k(\epsilon_1,\ldots,\epsilon_r)=[E:WE^+]^{-1}$. Enfin les coefficients δ_i valent 1 pour k^+, et 2 pour k, donc $R_k(\epsilon_1,\ldots,\epsilon_r)=2^rR_{k^+}(\epsilon_1,\ldots,\epsilon_r)$.

Ces résultats permettent souvent, dans l'étude des corps abéliens, de se limiter au cas totalement réel.

§2. Le rang p-adique du groupe des unités.

Nous définissons d'abord le rang p-adique du groupe des unités en considérant l'adhérence de l'image, par le plongement canonique p-adique, d'un sous-groupe de type fini de E dans le produit des unités locales. Nous montrons ensuite que ce rang est égal au rang d'une matrice ; quand k est soit totalement réel, soit un corps C.M., on peut prendre une telle matrice qui soit carrée, et alors son déterminant est le régulateur p-adique. Dans le cas galoisien totalement réel ou C.M., le régulateur p-adique se calcule à l'aide du Gruppendeterminant en utilisant une unité de Minkowski.

a) Adhérence p-adique du groupe des unités.

Soient k un corps de nombres, et p un nombre premier. Pour chaque idéal $\mathfrak{p}$ de k au-dessus de p, on considère le complété $k_{\mathfrak{p}}$ ($=k_v$ si v est la place ultramétrique de k associée à $\mathfrak{p}$), le groupe des *unités locales* en $\mathfrak{p}$ que nous noterons $U_{\mathfrak{p}}$ (il était aussi noté A_v^* ou U_v dans les deux premiers chapitres), et le groupe $U_{\mathfrak{p}}^1$ (noté $U_{\mathfrak{p}}^{(1)}$ précédemment) des *unités principales* de $k_{\mathfrak{p}}$:

$$U_{\mathfrak{p}}^1 = 1+\mathfrak{p}.U_{\mathfrak{p}} = \{u\in U_{\mathfrak{p}} \ ; \ u\equiv 1 \bmod \mathfrak{p}\} = \{x\in k_{\mathfrak{p}} \ ; \ v_{\mathfrak{p}}(x-1)>0\}.$$

Par le logarithme p-adique, $U_{\mathfrak{p}}$ et $k_{\mathfrak{p}}$ sont localement isomorphes ; $U_{\mathfrak{p}}^1$ est un $\mathbb{Z}_p$-module : pour $u\in U_{\mathfrak{p}}^1$ et $a=\lim a_n\in\mathbb{Z}_p$ avec $a_n\in\mathbb{Z}$, $a_n\geq 0$,

$$u^a=\lim u^{a_n}=\sum_{i=0}^{\omega}\binom{a}{i}(u-1)^i \in U_{\mathfrak{p}}^1 ,$$

avec $\binom{a}{i}=a(a-1)\ldots(a-i+1)/i!$ (cf. Chap.II §1.a). Le rang sur $\mathbb{Z}_p$ de $U_{\mathfrak{p}}^1$ est égal au degré local $d_{\mathfrak{p}}=[k_{\mathfrak{p}}:\mathbb{Q}_p]=e_{\mathfrak{p}}f_{\mathfrak{p}}$.

On définit des groupes topologiques U et U^1 en prenant les produits directs :

$$U = \prod_{\mathfrak{p}\mid p} U_{\mathfrak{p}} \quad \text{et} \quad U^1 = \prod_{\mathfrak{p}\mid p} U_{\mathfrak{p}}^1 .$$

Ainsi U^1 est un $\mathbb{Z}_p$-module de rang $\sum_{\mathfrak{p}|p} d_{\mathfrak{p}}=d=[k:\mathbb{Q}]$, et U^1 est d'indice fini dans U :

$$[U:U']=\prod_{\mathfrak{p}|p}(N(\mathfrak{p})-1), \text{ car } U/U' \simeq \prod_{\mathfrak{p}|p}(\mathcal{O}/\mathfrak{p})^*.$$

Si on pose $n=\text{ppcm}\{Np-1 \ ; \ \mathfrak{p}|p\}$, on a $U^n \subset U^1$. Soit $\mathbf{i}:E \longrightarrow U$ le plongement diagonal ; le sous-groupe $E^1=\{\epsilon\in E \ ; \ \mathbf{i}(\epsilon)\in U^1\}$ de E est alors d'indice fini dans E ; c'est donc un $\mathbb{Z}$-module de rang r.

Soit $\overline{E}$ l'adhérence de $\mathbf{i}(E^1)$ dans le groupe topologique U^1 ; ainsi $\overline{E}$ est le sous-$\mathbb{Z}_p$-module de U^1 engendré par $\mathbf{i}(E^1)$. Comme E^1 est de rang r sur $\mathbb{Z}$, $\overline{E}$ est de rang $\leq r$ sur $\mathbb{Z}_p$.

La **conjecture de Leopoldt** s'énonce : *le rang sur* $\mathbb{Z}_p$ *de* $\overline{E}$ *est égal à* $r=r_1+r_2-1$.

Le rang sur $\mathbb{Z}_p$ de $\overline{E}$ est noté $r_p=r_p(k)$ et est appelé *rang p-adique* du groupe des unités de k. On a $r_p\leq r$, et la différence $r-r_p$ est le *défaut* de la conjecture de Leopoldt (pour le corps k).

(N.B.- On ne confondra pas le rang 2-adique r_2 du groupe des unités de k avec le nombre r_2 de plongements imaginaires deux-à-deux non conjugués de k dans $\mathbb{C}$.)

Si k est un corps de nombres vérifiant la conjecture de Leopoldt (c'est-à-dire pour lequel $r_p=r$), et si k' est un sous-corps de k, alors k' vérifie aussi la conjecture de Leopoldt. Plus précisément $\delta(k')\leq\delta(k)$. En effet, on peut compléter une base du groupe des unités de k' en un système indépendant d'unités de k de rang maximal, et ces dernières ne vérifient pas de relation non triviale à coefficients dans $\mathbb{Z}_p$, donc à fortiori les premières non plus. Cela montre par exemple que, si on veut démontrer la conjecture de Leopoldt pour tous les corps de nombres, alors il suffit de le faire pour les extensions galoisiennes de $\mathbb{Q}$.

b) Les régulateurs p-adiques.

Nous reprenons les notations du a) ci-dessus. De plus nous notons $\mathbf{i}=(i_v)_{v|p}$ le plongement canonique de k dans $\prod_{\mathfrak{p}|p} k_{\mathfrak{p}}$, et $\sigma_1,\ldots,\sigma_d$ les

différents plongements de k dans $\mathbb{C}_p$.

Pour chaque $v|p$, notons $\varphi_{v,1},\dots,\varphi_{v,d_v}$ les homomorphismes continus (c'est-à-dire les $\mathbb{Q}_p$-isomorphismes) de k_v dans $\mathbb{C}_p$; on a

$$\{\varphi_{v,j}\ ;\ 1\le j\le d_v\} = \{\tau\circ\varphi_{v,1}\ ;\ \tau\ \mathbb{Q}_p\text{-automorphisme de } \mathbb{C}_p\},$$

et

$$\{\sigma_1,\dots,\sigma_d\} = \{\varphi_{v,j}\circ i_v\ ;\ 1\le j\le d_v,\ v|p\}.$$

Soit $\epsilon_1,\dots,\epsilon_r$ une famille indépendante d'éléments de E^1, et soit $(a_1,\dots,a_r)\in\mathbb{Z}_p^r$. Les conditions suivantes sont clairement équivalentes :

(i) $\mathbf{i}(\epsilon_1)^{a_1}\dots\mathbf{i}(\epsilon_r)^{a_r}$ est un élément de torsion dans U^1 ;

(ii) $\sum_{j=1}^{r} a_j \log_p \varphi_{v,1}\circ i_v(\epsilon_j)=0$ pour tout $v|p$;

(iii) $\sum_{j=1}^{r} a_j \log_p \sigma_i\epsilon_j=0$ pour $1\le i\le d$.

Définissons $\mathbf{y}_1,\dots,\mathbf{y}_r$ dans $\mathbb{C}_p^g$, où g est le nombre d'idéaux de k au-dessus de p, par

$$\mathbf{y}_j=(\log_p\varphi_{v,1}\circ i_v(\epsilon_j))_{v|p}\ , \qquad (1\le j\le r),$$

et $\mathbf{z}_1,\dots,\mathbf{z}_r$ dans $\mathbb{C}_p^d$ par

$$\mathbf{z}_j=(\log_p\sigma_i\epsilon_j)_{1\le i\le d}\ , \qquad (1\le j\le r).$$

On obtient donc :

Lemme 2.1.- *Le nombre r_p est égal au rang sur $\mathbb{Z}_p$ du sous-groupe de $\mathbb{C}_p^g$ engendré par $\mathbf{y}_1,\dots,\mathbf{y}_r$, et c'est aussi le rang sur $\mathbb{Z}_p$ du sous-groupe de $\mathbb{C}_p^d$ engendré par $\mathbf{z}_1,\dots,\mathbf{z}_r$,.*

Voici le lien entre le rang p-adique du groupe des unités de k et le rang d'une matrice dont les coefficients sont des logarithmes p-adiques de nombres algébriques.

Lemme 2.2.- *La matrice* $d\times r$ *à coefficients dans* $\mathbb{C}_p$:

$$(\log_p \sigma_i \epsilon_j)_{1\le j\le r,\, 1\le i\le d} = \begin{bmatrix} \log_p \sigma_1 \epsilon_1 & \dots & \log_p \sigma_1 \epsilon_r \\ \vdots & & \vdots \\ \log_p \sigma_d \epsilon_1 & \dots & \log_p \sigma_d \epsilon_r \end{bmatrix}$$

a pour rang r_p.

Démonstration.- D'après le lemme 2.1, r_p est le rang sur $\mathbb{Z}_p$ des colonnes de cette matrice. Il faut voir que le rang ρ de la matrice est égal au rang sur $\mathbb{Z}_p$ des colonnes. L'inégalité $\rho\le r_p$ est claire. Montrons inversement que toute relation linéaire à coefficients dans $\mathbb{C}_p$ entre les colonnes donne une relation linéaire à coefficients dans $\mathbb{Z}_p$.

Soit L l'adhérence topologique de la clôture galoisienne de $\sigma_1 k$ dans $\mathbb{C}_p$. Alors L est une extension finie de $\mathbb{Q}_p$ contenant tous les $\sigma_i(k)$; comme L est complet, on a $\log_p \sigma_i \epsilon_j \in L$ pour $1\le i\le d$ et $1\le j\le r$, et on peut partir d'une relation à coefficients dans L : soit $(b_1,\dots,b_r)\in L^r$, $\neq(0,\dots,0)$, tel que

$$\sum_{j=1}^{r} b_j \log_p \sigma_i \epsilon_j = 0, \qquad (1\le i\le d).$$

Quitte à diviser tous les b_j par l'un d'eux, on peut se ramener au cas où il existe un j_o, $1\le j_o\le r$, tel que $b_{j_o}=1$. Pour tout $\mathbb{Q}_p$-automorphisme τ de L, on a $\tau \log_p \sigma_i \epsilon_j = \log_p \tau\circ\sigma_i \epsilon_j$, donc

$$\sum_{j=1}^{r} (\tau b_j) \log_p \tau\circ\sigma_i \epsilon_j = 0, \qquad (1\le i\le d).$$

Mais $G(L/\mathbb{Q}_p)$ permute les σ_i : pour tout $\tau\in G(L/\mathbb{Q}_p)$, on a

$$\{\tau\circ\sigma_i \ ; \ 1\le i\le d\} = \{\sigma_i \ ; \ 1\le i\le d\} \ ;$$

on a donc encore

$$\sum_{j=1}^{r} (\tau b_j) \log_p \sigma_i \epsilon_j = 0, \qquad (1\le i\le d).$$

Alors

$$\sum_{j=1}^{r} (\mathrm{Tr}_{L/\mathbb{Q}_p} b_j) \log_p \sigma_i \epsilon_j = 0, \qquad (1\le i\le d).$$

Mais $a_j = \mathrm{Tr}_{L/\mathbb{Q}_p} b_j \in \mathbb{Q}_p$, $(1\le j\le r)$, et $a_{j_o} = \mathrm{Tr}_{L/\mathbb{Q}_p} b_{j_o} \neq 0$.

Enfin si on a des relations indépendantes

$$\sum_{j=1}^{r} b_j^{(\lambda)} \log_p \sigma_i \epsilon_j = 0, \quad (1 \leq i \leq d,\ 1 \leq \lambda \leq \ell)$$

avec $b^{(1)},\ldots,b^{(\ell)}$ dans L^r linéairement indépendants sur L, par combinaisons linéaires, et après éventuelle permutation des ϵ_j, on peut se ramener au cas où

$$b_j^{(\lambda)} = 0 \quad \text{pour} \quad 1 \leq j \leq r,\ 1 \leq \lambda \leq \ell, \text{ et } j < \lambda,$$

et

$$b_\lambda^{(\lambda)} = 1 \quad \text{pour} \quad 1 \leq \lambda \leq \ell.$$

En posant $a_j^{(\lambda)} = \mathrm{Tr}_{L/\mathbb{Q}_p} b_j^{(\lambda)}$, $(1 \leq j \leq r,\ 1 \leq \lambda \leq \ell)$, et $a^{(\lambda)} = (a_j^{(\lambda)})_{1 \leq j \leq r}$, $(1 \leq \lambda \leq \ell)$, on voit que $a^{(1)},\ldots,a^{(\ell)}$ sont $\mathbb{Z}_p$-linéairement indépendants dans $\mathbb{Q}_p^r$. Le lemme 2.2 s'en déduit facilement.

La somme des composantes de chacune des r lignes de la matrice transposée $(\log_p \sigma_i \epsilon_j)_{1 \leq j \leq r,\, 1 \leq i \leq d}$ est nulle, puisque $\epsilon_1,\ldots,\epsilon_r$ sont des unités. Donc r_p est aussi égal au rang de la matrice $r \times (d-1)$

$$(\log_p \sigma_i \epsilon_j)_{1 \leq j \leq r,\, 1 \leq i \leq d-1}.$$

Si k est totalement réel, c'est-à-dire si $r=d-1$, cette dernière matrice est carrée, et son déterminant, qui ne dépend de la numérotation des σ_i que par un facteur ± 1, est *le régulateur p-adique* $\pm R_p(k) = \pm R_p$ de k (pour se débarrasser de l'indétermination provenant du signe, il suffit de considérer le carré du déterminant, qui définit R_p^2 sans ambiguïté ; suivant Amice-Fresnel, on choisit le signe de R_p en même temps que celui de la racine carrée du discriminant en étudiant les valeurs des fonctions L p-adiques au point $s=1$; voir à ce sujet le livre d'Iwasawa).

Si k est un corps C.M., τ la conjugaison complexe (lemme 1.7), et σ un plongement de k dans $\mathbb{C}_p$, on a

$$\log_p \sigma\epsilon = \log_p \sigma\tau\epsilon \qquad \text{pour tout } \epsilon \in E^1 ;$$

en effet, le lemme 1.8 donne $[E:WE^+] \leq 2$, donc on peut écrire $\epsilon^2 = \zeta\epsilon_1$, avec $\zeta \in W$ et $\epsilon_1 \in E^+$; alors $\tau\epsilon_1 = \epsilon_1$, et $\log_p \sigma\zeta = \log_p \sigma\tau\zeta = 0$, donc

$$\log_p \sigma\tau\epsilon = \tfrac{1}{2} \log_p \sigma\epsilon_1 = \log_p \sigma\epsilon.$$

Si on choisit r plongements $\sigma_1,\dots,\sigma_r$ (avec $r=\frac{d}{2}-1$) de k dans $\mathbb{C}_p$ de telle sorte que $\sigma_i\neq\sigma_j\circ\tau$ pour $1\leq i\neq j\leq r$, alors le déterminant de la matrice $(\log_p\sigma_i\epsilon_j)_{1\leq i,j\leq r}$ ne dépend de ce choix que par un facteur ±1 ; on le note encore $\pm R_p(k)=\pm R_p$. On vérifie que si k est un corps C.M., on a

$$\pm R_p(k)=\pm R_p(k^+)R_k/R_{k^+}\ .$$

Quand k est un corps totalement réel ou C.M., le lemme 2.2 montre que *la conjecture de Leopoldt est équivalente au fait que le régulateur p-adique de* k *ne s'annule pas.*

On peut encore définir *des régulateurs p-adiques* quand le corps k n'est ni totalement réel, ni C.M. (voir l'introduction, §5b), et plus généralement, en gardant les notations de l'introduction, si $\eta_1,\dots,\eta_r$ est un système indépendant d'unités de k, on peut définir un *régulateur p-adique* de $(\eta_1,\dots,\eta_r)$ par

$$R_p(\eta_1,\dots,\eta_r)=\det(\delta_i\log_p\sigma_i\eta_j)_{1\leq i,j\leq r}\ ;$$

pour tout entier $\eta_{r+1}>1$ qui n'est pas une puissance de p, on a

$$R_p(\eta_1,\dots,\eta_r)=\pm(d\log_p\eta_{r+1})^{-1}.\det(\delta_i\log_p\sigma_i\eta_j)_{1\leq i,j\leq r+1}\ .$$

Ce nombre dépend en général du choix du plongement de $\mathbb{C}_p$ dans $\mathbb{C}$ et de la numérotation des $\sigma_1,\dots,\sigma_d$ (avec $\sigma_1,\dots,\sigma_{r_1}$ réels, et $\sigma_{r_1+1},\dots,\sigma_{r_1+r_2}$ conjugués complexes de $\sigma_{r_1+r_2+1},\dots,\sigma_d$ respectivement). Si on choisit la même numérotation pour définir $R_p(\epsilon_1,\dots,\epsilon_r)$ pour un système fondamental d'unités $\epsilon_1,\dots,\epsilon_r$ de k, et si E' est le sous-groupe de E engendré par $\eta_1,\dots,\eta_r$ et W, alors on a

$$R_p(\eta_1,\dots,\eta_r)=\pm[E:E'].R_p(\epsilon_1,\dots,\epsilon_r).$$

En particulier $R_p(\epsilon_1,\dots,\epsilon_r)\neq0$ si et seulement si $R_p(\eta_1,\dots,\eta_r)\neq0$, et *la conjecture de Leopoldt équivaut à dire qu'il existe une numérotation des* σ_i *compatible avec un plongement de* $\mathbb{C}_p$ *dans* $\mathbb{C}$ *telle que* $R_p(\epsilon_1,\dots,\epsilon_r)\neq0$.

Dans le cas général, $R_p(k)$ dépend du choix des plongements "réels" et "imaginaires" de k dans $\mathbb{C}_p$. Par exemple (cf. livre de Washington), pour $k=\mathbb{Q}(\alpha)$ avec $\alpha^3=2$, une unité fondamentale est $\epsilon=\alpha-1$; on a trois plongements σ_1, σ_2, σ_3 de k dans $\mathbb{C}_p$; pour chaque i=1,2,3, il existe un

plongement (non continu!) de $\mathbb{C}_p$ dans $\mathbb{C}$ qui envoie $\sigma_i\epsilon$ sur le nombre complexe $\sqrt[3]{2}$ -1 ; on a donc trois régulateurs p-adiques, qui sont respectivement, au signe près,

$$\log_p\epsilon_1,\ \log_p\epsilon_2,\ \log_p\epsilon_3,$$

où ϵ_1, ϵ_2, ϵ_3 sont les trois racines dans $\mathbb{C}_p$ du polynôme $(X+1)^3-2$. Ces trois valeurs possibles pour $R_p(k)$ sont linéairement dépendantes sur $\overline{\mathbb{Q}}$ puisque $\epsilon_1\epsilon_2\epsilon_3=1$, mais le quotient de deux d'entre elles est un nombre transcendant par le théorème de Baker-Brumer (Introduction, th. 4.1).

Enfin, une fois choisie la numérotation de $\sigma_1,\dots,\sigma_d$, on peut encore définir un régulateur p-adique en prenant, comme le propose Fresnel :

$$\pm(r_1+r_2)^{-1}.\det\begin{bmatrix} 1 & \log_p\sigma_1\epsilon_1 & \dots & \log_p\sigma_1\epsilon_r \\ \vdots & \vdots & & \vdots \\ 1 & \log_p\sigma_{r_1}\epsilon_1 & \dots & \log_p\sigma_{r_1}\epsilon_r \\ 1 & \log_p(\sigma_{r_1+1}\epsilon_1.\sigma_{r_1+r_2+1}\epsilon_1) & \dots & \log_p(\sigma_{r_1+1}\epsilon_r.\sigma_{r_1+r_2+1}\epsilon_r) \\ \vdots & \vdots & & \vdots \\ 1 & \log_p(\sigma_{r_1+r_2}\epsilon_1.\sigma_{r_1+2r_2}\epsilon_1) & \dots & \log_p(\sigma_{r_1+r_2}\epsilon_r.\sigma_{r_1+2r_2}\epsilon_r) \end{bmatrix}$$

Dans le cas totalement réel ou C.M., on retrouve bien sûr $\pm R_p(k)$.

Terminons par une présentation plus conceptuelle, due à M. Emsalem (Crelle J., **382** (1987), 181-198), de ce qui précède dans le cas galoisien.

Soit donc k une extension galoisienne finie de $\mathbb{Q}$; notons $G=G(k/\mathbb{Q})$. Nous avons considéré ci-dessus la p-partie

$$k\otimes_{\mathbb{Q}}\mathbb{Q}_p=\prod_{v|p}k_v$$

de l'anneau des adèles de k, avec le plongement canonique $k\longrightarrow\prod_{v|p}k_v$ noté $\mathbf{i}=(i_v)_{v|p}$.

Fixons maintenant un plongement Φ de k dans $\mathbb{C}_p$, et soit K l'adhérence de $\Phi(k)$ dans $\mathbb{C}_p$. Evidemment chaque k_v, $(v|p)$, est isomorphe à K. On plonge ensuite k dans K^G par l'application $\mathbf{j}$ définie par

$$\mathbf{j}(\alpha)=(\Phi\circ\sigma(\alpha))_{\sigma\in G}.$$

Comme $\mathbb{Q}_p$-espace vectoriel, $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ est isomorphe à K^g, où g est le nombre d'idéaux premiers de k au dessus de p, donc

$$\dim_{\mathbb{Q}_p} k\otimes_{\mathbb{Q}}\mathbb{Q}_p = g.\dim_{\mathbb{Q}_p} K = efg = d,$$

alors que K^G est un K-espace vectoriel de dimension d. Si p est totalement décomposé dans k, alors on a $g=d$ et $K=\mathbb{Q}_p$, donc $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ est naturellement isomorphe à K^G.

Si on remplaçait p par la place archimédienne de $\mathbb{Q}$, on aurait $k\otimes_{\mathbb{Q}}\mathbb{R}\simeq\mathbb{R}^d$, et le corps K est $\mathbb{R}$ si k est (totalement) réel (auquel cas $K^G=\mathbb{R}^d$), tandis que K est $\mathbb{C}$ si k est (totalement) imaginaire (et alors $K^G=\mathbb{C}^d$).

Lemme 2.3.- *Il existe un unique isomorphisme continu* $\theta : k\otimes_{\mathbb{Q}}\mathbb{Q}_p \longrightarrow K^G$ *tel que* $\theta\circ\mathbf{i}=\mathbf{j}$.

Démonstration.- L'unicité est claire : $\mathbf{i}(k)$ est dense dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ (théorème d'approximation faible).

Avant de construire θ, voici quelques généralités qui complètent le fascicule 3 et le §3.d du chapitre 2.

Comme on a choisi un plongement Φ de k dans $\mathbb{C}_p$, on dispose d'une bijection $\sigma \longrightarrow \Phi\circ\sigma$ entre G et l'ensemble des plongements de k dans $\mathbb{C}_p$.

Soit $S=\{v\ ;\ v|p\}$ l'ensemble des places de k au-dessus de p. On fait agir G sur S par $(\sigma,v) \longrightarrow \sigma^{-1}v$. Cette action est transitive. Notons v_o la place de k définie par

$$|\alpha|_{v_o} = |\Phi(\alpha)|_p, \qquad (\alpha\in k),$$

et $v_\sigma=\sigma^{-1}v_o$, pour $\sigma\in G$. Le stabilisateur de v_o (=groupe de décomposition en v_o) est le groupe de Galois D de K sur $\mathbb{Q}_p$ (cf. S. Lang, Algebra, Chap.XII Proposition 3.2 = A.N.T., Chap.II Th.2). On a donc une bijection entre S et les classes à droite de G modulo D : pour σ et τ dans G, on a

$$v_\sigma = v_\tau \quad \text{si et seulement si} \quad \sigma\in D\tau\ ;$$

ces conditions sont équivalentes à

$$|\phi\circ\sigma(\alpha)|_p = |\phi\circ\tau(\alpha)|_p \quad \text{pour tout} \quad \alpha\in k.$$

Pour chaque place v de k au-dessus de p, choisissons un élément σ_v de G tel que $v_{\sigma_v}=v$; ainsi $\{\sigma_v\}_{v|p}$ est un système de représentants des classes à droite de G modulo D.

Soient $v|p$ et $\tau\in G$; on a

$$D\sigma_{\tau v}=D\sigma_v\circ\tau^{-1} ;$$

en effet, en posant $w=\tau v$, on a

$$|\phi\circ\sigma_w(\alpha)|_p=|\alpha|_w=|\tau^{-1}\alpha|_v=|\phi\circ\sigma_v\circ\tau^{-1}(\alpha)|_p$$

On peut maintenant construire θ. Pour chaque $v|p$ et chaque $s\in D$, il existe un unique isomorphisme continu $\theta_{s,v}$ de k_v sur K rendant commutatif le diagramme

$$\begin{array}{ccc} k & \xrightarrow{i_v} & k_v \\ {\scriptstyle s\circ\sigma_v}\downarrow & & \downarrow{\scriptstyle \theta_{s,v}} \\ k & \xrightarrow[\phi]{} & K \end{array}$$

On envoie k_v dans $K^{D\sigma_v}$ par $\theta_v=(\theta_{s,v})_{s\sigma_v\in D\sigma_v}$, puis $\prod_{v|p} k_v$ dans $K^G=\prod_{v|p} K^{D\sigma_v}$ par $\theta(\mathbf{x})=(\theta_v(x_v))_{v|p}$.

Il est clair que θ répond au problème.

Lemme 2.4.- *Si* $\mathbf{x}_1,\ldots,\mathbf{x}_s$ *sont des éléments* $\mathbb{Q}_p$*-linéairement indépendants de* $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$, *alors* $\theta(\mathbf{x}_1),\ldots,\theta(\mathbf{x}_s)$ *sont* K*-linéairement indépendants dans* K^G.

Comme $\dim_{\mathbb{Q}_p} k\otimes_{\mathbb{Q}}\mathbb{Q}_p=d=\dim_K K^G$, cela revient à dire que l'application θ induit un isomorphisme entre $(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)\otimes_{\mathbb{Q}_p} K$ et K^G.

Démonstration.- Il suffit de vérifier que θ transforme *une* base de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ en une base de K^G, et alors ce sera vrai pour toute base. On reprend la démonstration du lemme 2.2. Soient $\alpha_1,\ldots,\alpha_d$ des éléments de k dont les images par $\mathbf{i}$ sont linéairement indépendantes sur $\mathbb{Q}_p$. Supposons que l'on ait

$$a_1\theta\circ\mathbf{i}(\alpha_1)+\ldots+a_d\theta\circ\mathbf{i}(\alpha_d)=0$$

avec $a_1,\ldots,a_d$ dans K non tous nuls. On peut supposer que l'un des a_j vaut 1. On a donc

$$\sum_{j=1}^{d} a_j \Phi\circ\sigma(\alpha_j)=0 \qquad \text{pour tout } \sigma\in G ;$$

alors, pour tout $\tau\in G(K/\mathbb{Q}_p)$ et tout $\sigma\in G$, on a

$$\sum_{j=1}^{d} (\tau a_j).\tau\circ\Phi\circ\sigma(\alpha_j)=0 ;$$

or, pour chaque $\tau\in G(K/\mathbb{Q}_p)$, $\tau\circ\Phi\circ\sigma$ décrit l'ensemble des plongements de k dans K quand σ décrit G ; donc

$$\sum_{j=1}^{d} (\tau a_j).\Phi\circ\sigma(\alpha_j)=0 \quad \text{pour tout } \sigma\in G \text{ et tout } \tau\in G(K/\mathbb{Q}_p),$$

et

$$\sum_{j=1}^{d} \mathrm{Tr}_{K/\mathbb{Q}_p}(a_j).\Phi\circ\sigma(\alpha_j)=0 \qquad \text{pour tout } \sigma\in G ;$$

posons $b_j=\mathrm{Tr}_{K/\mathbb{Q}_p}(a_j)$, $(1\leq j\leq d)$; les éléments $b_1,\ldots,b_d$ de $\mathbb{Q}_p$ ne sont pas tous nuls, donc les $\Phi\circ\sigma(\alpha_j)$ sont $\mathbb{Q}_p$-linéairement dépendants.

Conséquence.- L'application

$$\mathrm{LOG} : (k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^* \longrightarrow k\otimes_{\mathbb{Q}}\mathbb{Q}_p$$

qui envoie $(x_v)_{v|p}\in(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^*=\prod_{v|p} k_v^*$ sur $(\log_p x_v)_{v|p}$ définit un homomorphisme continu, et c'est un isomorphisme local (d'un voisinage de 1 sur un voisinage de 0). Le sous-$\mathbb{Q}_p$-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ engendré par l'image $\mathrm{LOG}(E)$ de E par LOG a évidemment pour dimension r_p (lemme 2.1).

On a aussi un homomorphisme $\mathscr{LOG}$ de K^{*G} dans K^G qui envoie $(x_\sigma)_{\sigma\in G}$ sur $(\log_p x_\sigma)_{\sigma\in G}$, et c'est un isomorphisme local.

Comme les coefficients de la série de Taylor de $\log_p$ au point 1 sont dans $\mathbb{Q}$, donc dans $\mathbb{Q}_p$, on en déduit que le diagramme

$$\begin{array}{ccc} (k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^* & \xrightarrow{\ \mathrm{LOG}\ } & k\otimes_{\mathbb{Q}}\mathbb{Q}_p \\ \theta\downarrow & & \downarrow\theta \\ K^{*G} & \xrightarrow[\mathscr{LOG}]{} & K^G \end{array}$$

est commutatif. Le régulateur p-adique est la matrice d'un endomorphisme

K-linéaire $\mathcal{L}$ de K^G, et cette matrice a même rang que l'endomorphisme $\mathbb{Q}_p$-linéaire $\theta^{-1}\circ\mathcal{L}\circ\theta$ de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$:

$$\begin{array}{ccc} k\otimes_{\mathbb{Q}}\mathbb{Q}_p & \xrightarrow{\theta^{-1}\circ\mathcal{L}\circ\theta} & k\otimes_{\mathbb{Q}}\mathbb{Q}_p \\ \theta\downarrow & & \downarrow\theta \\ K^G & \xrightarrow[\mathcal{L}]{} & K^G \end{array}$$

on retrouve le lemme 2.2.

Nous allons définir une action de G sur chacun des espaces $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ et K^G qui induise l'action naturelle de G sur k via $\mathbf{i}$ et $\mathbf{j}$ respectivement, et nous verrons que θ commute avec cette action.

Pour $x=(x_v)_{v|p}\in k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ et $\tau\in G$, on définit $\tau x=(\tau_v x_{\tau^{-1}v})_{v|p}$, où, pour chaque $v|p$, en posant $w=\tau^{-1}v$, on définit $\tau_v : k_w\longrightarrow k_v$ par le diagramme commutatif

$$\begin{array}{ccc} k & \xrightarrow{i_w} & k_w \\ \tau\downarrow & & \downarrow\tau_v \\ k & \xrightarrow[i_v]{} & k_v \end{array}$$

A chaque $\tau\in G$ on associe ainsi un homomorphisme continu de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ dans lui-même que l'on notera encore τ, et on a $\tau\circ\mathbf{i}(\alpha)=\mathbf{i}(\tau\alpha)$ pour tout $\alpha\in k$.

Pour $z=(z_\sigma)_{\sigma\in G}$ dans K^G et $\tau\in G$, on pose $\tau z=(z_{\sigma\tau})_{\sigma\in G}$. Cela revient à identifier K^G avec l'algèbre de groupe $K[G]$ en envoyant $z=(z_\sigma)_{\sigma\in G}$ sur $\sum_{\sigma\in G} z_\sigma\sigma^{-1}$, et en faisant agir G à gauche :

$$\tau\Big(\sum_{\sigma\in G} z_\sigma\sigma^{-1}\Big)=\sum_{\sigma\in G} z_\sigma\tau\circ\sigma^{-1}$$

A chaque $\tau\in G$ on associe ainsi un endomorphisme continu de K^G que l'on notera encore τ, et on a $\tau\circ\mathbf{j}(\alpha)=\mathbf{j}(\tau\alpha)$ pour tout $\alpha\in k$.

Lemme 2.5.- *Pour tout* $\tau\in G$ *on a* $\theta\circ\tau=\tau\circ\theta$; *autrement dit le diagramme*

$$\begin{array}{ccc} k\otimes_{\mathbb{Q}}\mathbb{Q}_p & \xrightarrow{\theta} & K^G \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ k\otimes_{\mathbb{Q}}\mathbb{Q}_p & \xrightarrow[\theta]{} & K^G \end{array}$$

est commutatif.

Démonstration.- Partons de $\mathbf{x}\in k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ dont toutes les coordonnées sont nulles sauf une, d'indice v_0, pour une place v_0 divisant p quelconque. Alors toutes les coordonnées de $\tau\mathbf{x}$ sont nulles, sauf celle d'indice $v_1=\tau v_0$, qui vaut $\tau_{v_1}x_{v_0}$. On trouve $\theta\circ\tau(\mathbf{x})=(y_\sigma)_{\sigma\in G}$, où y_σ est nul si $\sigma\notin D\sigma_{v_1}$, et $y_\sigma=\theta_{s_1,v_1}(\tau_{v_1}x_{v_0})$ si $\sigma=s_1\circ\sigma_{v_1}$, $s_1\in D$.

D'un autre côté on peut écrire $\theta(\mathbf{x})=(z_\sigma)_{\sigma\in G}$, où $z_\sigma=0$ si $\sigma\notin D\sigma_{v_0}$, et $z_\sigma=\theta_{s_2,v_0}(x_{v_0})$ si $\sigma=s_2\circ\sigma_{v_0}$, $s_2\in D$; alors $\tau\circ\theta(\mathbf{x})=(u_\sigma)_{\sigma\in G}$, où $u_\sigma=0$ si $\sigma\notin D\sigma_{v_0}\circ\tau^{-1}$, et $u_\sigma=\theta_{s_2,v_0}(x_{v_0})$ si $\sigma=s_2\circ\sigma_{v_0}\circ\tau^{-1}$, $s_2\in D$.

Nous avons vu que $D\sigma_{v_0}\circ\tau^{-1}=D\sigma_{v_1}$, puisque $v_1=\tau v_0$. Il reste à vérifier que quand $s_1\circ\sigma_{v_1}=s_2\circ\sigma_{v_0}\circ\tau^{-1}$, on a $\theta_{s_1,v_1}(\tau_{v_1}x_{v_0})=\theta_{s_2,v_0}(x_{v_0})$. En effet, pour vérifier que le diagramme

$$\begin{array}{ccc} k_{v_0} & & \\ {\scriptstyle\tau_{v_1}}\downarrow & \searrow^{\theta_{s_2,v_0}} & \\ k_{v_1} & \xrightarrow[\theta_{s_1,v_1}]{} & K \end{array}$$

est commutatif, il suffit de le restreindre à k, et de constater que les restrictions à k de τ_{v_1}, θ_{s_1,v_1} et θ_{s_2,v_0} sont respectivement τ, $\Phi\circ s_1\circ\sigma_{v_1}$ et $\Phi\circ s_2\circ\sigma_{v_0}$. D'où le lemme 2.5.

Lemme 2.6.- *L'image de* θ *est* $\{\mathbf{y}=(y_\sigma)_{\sigma\in G}$; $\tau y_\sigma=y_{\tau\circ\sigma}$ *pour tout* $(\tau,\sigma)\in D\times G\}$.

Démonstration.- Montrons d'abord que l'image de θ est contenue dans ce sous-espace. Pour $\mathbf{x}=(x_v)_{v|p}\in k\otimes_{\mathbb{Q}}\mathbb{Q}_p$, on a $\theta(\mathbf{x})=\mathbf{y}=(y_\sigma)_{\sigma\in G}$, avec $y_\sigma=\theta_{s,v}(x_v)$, pour $\sigma=s\circ\sigma_v$, $s\in D$, $v|p$. Si $\tau\in D$, alors $y_{\tau\circ\sigma}=\theta_{\tau\circ s,v}(x_v)$, et il reste à remarquer que $\theta_{\tau\circ s,v}=\tau\circ\theta_{s,v}$, comme on le voit en considérant le diagramme

$$\begin{array}{ccc} k & \xrightarrow{i_v} & k_v \\ {\scriptstyle s\circ\sigma_v}\downarrow & & \downarrow{\scriptstyle \theta_{s,v}} \\ k & \xrightarrow[\Phi]{} & K \\ {\scriptstyle \tau}\downarrow & & \downarrow{\scriptstyle \tau} \\ k & \xrightarrow[\Phi]{} & K \end{array}$$

Ceci montre une inclusion, mais comme les deux espaces considérés ont la même dimension, le lemme 2.6 en résulte.

Nous avons identifié K^G avec l'algèbre $K[G]$ en envoyant $x=(x_\sigma)_{\sigma\in G}$ sur $\sum_{\sigma\in G} x_\sigma \sigma^{-1}$; notons $y \longmapsto y^\tau$ l'action de $\tau\in G$ à droite : $y^\tau=(\tau^{-1}y_{\tau\circ\sigma})_{\sigma\in G}$; alors le lemme 2.6 s'énonce :

$$\mathrm{Im}\theta=\{y\in K^G \ ; \ y^\tau=y \ \text{ pour tout } \ \tau\in D\}.$$

Remarque (M. Laurent, rang p-adique d'unités et action de groupes, Crelle J.) L'existence de l'application canonique θ, et les propriétés de θ que nous avons énoncées dans les lemmes précédents, s'obtiennent à moins de frais en utilisant des produits tensoriels : K^G n'est autre que $k\otimes_{\mathbb{Q}}K$, et, si $\iota : \mathbb{Q}_p \longrightarrow K$ désigne l'inclusion, alors $\theta=1\otimes\iota$.

Reprenons un corps de nombres galoisien sur $\mathbb{Q}$, et écrivons $k=\mathbb{Q}(\alpha)$, où α a pour polynôme minimal $P\in\mathbb{Z}[X]$. Quand on décompose P en polynômes irréductibles dans $\mathbb{Q}_p[X]$, on trouve $P=\prod_{v|p} P_v$, avec P_v irréductible sur $\mathbb{Q}_p$, et le corps de décomposition de P_v sur $\mathbb{Q}_p$ est $k_v=\mathbb{Q}_p(\alpha_v)$. L'application $i_v : k \longrightarrow k_v$ envoie α sur α_v, et l'homomorphisme θ envoie α_v sur

$$\sum_{\sigma\in D\sigma_v} \sigma(\alpha)\sigma^{-1}.$$

c) Le Gruppendeterminant.

Définition.- Soit G un groupe fini d'ordre d, et soient X_s, $s\in G$, d inconnues indexées par G. Le *Gruppendeterminant*, ou *déterminant du groupe* G, est le polynôme

$$\Delta_G(\mathbf{X})=\det\ |X_{\sigma\tau^{-1}}|_{(\sigma,\tau)\in G}\ \in \mathbb{Z}[\mathbf{X}],$$

(avec $\mathbf{X}=(X_s)_{s\in G}$), où σ est l'indice de ligne et τ l'indice de colonne. C'est la table de multiplication du groupe : si on choisit $\sigma_1=1$ (élément neutre de G), on a

$$\Delta_G(\mathbf{X}) = \det \begin{bmatrix} X_1 & X_{\sigma_2^{-1}} & \dots & X_{\tau^{-1}} & \dots & X_{\sigma_d^{-1}} \\ X_{\sigma_2} & X_1 & \dots & X_{\sigma_2\circ\tau^{-1}} & \dots & X_{\sigma_2\circ\sigma_d^{-1}} \\ \vdots & \vdots & & \vdots & & \vdots \\ X_{\sigma} & X_{\sigma\circ\sigma_2^{-1}} & \dots & X_{\sigma\circ\tau^{-1}} & \dots & X_{\sigma\circ\sigma_d^{-1}} \\ \vdots & \vdots & & \vdots & & \vdots \\ X_{\sigma_d} & X_{\sigma_d\circ\sigma_2^{-1}} & \dots & X_{\sigma_d\circ\tau^{-1}} & \dots & X_1 \end{bmatrix}.$$

Le polynôme Δ_G est homogène de degré d, et le coefficient du monôme X_1^d est 1. Ce polynôme a été décomposé par Frobenius en produit de facteurs irréductibles (voir la notice historique de Bourbaki, Algèbre Ch.8, et les oeuvres de Frobenius, vol.III, p.1-77).

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Il nous suffira ici de trouver certains diviseurs de degré 1 de $\Delta_G(\mathbf{X})$ dans $\overline{\mathbb{Q}}[\mathbf{X}]$ (ce sont en fait les seuls).

Lemme 2.7.- *Soit* χ *un caractère (de degré 1) de* G *dans* $\overline{\mathbb{Q}}$, *c'est-à-dire un homomorphisme de* G *dans* $\overline{\mathbb{Q}}^*$. *Alors le polynôme* $\Delta_G(\mathbf{X})$ *est divisible par*

$$\sum_{s\in G}\chi(s)X_s.$$

Démonstration.- Quand on multiplie, pour chaque $\tau\in G$, la colonne d'indice τ par $\overline{\chi(\tau)}$, la somme des nouvelles colonnes a pour composante d'indice σ :

$$\sum_{\tau\in G}\overline{\chi(\tau)}.X_{\sigma\tau^{-1}} = \overline{\chi(\sigma)}.\sum_{\tau\in G}\chi(\tau\sigma^{-1})X_{\sigma\tau^{-1}} = \overline{\chi(\sigma)}.\sum_{s\in G}\chi(s)X_s,$$

d'où le lemme.

En particulier le polynôme $\Delta_G(X)$ est divisible par $\sum_{s\in G} X_s$; *on notera* $P_G(X)$ le quotient.

Lemme 2.8.- *Si* G *est abélien, alors*

$$\Delta_G(X)=\prod_{\chi\in\hat{G}} \sum_{s\in G} \chi(s)X_s$$

où $\hat{G}=\mathrm{Hom}(G,\bar{\mathbb{Q}}^*)$ *est le dual de* G.

Démonstration.- Chacun des polynômes $\sum_{s\in G} \chi(s)X_s$, $(\chi\in\hat{G})$, divise $\Delta_G(X)$, et ces polynômes sont premiers entre eux dans l'anneau factoriel $\bar{\mathbb{Q}}[X]$ (ils sont irréductibles, puisque de degré 1, et deux-à-deux non associés). Il ne reste plus qu'à comparer les coefficients de X_1^d dans les deux membres.

Soit φ (resp. φ_p) un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$ (resp. $\mathbb{C}_p$). Comme Δ_G et P_G sont à coefficients rationnels, on peut les considérer comme éléments de $\mathbb{C}[X]$ ou de $\mathbb{C}_p[X]$. Le lemme 2.8 entraîne alors que, pour G abélien, on a

$$P_G(X) = \prod_{\substack{\chi\in\hat{G}\\ \chi\neq\chi^0}} \sum_{s\in G} \varphi(\chi(s)).X_s \qquad \text{dans } \mathbb{C}[X],$$

et

$$P_G(X) = \prod_{\substack{\chi\in\hat{G}\\ \chi\neq\chi^0}} \sum_{s\in G} \varphi_p(\chi(s)).X_s \qquad \text{dans } \mathbb{C}_p[X],$$

où χ^0 est l'élément neutre de $\hat{G}$.

Soit k un corps de nombres ; nous supposons que l'extension $k/\mathbb{Q}$ est galoisienne, et nous notons $G=G(k/\mathbb{Q})$. Choisissons une unité de Minkowski $\epsilon\in E^1$ (si ϵ est une unité de Minkowski mais n'appartient pas à E^1, on la remplace par ϵ^n, avec $n=\mathrm{ppcm}\{Np-1 \ ; \ p|p\}$).

Soit E' le sous-groupe de E engendré par W et les conjugués de ϵ. Le rang p-adique du groupe des unités de k est égal au rang de la matrice

$$\left(\log_p\varphi_p(\sigma\tau^{-1}\epsilon)\right)_{\sigma,\tau\in G-\{1\}}.$$

De plus, si le corps k est totalement réel, son régulateur est alors égal à

$$\pm[E:E']^{-1}.\det\left(\log|\varphi(\sigma\tau^{-1}\epsilon)|\right)_{\sigma,\tau\in G-\{1\}},$$

tandis que son régulateur p-adique est égal à

$$\pm[E:E']^{-1}.\det\left(\log_p\varphi_p(\sigma\tau^{-1}\epsilon)\right)_{\sigma,\tau\in G-\{1\}}.$$

Lemme 2.9.- *Soient* Ω *un corps quelconque de caractéristique nulle,* G *un groupe fini d'ordre* d, *et* ξ_s, $(s\in G)$ *des éléments de* Ω *de somme nulle. On a*

$$\det\left(\xi_{\sigma\tau^{-1}}\right)_{\sigma,\tau\in G-\{1\}} = \pm d^{-1}\ P_G\left((\xi_s)_{s\in G}\right).$$

Démonstration.- Le polynôme P_G est le déterminant de la matrice $d\times d$ dont les coefficients $a_{\sigma\tau}$ (σ et τ parcourant G) sont donnés par :

$$a_{\sigma\tau} = X_{\sigma\tau^{-1}} \qquad \text{pour } \sigma\neq 1$$

et

$$a_{1\tau}=1.$$

On développe par rapport à la ligne $a_{1\tau}$, et on voit que pour toute spécialisation $(\xi_s)_{s\in G}$ vérifiant $\sum_{s\in G}\xi_s=0$, tous les cofacteurs sont égaux. D'où le résultat.

Corollaire 2.10.- *Supposons l'extension* $k/\mathbb{Q}$ *abélienne et totalement réelle, et notons* χ^o *l'élément neutre de* $\hat{G}$; *alors*

$$R(k) = c\prod_{\chi\neq\chi^o}\sum_{s\in G}\varphi(\chi(s))\log|\varphi\circ s\epsilon|.$$

et

$$R_p(k) = \pm c\prod_{\chi\neq\chi^o}\sum_{s\in G}\varphi_p(\chi(s))\log_p\varphi_p\circ s\epsilon.$$

où c *est un nombre rationnel non nul.*

La conjecture de Leopoldt pour tous les corps totalement réels équivaut à la conjecture de Leopoldt pour tous les corps C.M. (tout corps totalement

réel possède une extension quadratique qui est un corps C.M.), et le lemme 2.9 montre que dans ce cas elle est une conséquence de la conjecture suivante (cf. Introduction, conjecture 2.5)

Conjecture 2.11.- *Soient* $\alpha_1,\ldots,\alpha_n$ *des éléments non nuls de* $\mathbb{C}_p$ *algébriques sur* $\mathbb{Q}$ *; on suppose que les nombres* $\log_p\alpha_1,\ldots,\log_p\alpha_n$ *sont linéairement indépendants sur* $\mathbb{Q}$. *Alors ces nombres sont algébriquement indépendants.*

(Il suffirait d'ailleurs de savoir qu'il n'y a pas de relation de dépendance algébrique *homogène* non triviale en les $\log_p\alpha_i$).

Nous verrons au §4 que la conjecture 2.11 implique la conjecture de Leopoldt même pour les corps qui ne sont pas totalement réels ou C.M..

Références pour le §2.-

M. Emsalem.

-Rang p-adique de groupe de S-unités d'un corps de nombres ; C.R.Acad.Sc.Paris, **297** (1983) ;
-Une minoration du rang p-adique du groupe des unités d'un corps de nombres totalement réel ; Problèmes Diophantiens 1980/81, Publ. Math. Univ. P. et M. Curie (Paris VI) **43** (1981), n°1, 18 p.
-Sur les idéaux dont l'image par l'application d'Artin dans une $\mathbb{Z}_p$-extension est triviale ; J. reine angew. Math (=Crelle J.), **382** (1987), 181-198.

J. Fresnel.

-Rang p-adique du groupe des unités d'un corps de nombres ; Sém. Th. Nombres Bordeaux , 1968-69, n°9, 18 p.

M. Laurent.

-Rang p-adique d'unités et action de groupes ; J. reine und angew. Math. (=Crelle J.), à paraître.

L. Washington.

-Introduction to cyclotomic fields ; Springer Verlag, G.T.M., vol.**83**, 1982.

§3. Extensions abéliennes de $\mathbb{Q}$.

Nous énonçons d'abord une conséquence du théorème de Baker-Brumer sur l'indépendance linéaire de logarithmes de nombres algébriques : si une forme linéaire à coefficients algébriques de logarithmes (usuels) de valeurs absolues de nombres algébriques n'est pas nulle, alors la forme linéaire correspondante de logarithmes p-adiques ne s'annule pas non plus. Nous en déduisons, suivant Ax et Brumer, la conjecture de Leopoldt pour les extensions abéliennes de $\mathbb{Q}$, et plus généralement pour les sous-corps d'une extension abélienne d'un corps imaginaire quadratique. Le cas abélien donne d'intéressantes propriétés des valeurs des fonctions L p-adiques au point 1.

a) Indépendance linéaire de logarithmes

Du théorème de Baker-Brumer sur l'indépendance linéaire de logarithmes p-adiques de nombres algébriques, nous allons déduire le corollaire suivant :

Corollaire 3.1.- *Soient* k *un corps de nombres,* φ *un plongement de* k *dans* $\mathbb{C}$, p *un nombre premier,* φ_p *un plongement de* k *dans* $\mathbb{C}_p$, *et* $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_n$ *des éléments de* k. *On suppose*

$$|\varphi_p\alpha_j|_p=1 \quad \textit{pour} \quad 1\leq j\leq n.$$

Si le nombre complexe

$$\sum_{j=1}^{n} \varphi\beta_j \log|\varphi\alpha_j|$$

n'est pas nul, alors le nombre p-*adique*

$$\sum_{j=1}^{n} \varphi_p\beta_j \log_p\varphi_p\alpha_j$$

n'est pas nul.

Démonstration.- Le sous-groupe de $\{z\in\mathbb{C}_p^* \ ; \ |z|_p=1\}$ engendré par les $\varphi_p\alpha_j$, $(1\leq j\leq n)$, est de type fini ; on prend une base de sa partie libre, disons

$\varphi_p\gamma_1,\ldots,\varphi_p\gamma_r$, et on écrit

$$\varphi_p\alpha_j=\varphi_p\zeta_j\cdot\prod_{i=1}^{r}(\varphi_p\gamma_i)^{c_{ij}},\qquad(1\leq j\leq n).$$

avec $\zeta_j\in W_k$ et $c_{ij}\in\mathbb{Z}$; autrement dit

$$\alpha_j=\zeta_j\cdot\prod_{i=1}^{r}\gamma_i^{c_{ij}},\qquad(1\leq j\leq n).$$

Supposons

$$\sum_{j=1}^{n}\varphi_p\beta_j\log\varphi_p\alpha_j=0\ :$$

alors

$$\sum_{j=1}^{n}\varphi_p\beta_j\sum_{i=1}^{r}c_{ij}\log_p\varphi_p\gamma_i=0,$$

c'est-à-dire

$$\sum_{i=1}^{r}\Big(\sum_{j=1}^{n}c_{ij}\,\varphi_p\beta_j\Big)\log_p\varphi_p\gamma_i=0.$$

Mais comme $\varphi_p\gamma_1,\ldots,\varphi_p\gamma_r$ sont multiplicativement indépendants et de valeur absolue p-adique égale à 1, les nombres $\log_p\varphi_p\gamma_1,\ldots,\log_p\varphi_p\gamma_r$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$ par le théorème de Baker-Brumer :

$$\sum_{j=1}^{n}c_{ij}\,\varphi_p\beta_j=0\qquad\text{pour}\quad 1\leq i\leq r.$$

Mais

$$\log|\varphi\alpha_j|=\sum_{i=1}^{r}c_{ij}\log|\varphi\gamma_i|,\qquad(1\leq j\leq n).$$

donc

$$\sum_{j=1}^{n}\varphi\beta_j\log|\varphi\alpha_j|=0.$$

b) Le théorème d'Ax-Brumer.

Commençons par les extensions abéliennes de $\mathbb{Q}$.

Théorème 3.2.- *Soit k un corps de nombres. On suppose que k est une extension abélienne de $\mathbb{Q}$. Alors pour tout nombre premier p, le corps k vérifie la conjecture de Leopoldt.*

Démonstration.- Le groupe des unités de k^+ est d'indice fini dans celui de k, et $r_p(k)$ est non nul si et seulement si $r_p(k^+)$ est non nul. Il n'y a donc pas de restriction à supposer k totalement réel. Dans ce cas le régulateur p-adique de k s'écrit (corollaire 2.10)

$$\pm c.\prod_{\chi\neq\chi^o}\sum_{s\in G}\varphi_p(\chi(s)).\log_p\varphi_p\circ s\epsilon,$$

où ϵ est une unité de Minkowski de k, c un nombre rationnel non nul, et φ_p un plongement du corps $k(\chi)=k(\{\chi(s)\ ;\ s\in G\})$ dans $\mathbb{C}_p$. De même le régulateur (réel) R_k de k est le module du nombre

$$c.\prod_{\chi\neq\chi^o}\sum_{s\in G}\varphi(\chi(s)).\log|\varphi\circ s\epsilon|,$$

avec le même coefficient c, φ étant un plongement de $k(\chi)$ dans $\mathbb{C}$. Comme R_k n'est pas nul, il résulte du corollaire 3.1 qu'aucune des combinaisons linéaires $\sum_{s\in G}\varphi_p(\chi(s)).\log_p\varphi_p\circ s(\epsilon)$ n'est nulle, donc $R_p\neq 0$.

Si $k/\mathbb{Q}$ est une extension abélienne, il existe $d\in\mathbb{Z}$, $d>1$, tel que $\sqrt{-d}\notin k$; alors $k(\sqrt{-d})$ est une extension abélienne de $\mathbb{Q}(\sqrt{-d})$; par conséquent le théorème 3.2 est un cas particulier de l'énoncé suivant :

Théorème 3.3.- *Soit* k *un corps de nombres. On suppose que* k *est contenu dans une extension abélienne d'un corps imaginaire quadratique. Alors pour tout nombre premier* p, *le corps* k *vérifie la conjecture de Leopoldt.*

Démonstration.- On peut supposer que k est une extension abélienne d'un corps quadratique imaginaire k_o. Soit $A=G(k/k_o)$, et soit $n=[k:k_o]$. Le cas $n=1$ est banal. Fixons un plongement φ de k dans $\mathbb{C}$. Pour $\sigma\in A$, on pose $\varphi_\sigma(\alpha)=\varphi(\sigma\alpha)$, $\alpha\in k$. On obtient ainsi n plongements de k dans $\mathbb{C}$, deux à deux non conjugués.

Le corps k_o étant totalement imaginaire, il en résulte que k est totalement imaginaire, et par conséquent le nombre de Dirichlet de k est n-1.

Soit ϵ une unité de k satisfaisant

$$|\varphi(\epsilon)|>1 \qquad \text{et} \qquad |\varphi_\sigma(\epsilon)|<1 \quad \text{pour tout} \quad \sigma\in\Delta,\ \sigma\neq 1$$

(cf. lemme 1.4). Alors les unités $\sigma\epsilon$, $\sigma\in\Delta$ engendrent un sous-groupe de E d'indice fini. Comme

$$\prod_{\sigma\in\Delta} \sigma\epsilon = N_{k/k_0}\epsilon$$

est une unité de k_0, donc une racine de l'unité, $n-1$ quelconques des unités $\sigma\epsilon$, $\sigma\in\Delta$, sont indépendantes.

Un régulateur p-adique de k s'écrit

$$\pm c.\det(\log_p \sigma\tau^{-1}\epsilon)_{\sigma,\tau\in\Delta-\{1\}} = c.\prod_{\chi\neq\chi^0} \sum_{s\in\Delta} \chi(s).\log_p s\epsilon,$$

où χ décrit les caractères non triviaux de Δ, et c est un nombre rationnel non nul, tandis que le régulateur (réel) R_k de k est

$$c.\prod_{\chi\neq\chi^0} \sum_{s\in\Delta} \chi(s).\log|s\epsilon|,$$

avec le même coefficient c. Comme ci-dessus, le fait que R_k soit non nul assure $r_p=r=n-1$.

(Le théorème de Herbrand précise la structure du groupe des unités d'un corps de nombres k sous l'action d'un groupe de Galois $G(k/k_0)$ quand k est une extension galoisienne d'un corps de nombres k_0 ; le cas $k_0=\mathbb{Q}$ est l'existence d'une unité de Minkowski : Prop. 1.5 ; voir à ce sujet l'exposé de J.Martinet : Sém. Th. Nombres Bordeaux, 1968-69, n°10, 11 p.)

Exemple : le corps $\mathbb{Q}(\sqrt[3]{2})$ est contenu dans le corps $k=\mathbb{Q}(j,\sqrt[3]{2})$, où j est une racine cubique de l'unité ; comme k est une extension cyclique (cubique) du corps imaginaire quadratique $\mathbb{Q}(j)$, le corps $\mathbb{Q}(\sqrt[3]{2})$ vérifie la conjecture de Leopoldt ; d'ailleurs il est facile d'en calculer un régulateur p-adique et de le décomposer en produit de facteurs linéaires :

$$(\log_p\eta_1 - j\log_p\eta_2)(\log_p\eta_1 - j^2\log_p\eta_2)$$

(cf la fin de l'Introduction).

c) Fonctions L p-adiques.

Nous avons vu au §1c les séries L associées aux caractères de Dirichlet. Si χ est un caractère primitif modulo f, la fonction $L(s,\chi)$ prend des valeurs algébriques aux entiers négatifs :

$$L(1-n, \chi) = -\frac{1}{n}.B_{n,\chi} ,$$

où les *nombres de Bernouilli généralisés* $B_{n,\chi}$ sont définis par :

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

On a

$$B_{n,\chi}=f^{n-1} \sum_{a=1}^{f} \chi(a)B_n(a/f),$$

où les $B_n(X)$ sont les *polynômes de Bernouilli* :

$$\frac{te^{(1+X)t}}{e^t-1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!}.$$

Les nombres de Bernouilli $B_n=B_{n,\chi^o}$ vérifient :

$$B_n(X)= \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.$$

On fixe un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$, on considère les nombres p-adiques $L(1-n, \chi)$, et on cherche à les interpoler p-adiquement, c'est-à-dire à trouver une fonction continue de $\mathbb{Z}_p$ dans $\mathbb{C}_p$, dont les valeurs aux points $1-n$, ($n\in\mathbb{Z}$, $n>0$) soient $L(1-n,\chi)$. Par densité des entiers négatifs dans $\mathbb{Z}_p$, si une telle fonction existe, elle est unique.

Dans la série de Dirichlet définissant $L(s,\chi)$, on ne peut pas garder les termes en m^{-s} quand m est divisible par p. Or

$$\sum_{(m,p)=1} \chi(m)m^{-s}=(1-\chi(p)p^{-s}). \sum_{m\geq 1} \chi(m)m^{-s}.$$

Le résultat est le suivant : il existe une fonction $L_p(s,\chi)$, analytique au voisinage de 1 si $\chi\neq\chi^o$ (c'est-à-dire somme d'une série entière convergente), et avec un seul pôle, simple, au point $s=1$ si $\chi=\chi^o$, telle que

(3.4) $$L_p(1-n,\chi)=(1-\chi(p)p^{n-1}).L(1-n,\chi)$$

pour tout $n\in\mathbb{Z}$, $n\geq 1$ vérifiant $n\equiv 0 \bmod q$, avec $q=p-1$ si $p\geq 3$, et $q=2$ si $p=2$.

On peut aussi relier les valeurs $L_p(1-n,\chi)$ aux nombres $L(1-n,\chi)$ si n n'est pas congru à 0 mod q.

Cette fonction est identiquement nulle si χ est impair (car $B_{n,\chi}=0$ pour $n\equiv 0 \mod q$, $n\geq 1$), tandis que si χ est pair, $\chi\neq\chi^o$, on a $L_p(1-n,\chi)\neq 0$ pour $n\equiv 0 \mod q$, $n\geq 1$.

La formule (3.4) ne vaut que pour $n\geq 1$, mais on peut l'étendre à $n=0$ si on remplace le logarithme du module par le logarithme p-adique dans la formule donnant $L(1,\chi)$:

Proposition 3.5.– *Soit χ un caractère de Dirichlet primitif non trivial pair de conducteur f ; soit ζ une racine primitive f-ième de l'unité. On a*

$$L_p(1,\chi)=-\left(1-\frac{\chi(p)}{p}\right).\frac{\tau(\chi)}{f}.\sum_{\substack{a=1\\(a,f)=1}}^{f}\overline{\chi}(a)\log_p(1-\zeta^a).$$

Sachant que $L(1,\chi)$ n'est pas nul pour χ pair, $\chi\neq\chi^o$, on déduit du corollaire 3.1 $L_p(1,\chi)\neq 0$; on obtient même que ce nombre est transcendant, et on peut en donner une minoration explicite (cf. Y. Morita, Transcendental numbers and related topics, Kyoto University, R.I.M.S. Kokyuroku 599, Oct. 1986, 95-107.).

Soit k un corps de nombres abélien sur $\mathbb{Q}$ et totalement réel ; k est contenu dans un corps cyclotomique $\mathbb{Q}(\zeta_m)$, où ζ_m est une racine primitive de l'unité, et le plus petit m avec cette propriété est le conducteur f du corps k. Le groupe de Galois de k sur $\mathbb{Q}$ est formé de restrictions à k d'automorphismes de $\mathbb{Q}(\zeta_f)$, de la forme $\zeta_f \longrightarrow \zeta_f^s$, avec $(s,f)=1$, et les caractères de $G(k/\mathbb{Q})$ s'identifient à des caractères de Dirichlet modulo f. Soit X le groupe de caractères de Dirichlet correspondant ainsi à k. Alors on peut déterminer le signe de $R_p(k)$, et choisir une racine carrée du discriminant D de k dans $\mathbb{C}_p$, de telle sorte que

$$\frac{2^{d-1}hR_p(k)}{\sqrt{D}}=\prod_{\substack{\chi\neq\chi^o\\ \chi\in X}}\left(1-\frac{\chi(p)}{p}\right)^{-1}.\ L_p(1,\chi).$$

La fonction zêta p-adique du corps k :

$$\zeta_{k,p}(s) = \prod_{\chi \in X} L_p(s,\chi)$$

a donc un pôle simple au point s=1, de résidu

$$\lim_{s \longrightarrow 1} (s-1)\zeta_{k,p}(s) = \frac{2^{d-1} h R_p(k)}{\sqrt{D}} \prod_{\chi \in X} (1 - \frac{\chi(p)}{p})$$

On peut donc exprimer le nombre $R_p(k)$ comme produit de facteurs, dont chacun est une combinaison linéaire de logarithmes p-adiques de nombres algébriques, et on peut minorer chacun des facteurs (cf. V.K. Grover, On the p-adic regulator of an abelian extension, Problèmes diophantiens 1979, Publ. Math. P. et M. Curie n°25, exp. n°4, 9p.) ; on trouve

$$|R_p(k)| > \exp\{-8f^2 p^{104f^2}\}.$$

On peut majorer f par $\Delta = |D|$, car le discriminant de k peut s'écrire

$$D = \prod_{\chi} \chi(-1) f(\chi),$$

tandis que f est le p.p.c.m. des $f(\chi)$.

Dans certains cas particuliers où on connait une démonstration purement algébrique (i.e. n'utilisant pas le théorème de Baker-Brumer) de la conjecture de Leopoldt, on peut donner des minorations plus précises de $R_p(k)$. Il en est ainsi par exemple si k est un corps cyclique totalement réel de degré premier (H.Miki, J.N.T., **26** (1987), 117-128).

Ce qui précède concerne le cas d'un corps de nombres totalement réel abélien sur $\mathbb{Q}$. Si on supprime l'hypothèse que $k/\mathbb{Q}$ est une extension abélienne, on sait encore que le résidu de la fonction zêta de Dedekind ζ_k du corps k (supposé totalement réel) est donné par

$$\frac{2^{d-1} h R(k)}{\sqrt{D}},$$

et que les nombres $\zeta_k(1-n)$, pour n entier ≥ 1, sont rationnels (Siegel, Shintani). On sait aussi construire une fonction p-adique $\zeta_{k,p}$ continue sur $\mathbb{Z}_p - \{1\}$ telle que

$$\zeta_{k,p}(1-n) = \zeta_k(1-n) E_p(-n) \quad \text{pour tout} \quad n \equiv 0 \bmod \varphi(q)$$

avec $E_p(s)=\prod_{\mathfrak{p}|p}(1-N\mathfrak{p}^{-s})$, et φ est l'indicatrice d'Euler (c.f. Serre, Cassou-Noguès, Barsky).

Le résidu en $s=1$ de $\zeta_{k,p}$ n'a pu être calculé que récemment, par P. Colmez, qui obtient la valeur

$$\frac{2^{d-1}hR_p(k)}{\sqrt{D}}.E_p(1).$$

(P. Colmez, Résidu en $s=1$ des fonctions zêta p-adiques ; manuscrit).

Références pour le §3.

J. AX.-
On the units of an algebraic number field ; Illinois Journal of Math., **8** (1967), 584-589.

A. BRUMER.-
On the units of algebraic number fields ; Mathematika, 14 (1967), 121-124.

J. FRESNEL.-
Rang p-adique du groupe des unités d'un corps de nombres ; Sém. Théorie Nombres Bordeaux, 1968-69, n°9, 18p.

K. IWASAWA.-
Lectures on p-adic L-functions ; Annals of Math. Studies, **74**, Princeton Univ. Press, 1972.

S. LANG.-
Cyclotomic fields ; Graduate texts in Math., **59**, Springer Verlag 1978 (en particulier §4.4 : the p-adic regulator).

L. WASHINGTON.-
Introduction to cyclotomic fields ; Graduate texts in Math., **83**, Springer Verlag 1982 (en particulier Chap. 5 : p-adic L-functions and Bernouilli numbers).

§4. Minorations du rang p-adique.

Après quelques généralités sur les représentations linéaires des groupes finis, nous présentons certains des résultats obtenus par Miyake (J. Math. Soc. Japan, **34** (1982), 515-525), Emsalem, Kisilevsky et Wales (J.N.T., **19** (1984), 384-391) ; en généralisant la méthode d'Ax, ils donnent des minorations du rang p-adique du groupe des unités d'une extension galoisienne de $\mathbb{Q}$, faisant intervenir les degrés des représentations du groupe de Galois. Par exemple, dans le cas d'une extension totalement imaginaire de groupe de Galois A_4 (groupe alterné d'ordre 12), la conjecture de Leopoldt est vérifiée. L'outil principal est le théorème de transcendance de Baker-Brumer.

Le théorème des six exponentielles permet de démontrer la conjecture de Leopoldt dans certains cas bien particuliers (pour une extension cubique, elle se déduit de la conjecture des quatre exponentielles p-adiques). Une généralisation de ce théorème de transcendance à plusieurs variables permet de minorer $r_p(k)$ par $r(k)/2$ pour tout corps de nombres k ; la conjecture de Leopoldt s'énonce $r_p(k)=r(k)$, et nous montrons qu'elle est une conséquence de la conjecture 2.11 sur l'indépendance algébrique de logarithmes p-adiques de nombres algébriques.

a) Représentations linéaires.

Nous avons déjà rencontré des représentations linéaires de groupes compacts (Chap.2, §4a). Nous avons besoin maintenant de renseignements plus précis (classiques) sur les représentations linéaires des groupes finis (Cf. Serre, Représentations linéaires des groupes finis, §1,2 et 6 ; Lang, Algebra, 2nd Ed. 1984, Chap.18).

Soit K un corps de caractéristique nulle, et soit G un groupe fini d'ordre d. L'ensemble $X=X(K)=\{\chi_1,\dots,\chi_h\}$ des caractères de G irréductibles sur K est fini ; le nombre $h=h(K)$ d'éléments de X dépend de K ; si K est algébriquement clos, alors h est le nombre de classes de conjugaisons de G, et X forme une base de l'espace des fonctions centrales sur G à valeurs dans K.

Toute représentation linéaire $\rho : G \longrightarrow GL(V)$ de G (où V est un K-espace vectoriel de dimension finie) se décompose de manière canonique en somme directe $\rho=\bigoplus_{\chi\in X}\rho_\chi$, où chaque ρ_χ est somme directe de représentations irréductibles $\rho_{\chi,1},\dots,\rho_{\chi,m_\chi}$ ayant toutes pour caractère χ, de sorte que le caractère χ_ρ de ρ est donné par :

$$\chi_\rho=\sum_{\chi\in X} m_\chi\chi.$$

Deux représentations sont isomorphes si et seulement si elles ont même caractère, c'est-à-dire les mêmes coefficients m_χ. Le nombre m_χ est *la multiplicité du caractère* χ *dans la représentation* ρ, et on dit qu'un caractère χ *intervient dans la représentation* ρ si $m_\chi>0$.

La *représentation régulière* de G est définie de la manière suivante : soit V un K-espace vectoriel de dimension d égale à l'ordre de G ; on choisit une base $(e_\sigma)_{\sigma\in G}$ de V indexée par G, et on définit

$$r=r^{(G)} : G \longrightarrow GL(V)$$

par

$$r_\sigma\Big(\sum_{s\in G} a_s e_s\Big) = \sum_{s\in G} a_s e_{\sigma s} \qquad (\sigma\in G,\ a_s\in K).$$

Le sous-espace W de dimension 1 de V engendré par l'élément $\sum_{s\in G} e_s$ est stable sous l'action de G, et un supplémentaire stable est l'hyperplan

$$W^o=\Big\{\sum_{s\in G} x_s e_s\in V\ ;\ \sum_{s\in G} x_s=0\Big\}$$

La sous-représentation W a pour caractère χ^o, et W^o a pour caractère $\chi_{reg}-\chi^o$, où χ_{reg} est le caractère de la représentation régulière.

Par exemple, si G est cyclique d'ordre 3, la représentation W^o est irréductible sur $\mathbb{Q}$, de degré 2.

Si K est algébriquement clos, alors

$$\chi_{reg} = \sum_{\chi \in X} d_\chi \chi,$$

où d_χ est le degré de χ, de sorte que $d = \sum_{\chi \in X} d_\chi^2$.

Considérer une représentation linéaire $\rho : G \longrightarrow GL(V)$ comme ci-dessus revient à considérer un $K[G]$-module à gauche V, avec l'action

$$\Big(\sum_{\sigma \in G} a_\sigma \sigma\Big).x = \sum_{\sigma \in G} a_\sigma \rho_\sigma(x), \qquad (x \in V,\ a_\sigma \in K).$$

La décomposition précédente de ρ correspond à une décomposition $V = \bigoplus_{\chi \in X} V_\chi$ de V en somme directe de sous-$K[G]$-modules V_χ appelés *composantes isotypiques de* V ; pour chaque $\chi \in X$, V_χ, qui est *la* χ*-partie de* V, est somme directe de $K[G]$-sous-modules simples $W_{\chi,j}$ $(1 \leq j \leq m_\chi)$ tous isomorphes :

$$V_\chi = W_{\chi,1} \oplus \ldots \oplus W_{\chi,m_\chi}$$

(cf. Lang, op. cit., Chap.17 §1). La dimension de $W_{\chi,j}$ est égale au degré d_χ du caractère χ, et $\dim V = \sum_{\chi \in X} d_\chi m_\chi$.

Dans une base de V réunion de bases des V_χ, pour chaque $\sigma \in G$ la matrice N^σ associée à ρ_σ s'écrit comme une matrice diagonale par blocs :

$$N^\sigma = \begin{bmatrix} N^\sigma_{\chi_1} & & 0 \\ & \ddots & \\ 0 & & N^\sigma_{\chi_h} \end{bmatrix}$$

où chaque N^σ_χ $(\chi \in X)$, correspond à un automorphisme de V_χ (restriction de ρ_σ à V_χ) ; si la base de V_χ est réunion de bases des $W_{\chi,j}$, la matrice N^σ_χ est aussi diagonale par blocs :

$$N^\sigma_\chi = \begin{bmatrix} N^\sigma_{\chi,1} & & 0 \\ & \ddots & \\ 0 & & N^\sigma_{\chi,m_\chi} \end{bmatrix}$$

où chaque $N^\sigma_{\chi,j}$ $(\chi \in X)$, est une matrice $d_\chi \times d_\chi$ inversible.

Il reste donc à étudier les $K[G]$-modules irréductibles, et pour cela on va regarder l'anneau $R = K[G]$ comme module sur lui-même (à gauche, disons ; c'est la représentation régulière). Comme l'anneau R est semi-simple, on commence par étudier les idéaux à gauche simples (Lang, op. cit., Chap.17 §4).

Il n'y a qu'un nombre fini de classes d'isomorphisme d'idéaux à gauche simples de $K[G]$; pour $\chi\in X(K)$, notons C_χ la classe d'isomorphisme de R-modules simples ayant pour caractère χ. Pour chaque $\chi\in X$, soit R_χ la somme des idéaux à gauche simples de R dans la classe C_χ. Alors R_χ est un idéal bilatère de R, et la restriction à R_χ des opérations de R donne à R_χ une structure d'anneau, de sorte que R soit isomorphe au produit direct des R_χ. Soit ϵ_χ l'élément unité de R_χ. Alors $(\epsilon_\chi)_{\chi\in X}$ forme une famille d'idempotents centraux primitifs orthogonaux de somme 1 ; autrement dit les ϵ_χ sont idempotents : $\epsilon_\chi^2=\epsilon_\chi$, orthogonaux : $\epsilon_\chi\epsilon_\psi=0$ pour $\chi\neq\psi$, ils sont centraux : $\epsilon_\chi\alpha=\alpha\epsilon_\chi$ pour tout $\alpha\in K[G]$ (il suffit de le vérifier pour $\alpha\in G$), ils sont primitifs, c'est-à-dire que ϵ_χ n'est pas nul et n'est pas somme de plusieurs idempotents centraux non nuls ; enfin $\sum_{\chi\in X}\epsilon_\chi=1$.

L'idéal bilatère R_χ est la χ-composante de la décomposition isotypique de $K[G]$, et plus généralement, si V est un $K[G]$-module, alors

$$V=\bigoplus_{\chi\in X} R_\chi V$$

et $R_\chi V=\epsilon_\chi V$ est la χ-composante isotypique de V.

On peut écrire explicitement un système complet d'idempotents centraux de $K[G]$:

$$\epsilon_\chi=\frac{r_\chi}{d}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\ ;$$

chaque R_χ est somme directe de d_χ idéaux à gauche minimaux isomorphes entre eux

$$R_\chi=W_{\chi 1}\oplus\ldots\oplus W_{\chi d_\chi}\ ,$$

et pour $1\leq i\leq d_\chi$ il existe $\ell_{\chi i}\in K[G]$ tel que $W_{\chi i}=W_{\chi 1}\ell_{\chi i}$; la dimension de $W_{\chi i}$ sur K est r_χ, celle de R_χ est $r_\chi d_\chi$. Si K est algébriquement clos, on a $r_\chi=d_\chi$.

Pour chaque $\chi\in X$, soit $\rho_\chi : G\longrightarrow GL_{d_\chi}(K)$ la représentation de G de caractère χ (unique à isomorphisme près). On prolonge ρ_χ en un homomorphisme d'algèbres de $K[G]$ dans l'algèbre $M(K,d_\chi)$ des matrices $d_\chi\times d_\chi$ à coefficients dans K, et, quand K est algébriquement clos, leur

somme directe donne un isomorphisme entre $K[G]$ et $\prod_{\chi\in X} M(K,d_\chi)$; l'image de l'idempotent e_χ a toutes ses composantes nulles, sauf celle d'indice χ qui vaut 1.

A un $\mathbb{Z}[G]$-module de type fini M, on associe un $K[G]$-module $V=M\otimes_{\mathbb{Z}}K$ (le corps K étant de caractéristique nulle), de dimension sur K égale au rang sur $\mathbb{Z}$ de M ; en termes de représentations linéaires, si $\alpha_1,\dots,\alpha_m$ est une base de M/M_{tors}, on prend pour V un K-espace vectoriel de dimension m, avec une base $e_1,\dots,e_m$, et, en écrivant

$$\sigma\alpha_i=\zeta_i \prod_{j=1}^{m} \alpha_j^{m_{ij}},$$

la représentation est définie par

$$\rho_\sigma(e_i)=\sum_{j=1}^{m} m_{ij}e_j.$$

De même si K est une extension de $\mathbb{Q}_p$, à un $\mathbb{Z}_p$-module de type fini M, on associe un $K[G]$-module $V=M\otimes_{\mathbb{Z}_p} K$ (et une représentation linéaire de degré égal au rang sur $\mathbb{Z}_p$ de M).

b) La méthode d'Ax.

Soient K un corps de caractéristique nulle, G un groupe fini, et M la matrice du groupe G :

$$M = \left(X_{\sigma\circ\tau^{-1}}\right)_{(\sigma,\tau)\in G\times G},$$

à coefficients dans le corps $F=K(\mathbf{X})$, $\mathbf{X}=(X_\sigma)_{\sigma\in G}$, dont nous avons étudié le déterminant au §2.c.

Pour $\sigma\in G$, la matrice représentant l'automorphisme r_σ (où r est la représentation régulière de G), dans la base $(e_s)_{s\in G}$ pour laquelle $r_\sigma(e_s)=e_{\sigma s}$, est obtenue en remplaçant dans M les variables $(X_\tau)_{\tau\in G}$ par $(\delta_{\sigma\tau})_{\tau\in G}$, avec $\delta_{\sigma\tau}=1$ si $\sigma=\tau$, et $\delta_{\sigma\tau}=0$ si $\sigma\neq\tau$.

Cette matrice M est associée à l'endomorphisme f de $F[G]$ qui envoie $\sum_{\tau\in G} a_\tau \tau$ sur

$$\sum_{\sigma\in G}\ \sum_{\tau\in G} a_\tau X_{\sigma\circ\tau^{-1}\sigma}.$$

Comme

$$\sum_{\sigma\in G} X_{\sigma\circ\tau^{-1}\sigma} = \sum_{s\in G} X_s s\circ\tau,$$

l'endomorphisme f n'est autre que la multiplication à gauche par $\sum_{s\in G} X_s s$. On notera encore $f=\sum_{s\in G} X_s s\in F[G]$, de sorte que $f(\tau)=f.\tau$ dans $F[G]$.

Supposons pour commencer K algébriquement clos, et choisissons une base de $K[G]$ de la forme

$$\{e_{j,\chi}.\iota_{\chi i}\ ;\ 1\le i,j\le d_\chi,\ \chi \text{ caractère irréductible de } G\},$$

où, pour chaque χ, $\{e_{j,\chi}\ ;\ 1\le j\le d_\chi\}$ est une base de $W_{\chi 1}$.

Dans cette nouvelle base (que nous prenons comme base sur F de $F[G]=K[G]\otimes_K F$), la matrice N associée à f est formée de blocs diagonaux :

$$N = \begin{bmatrix} N_{\chi_1} & & 0 \\ & \ddots & \\ 0 & & N_{\chi_h} \end{bmatrix}$$

où chaque N_χ $(\chi\in X)$, est de la forme :

$$N_\chi = \begin{bmatrix} N_{\chi 1}. & & 0 \\ & \ddots & \\ 0 & & N_{\chi d_\chi} \end{bmatrix},$$

d_χ étant le degré du caractère χ. Pour $\chi\in X$ et $1\le j\le d_\chi$, la matrice $N_{\chi j}$ représente l'action de la multiplication à gauche par $f=\sum_{\sigma\in G} X_\sigma\sigma$ sur l'idéal à gauche minimal $W_{\chi j}\otimes_K F$. Grâce au choix que nous avons fait pour la nouvelle base, on a $N_{\chi j}=N_{\chi 1}$ pour $\chi\in X$ et $1\le j\le d_\chi$:

$$N_\chi = \begin{bmatrix} N_{\chi 1}. & & 0 \\ & \ddots & \\ 0 & & N_{\chi 1} \end{bmatrix}.$$

D'autre part il existe une matrice inversible $P\in GL_d(K)$ telle que $M=P^{-1}NP$. Les coefficients des matrices $N_{\chi 1}$ sont donc des formes linéaires (de degré 1) en $X=(X_\sigma)_{\sigma\in G}$ à coefficients dans K.

On remarque que les représentations de degré 1 donnent bien des valeurs propres de M : si χ est un caractère de degré 1 sur K, on a

$$\sum_{\sigma\in G}\chi_\sigma\sigma.\sum_{\tau\in G}\chi(\tau^{-1})\tau=\sum_{\sigma\in G}\chi(\sigma)X_\sigma.\sum_{\tau\in G}\chi(\tau^{-1})\tau,$$

et $\sum_{\sigma\in G}\chi(\sigma)X_\sigma$ est une valeur propre de f.

Considérons maintenant un corps de nombres k totalement réel galoisien sur $\mathbb{Q}$, fixons un plongement de k dans $\mathbb{C}_p$, prenons $G=G(k/\mathbb{Q})$, et choisissons une unité de Minkowski ϵ dans k. Le rang p-adique du groupe des unités de k est le rang r_p de la matrice

$$M^{(p)}=\left(\log_p\sigma\circ\tau^{-1}\epsilon\right)_{\sigma,\tau\in G}$$

dont les coefficients sont dans $\mathbb{C}_p$. Quand on remplace dans la matrice M ci-dessus (avec $K=\bar{\mathbb{Q}}\subset\mathbb{C}_p$) les indéterminées X_σ par $\log_p\sigma\epsilon$, on voit que $M^{(p)}$ est la matrice associée à l'action à gauche de $f_p=\sum_{\sigma\in G}(\log_p\sigma\epsilon).\sigma\in\mathbb{C}_p[G]$ sur $\mathbb{C}_p[G]$. Notons $N^{(p)},N_\chi^{(p)},N_{\chi j}^{(p)}$ les matrices obtenues à partir de N, N_χ, $N_{\chi j}$ en remplaçant χ_σ par $\log_p\sigma\epsilon$. On a encore $M^{(p)}=P^{-1}N^{(p)}P$, $N_{\chi j}^{(p)}=N_{\chi 1}^{(p)}$, et $N_{\chi j}^{(p)}$ représente l'action de la multiplication à gauche par f_p sur $W_{\chi j}$. Les coefficients des matrices $N_{\chi j}^{(p)}$ sont des combinaisons linéaires des $\log_p\sigma\epsilon$ à coefficients algébriques sur $\mathbb{Q}$.

Si χ est un caractère de degré 1, M_χ a une seule ligne et une seule colonne, et, grâce au théorème de Baker-Brumer, la valeur propre, qui est :

$$\sum_{\sigma\in G}\chi(\sigma)\log_p\sigma\epsilon=\sum_{\sigma\neq 1}(\chi(\sigma)-\chi^0(\sigma))\log_p\sigma\epsilon,$$

est non nulle si et seulement si $\chi\neq\chi^0$: en effet, les nombres $\log_p\sigma\epsilon$, $(\sigma\in G,\ \sigma\neq 1)$, sont $\mathbb{Q}$-linéairement indépendants, et les coefficients $\chi(\sigma)-\chi^0(\sigma)=\chi(\sigma)-1$ sont des nombres algébriques qui ne sont pas tous nuls si $\chi\neq\chi^0$.

Si χ est le caractère d'une représentation irréductible de degré >1, montrons que la matrice N_χ n'est pas nulle. Cela revient à voir que l'action de f sur $R_\chi\otimes_K\mathbb{C}_p$ n'est pas triviale. Or l'image par $f=\sum_{\sigma\in G}(\log_p\sigma\epsilon)\sigma$ de $\epsilon_\chi=\frac{d_\chi}{d}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma$ a comme composante sur $\sigma=1$ dans $\mathbb{C}_p[G]$

$$\frac{d_\chi}{d}\sum_{\sigma\in G}\chi(\sigma)\log_p\sigma\epsilon,$$

et ce nombre n'est pas nul grâce au théorème de Baker-Brumer.

Par conséquent : *si* k *est un corps de nombres galoisien sur* $\mathbb{Q}$ *et totalement réel, alors* $r_p(k) \geq \sum_{\chi \neq \chi^o} d_\chi$, *où la somme est étendue aux caractères de* G *irréductibles sur* $\mathbb{C}_p$, *avec* $\chi \neq \chi^o$.

Nous allons étendre ce qui précède à un corps de nombres galoisien sur $\mathbb{Q}$ et imaginaire, et aussi à une extension galoisienne d'un corps quadratique imaginaire k_o. En même temps nous raffinerons un peu le résultat en considérant la décomposition en caractères irréductibles sur $\mathbb{Q}_p$.

On prend donc un corps k_o qui est ou bien le corps $\mathbb{Q}$, ou bien un corps imaginaire quadratique ; soit k une extension galoisienne de k_o. Notons $G=G(k/k_o)$ le groupe de Galois.

Le groupe des unités E de k est un $\mathbb{Z}[G]$-module ; notons χ_E le caractère sur $\mathbb{Q}$ de $E\otimes_{\mathbb{Z}}\mathbb{Q}$. Le degré de χ_E est le nombre de Dirichlet r.

Commençons par supposer k totalement réel, et montrons $\chi_E=\chi_{reg}-\chi^o$. On peut utiliser l'existence d'une unité de Minkowski (proposition 1.5) : le $\mathbb{Z}[G]$-module engendré par ϵ est d'indice fini dans E, c'est-à-dire $E\otimes_{\mathbb{Z}}\mathbb{Q}\simeq\mathbb{Q}[G]\epsilon$. Si a_σ, $(\sigma\in G)$ sont des entiers rationnels tels que

$$\prod_{\sigma\in G} \sigma\epsilon^{a_\sigma}=1,$$

alors $a_\sigma=a_1$ pour tout $\sigma\in G$. Autrement dit l'annulateur de $E\otimes_{\mathbb{Z}}\mathbb{Q}$ dans $\mathbb{Q}[G]$

$$I=\{\sum_{\sigma\in G} a_\sigma\sigma\in\mathbb{Q}[G] \ ; \ \prod_{\sigma\in G}\sigma\epsilon^{a_\sigma}=1\}$$

est l'idéal principal engendré par $\sum_{\sigma\in G}\sigma$. Le quotient a pour caractère $\chi_{reg}-\chi^o$.

On peut aussi démontrer l'égalité $\chi_E=\chi_{reg}-\chi^o$ dans le cas totalement réel en se plaçant sur $\mathbb{R}$: dans le plongement logarithmique (dont la restriction à E est de noyau fini), le $\mathbb{R}$-espace vectoriel engendré par l'image de E est l'hyperplan $x_1+\ldots+x_d=0$ de $\mathbb{R}^d$; l'action de G sur $\mathbb{R}^d$ est donnée par la représentation régulière (en écrivant $\mathbb{R}^d=\mathbb{R}[G]$) ; l'action de G sur l'hyperplan est, nous l'avons vu, donnée par le caractère $\chi_{reg}-\chi^o$.

Si k est une extension d'un corps imaginaire quadratique k_o, on a encore $\chi_E=\chi_{reg}-\chi^o$; on le voit par exemple en utilisant le théorème de Herbrand (cf. théorème 3.3). Enfin, si k est une extension galoisienne de $\mathbb{Q}$ totalement imaginaire de groupe de Galois G, on choisit un plongement de k dans $\mathbb{C}$, et on désigne par $\tau\in G$ la restriction à k de la conjugaison complexe ; dans le plongement logarithmique de k^* dans $\mathbb{R}^{d/2}$, l'action de G sur $\mathbb{R}^{d/2}$ est la représentation de permutation des classes à droite modulo $\{1,\tau\}$, et le caractère χ_E est le caractère de cette représentation moins le caractère unité. Sur une clôture algébrique,

$$\chi_E=\sum_{\chi\in X(\overline{\mathbb{Q}}),\,\chi\neq\chi^o}\frac{1}{2}(\chi(1)+\chi(\tau))\chi.$$

Bien entendu, si k est à la fois une extension galoisienne de $\mathbb{Q}$ et une extension galoisienne d'un corps imaginaire quadratique, on obtient deux descriptions équivalentes de χ_E.

On plonge un sous-groupe d'indice fini des unités globales de k dans le groupe U^1 des unités semi-locales (§2.a), et c'est le $\mathbb{Z}_p$-module $\overline{E}$ engendré par l'image qui nous intéresse. Dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^*$, $\overline{E}$ est stable sous l'action de G (l'action de G sur $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ a été définie avant le lemme 2.5). Donc $\overline{E}$ est un $\mathbb{Z}_p[G]$-module ; soit $\chi_{\overline{E}}$ le caractère de G sur $\mathbb{Q}_p$ correspondant à $\overline{E}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$. Le rang p-adique des unités de k est donc le degré de $\chi_{\overline{E}}$.

Il s'agit maintenant de comparer les deux caractères $\chi_{\overline{E}}$ et χ_E. La conjecture de Leopoldt revient à dire qu'ils coïncident sur $\mathbb{Q}_p$ (i.e. $\chi_{\overline{E}}=\chi_{E\otimes\mathbb{Q}_p}$). Décomposons-les tous deux en somme de caractères irréductibles sur $\mathbb{Q}_p$.

Lemme 4.1.- *Soit χ un caractère de G irréductible sur $\mathbb{Q}_p$. Si χ intervient dans la décomposition de $E\otimes_{\mathbb{Z}}\mathbb{Q}_p$, alors χ intervient aussi dans la décomposition de $\overline{E}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.*

Démonstration.- Notons L la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{Q}_p$; si $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_p$, alors $L=\overline{\mathbb{Q}}\cap\mathbb{Q}_p$. Les caractères irréductibles sur $\mathbb{Q}_p$ ou sur L sont les mêmes. D'autre part le théorème de Baker-Brumer (introduction, théorème 4.1) entraîne que l'injection de E^1 dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^*$ se prolonge en un homomorphisme injectif de $E^1\otimes_{\mathbb{Z}}L$ dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^*$: des éléments de E^1 linéairement indépendants sur $\mathbb{Q}$ restent linéairement indépendants sur L. Si E' est le L-espace vectoriel engendré par l'image de E^1, on a $E'\simeq E\otimes_{\mathbb{Z}}L$, et $\chi_{E'}=\chi_{E\otimes_{\mathbb{Z}}L}$.

Dire que la χ-composante de $E\otimes_{\mathbb{Z}}L$ n'est pas nulle revient à dire que $\epsilon_\chi E'$ n'est pas réduit à 0, quand ϵ_χ est l'idempotent associé à χ. Mais comme $\overline{E}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ est l'adhérence de E' dans $(k\otimes_{\mathbb{Q}}\mathbb{Q}_p)^*$, ceci équivaut à $\epsilon_\chi(\overline{E}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)\neq 0$; donc les caractères irréductibles qui interviennent dans la décomposition de $\overline{E}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ sur $\mathbb{Q}_p$ sont les mêmes que ceux qui interviennent dans la décomposition de $E\otimes_{\mathbb{Z}}\mathbb{Q}_p$.

Nous avons donc démontré :

Théorème 4.2.- *Soit* k *un corps de nombres galoisien sur* $\mathbb{Q}$ *(resp. sur un corps imaginaire quadratique* k_0*), et soit* $G=G(k/\mathbb{Q})$ *(resp.* $G=G(k/k_0)$*). Soit* S *la famille des caractères irréductibles de* G *qui interviennent dans la décomposition de* $E\otimes_{\mathbb{Z}}\mathbb{Q}_p$*. Alors*

$$r_p \geq \sum_{\chi\in S} d_\chi,$$

où d_χ *est le degré de* χ.

On retrouve en particulier le théorème 3.3 (Ax-Brumer) : si G est abélien, alors $r_p=r$. On obtient plus généralement $r_p=r$ si $r_\chi=1$ pour tout χ caractère de G irréductible sur $\mathbb{Q}_p$, c'est-à-dire si $\mathbb{Q}_p[G]$ est un produit de corps (pour $p\neq 2$, cela ne se produit que si G est abélien ; voir Miyake, Prop.5).

Voici un autre corollaire intéressant :

Corollaire 4.3.- *Soit* k *un corps de nombres imaginaire galoisien sur* $\mathbb{Q}$ *de groupe de Galois* $G(k/\mathbb{Q})=A_4$ *(groupe alterné d'ordre 12). Alors pour tout nombre premier* p, *le corps* k *vérifie la conjecture de Leopoldt.*

Démonstration.- En effet, A_4 admet quatre représentations irréductibles, trois de degré 1, disons χ^o, χ_1, χ_2, et une de degré 3, disons Ψ. Le nombre de Dirichlet est 5, donc la multiplicité de Ψ dans χ_E est au plus 1 ; comme $\chi_E \leq \chi_{reg}-\chi^o=\chi_1+\chi_2+3\Psi$, on en déduit $\chi_E=\chi_1+\chi_2+\Psi$; la somme des degrés des représentations χ_1, χ_2, Ψ est 5, d'où le corollaire.

Exercice.- Soient k un corps de nombres galoisien sur $\mathbb{Q}$ totalement réel, et soit A (resp. B) un sous-groupe (resp. un quotient) abélien de G d'ordre a (resp. b). Vérifier $r_p \geq a-1$ (resp. b-1).

c) Minoration par la moitié du nombre de Dirichlet.

Nous allons utiliser le résultat de transcendance suivant (cf. M. Waldschmidt, Transcendance et exponentielles en plusieurs variables, Invent. Math. **63** (1981), 97-127)

Théorème 4.4.- *Soient* k *un corps de nombres,* φ *un plongement de* k *dans* $\mathbb{C}$, p *un nombre premier,* φ_p *un plongement de* k *dans* $\mathbb{C}_p$, *et* α_{ij}, $(1\leq i\leq d,\ 1\leq j\leq \ell)$ *des éléments de* k. *On suppose*

$$|\varphi_p \alpha_{ij}|_p = 1 \quad \text{pour} \quad 1\leq i\leq d,\ 1\leq j\leq \ell.$$

Soit r *le rang de la matrice à coefficients réels*

$$\left(\log|\varphi\alpha_{ij}|\right)_{(1\leq i\leq d,\ 1\leq j\leq \ell)},$$

et soit r_p *le rang de la matrice à coefficients p-adiques*

$$\left(\log_p \varphi_p \alpha_{ij}\right)_{(1\leq i\leq d,\ 1\leq j\leq \ell)}.$$

Alors $r_p \geq r/2$.

Nous en déduisons :

Corollaire 4.5.- *Soient* k *un corps de nombres,* p *un nombre premier,* r *le nombre de Dirichlet de* k, *et* r_p *le rang* p-*adique du groupe des unités de* k. *Alors* $r_p \geq r/2$.

Autrement dit le défaut $\delta_p(k)=r-r_p$ de la conjecture de Leopoldt est majoré par $r/2$.

Démonstration du corollaire 4.5.- Soit K une clôture galoisienne de k sur $\mathbb{Q}$, et soient $\sigma_1,\ldots,\sigma_d$ les plongements de k dans K. Le nombre r_p est égal au rang de la matrice

$$\left(\log_p \varphi_p \circ \sigma_j \epsilon_i\right)_{1\leq j\leq d,\ 1\leq i\leq r'}$$

quand $\epsilon_1,\ldots,\epsilon_r$ est un système indépendants d'unités de k, et φ_p un plongement de K dans $\mathbb{C}_p$. Mais si φ est un plongement de K dans $\mathbb{C}$, la matrice

$$\left(\log|\varphi\circ\sigma_j \epsilon_i|\right)_{1\leq j\leq d,\ 1\leq i\leq r}$$

a pour rang r, par le théorème de Dirichlet ; d'où le résultat grâce au théorème 4.4.

Si $r_p<r$ pour un corps de nombres k, alors on construit un caractère p-adique de $Gal(k^{ab}/k)$ qui n'est pas localement rationnel de la manière suivante : l'hypothèse $r_p<r$ montre qu'il existe des entiers p-adiques $a_1,\ldots,a_d$ non tous nuls tels que

$$\sum_{i=1}^{d} a_i \log_p \varphi_i \epsilon = 0 \qquad \text{pour tout } \epsilon\in E,$$

$\varphi_1,\ldots,\varphi_d$ désignant les plongements de k dans $\mathbb{C}_p$. Alors on définit, sur un voisinage de 1, un homomorphisme de k^* dans $\mathbb{C}_p^*$ en envoyant $\alpha\in k^*$ sur $\prod_{i=1}^{d} \varphi_i\alpha^{a_i}$, et cet homomorphisme est trivial sur E. Si les a_i ne sont pas tous multiples rationnels de l'un d'eux, on obtient un caractère p-adique de $\mathbf{C}_k$ qui n'est pas de type (A).

d) Indépendance algébrique de logarithmes p-adiques.

Pour terminer, nous montrons que la conjecture de Leopoldt est une conséquence de la conjecture sur l'indépendance algébrique de logarithmes p-adiques de nombres algébriques. Il est clair, d'après la démonstration du corollaire 4.5, qu'il suffit d'établir le résultat suivant :

Proposition 4.6.- *Admettons la conjecture* 2.11. *Alors, sous les hypothèses du théorème* 4.4, *on a* $r_p=r$.

Démonstration.- On peut évidemment supposer $\ell=d=r$. On reprend les arguments de la démonstration du corollaire 3.1. On écrit

$$\alpha_{ij}=\zeta_{ij}\cdot\prod_{\tau=1}^{t}\gamma_\tau^{c_{ij\tau}},\quad (1\le i\le j\le r),$$

avec $\zeta_{ij}\in W_k$, $c_{ij\tau}\in\mathbb{Z}$, et $\gamma_1,\dots,\gamma_t$ multiplicativement indépendants dans k^*, vérifiant $|\varphi_p(\gamma_\tau)|_p=1$.

Supposons que le déterminant de la matrice

$$\left(\log_p\varphi_p\alpha_{ij}\right)_{(1\le i\le j\le r)}$$

soit nul ; alors le polynôme

$$\det\left(\sum_{\tau=1}^{t}c_{ij\tau}X_\tau\right)_{1\le i,j\le r}$$

s'annule au point $(\log_p\varphi_p\gamma_\tau)_{1\le\tau\le t}$; mais les nombres p-adiques $\log_p\varphi_p\gamma_1,\dots,\log_p\varphi_p\gamma_t$ sont linéairement indépendants sur $\mathbb{Q}$, donc la conjecture 2.11 entraîne que ce polynôme est nul dans $\mathbb{Q}[X_1,\dots,X_t]$. Ecrivons que ce polynôme s'annule au point $(\log|\varphi\gamma_\tau|)_{1\le\tau\le t}$: on trouve que le déterminant de la matrice

$$\left(\log|\varphi\alpha_{ij}|\right)_{(1\le i\le j\le r)}$$

est nul, ce qui donne la contradiction voulue.

Remarque.- On peut généraliser la proposition 4.6 aux matrices dont les coefficients sont des combinaisons linéaires de logarithmes de nombres algébriques :

$$\left[\sum_{\sigma=1}^{s} \varphi_p \beta_{ij\sigma} \cdot \log_p \varphi_p \alpha_{ij\sigma}\right]$$

de manière à contenir le corollaire 3.1.

Références pour le §4.-

M. EMSALEM.-
Une minoration du rang p-adique du groupe des unités d'un corps de nombres totalement réel ; Problèmes Diophantiens, (1980/81), Publ. Math. Univ. P.et M.Curie, N°**43** , 18p.

M. EMSALEM, H.H. KISILEVSKY, and D.B. WALES.-
Indépendance linéaire sur $\overline{\mathbb{Q}}$ de logarithmes de nombres algébriques et rang p-adique du groupe des unités d'un corps de nombres ; J. Number Theory, **19** (1984), 384-391.

K. MIYAKE.-
On the units of an algebraic number field ; J. Math. Soc. Japan, **34** (1982), 515-525.

M. WALDSCHMIDT.-
A lower bound for the p-adic rank of the units of an algebraic number field ; Coll. Math. Soc. Janos Bolyai **34**., Topics in Classical Number Theory, Budapest 1981, p.1617-1650.

§5. Rang p-adique de sous-$\mathbb{Z}[G]$ modules de k^*.

Soit k un corps de nombres galoisien sur $\mathbb{Q}$. On remplace, dans l'étude qui précède, le groupe E des unités de k par un sous-groupe M de type fini de k^* stable sous l'action de $G(k/\mathbb{Q})$. Jaulent décrit de manière conjecturale le caractère p-adique de l'image de M dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ par l'application logarithme LOG. Le statut de cette conjecture est analogue à celui de la conjecture de Leopoldt : on sait la démontrer pour une extension abélienne de $\mathbb{Q}$ ou d'un corps imaginaire quadratique ; on peut aussi la déduire de la conjecture sur l'indépendance algébrique de logarithmes p-adiques ; les minorations du rang par la somme des degrés des caractères irréductibles s'étendent bien. Mais ici, en plus, on peut la démontrer en supposant le groupe M suffisamment gros.

a) La conjecture de Jaulent.

Soient k un corps de nombres galoisien sur $\mathbb{Q}$, p un nombre premier, et M un sous-groupe de type fini de k^*, stable sous l'action de $G=G(k/\mathbb{Q})$, c'est-à-dire un sous-$\mathbb{Z}[G]$-module de k^*. On notera χ_M le caractère du $\mathbb{Q}[G]$-module $M\otimes_{\mathbb{Z}}\mathbb{Q}$.

Pour simplifier nous supposerons que les éléments de M sont étrangers à p, c'est-à-dire que M est contenu dans le sous-groupe k' de k^* suivant :

$$k'=\{\alpha\in k \ ; \ v_p(\alpha)=0 \ \text{ pour tout } \ \mathfrak{p}|p\}.$$

On reprend la construction du §2 en remplaçant E par M : désignons par $\overline{M}$ l'adhérence de $\mathrm{LOG}(M)$ dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$, c'est-à-dire le $\mathbb{Z}_p$-module engendré par les logarithmes des éléments de M dans $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$. Comme M est stable sous l'action de G, il en est de même de $\overline{M}$, et $\overline{M}$ est un $\mathbb{Z}_p[G]$-sous-module de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$.

Quand on plonge M dans le groupe des unités semi-locales $U^1=\prod_{p|p} U^1_p$, le sous-groupe $M^1=\{x\in M \ ; \ i(x)\in U^1\}$ est d'indice fini dans M, et le $\mathbb{Z}_p[G]$-module $\overline{M}$ a même rang sur $\mathbb{Z}_p$ que l'adhérence de $i(M^1)$ dans U^1.

Une troisième description de $\overline{M}$ est obtenue en fixant un plongement de k dans $\mathbb{C}_p$, en notant K l'adhérence de k, et en prenant l'adhérence de l'image de M dans $K[G]$ par $\mathcal{LOG}$ (cf. §2.b).

Nous nous intéressons au caractère $\chi_{\overline{M}}$ de $\overline{M}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, et à son degré $r_M^{(p)}$, qui est le rang sur $\mathbb{Z}_p$ de $\overline{M}$ (et la dimension sur $\mathbb{Q}_p$ de $\overline{M}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$).

Quand ψ_1 et ψ_2 sont deux caractères de G sur $\mathbb{Q}_p$ dont la décomposition en somme de caractères irréductibles sur $\mathbb{Q}_p$ est

$$\psi_i=\sum_{\chi\in X(\mathbb{Q}_p)} m_i(\chi)\chi, \qquad (i=1,2),$$

nous désignerons par $\psi_1\wedge\psi_2$ le caractère

$$\sum_{\chi\in X(\mathbb{Q}_p)} \min\{m_1(\chi),m_2(\chi)\}\chi.$$

Nous convenons d'écrire $\psi_1\leq\psi_2$ si $\psi_1\wedge\psi_2=\psi_1$, c'est-à-dire si $m_1(\chi)\leq m_2(\chi)$ pour tout caractère χ de G irréductible sur $\mathbb{Q}_p$, ou encore si la représentation associée à ψ_1 est isomorphe à une sous-représentation de la représentation associée à ψ_2.

Ainsi on a évidemment $\chi_{\overline{M}}\leq\chi_M$. D'autre part $\overline{M}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ est un sous-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$, et ce dernier est isomorphe à $\mathbb{Q}_p[G]$. Donc $\chi_{\overline{M}}\leq\chi_{reg}$, et

$$\chi_{\overline{M}}\leq\chi_M\wedge\chi_{reg}.$$

Conjecture 5.1.–(Jaulent). *On a*

$$\chi_{\overline{M}}=\chi_M\wedge\chi_{reg}.$$

Nous noterons r_M^{conj} le degré du caractère $\chi_M\wedge\chi_{reg}$. On a évidemment $r_M^{(p)}\leq r_M^{conj}$, et la conjecture de Jaulent équivaut à dire que ces deux nombres sont égaux.

On écrira

$$\chi_M = \sum_{\chi\in X} m_\chi \chi,\ \chi_{\overline{M}} = \sum_{\chi\in X} \overline{m}_\chi \chi \quad \text{et} \quad \chi_{reg} = \sum_{\chi\in X} r_\chi \chi,$$

avec $X=X(\mathbb{Q}_p)$, de sorte que

$$\overline{m}_\chi \leq \min\{m_\chi,\ r_\chi\}$$

et

$$r_M^{conj} = \sum_\chi \min\{m_\chi,\ r_\chi\} d_\chi,$$

(d_χ est le degré de χ) ; la conjecture de Jaulent s'écrit

$$\overline{m}_\chi = \min\{m_\chi,\ r_\chi\}$$

pour tout caractère χ de G irréductible sur $\mathbb{Q}$.

Bien entendu, si on prend pour M le groupe E des unités de k, on retrouve la conjecture de Leopoldt.

b) Le cas archimédien.

On peut aussi présenter le problème en remplaçant le plongement p-adique par le plongement archimédien (comparer avec le §3 du chapitre 1), c'est-à-dire remplacer le nombre premier p par la place archimédienne de $\mathbb{Q}$. Soit M un sous-groupe de type fini de k^*.

a) Supposons k totalement réel. On désigne par $\overline{M}$ l'espace vectoriel engendré par l'image de M dans $k\otimes_{\mathbb{Q}}\mathbb{R}$ par le plongement logarithmique, et par $r_M^{(\infty)}$ la dimension du $\mathbb{R}$-espace vectoriel engendré par $\overline{M}$. Autrement dit $r_M^{(\infty)}$ est la dimension du $\mathbb{R}$-sous-espace vectoriel de $k\otimes_{\mathbb{Q}}\mathbb{R}$ engendré par les $(\log|\sigma_i\alpha|)_{1\leq i\leq d}$, pour α décrivant M.

Par exemple, supposons $M\otimes_{\mathbb{Z}}\mathbb{Q}$ isomorphe à $\mathbb{Q}[G]$; cela signifie $\chi_M=\chi_{reg}$ (nous verrons plus loin -lemme 5.4- que l'étude du cas général se ramène à celui de ce cas particulier). Alors $M\otimes_{\mathbb{Z}}\mathbb{Q}$ est monogène, c'est-à-dire qu'il existe $\alpha\in k^*$ tel que M soit engendré comme $\mathbb{Q}$-espace vectoriel par $\{\sigma\alpha\ ;\ \sigma\in G\}$. D'après ce que nous avons vu, dire que le rang de la matrice

$$(\log|\sigma\circ\tau^{-1}\alpha|)_{(\sigma,\tau)\in G\times G}$$

est égal à d (autrement dit que la matrice est inversible) revient à dire que l'image de M dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^* \simeq \mathbb{R}^{*d}$ par le plongement canonique est discret

b) Supposons k totalement imaginaire. On plonge k dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^* \simeq \mathbb{C}^{*d}$ par le plongement canonique $i(\alpha)=(\sigma_1\alpha,\ldots,\sigma_d\alpha)$, et on désigne par $r_M^{(\infty)}$ le minimum des nombres $\dim_{\mathbb{C}}(\mathbb{C}z_1+\ldots+\mathbb{C}z_m)$, quand $(z_1,\ldots,z_m)$ parcourt les m-uplets d'éléments de $\mathbb{C}[G]$ tels que $\exp z_1,\ldots,\exp z_m$ engendrent un sous-groupe d'indice fini de $i(M)$, et tels que G permute entre eux les z_i.

On choisit un tel m-uplet $(z_1,\ldots,z_m)$ engendrant un sous-espace vectoriel de $\mathbb{C}^d$ de dimension $r_M^{(\infty)}$, et on désigne par $\overline{M}$ le $\mathbb{C}$-espace vectoriel $\mathbb{C}z_1+\ldots+\mathbb{C}z_m$. On peut écrire $z_j=(\log\sigma\alpha_j)_{\sigma\in G}$, $(1\leq j\leq m)$, où $\alpha_1,\ldots,\alpha_m$ engendrent un sous-groupe d'indice fini de M, et $r_M^{(\infty)}$ est le rang de la matrice $\left(\log\sigma\alpha_j\right)_{\sigma\in G,\ 1\leq j\leq m}$.

Dans les deux cas, on peut encore conjecturer que le caractère du $\mathbb{R}[G]$ module $\overline{M}$ est $\chi_M\wedge\chi_{reg}$. Cela revient à dire que $r_M^{(\infty)}$ est égal au degré r_M^{conj} de $\chi_M\wedge\chi_{reg}$.

[On peut remplacer les groupes multiplicatifs $\mathbb{R}^{*d}$ et $\mathbb{C}^{*d}$ par des groupes algébriques commutatifs quelconques ; cf. M. Waldschmidt, Dépendance de logarithmes dans les groupes algébriques, Approximations diophantiennes et nombres transcendants, Luminy 1982, Progress in Math. **31** (1983), 289-328].

c) Minorations du rang p-adique.

On reprend les notations de a) : p est un nombre premier, et M est un sous-$\mathbb{Z}[G]$-module de k'. Un caractère p-adique est un caractère sur $\mathbb{Q}_p$. Nous pourrions aussi dans tout ce qui suit remplacer le nombre premier p par la place archimédienne de $\mathbb{Q}$; on remplace dans ce cas $\mathbb{Q}_p$ par $\mathbb{R}$, et on pose $k'=k^*$.

Proposition 5.2- *Soit S l'ensemble des caractères p-adiques irréductibles qui interviennent dans la décomposition de* χ_M. *Alors*

$$\chi_{\overline{M}} \geq \sum_{\psi\in S}\psi.$$

Autrement dit la condition $m_\chi \neq 0$ *implique* $\overline{m}_\chi \neq 0$. *En particulier, si* G *est abélien, alors la conjecture de Jaulent est vraie.*

Démonstration.- Soit χ un caractère irréductible sur $\mathbb{Q}$ intervenant dans la décomposition de χ_M. Il existe donc $x \in M$ tel que le $\mathbb{Q}[G]$-sous-module de M engendré par x soit irréductible de caractère χ.

Si χ est encore irréductible sur $\mathbb{Q}_p$, $\overline{M}$ contient le sous-$\mathbb{Q}_p[G]$-module engendré par i(x), qui est irréductible de caractère χ.

Sinon, on décompose χ en somme de caractères Ψ irréductibles sur $\mathbb{Q}_p$, à valeurs dans $\overline{\mathbb{Q}}\cap\mathbb{Q}_p$. Si un de ces Ψ n'était pas représenté dans la représentation de $\overline{M}$, on aurait dans $M\otimes_{\mathbb{Q}}\mathbb{Q}_p$:

$$\prod_{\sigma\in G} \sigma(x)^{\Psi(\sigma^{-1})} \neq 1,$$

et, dans $\overline{i(M)}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$:

$$\prod_{\sigma\in G} \sigma\circ i(x)^{\Psi(\sigma^{-1})} = 1.$$

ou encore

$$\sum_{\sigma\in G} \Psi(\sigma^{-1}) \log_p \sigma\circ i(x) = 0 ;$$

ceci contredit le théorème de Baker-Brumer.

Proposition 5.3.- *La conjecture de Jaulent est une conséquence de la conjecture 2.11 sur l'indépendance algébrique de logarithmes p-adiques*

Démonstration.- On se ramène au cas où $\chi_M \leq \chi_{reg}$ en remplaçant au besoin M par un sous-module. Supposons d'abord $\chi_M = \chi_{reg}$; soit x un générateur de $M\otimes_{\mathbb{Z}}\mathbb{Q}$ sur $\mathbb{Q}[G]$ (correspondant à l'élément de la base e_1 dans la représentation régulière). On fait intervenir l'application $\mathcal{LOG}\circ\theta$ du §2.b. Le déterminant de la matrice

$$\left(\log_p \sigma\circ\tau^{-1}(x)\right)_{(\sigma,\tau)\in G\times G}$$

est égal à $\Delta_G((\log_p \sigma(x))_{\sigma\in G})$, donc il n'est pas nul, et la dimension sur $\mathbb{Q}_p$ de l'espace vectoriel engendré par $\overline{M}$ est d.

Le cas général en résulte immédiatement, grâce au lemme suivant :

Lemme 5.4.- *Soit* M *un sous-*$\mathbb{Z}[G]$ *module de type fini de* k^*; *on suppose* $\chi_M \leq \chi_{reg}$. *Alors il existe un sous-*$\mathbb{Z}[G]$*-module* N *de type fini de* k^* *contenant (un sous-module isomorphe à)* M *tel que*

1) le $\mathbb{Q}[G]$*-module* $N\otimes_{\mathbb{Z}}\mathbb{Q}$ *soit isomorphe à* $\mathbb{Q}[G]$, *et*

2) (l'image de) $M\otimes_{\mathbb{Z}}\mathbb{Q}$ *soit facteur direct dans* $N\otimes_{\mathbb{Z}}\mathbb{Q}$.

De plus, si $M\subset k'$, *alors on peut prendre* $N\subset k'$.

Démonstration.- Comme M est de type fini, il existe un nombre premier $\ell\neq p$ complètement décomposé dans l'extension $k/\mathbb{Q}$. Soit $\mathfrak{p}$ un idéal premier de k au-dessus de ℓ, et soit $y\in k$ un générateur d'une puissance principale de $\mathfrak{p}$. Comme ℓ est totalement décomposé, le $\mathbb{Z}[G]$-module P engendré par y dans k^* est isomorphe à $\mathbb{Z}[G]$. Soit $Q=\mathbb{Q}\otimes_{\mathbb{Z}}(M\oplus P)$ le $\mathbb{Q}[G]$-module engendré par M et P dans k^* ; il contient la représentation régulière. Soit $\overline{N}$ un sous-$\mathbb{Q}[G]$-module de Q, contenant M, isomorphe à $\mathbb{Q}[G]$. Alors $\chi_{\overline{N}} = \chi_{reg}$, et on prend $N=\overline{N}\cap(M\oplus P)$.

Remarque. Tout idéal à gauche de $\mathbb{Q}[G]$ est monogène. Pour le voir, partons d'un $\mathbb{Q}[G]$-module M de caractère $\chi_M\leq\chi_{reg}$, et montrons que M est monogène. On décompose χ_M en caractères irréductibles sur $\mathbb{Q}$:

$$\chi_M = \sum_{\chi\in X} m_\chi \chi,$$

ce qui donne un isomorphisme de $\mathbb{Q}[G]$-modules

$$\prod_{\chi\in X}\prod_{j=1}^{m_\chi} W_{\chi j} \xrightarrow{\varphi} M\otimes_{\mathbb{Z}}\mathbb{Q}.$$

La représentation régulière correspond à la décomposition de $\mathbb{Q}[G]$ en composantes simples

$$\mathbb{Q}[G] \simeq \prod_{\chi\in X}\prod_{j=1}^{r_\chi} W_{\chi j}$$

avec $W_{\chi j}=\mathbb{Q}[G]\epsilon_{\chi j}$. Les $\epsilon_{\chi j}$ forment un système complet d'idempotents primitifs orthogonaux (non centraux si $r_\chi>1$). Soit $x_{\chi j}=\varphi(\epsilon_{\chi j})$, et soit

$$x = \sum_{\chi\in X}\sum_{j=1}^{m_\chi} x_{\chi j}.$$

Comme $m_\chi\leq r_\chi$ pour tout χ, on a

$$\mathbb{Q}[G]x = \prod_{\chi\in X}\prod_{j=1}^{m_\chi}\mathbb{Q}[G]x_{\chi j} = \prod_{\chi\in X}\prod_{j=1}^{m_\chi}\varphi(W_{\chi j}),$$

d'où $M\otimes_{\mathbb{Z}}\mathbb{Q}=\mathbb{Q}[G]x$.

Il est facile de voir que pour p fixé, il existe un $\mathbb{Z}[G]$-sous-module $M(p)$ de k' tel que $\chi_{\overline{M(p)}} = \chi_{reg}$, et alors $\chi_{\overline{M}} = \chi_{reg}$ pour tout $M\supset M(p)$. Un résultat plus profond, dû à M. Emsalem, montre que la conjecture de Jaulent est vraie pour des $\mathbb{Z}[G]$-modules M "suffisamment gros" en un sens indépendant de p :

Proposition 5.5.- *Soit M un sous-$\mathbb{Z}[G]$ module de k' de type fini. On décompose le caractère χ_M en somme directe de caractères irréductibles sur $\mathbb{Q}$:*

$$\chi_M = \sum_{\chi\in X} m_\chi \chi,$$

avec $X=X(\mathbb{Q})$. Pour $\chi\in X$, soit d_χ le degré de χ, soit r_χ la multiplicité de χ dans la représentation régulière de G sur $\mathbb{Q}$, et soit $k_\chi=[m_\chi/r_\chi]$. Alors

$$r_M^{(p)} \geq \sum_{\chi\in X} \frac{k_\chi}{k_\chi+1}\, r_\chi d_\chi.$$

De plus, si, pour tout $\chi\in X(\mathbb{Q})$, on a soit $m_\chi=0$, soit $m_\chi\geq r_\chi^2 d_\chi$, alors la conjecture de Jaulent est vraie pour M.

Voici le principe de la démonstration. On se ramène au cas où M est isotypique de caractère $m\chi$, et il s'agit de voir que

$$r_M^{(p)} \geq \frac{k}{k+1}\, r_\chi d_\chi,$$

avec $k=[m/r_\chi]$. Comme $\chi_M \geq k r_\chi \chi$, on peut trouver dans M des éléments $x_1,\ldots,x_k$ tels que

1) M contienne la somme directe des $\mathbb{Z}[G]$-modules $N_1,\ldots,N_k$, où $N_i=\mathbb{Z}[G]x_i$;

2) le caractère de $\mathbb{Q}[G]x_i$ soit $r_\chi\chi$.

Alors pour chaque $i=1,\ldots,k$ et chaque $\tau\in G$, $\overline{M}$ contient le vecteur $\left[\log_p(\sigma\circ\tau x_i)\right]_{\sigma\in G}$ de $\mathbb{C}_p[G]$, et il reste à minorer le rang de la matrice formée

par ces vecteurs. Par un argument de transcendance analogue au théorème 4.2 de l'introduction, on montre que le rang de cette matrice est au moins

$$\frac{k}{k+1}\, r_\chi d_\chi$$

(dans les bons cas, on peut minorer le rang d'une matrice à coefficients logarithmes de nombres algébriques de taille $\ell \times d$ par $\ell d/(\ell+d)$; ici $\ell = r_\chi d_\chi$ et $d = k r_\chi d_\chi$, car on peut restreindre σ et τ à parcourir un sous-ensemble de G ayant $r_\chi d_\chi = \dim R_\chi$ éléments).

Enfin, quand $m \geq r_\chi^2 d_\chi$, on a $k+1 > r_\chi d_\chi$, donc $\frac{k}{k+1} r_\chi d_\chi > r_\chi d_\chi - 1$; or si $m_\chi \geq r_\chi^2 d_\chi$ pour tout χ intervenant dans χ_M, on a

$$r_m^{conj} = \sum r_\chi d_\chi,$$

où la somme est étendue aux caractères irréductibles χ tels que $m_\chi \neq 0$. La proposition 5.5 en résulte.

On peut raffiner la proposition 5.5 (Jaulent, thèse) : chaque $\chi \in X$ se décompose en $\chi = s_\chi \cdot \sum_{\varphi | \chi} \varphi$, où les caractères φ sont irréductibles sur $\overline{\mathbb{Q}}$ et tous de même degré ; on peut alors remplacer la condition $m \geq r_\chi^2 d_\chi$ par $m \geq r_\chi^2 d_\chi / \deg \varphi$.

Complément.- Dans un exposé de M. Emsalem au Groupe d'Etude d'Analyse Ultramétrique (Comportement des fonctions L p-adiques au voisinage de zéro ; 9è année, 1981/82, n°17, 19 p.), et dans la thèse de Jaulent (Ch.2 §1.3), on trouvera des développements de ce qui précède en liaison avec une conjecture de Gross sur les fonctions L d'Artin.

Références pour le §5.-

M. Emsalem.-
Rang p-adique de groupes de S-unités d'un corps de nombres ; C.R. Acad. Sc. Paris, **297** (1983), 225-227. Voir aussi les comptes rendus des Journées de Saint-Etienne : Algorithmique, Calcul Formel, Arithmétique ; , 3-8 Octobre 1983, exp. n°32, 8p.

J.F. Jaulent.-
Sur l'indépendance ℓ-adique de nombres algébriques ; J. Number Theory, **20** (1985), 149-158.

J.F. Jaulent.-
L'arithmétique des ℓ-extensions ; Thèse Doctorat d'Etat, Univ. Franche-Comté, 24 Janvier 1986.

§6. $\mathbb{Z}_p$-extensions.

Une $\mathbb{Z}_p$-extension est une extension galoisienne de groupe de Galois $\mathbb{Z}_p$. Tout corps de nombres possède au moins une $\mathbb{Z}_p$-extension : la $\mathbb{Z}_p$-extension cyclotomique. Une $\mathbb{Z}_p$-extension d'un corps de nombres k est ramifiée en un nombre fini de places, qui divisent toutes p. L'extension maximale abélienne de k non ramifiée en dehors de p contient donc le compositum de toutes les $\mathbb{Z}_p$-extensions de k, et en est une extension finie.

Le nombre de $\mathbb{Z}_p$-extensions indépendantes d'un corps de nombres k est $1+r_2+\delta_p$, où δ_p est le défaut de la conjecture de Leopoldt de k. En particulier, si la conjecture de Leopoldt est vraie pour k, et si k est totalement réel, alors la seule $\mathbb{Z}_p$-extension de k est l'extension cyclotomique.

Pour terminer nous présentons brièvement un article récent de M. Emsalem sur l'application d'Artin dans les $\mathbb{Z}_p$-extensions.

a) Définition et exemples.

Soient p un nombre premier, k un corps, et K une extension galoisienne de k. Les deux propriétés suivantes sont équivalentes :

(i) $G(K/k)\simeq\mathbb{Z}_p$;

(ii) il existe une suite d'extensions de k dans K

$$k=k_0\subset k_1\subset\ldots\subset k_n\subset\ldots\subset K$$

telle que $K=\bigcup_{n\geq 0} k_n$ et que k_n/k soit cyclique de degré p^n.

L'équivalence entre ces deux propriétés est claire : (i)⇒(ii) résulte de la théorie de Galois infini (Chap.II, §3.b), en prenant pour k_n le corps fixé par le sous-groupe $p^n\mathbb{Z}_p$ de $\mathbb{Z}_p$; d'autre part (ii) implique que $G(K/k)$ est la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$.

Quand ces propriétés sont satisfaites, on dit que l'extension K/k est une $\mathbb{Z}_p$-*extension* (ou une Γ-extension).

Comme les seuls sous-groupes fermés de $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$, les seules extensions de k contenues dans K sont les k_n, $n\geq 0$.

Exemple.- Soit p un nombre premier. Pour chaque nombre entier $n\geq 1$, soit ζ_{p^n} une racine primitive p^n-ième de l'unité. L'extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ est galoisienne de groupe de Galois $(\mathbb{Z}/p^n\mathbb{Z})^*$. Si p est impair, $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique, d'ordre $\varphi(p^n)=(p-1)p^{n-1}$, tandis que $(\mathbb{Z}/2^n\mathbb{Z})^*$, pour $n\geq 2$, est isomorphe au produit d'un groupe cyclique d'ordre 2 par un groupe cyclique d'ordre 2^{n-2}.

Posons $q=p$ si p est impair, et $q=4$ si $p=2$. On a donc

$$(\mathbb{Z}/p^nq\mathbb{Z})^*\simeq(\mathbb{Z}/q\mathbb{Z})^*\times(\mathbb{Z}/p^n\mathbb{Z}) \quad \text{pour tout } n\geq 0,$$

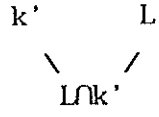
et $\mathbb{Q}(\zeta_{p^nq})$ est une extension cyclique de $\mathbb{Q}(\zeta_q)$ de degré p^n. Notons $\mathbb{Q}(\zeta_{p^\infty})$ la réunion des corps $\mathbb{Q}(\zeta_{p^n})$, $n\geq 0$; ainsi $\mathbb{Q}(\zeta_{p^\infty})$ est une $\mathbb{Z}_p$-extension de $\mathbb{Q}(\zeta_q)$.

On obtient une $\mathbb{Z}_p$-extension de $\mathbb{Q}$ de la manière suivante : pour chaque entier $n\geq 1$, il existe un et un seul sous-groupe de $(\mathbb{Z}/p^nq\mathbb{Z})^*$ pour lequel le quotient soit cyclique d'ordre p^n ; donc il existe un et un seul sous-corps F_n de $\mathbb{Q}(\zeta_{p^nq})$ qui soit une extension cyclique de $\mathbb{Q}$ d'ordre p^n. La réunion F_∞ des F_n, qui est aussi le sous-corps de $\mathbb{Q}(\zeta_{p^\infty})$ fixé par le sous-groupe de torsion de $G(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, est une $\mathbb{Z}_p$-extension de $\mathbb{Q}$. Nous verrons plus loin que c'est la seule. On l'appelle *l'extension cyclotomique* de $\mathbb{Q}$.

Lemme 6.1.- *Soient* L/k *une* $\mathbb{Z}_p$*-extension, et* k' *une extension finie de* k. *Alors le compositum* $k'L$ *est une* $\mathbb{Z}_p$*-extension de* k'.

Par exemple tout corps de nombres k possède au moins une $\mathbb{Z}_p$-extension : la $\mathbb{Z}_p$*-extension cyclotomique de* k qui est le compositum de k et de la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$.

Démonstration du lemme 6.1.- Ecrivons $L=\bigcup_{n\geq 0} k_n$, avec k_n/k cyclique d'ordre p^n. Comme $L\cap k'$ est une extension finie de k contenue dans L, il existe un entier n_o tel que $k_{n_o}=L\cap k'$. On a :



$$G(k'L/k') \simeq G(L/L\cap k') \simeq p^{n_o}\mathbb{Z}_p \simeq \mathbb{Z}_p,$$

donc $k'L$ est une $\mathbb{Z}_p$-extension de k'.

Nous allons voir que si k est un corps totalement réel, alors toute $\mathbb{Z}_p$-extension L de k est totalement réelle (c'est-à-dire que tout plongement de L dans $\mathbb{C}$ a une image contenue dans $\mathbb{R}$). Plus précisément :

Lemme 6.2.- *Soient k un corps de nombres, L une $\mathbb{Z}_p$-extension de k, $\sigma:L\longrightarrow\mathbb{C}$ un plongement de L dans $\mathbb{C}$. Si $\sigma(k)\subset\mathbb{R}$, alors $\sigma(L)\subset\mathbb{R}$.*

Démonstration.- Si p est impair, toute extension finie k_n de k contenue dans L est de degré impair ; donc $\sigma(k_n)\subset\mathbb{R}$, et $\bigcup_{n\geq 0}\sigma(k_n)=\sigma(L)\subset\mathbb{R}$.

Il reste à traiter le cas $p=2$. Supposons que $\sigma(L)$ ne soit pas contenu dans $\mathbb{R}$; soit $n\geq 1$ le plus petit entier tel que $\sigma(k_n)$ ne soit pas contenu dans $\mathbb{R}$. Soit m un entier, $m\geq n$; le corps k_m est galoisien sur k, et la restriction à $\sigma(k_m)$ de la conjugaison complexe définit un élément τ de $G(k_m/k)$, d'ordre 2 ; le sous-corps de k_m fixé par τ est un sous-corps de k_m sur lequel k_m est de degré 2 ; or il n'y en a qu'un : c'est k_{m-1}. Cela est impossible pour $m\geq n+1$.

Dans les conditions du lemme 6.2, on dit que la place archimédienne v de k associée au plongement σ est *non ramifiée* dans l'extension L/k.

Soient k un corps de nombres, k^{ab} l'extension abélienne maximale de k, et $G_k=G(k^{ab}/k)$ l'abélianisé du groupe de Galois absolu de k. La théorie de Galois établit une bijection entre les $\mathbb{Z}_p$-extensions de k et les noyaux des homomorphismes continus et non nuls de G_k dans $\mathbb{Z}_p$: à une $\mathbb{Z}_p$-extension

L/k on associe le sous-groupe $H=G(k^{ab}/L)$ de G_k, qui est le noyau de $G_k \longrightarrow G_k/H \simeq \mathbb{Z}_p$.

L'ensemble A des homomorphismes continus de G_k dans $\mathbb{Z}_p$ est naturellement muni d'une structure de $\mathbb{Z}_p$-module ; deux $\mathbb{Z}_p$-extensions L_1, L_2 de k seront dites *indépendantes* si, en notant $H_i=G(k^{ab}/L_i)$, (i=1,2), les deux homomorphismes $G_k \longrightarrow G_k/H_i \simeq \mathbb{Z}_p$ (i=1,2) sont linéairement indépendants sur $\mathbb{Z}_p$ dans A. Le rang de A sur $\mathbb{Z}_p$ est par définition le *nombre de $\mathbb{Z}_p$-extensions indépendantes de* k.

Nous désignerons par $\hat{k}$ le compositum de toutes les $\mathbb{Z}_p$-extensions de k. Le $\mathbb{Z}_p$-module $A=\mathrm{Hom}_{\mathrm{cont}}(G_k,\mathbb{Z}_p)$ est isomorphe au $\mathbb{Z}_p$-module $\mathrm{Hom}_{\mathrm{cont}}(G(\hat{k}/k),\mathbb{Z}_p)$. En effet, si $\varphi: G_k \longrightarrow \mathbb{Z}_p$ est un homomorphisme continu, le sous-corps L de k^{ab} fixé par $\ker\varphi$ est une $\mathbb{Z}_p$ extension de k, donc est contenu dans $\hat{k}$; alors $\ker\varphi$ contient $G(k^{ab}/\hat{k})$, et φ se factorise par $G_k \longrightarrow G(\hat{k}/k)$ en un homomorphisme continu de $G(\hat{k}/k)$ dans $\mathbb{Z}_p$.

Exemple.- Prenons $k=\mathbb{Q}$. On a $G_k \simeq \hat{\mathbb{Z}}^*$; or il existe un et un seul sous-groupe H de $\hat{\mathbb{Z}}^*$ tel que $\hat{\mathbb{Z}}/H$ soit isomorphe à $\mathbb{Z}_p$ (cf Chap.2, §1). Donc la seule $\mathbb{Z}_p$-extension de $\mathbb{Q}$ est l'extension cyclotomique, et le nombre de $\mathbb{Z}_p$-extensions indépendantes de $\mathbb{Q}$ est 1.

Enfin une *$\mathbb{Z}_p$-extension multiple* de k est une extension dont le groupe de Galois est isomorphe à un produit direct $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$.

b) Ramification dans les $\mathbb{Z}_p$-extensions.

Commençons par étudier la ramification dans les $\mathbb{Z}_p$-extensions. Le lemme 6.2 signifie que les places archimédiennes de k ne se ramifient pas dans une $\mathbb{Z}_p$-extension de k. Passons aux places finies ; rappelons (Chap.2 §3d) qu'une extension abélienne L/k est non ramifiée en une place v de k si le groupe d'inertie en v est trivial.

Lemme 6.3.- *Soient* k *un corps de nombres et* L *une* $\mathbb{Z}_p$*-extension de* k. *Soit* v *une place de* k *ramifiée dans* L. *Alors* $v|p$.

Démonstration.- Voir par exemple Washington, proposition 13.2.

Il résulte du lemme 6.3 que dans une $\mathbb{Z}_p$-extension d'un corps de nombres, au moins une place est ramifiée (l'extension abélienne maximale non ramifiée de k est une extension finie de k, car c'est le corps de classes de Hilbert, dont le degré sur k est égal au nombre de classes de k), et il n'y a qu'un nombre fini de places ramifiées (ce sont des diviseurs de p).

Soit $\tilde{k}$ l'extension abélienne de k, non ramifiée en dehors de p, et maximale pour ces propriétés. Le lemme 6.3 montre que $\hat{k}$ est un sous-corps de $\tilde{k}$, et nous allons voir que $\tilde{k}$ est une extension finie de $\hat{k}$.

c) Nombre de $\mathbb{Z}_p$-extensions indépendantes.

Soient k un corps de nombres, et $L = \bigcup_{n\geq 0} k_n$ une $\mathbb{Z}_p$-extension de k. L'application de réciprocité d'Artin (Chap.2, §3.e) donne un homomorphisme surjectif continu ψ de $\mathfrak{S}_k$ sur $G(L/k)$, dont le noyau contient k^*. Donc $\ker\psi$ est un sous-groupe fermé de $\mathfrak{S}_k$, contenant k^*, et tel que $\mathfrak{S}_k/\ker\psi \simeq \mathbb{Z}_p$.

Inversement, si N est un sous-groupe fermé de $\mathfrak{S}_k$, contenant k^*, et tel que $\mathfrak{S}_k/N \simeq \mathbb{Z}_p$, alors la surjection $\mathfrak{S}_k \longrightarrow \mathfrak{S}_k/N$ est l'application d'Artin d'une $\mathbb{Z}_p$-extension.

Soit H le sous-groupe ouvert de $\mathfrak{S}_k$ défini par

$$H = \prod_{(v,p)=1} U_v \times \prod_{v|\infty} k_v^*.$$

Lemme 6.4.- *On obtient une bijection entre l'ensemble des* $\mathbb{Z}_p$*-extensions* L *de* k *et l'ensemble des sous-groupes fermés* N *de* $\mathfrak{S}_k$ *contenant* k^*H *et vérifiant* $\mathfrak{S}_k/N \simeq \mathbb{Z}_p$, *en associant à* L *le noyau de l'application d'Artin* $\psi : \mathfrak{S}_k \longrightarrow G(L/k)$. *L'application d'Artin de la* $\mathbb{Z}_p$*-extension définie par* N *est la surjection canonique* $\mathfrak{S}_k \longrightarrow \mathfrak{S}_k/N$

Par la théorie du corps de classes, le quotient de $\mathfrak{S}_k$ par l'adhérence de k^*H est isomorphe au groupe de Galois $G(\tilde{k}/k)$ (rappelons que $\tilde{k}$ est l'extension abélienne maximale de k non ramifiée en dehors de p et que $G_k=G(k^{ab}/k)$)

Nous avons construit (Chap.1 §6.a), pour tout ensemble fini S de places de k contenant l'ensemble S_∞ des places archimédiennes, un homomorphisme surjectif $x \longrightarrow (x)^S$ de $\mathfrak{S}_k^S$ dans I_k^S, de noyau U^S. Reprenons cette construction avec $S=S_\infty$: on obtient un homomorphisme surjectif de $\mathfrak{S}_k$ sur I_k, et quand on le compose avec la surjection de I_k sur le groupe $Cl(k)$ des classes d'idéaux de k et avec l'application d'Artin, cela donne une suite exacte (cf Neukirch, Chap.4 §7 Th.7.8 ; Lang, Cyclotomic fields, Chap.5 §5):

$$1 \longrightarrow (\prod_{p|p} U_p)/\overline{E} \longrightarrow G(\tilde{k}/k) \longrightarrow Cl(k) \longrightarrow 1, \tag{6.5}$$

où $\overline{E}$ est l'adhérence dans $U=\prod_{p|p} U_p$ de l'image de E par le plongement diagonal (cf §2a ci-dessus). Si p est un idéal premier de k, non ramifié dans $\tilde{k}/k$, et si $\alpha \in k^*$ est un générateur d'une puissance principale p^h de p, l'image dans $G(\tilde{k}/k)$ de α^{-1} (où $\alpha^{-1} \in (\prod_{p|p} U_p)/\overline{E}$ est l'image de $\alpha^{-1} \in k^*$ par le plongement diagonal et la surjection canonique) est F_p^h , $F_p \in G(\tilde{k}/k)$ désignant le Frobenius en p dans l'extension $\tilde{k}/k$.

Le $\mathbb{Z}_p$-module U est isomorphe au produit d'un groupe fini par $\mathbb{Z}_p^d$, et la suite exacte montre que $G(\tilde{k}/k)$ est isomorphe au produit d'un groupe fini par $\mathbb{Z}_p^{d-r_p}$, puisque $\overline{E}$ est de rang r_p sur $\mathbb{Z}_p$. Comme $d-r_p=r_2+1+\delta_p$ où δ_p est le défaut de la conjecture de Leopoldt, on obtient

Proposition 6.6.- *Le nombre de $\mathbb{Z}_p$-extensions indépendantes d'un corps de nombres k est égal à $r_2+1+\delta_p$ où δ_p est le défaut de la conjecture de Leopoldt.*

Ainsi ce nombre est au moins r_2+1 et au plus d ; si la conjecture de Leopoldt est vraie, tout corps de nombres k possède exactement r_2+1 $\mathbb{Z}_p$-extensions indépendantes ; si elle est fausse, il y en a quelquefois plus. Comme $\delta_p \leq r/2$, le nombre de $\mathbb{Z}_p$-extensions indépendantes est toujours majoré par $r_2+1+(r/2)$.

Corollaire 6.7.- *Soit* k *une extension abélienne finie de* $\mathbb{Q}$ *de degré* d. *Si* k *est totalement réelle, alors* k *possède une seule* $\mathbb{Z}_p$*-extension (la* $\mathbb{Z}_p$*-extension cyclotomique). Si* k *est totalement imaginaire, alors le nombre de* $\mathbb{Z}_p$*-extensions indépendantes de* k *est* $r_2+1=(d/2)+1$.

Pour terminer cette section, introduisons la conjecture faible de Leopoldt. Soient p un nombre premier, k un corps de nombres, et L une extension galoisienne de k. Pour chaque extension finie E de k contenue dans L, on désigne par $\delta_p(E)$ le défaut de la conjecture de Leopoldt pour E. On dit que l'extension L/k satisfait la *conjecture faible de Leopoldt* si la borne supérieure $\delta_p(L)$ des nombres $\delta_p(E)$, (pour $k \subset E \subset L$, $[E:k]<\infty$) est finie.

La théorie d'Iwasawa permet de démontrer la conjecture faible de Leopoldt pour certaines $\mathbb{Z}_p$-extensions, en particulier les $\mathbb{Z}_p$-extensions cyclotomiques (voir à ce sujet V. Fleckinger, Une interprétation de la conjecture de Leopoldt, C.R.A.S. **302** (1986), 607-610).

d) Décomposition des idéaux premiers dans les $\mathbb{Z}_p$-extensions (d'après M. Emsalem).

Soient k un corps de nombres galoisien sur $\mathbb{Q}$, $G=G(k/\mathbb{Q})$, et L/k une $\mathbb{Z}_p$-extension. On se propose d'étudier les idéaux premiers p de k qui sont *totalement décomposés* dans L (c'est-à-dire totalement décomposés dans toutes les extensions finies k_n de k contenues dans L).

Si $\mathfrak{p}$ est un tel idéal, il n'est pas ramifié dans L, et son image dans G(L/k) (c'est-à-dire l'image du Frobenius en $\mathfrak{p}$) par l'application d'Artin est triviale. Inversement, si l'image de $\mathfrak{p}$ par l'application d'Artin est triviale, alors $\mathfrak{p}$ est totalement décomposé dans L.

Nous allons voir qu'"en général", les idéaux premiers $\mathfrak{p}$ de k dont l'image par l'application d'Artin est triviale engendrent un sous-groupe de rang fini dans le groupe des idéaux fractionnaires de k.

Ce problème a été étudié d'abord par Greenberg qui a montré, à l'aide du théorème des 6 exponentielles p-adiques, que si k est un corps quadratique imaginaire, à part une $\mathbb{Z}_p$-extension (appelée anticyclotomique ou diédrale suivant les auteurs), le rang en question est au plus 2.

Pour simplifier l'exposé, nous supposerons que le nombre p est totalement décomposé dans l'extension k/$\mathbb{Q}$. La seule raison pour laquelle nous introduisons cette hypothèse est que dans ce cas, les lemmes 2.3, 2.4 et 2.5 sont triviaux : $k\otimes_{\mathbb{Q}}\mathbb{Q}_p = \prod_{v|p} k_v$ est isomorphe à $\mathbb{Q}_p[G]$ comme $\mathbb{Q}_p[G]$-module à gauche par $(x_\sigma)_{\sigma\in G} \longrightarrow \sum_{\sigma\in G} x_\sigma \sigma^{-1}$. Pour le cas général, il suffit d'utiliser les lemmes du §2 avec l'homomorphisme θ (voir l'article de M. Emsalem, Crelle J.).

Un sous-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ sur $\mathbb{Q}_p$ est dit *rationnel* sur $\mathbb{Q}$ s'il est intersection, dans $\mathbb{Q}_p[G]$ (identifié naturellement à $\mathbb{Q}_p^d$), de noyaux de formes linéaires à coefficients dans $\mathbb{Q}$, ou, ce qui revient au même, s'il possède une base formée d'éléments de $\mathbb{Q}^d$.

Soit V un sous-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ sur $\mathbb{Q}_p$; l'intersection $(\prod_{\mathfrak{p}|p} U_{\mathfrak{p}})\cap LOG^{-1}(V)$ est un sous-$\mathbb{Z}_p$-module de $\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$; par abus de notation, on écrira $(V+\overline{E})/\overline{E}$ le quotient $\left[(\prod_{\mathfrak{p}|p} U_{\mathfrak{p}})\cap LOG^{-1}(V)\right].\overline{E}/\overline{E}$; ce quotient donne, par la suite exacte (6.5) et la surjection (de noyau fini) $G(\tilde{k}/k) \longrightarrow G(\hat{k}/k)$, un sous-$\mathbb{Z}_p$-module $\mathcal{H}_V$ de $G(\hat{k}/k)$; notons k_V le sous-corps de $\hat{k}$ fixé par $\mathcal{H}_V$.

Lemme 6.8.- *L'application* $V \longrightarrow k_V$ *établit une bijection décroissante entre les sous-espaces vectoriels* V *de* $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ *sur* $\mathbb{Q}_p$ *contenant* $\overline{E}$ *et les* $\mathbb{Z}_p$*-extensions multiples de* k.

Démonstration.- Montrons d'abord que si $V_1 \subset V_2$, alors $k_{V_1} \supset k_{V_2}$. En effet, comme $V_1 \subset V_2$, on a

$$\frac{V_1+\overline{E}}{\overline{E}} \subset \frac{V_2+\overline{E}}{\overline{E}},$$

donc $\mathcal{H}_{V_1} \subset \mathcal{H}_{V_2}$, et finalement $k_{V_1} \supset k_{V_2}$.

Pour chaque $V \supset \overline{E}$, le corps k_V est une extension galoisienne de k et $G(k_V/k)$ est isomorphe à une puissance de $\mathbb{Z}_p$, donc k_V/k est une $\mathbb{Z}_p$-extension multiple.

Inversement, si L est une $\mathbb{Z}_p$-extension multiple, en posant $\mathcal{H}=G(\hat{k}/L)$, on obtient par la suite exacte un sous-espace V de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ sur $\mathbb{Q}_p$ dont l'image par LOG contient $\overline{E}$. Il reste à voir que ces deux applications sont bien des bijections réciproques l'une de l'autre.

Quand on part de V, on trouve k_V avec $G(\hat{k}/k_V)=\mathcal{H}_V$, et le sous-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ contenant $\overline{E}$ qui lui est associé est bien V.

Inversement, étant donné $\mathcal{H}$, on lui associe V, puis à V on associe un sous-groupe $\mathcal{H}_V$ de $G(\hat{k}/k)$. On a évidemment $\mathcal{H}_V \supset \mathcal{H}$, et comme $\mathcal{H}$ et $\mathcal{H}_V$ ont pour quotients des $\mathbb{Z}_p$-modules libres de mêmes rangs (ce sont des groupes de Galois de $\mathbb{Z}_p$-extensions multiples), on en déduit $\mathcal{H}=\mathcal{H}_V$.

Un des résultats de M. Emsalem est le suivant : *si* L/k *est une* $\mathbb{Z}_p$*-extension multiple dans laquelle une infinité de places se décomposent totalement, alors il existe un idéal à droite* W *de* $\mathbb{Q}_p[G]$, *rationnel sur* $\mathbb{Q}$, *tel que* L *soit contenu dans* k_W.

L'outil essentiel de la démonstration est le théorème de transcendance 4.2 de l'introduction. Il intervient de la manière suivante : si p est un idéal premier de k totalement décomposé dans l'extension L/k, le Frobenius en p vaut 1 dans $G(L/k)$, donc le Frobenius $F_p \in G(\hat{k}/k)$ appartient à $G(\hat{k}/L)=\mathcal{H}$. Soit V le sous-espace de $k\otimes_{\mathbb{Q}}\mathbb{Q}_p$ tel que $\mathcal{H}=\mathcal{H}_V$, et soit $\alpha \in k^*$ un

générateur d'une puissance principale de p. Notons aussi $\lambda : k^* \longrightarrow k \otimes_{\mathbb{Q}} \mathbb{Q}_p$ le plongement logarithmique p-adique, et identifions $k \otimes_{\mathbb{Q}} \mathbb{Q}_p$ avec $\mathbb{Q}_p[G]$, ce qui fait que, pour $x \in k^*$, on peut écrire :

$$\lambda(x) = \sum_{\sigma \in G} \log_p(\sigma^{-1}x).\sigma \in \mathbb{Q}_p[G].$$

Alors $\lambda(\alpha) \in V$. Donc une $\mathbb{Z}_p$-extension contenant "beaucoup" d'idéaux premiers totalement décomposés donne un espace V contenant "beaucoup" de points dont les coordonnées sont des logarithmes de nombres algébriques, et le résultat de transcendance permet de conclure que cela n'a lieu que dans des cas "triviaux".

Voici comment se fait le lien avec les idéaux à droite. Comme au §5, nous notons k' le sous-groupe de k^* formé des éléments premiers à p. Supposons que $\alpha \in k'$ et $a_\sigma \in \mathbb{Z}$, $(\sigma \in G)$ soient tels que

$$\sum_{\sigma \in G} a_\sigma \log_p \sigma^{-1}\alpha = 0.$$

Alors on a

$$\sum_{\sigma \in G} a_\sigma \log_p (\sigma \circ \tau)^{-1}(\alpha) = 0 \qquad \text{pour tout } \tau \in G.$$

En effet, l'hypothèse s'écrit

$$\prod_{\sigma \in G} (\sigma^{-1}\alpha)^{a_\sigma} \in W$$

(où W est le groupe des racines de l'unité de k), donc

$$\prod_{\sigma \in G} (\tau^{-1} \circ \sigma^{-1}\alpha)^{a_\sigma} \in W \qquad \text{pour tout } \tau \in G,$$

ce qui donne le résultat annoncé.

Cela étant, si, pour $\alpha \in k'$, l'élément

$$\lambda(\alpha) = \sum_{\sigma \in G} \log_p(\sigma^{-1}\alpha).\sigma \in \mathbb{Q}[G]$$

appartient à un hyperplan rationnel sur $\mathbb{Q}$ d'équation

$$\sum_{\sigma \in G} a_\sigma . x_\sigma = 0,$$

alors $\lambda(\alpha)$ appartient à l'idéal W de $\mathbb{Q}_p[G]$ défini par

$$W = \{ \sum_{s \in G} x_s . s \ ; \ (\sum_{\sigma \in G} a_\sigma . \sigma^{-1}).(\sum_{s \in G} x_s . s) = 0 \} \ ;$$

en effet, les équations définissant W s'écrivent

$$\sum_{\sigma \in G} a_\sigma x_{\sigma \circ \tau} = 0 \qquad \text{pour tout } \tau \in G.$$

Notons $\mathfrak{L}$ l'image de k' dans $\mathbb{Q}_p[G]$ par l'application λ. Si V est un sous-espace vectoriel de $\mathbb{Q}_p[G]$ rationnel sur $\mathbb{Q}$ tel que $V \cap \mathfrak{L}$ soit non nul, alors l'idéal à droite W de $\mathbb{Q}_p[G]$, défini par les équations

$$\sum_{\sigma \in G} a_\sigma . x_{\sigma \circ \tau} = 0 \text{ pour tout } \tau \in G$$

est rationnel sur $\mathbb{Q}$, contenu dans V, et vérifie $V \cap \mathfrak{L} = W \cap \mathfrak{L}$.

Pour chaque sous-groupe cyclique D de G, notons W_D l'idéal à droite de $\mathbb{Q}_p[G]$ défini par

$$W_D = \{ \sum_{\sigma \in G} x_\sigma . \sigma \ ; \ x_{\tau \circ \sigma} = x_\sigma \text{ pour tout } \tau \in D \}.$$

Un résultat plus précis de M. Emsalem est le suivant.

Théorème 6.9.- *Les $\mathbb{Z}_p$-extensions multiples de k maximales parmi les $\mathbb{Z}_p$-extensions multiples de k où une infinité de places se décomposent totalement sont les k_{W_D} où D parcourt l'ensemble des sous-groupes cycliques maximaux de G.*

Références pour le §6 :

M. Emsalem.-
Sur les idéaux dont l'application d'Artin dans une $\mathbb{Z}_p$-extension est triviale ; J. reine angew. Math. (Crelle J.), **382** (1987), 181-198.

J. Fresnel.-
Rang p-adique du groupe des unités d'un corps de nombres ; Sém. Th. Nombres Bordeaux, 1968-69, N°9, 18 p.

S. Lang.-
Cyclotomic fields ; G.T.M. **59**, Springer-Verlag 1978 ; voir en particulier : le chapitre 5 : Iwasawa Theory and ideal class groups, §4 : $\mathbb{Z}_p$-extensions and ideal class groups ; §5 : the maximal p-abelian p-ramified extension ; Chap. 6 : Kummer theory over cyclotomic $\mathbb{Z}_p$-extensions, §1 : the cyclotomic $\mathbb{Z}_p$-extension ; §2 : the maximal p-abelian p-ramified extension of the cyclotomic $\mathbb{Z}_p$-extension.

J. Neukirch.-
Class field theory ; Grund. der math. Wiss. **280**, Springer-Verlag 1986 ; voir en particulier : le chapitre IV : Global class field theory, §7 : Global class fields.

L. Washington.-
Introduction to cyclotomic fields ; G.T.M. **83**, Springer-Verlag 1982; voir en particulier : le chapitre 13 (Iwasawa theory of $\mathbb{Z}_p$-extensions ; §13.1 : basic facts ; §13.5 : the maximal abelian p-extension unramified outside p ; et l'appendice : class field theory.

PROBLEME.

I.- Soit k un corps quadratique. On désigne par $s(k)$ le rang minimum d'un sous-groupe de type fini de k^* dont l'image par le plongement canonique σ est dense dans la composante neutre de $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

En admettant la conjecture des 4 exponentielles, donner la valeur de $s(k)$.

II.- Soient E et k deux corps de nombres, λ une place de E, E_λ le complété, $G=G(k^{ab}/k)$ le groupe de Galois de l'extension abélienne maximale de k, et $\rho:G\longrightarrow E_\lambda^*$ un homomorphisme continu. On suppose que pour tout entier $n\geq 1$, ρ^n n'est pas localement algébrique.

Soient $v_1,\ldots,v_m$ des places finies deux-à-deux distinctes de k où ρ n'est pas ramifié ; on désigne par F_{v_i} le Frobenius en une place de k^{ab} au dessus de v_i, $(1\leq i\leq m)$. On suppose $\rho(F_{v_i})\in E^*$ pour $1\leq i\leq m$. Donner une majoration de m en fonction du degré d de k sur $\mathbb{Q}$.

III.-

A) Soient ℓ un nombre premier, et k une extension galoisienne totalement imaginaire de $\mathbb{Q}$ de degré 2ℓ. Montrer que k vérifie la conjecture de Leopoldt.

B) Soient k un corps de nombres, p un nombre premier, r le nombre de Dirichlet et r_p le rang p-adique du groupe des unités de k.

1) On suppose que k satisfait l'une des deux propriétés suivantes :

(a) $[k:\mathbb{Q}]=4$ et k n'est pas totalement réel ;

(b) $[k:\mathbb{Q}]=5$ et k a un seul plongement réel.

Montrer que k vérifie la conjecture de Leopoldt.

[Indications.- On pourra montrer que si $r_p<r$, alors

a) pour tout triplet $(\sigma_1,\sigma_2,\sigma_3)$ où les σ_i sont des plongements de k dans une clôture galoisienne, il existe $(m_1,m_2,m_3)\in\mathbb{Z}^3$, $(m_1,m_2,m_3)\neq(0,0,0)$, tel que

$$\sigma_1\epsilon^{m_1}\sigma_2\epsilon^{m_2}\sigma_3\epsilon^{m_3}=1 \quad \text{pour toute unité } \epsilon \text{ de } k ;$$

pour cela on pourra utiliser le théorème des six exponentielles p-adiques ;

b) il existe une unité ϵ_0 de k telle que pour tout entier $n\geq 1$, on ait $k=\mathbb{Q}(\epsilon_0^n)$.]

2) On admet la conjecture des 4 exponentielles p-adiques. Montrer que si $r\geq 2$, alors pour tout nombre premier p on a $r_p\geq 2$.

En déduire que si $r\leq 2$, alors k vérifie la conjecture de Leopoldt.

Corrigé

I.- On admet la conjecture des 4 exponentielles.

a) Si V est un hyperplan de $\mathbb{R}^2$ tel que $V\cap\mathbb{Q}^2=\{0\}$, alors $V\cap\mathbb{L}^2$ est un $\mathbb{Q}$-espace vectoriel de dimension finie ≤ 1 (cf. Introduction, Th.2.3).

En effet, on peut écrire une équation de V sous la forme $x_1+tx_2=0$, avec t réel irrationnel. Si $V\cap\mathbb{L}^2\neq\{0\}$, on prend $(\log\alpha_1, \log\alpha_2)\in V\cap\mathbb{L}^2$, c'est-à-dire $\log\alpha_1+t\log\alpha_2=0$. Alors pour tout $(\log\beta_1, \log\beta_2)\in V\cap\mathbb{L}^2$, la matrice

$$\begin{bmatrix}\log\alpha_1 & \log\alpha_2\\ \log\beta_1 & \log\beta_2\end{bmatrix}$$

a pour rang 1, et la conjecture des 4 exponentielles donne

$$(\log\beta_1,\log\beta_2)\in\mathbb{Z}(\log\alpha_1,\log\alpha_2)$$

c'est-à-dire $\dim_{\mathbb{Q}} V\cap\mathbb{L}^2=1$.

b) Soient α_{ij}, $(1\leq j\leq m,\ i=1,2)$ des nombres algébriques non nuls. Pour $1\leq j\leq m$ et $i=1,2$, soit $\log\alpha_{ij}$ une détermination du logarithme de α_{ij}. On suppose que les $2m$ nombres $\log\alpha_{ij}$ $(1\leq j\leq m,\ i=1,2)$ sont linéairement indépendants sur $\mathbb{Q}$. Pour $1\leq j\leq m$, posons $y_j=(\log\alpha_{1j}, \log\alpha_{2j})\in\mathbb{R}^2$, et soit $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_m$. Alors pour tout hyperplan H de $\mathbb{R}^2$, on a $\dim_{\mathbb{Q}} Y\cap H\leq 1$.

En effet, c'est clair d'après a) si $H\cap\mathbb{Q}^2=\{0\}$, puisque $Y\subset\mathbb{L}^2$. Si $H\cap\mathbb{Q}^2\neq\{0\}$, montrons $Y\cap H=\{0\}$. Pour cela on écrit une équation de H sous la forme $ax_1+bx_2=0$, et l'hypothèse $H\cap\mathbb{Q}^2\neq\{0\}$ permet de choisir a et b rationnels. Si $\sum_{j=1}^{m} h_j y_j\in Y\cap H$, on a

$$\sum_{j=1}^{m} h_j(a\log\alpha_{1j}+b\log\alpha_{2j})=0,$$

d'où $h_j=0$ pour $1\leq j\leq m$.

c) On reprend alors la démonstration du corollaire 3.17 du Chapitre II, et on trouve $s(k)=3$.

II.- L'hypothèse que pour tout $n\geq 1$, ρ^n n'est pas localement algébrique signifie que l'homomorphisme $\chi_\rho : G_k \longrightarrow E_\lambda^{\times}$ associé n'est pas de type (A) (cf. Chap.II, §3.f). On reprend la démonstration du théorème 3.1 (p.II.30), en utilisant directement le théorème 2.1 (p.II.13) plutôt que le corollaire 2.5 (p.II.17). On trouve $m\leq d(d-1)$.

III.-

A) Le cas $\ell=2$ est facile : tout groupe d'ordre 4 est abélien ; on peut donc appliquer le théorème d'Ax-Brumer (Chap.III, Th.3.2, p.III.31).

Supposons donc ℓ impair. Comme $G=G(k/\mathbb{Q})$ est d'ordre 2ℓ, il possède (au moins) un sous-groupe d'ordre ℓ et un sous-groupe d'ordre 2. Soient k_0 un sous-corps de k quadratique sur $\mathbb{Q}$, et k_1 un sous-corps de k de degré ℓ sur $\mathbb{Q}$. Comme k_1 a un degré impair, il possède au moins un plongement réel. Mais k est le compositum de k_0 et de k_1, et k est totalement imaginaire. Donc k_0 ne possède pas de plongement réel, c'est-à- dire que k_0 est un corps quadratique imaginaire. Dans ce cas k est une extension cyclique (de degré ℓ) d'un corps quadratique imaginaire, et le théorème d'Ax-Brumer s'applique encore.

B)

1) Le cas $r_1=0$, $r_2=2$, $d=4$ est particulièrement facile : on a $r=1$, donc $r_p=1$ pour tout p.

Nous supposerons donc $r=2$ et $r_p=1$ pour un premier p, et nous obtiendrons une contradiction.

a) Soient σ_1, σ_2, σ_3 trois plongements de k dans une clôture galoisienne K. Fixons un plongement φ_p de K dans $\mathbb{C}_p$. Soit ϵ_0 une unité de k d'ordre infini. Si ϵ est une unité de k, la matrice

$$(1) \qquad \begin{bmatrix} \log_p \varphi_p \sigma_1 \epsilon_0 & \log_p \varphi_p \sigma_2 \epsilon_0 & \log_p \varphi_p \sigma_3 \epsilon_0 \\ \log_p \varphi_p \sigma_1 \epsilon & \log_p \varphi_p \sigma_2 \epsilon & \log_p \varphi_p \sigma_3 \epsilon \end{bmatrix}$$

a pour rang 1 (puisque $r_p=1$) : prenons d'abord pour ϵ une unité

indépendante de ϵ_0 ; le théorème des 6 exponentielles p-adiques montre que les trois nombres $\log_p\varphi_p\sigma_1\epsilon_0$, $\log_p\varphi_p\sigma_2\epsilon_0$, $\log_p\varphi_p\sigma_3\epsilon_0$ sont linéairement dépendants sur $\mathbb{Q}$: il existe des entiers h_1, h_2, h_3 tels que

$$h_1\log_p\varphi_p\sigma_1\epsilon_0 + h_2\log_p\varphi_p\sigma_2\epsilon_0 + h_3\log_p\varphi_p\sigma_3\epsilon_0 = 0.$$

On utilise de nouveau le fait que pour toute unité ϵ de k, la matrice (1) a pour rang 1 ; on en déduit

$$h_1\log_p\varphi_p\sigma_1\epsilon + h_2\log_p\varphi_p\sigma_2\epsilon + h_3\log_p\varphi_p\sigma_3\epsilon = 0.$$

Comme les $\sigma_i\epsilon$ sont des unités de K, les $\varphi_p\sigma_i\epsilon$ sont des unités p-adiques, et il en résulte que $\sigma_1\epsilon^{h_1}\sigma_2\epsilon^{h_2}\sigma_3\epsilon^{h_3}$ est une racine de l'unité dans K ; donc il existe des entiers m_1, m_2, m_3 non tous nuls tels que

$$\sigma_1\epsilon^{m_1}\sigma_2\epsilon^{m_2}\sigma_3\epsilon^{m_3}=1 \quad \text{pour tout } \epsilon.$$

b) Il existe une unité ϵ_0 de k telle que pour tout entier $n\geq 1$, on ait $k=\mathbb{Q}(\epsilon_0^n)$. C'est évident si $[k:\mathbb{Q}]=5$, puisque dans ce cas on a $k=\mathbb{Q}(\alpha)$ pour tout $\alpha\in k$, $\alpha\notin\mathbb{Q}$. Si $[k:\mathbb{Q}]=4$ et s'il existe une unité d'ordre infini ϵ_1 telle que $\mathbb{Q}(\epsilon_1)\neq k$, prenons une unité ϵ_0 dans k indépendante de ϵ_1. Pour tout $n\geq 1$, ϵ_0^n est une unité indépendante de ϵ_1. Si, pour un $n\geq 1$, on avait $\mathbb{Q}(\epsilon_0^n)\neq k$, alors k serait le compositum des deux corps quadratiques $\mathbb{Q}(\epsilon_1)$ et $\mathbb{Q}(\epsilon_0^n)$, donc $k=\mathbb{Q}(\epsilon_1,\epsilon_0^n)$ serait une extension galoisienne de $\mathbb{Q}$, de degré 4, ce qui contredirait le théorème d'Ax-Brumer.

c) On fixe un plongement de K dans $\mathbb{C}$. On utilise d'abord a) en prenant pour σ_1 un plongement réel et pour σ_2, σ_3 deux plongements imaginaires conjugués. On écrit

$$\sigma_1\epsilon^{m_1}\sigma_2\epsilon^{m_2}\sigma_3\epsilon^{m_3}=1$$

et on conjugue :

$$\sigma_1\epsilon^{m_1}\sigma_3\epsilon^{m_2}\sigma_2\epsilon^{m_3}=1.$$

Ceci est vrai pour tout ϵ, et en particulier pour le ϵ_0 donné par b). Par conséquent le nombre $\epsilon_0^{m_2-m_3}=\alpha$ vérifie $\sigma_2\alpha=\sigma_3\alpha$, ce qui montre qu'il est de degré <4. Grâce au choix de ϵ_0, ceci entraîne $m_2=m_3$, et

$$\sigma_1\epsilon^{m_1}|\sigma_2\epsilon|^{2m_2}=1$$

pour toute unité ϵ ; mais cela est incompatible avec le fait que le régulateur de k est non nul.

3) Si $r\geq 3$, on a $r_p\geq r/2\geq 3/2$, donc $r_p\geq 2$. On peut donc supposer $r=2$. D'après ce qui précède, les seuls cas où l'on ait $r\geq 2$ et où l'inégalité $r_p\geq 2$ ne soit pas démontrée sont : le cas cubique totalement réel non galoisien, et le cas d'un corps de nombres de degré 6 totalement imaginaire non galoisien.

De la conjecture des 4 exponentielles on déduit :

soient k un corps de nombres, $\varphi: k \longrightarrow \mathbb{C}$ et $\varphi_p: k \longrightarrow \mathbb{C}_p$ deux plongements, α_{ij} $(i=1,2\ ;\ j=1,2)$ quatre éléments de k vérifiant $|\varphi_p\alpha_{ij}|_p=1$. Si la matrice

$$\begin{bmatrix} \log|\varphi\alpha_{11}| & \log|\varphi\alpha_{21}| \\ \log|\varphi\alpha_{12}| & \log|\varphi\alpha_{22}| \end{bmatrix}$$

est régulière, alors la matrice

$$\begin{bmatrix} \log_p\varphi_p\alpha_{11} & \log_p\varphi_p\alpha_{21} \\ \log_p\varphi_p\alpha_{12} & \log_p\varphi_p\alpha_{22} \end{bmatrix}$$

est aussi régulière. Par conséquent si $r\geq 2$, alors $r_p\geq 2$ (cf. Ch.III §4).

En particulier, si $r=2$, alors $r_p=2$ pour tout p. Il est banal de voir que si $r\leq 1$, alors $r_p=r$ pour tout p.

On notera que ceci établit la conjecture de Leopoldt pour tous les corps cubiques (en admettant la conjecture des 4 exponentielles p-adiques pour le cas totalement réel non galoisien).