Séminaire de Théorie des Nombres.

- Besançon -

Année 1974 - 1975

QUELQUES CARACTERES UTILES A L'ARITHMETIQUE .

Bernard ORIAT
Faculté des Sciences. Mathématiques.
25030 BESANCON CEDEX

QUELQUES CARACTERES UTILES A L'ARITHMETIQUE .

par Bernard ORIAT .

Introduction

Le présent exposé n'a pas la prétention de traiter de questions originales . Nous avons voulu présenter des notions de caractères couramment utilisées par Leopoldt et sur lesquelles repose entre autres, l'article intitulé : Über Einheitengruppe und Klassenzahl abelscher Zahlkörper [5] . Celui-ci fera l'objet d'un autre exposé .

Les ouvrages traitant des représentations des groupes sont nombreux . Nous avons limité nos références à [1] , [2] et [8] . Mais il faut avouer qu'il y a une certaine distance entre les généralités exposées dans ces livres et l'emploi qu'il en est fait dans [5] . Par exemple, dans [2] et [8] les définitions et premières propriétés sont données avec le corps des nombres complexes comme « corps de base » , alors que dans [5] ne sont utilisés que des caractères sur le corps des nombres rationnels . En fait , les caractères complexes et les caractères rationnels d'un groupe sont reliés par la notion de $\Gamma_{\mathbb{Q}}$ - conjugaison . Celle-ci est traitée dans le chapitre II § 12 et 13 de [8] , mais cela est vu sous un angle général , alors que dans [5] , il n'est question que de groupes commutatifs et dans ce cadre restreint les choses peuvent être disséquées élémentairement .

Nous distinguerons cinq parties :
Dans la première il sera question de la structure de l'algèbre $\mathbb{Q}[G]$ et des caractères de G sur $\mathbb{Q}$ (G étant un groupe abélien fini) . Nous montrerons dans la deuxième que des résultats analogues peuvent être énoncés pour l'algèbre $\mathbb{Q}_p[G]$ et pour les caractères de G sur $\mathbb{Q}_p$. Dans la troisième , on traitera de l'algèbre $\mathbb{Z}[G]$ et de certains de ses modules. Dans la quatrième , seront introduits les caractères résiduels . Cette notion repose essentiellement sur le théorème de Kronecker-Weber . Il s'agit de caractères qui caractérisent (!) les extensions abéliennes de $\mathbb{Q}$. Cette partie est presque indépendante des précédentes . Enfin dans la cinquième , nous essayerons d'utiliser les notions présentées auparavant pour décomposer le p-sous-groupe de Sylow du groupe des classes d'extensions abéliennes de degré premier à p .

Nous supposerons connues les notions de base : c'est-à-dire celles contenues dans le chapitre I de [8] (ou dans les chapitres I à V de [2]) . Nous essayerons de présenter ces questions de la façon la plus élémentaire .

I

Caractères sur le corps des rationnels .

1) Notations. Rappels . On désigne par G un groupe abélien fini d'ordre g et par K un corps de caractéristique 0 . Rappelons rapidement les définitions essentielles ([8] ch I § 1 et ch II § 6) . Une représentation linéaire de G sur un corps K est un homomorphisme ρ de G dans le groupe linéaire d'un espace vectoriel V de dimension finie sur K :

$$\rho : G \to GL(V)$$
$$\sigma \to \rho_\sigma \ .$$

Il lui est associé une structure de K[G]-module sur V ainsi définie : Si $\sum_{\sigma \in G} a_\sigma \sigma$ est un élément de K[G] , l'action de K[G] sur V est donnée par :

$$\Big(\sum_{\sigma \in G} a_\sigma \sigma \ , \ x \Big) \longrightarrow \sum_{\sigma \in G} a_\sigma \rho_\sigma(x) \ .$$

Réciproquement , si V est un K-espace vectoriel de dimension finie et si V est muni d'une structure de K[G]-module , alors définissons pour tout σ de G , ρ_σ comme étant l'application de V dans V telle que $\rho_\sigma(x) = \sigma x$; cette application est un automorphisme de V et $\rho : G \to GL(V)$ est une représentation linéaire de G sur K . Se donner une représentation de G sur K est donc équivalent à se donner un K[G]-module et réciproquement.

On dit que deux représentations linéaires de G sur K sont isomorphes si elles correspondent à des K[G]-modules isomorphes.

Soit $\varkappa$ l'application de G dans K qui associe à tout σ de G la trace de ρ_σ . Rappelons que la propriété essentielle de $\varkappa$ est de caractériser (à un isomorphisme près) la représentation ρ ou le K[G]-module V . On dira que $\varkappa$ est le caractère de la représentation ρ , ou le caractère du K[G]-module V , ou encore plus brièvement , que $\varkappa$ est un caractère de G sur K . C'est donc la définition donnée en [8] , ch I § 2 , à ceci près que nous ne supposons pas $K = \mathbb{C}$.

Si V possède deux K[G]-sous-modules V' et V" non réduits à 0 et tels que $V = V' \oplus V"$, on dit que V est décomposable . Si ρ' et $\rho"$ sont les représentations de G sur K correspondant à V' et V" on dit que ρ est somme directe de ρ' et $\rho"$. Si $\varkappa'$ et $\varkappa"$ sont les caractères respectifs de V' et V" , on vérifie que $\varkappa$ est la somme de $\varkappa'$ et $\varkappa"$.

Si V n'est pas décomposable , on dit que V est un K[G]-module simple . La représentation ρ correspondante est dite irréductible et le caractère $\varkappa$ irréductible sur K ([8] ch I § 2) . Tout K[G]-module est somme directe de K[G]-modules simples ; ceux-ci sont uniques (à un isomorphisme près) . Il revient au même de dire que toute représentation de G sur K est somme directe de représentations irréductibles de G sur K . On en déduit qu'un caractère de G sur K s'écrit d'une façon et d'une seule comme combinaison linéaire à coefficients entiers positifs de caractères de G irréductibles sur K .

Rappelons aussi qu'un idéal minimal de K[G] est un K[G] - module simple et que réciproquement , tout K[G]-module simple est isomorphe à un idéal minimal de K[G] .

Soit $\mathfrak{X}$ l'ensemble des caractères irréductibles de G sur $\mathbb{C}$ (on dira aussi caractères complexes de G) . Ses éléments seront notés $\varkappa$, ψ , ... Ce sont les homomorphismes de G dans le groupe multiplicatif des nombres complexes de module 1 . Cet ensemble $\mathfrak{X}$, muni de la loi de composition ainsi définie : $(\varkappa\psi)(\sigma) = \varkappa(\sigma)\,\psi(\sigma)$ pour tout σ de G , est un groupe . On notera $g_\varkappa$ l'ordre de $\varkappa$. Cette quantité est aussi égale à l'ordre de $\varkappa(G)$.

Nous appellerons quelquefois $\mathfrak{X}$ le dual de G et nous adopterons alors la notation $G^\wedge$ au lieu de $\mathfrak{X}$. En effet il existe entre G et $G^\wedge$ des propriétés de dualité classiques .

Nous désignerons par : orthogonal du sous-groupe S de G ,
l'ensemble :

$$S^\perp = \{ \varkappa ; \varkappa \in \mathfrak{X} ; \varkappa(\sigma) = 1 \text{ pour tout } \sigma \in S \} ,$$

et orthogonal d'un sous-groupe Φ de $\mathfrak{X}$, l'ensemble :

$$\Phi^\perp = \{ \sigma ; \sigma \in G ; \varkappa(\sigma) = 1 \text{ pour tout } \varkappa \in \Phi \}$$

Il y a des isomorphismes canoniques entre $(G/S)^\wedge$ et $S^\perp$, entre $S^\wedge$ et $\mathfrak{X}/S^\perp$, entre $(G/\Phi^\perp)^\wedge$ et Φ etc ... que nous ne détaillerons pas . On peut voir par exemple [7] , ch III .

2) Décomposition de l'algèbre $\mathbb{Q}[G]$ (Le groupe G est toujours abélien) .

Lemme . Soient $\varkappa$ et ψ deux éléments de $\mathfrak{X}$.
Les sous-groupes de $\mathfrak{X}$ engendrés par $\varkappa$ et ψ sont égaux si et seulement si les noyaux de $\varkappa$ et ψ sont égaux .

La démonstration repose sur les propriétés de dualité existant entre $\mathfrak{X}$ et G . Si Φ est un sous-groupe de $\mathfrak{X}$, désignons par $\Phi^{\perp}$ l'orthogonal de Φ . L'application $\Phi \to \Phi^{\perp}$ réalise une bijection de l'ensemble des sous-groupes de $\mathfrak{X}$ sur l'ensemble des sous-groupes de G et Ker $\varkappa$ est l'orthogonal du sous-groupe engendré par $\varkappa$.

Définitions . Deux éléments $\varkappa$ et ψ de $\mathfrak{X}$ seront dits Γ-conjugués si et seulement si $\varkappa$ et ψ engendrent le même sous-groupe de $\mathfrak{X}$. (Il s'agit donc de la $\Gamma_{\mathbb{Q}}$-conjugaison de Serre, [8] , ch II , § 12) . On désigne par $\varkappa'$ la classe de $\varkappa$ modulo cette relation d'équivalence et par $\mathfrak{X}'$ l'ensemble de ces classes d'équivalence . Pour tout $\varkappa$ de $\mathfrak{X}$, on posera (g étant l'ordre du groupe G) $e_{\varkappa} = \frac{1}{g} \sum_{\sigma \in G} \varkappa(\sigma^{-1})\sigma$ et $e_{\varkappa'} = \sum_{\psi \in \varkappa'} e_{\psi}$.

Si $\varkappa$ et ψ sont Γ-conjugués , $g_{\varkappa}$ et g_{ψ} sont égaux . On posera $g_{\varkappa'} = g_{\varkappa}$.

Proposition I a . L'ensemble des $e_{\varkappa'}$, $\varkappa'$ parcourant $\mathfrak{X}'$, est un système d'idempotents orthogonaux et primitifs de l'algèbre $\mathbb{Q}[G]$. La décomposition de cette algèbre en somme directe d'idéaux minimaux est $\mathbb{Q}[G] = \bigoplus_{\varkappa' \in \mathfrak{X}'} \mathbb{Q}[G]\, e_{\varkappa'}$. L'idéal $\mathbb{Q}[G]\, e_{\varkappa'}$ est un anneau d'élément neutre $e_{\varkappa'}$, isomorphe au corps cyclotomique $\mathbb{Q}^{(g_{\varkappa})}$.

démonstration

Soit $\varkappa$ appartenant à $\mathfrak{X}$. On a :
$\varkappa' = \{\varkappa^k \ ; \ (k, g_{\varkappa}) = 1\}$ et pour tout σ de G , $\varkappa(\sigma)$ est une racine $g_{\varkappa}^{\text{ème}}$ de 1 . Comme le groupe de Galois de $\mathbb{Q}^{(g_{\varkappa})}/\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/g_{\varkappa}\mathbb{Z})^*$, on en déduit que $\sum_{\psi \in \varkappa'} \psi(\sigma) = \mathrm{Tr}_{\mathbb{Q}^{(g_{\varkappa})}/\mathbb{Q}}(\varkappa(\sigma))$ appartient à $\mathbb{Q}$. Donc

$e_{\chi'}$ appartient à $\mathbb{Q}[G]$. D'autre part l'ensemble des e_χ , χ parcourant $\mathfrak{X}$, est un système d'idempotents orthogonaux de $\mathbb{C}[G]$, c'est-à-dire que :

$$e_\chi^2 = e_\chi \ ,$$

$$e_\chi e_\psi = 0 \quad \text{si } \chi \neq \psi \ ,$$

$$1 = \sum_{\chi \in \mathfrak{X}} e_\chi \ .$$

On en déduit que l'ensemble des $e_{\chi'}$, χ' parcourant $\mathfrak{X}'$, est un système d'idempotents orthogonaux de $\mathbb{Q}[G]$, c'est-à-dire que :

$$e_{\chi'}^2 = e_{\chi'} \ ,$$

$$e_{\chi'} e_{\psi'} = 0 \quad \text{si } \chi' \neq \psi' \ ,$$

$$1 = \sum_{\chi' \in \mathfrak{X}'} e_{\chi'} \ .$$

L'algèbre $\mathbb{Q}[G]$ est donc somme directe des idéaux engendrés par $e_{\chi'}$:

$$\mathbb{Q}[G] = \bigoplus_{\chi' \in \mathfrak{X}'} \mathbb{Q}[G]\, e_{\chi'} \ .$$

Notons encore χ l'application déduite de χ par $\mathbb{Q}$-linéarité :

$$\chi : \mathbb{Q}[G] \longrightarrow \mathbb{Q}^{(g_\chi)} \ ,$$

c'est-à-dire telle que $\chi\Big(\sum_{\sigma \in G} a_\sigma \sigma\Big) = \sum_{\sigma \in G} a_\sigma \chi(\sigma)$. Il s'agit d'un $\mathbb{Q}$-homomorphisme d'anneaux surjectif . Montrons que $\chi(e_{\chi'}) = 1$.

Nous avons :

$$\chi(e_{\chi'}) = \frac{1}{g} \sum_{\sigma \in G} \sum_{(k, g_\chi) = 1} \chi^k(\sigma^{-1})\, \chi(\sigma) \ .$$

Soit σ_o un élément de G , tel que $\chi(\sigma_o)$ engendre $\chi(G)$.
Nous aurons alors :

$$\chi(e_{\chi'}) = (\,|\mathrm{Ker}\,\chi|\,/\,g) \sum_{u=1}^{g_\chi} \sum_{(k, g_\chi) = 1} \chi^k(\sigma_o^{-u})\, \chi(\sigma_o^u)$$

soit : $$\chi(e_{\chi'}) = (\,|\mathrm{Ker}\,\chi|\,/g) \sum_{(k, g_\chi) = 1} \sum_{u=1}^{g_\chi} \chi(\sigma_o)^{u(1-k)} \ .$$

Or la dernière somme est égale à g_χ si $k = 1$, sinon à 0 . D'où $\chi(e_{\chi'}) = 1$. On en déduit que la restriction de χ à l'idéal $\mathbb{Q}[G]\, e_{\chi'}$ est

encore une application surjective . Pour montrer que cette application est injective , on peut s'appuyer sur des considérations de dimension : En effet :

$$\dim_{\mathbb{Q}} \bigoplus_{\varkappa' \in \mathfrak{X}'} \mathbb{Q}^{(g_{\varkappa'})} = \sum_{\varkappa' \in \mathfrak{X}'} \varphi(g_{\varkappa'}) = |\mathfrak{X}| = |G| \quad .$$

D'où l'on déduit que $\dim_{\mathbb{Q}} \mathbb{Q}[G]\, e_{\varkappa'} = \varphi(g_{\varkappa})$ et que la restriction de $\varkappa$ à $\mathbb{Q}[G]\, e_{\varkappa'}$ est un isomorphisme :

$$\mathbb{Q}[G]\, e_{\varkappa'} \cong \mathbb{Q}^{(g_{\varkappa'})} \quad .$$

Exemple : Si G est cyclique , l'application $\varkappa' \to g_{\varkappa'}$ réalise une bijection de $\mathfrak{X}'$ sur l'ensemble des diviseurs de g et on a :

$$\mathbb{Q}[G] \cong \bigoplus_{d \mid g} \mathbb{Q}^{(d)} \quad .$$

Remarque . Nous avons utilisé la relation $\varkappa(e_{\varkappa'}) = 1$.
Nous avons également $\varkappa(e_{\psi'}) = 0$ si $\varkappa$ n'appartient pas à ψ' .

3) Calcul des caractères de G sur $\mathbb{Q}$. Soit $\overline{\varkappa}'$ le caractère irréductible de G sur $\mathbb{Q}$ correspondant à l'idéal minimal $\mathbb{Q}[G]\, e_{\varkappa'}$ de $\mathbb{Q}[G]$. Si σ appartient à G , $\overline{\varkappa}'(\sigma)$ est donc la trace du $\mathbb{Q}$-endomorphisme de $\mathbb{Q}[G]\, e_{\varkappa'}$: $x \to \sigma x$. Etendons le corps des scalaires $\mathbb{Q}$ de cet espace vectoriel à $\mathbb{C}$. Nous obtenons alors l'espace vectoriel $\mathbb{C}[G]\, e_{\varkappa'}$ qui a pour base $\{e_{\psi}\}_{\psi \in \varkappa'}$. Utilisant alors la relation $\sigma e_{\varkappa} = \varkappa(\sigma) e_{\varkappa}$, nous voyons que la matrice de l'endomorphisme $x \to \sigma x$ de $\mathbb{C}[G]\, e_{\varkappa'}$ est la matrice diagonale :

$$\begin{pmatrix} \ddots & & \\ & \psi(\sigma) & \\ & & \ddots \end{pmatrix}$$

où ψ parcourt la Γ-classe de $\varkappa$. On a donc $\overline{\varkappa}'(\sigma) = \sum_{\psi \in \varkappa'} \psi(\sigma)$, soit pour abréger : $\varkappa' = \sum_{\psi \in \varkappa'} \psi$. L'application $\varkappa' \to \overline{\varkappa}'$ réalise une bijection canonique de $\mathfrak{X}'$ sur l'ensemble des caractères rationnels de G .
Nous avons démontré :

Proposition 1b . L'ensemble des caractères irréductibles de G sur $\mathbb{Q}$ correspond bijectivement à l'ensemble $\mathfrak{X}'$ des Γ-classes de $\mathfrak{X}$. On confondra désormais la Γ-classe χ' de χ avec le caractère $\overline{\chi}'$. On a alors les formules :

$$\chi' = \sum_{\psi \in \chi'} \psi \ ,$$

$$\chi' = \mathrm{Tr}_{\mathbb{Q}(g_\chi)/\mathbb{Q}}(\chi) \ ,$$

$$e_{\chi'} = \frac{1}{g} \sum_{\sigma \in G} \chi'(\sigma^{-1})\sigma \ .$$

II

Caractères sur le corps des nombres p-adiques .

Soient p un nombre premier , n un entier . Ecrivons le sous la forme $n = p^\alpha m$, avec p ne divisant pas m .
On a un isomorphisme canonique :

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \ .$$

Si $\langle p \rangle$ désigne le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$ engendré par la classe de p modulo m , soit U_{pn} le sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ correspondant à $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \times \langle p \rangle$ dans l'isomorphisme ci-dessus .

Rappelons que le groupe de Galois de $\mathbb{Q}_p^{(n)}/\mathbb{Q}_p$ s'identifie canoniquement à U_{pn} .

1) Γ_p-conjugaison et décomposition de $\mathbb{Q}_p[G]$. On désigne toujours par G un groupe abélien fini d'ordre g et par n un multiple de l'exposant de G . Soient χ et ψ deux éléments de $\mathfrak{X}$. Nous dirons que χ et ψ sont Γ_p-conjugués s'il existe un entier k dont la classe modulo n se trouve dans U_{pn} et tel que $\chi = \psi^k$. Nous définissons ainsi une relation d'équivalence qui ne dépend pas de l'entier n choisi . Nous désignerons par χ'' la classe de χ et par $\mathfrak{X}''$ l'ensemble de ces classes d'équivalence . Nous pouvons considérer les caractères χ de G comme étant à valeurs dans une clôture algébrique de $\mathbb{Q}_p$. Nous poserons $e_{\chi''} = \sum_{\psi \in \chi''} e_\psi$.

Proposition II a . L'ensemble des $e_{\varkappa''}$, $\varkappa''$ parcourant $\mathfrak{X}''$, est un système d'idempotents orthogonaux et primitifs de l'algèbre $\mathbb{Q}_p[G]$. La décomposition de cette algèbre en somme directe d'idéaux minimaux est

$$\mathbb{Q}_p[G] = \bigoplus_{\varkappa'' \in \mathfrak{X}''} \mathbb{Q}_p[G]\, e_{\varkappa''} \ .$$

L'idéal $\mathbb{Q}_p[G]\, e_{\varkappa''}$ est isomorphe au corps cyclotomique p-adique $\mathbb{Q}_p^{(g_\varkappa)}$.

La démonstration est semblable à la démonstration de la proposition I a .

2) Calculs des caractères de G sur $\mathbb{Q}_p$. Soit $\overline{\varkappa}''$ le caractère de G sur $\mathbb{Q}_p$ correspondant à l'idéal minimal $\mathbb{Q}_p[G]\, e_{\varkappa''}$ de $\mathbb{Q}_p[G]$. Nous obtenons alors , comme précédemment :

Proposition II b . L'ensemble des caractères irréductibles de G sur $\mathbb{Q}_p$ correspond bijectivement à l'ensemble $\mathfrak{X}''$ des Γ_p-classes de $\mathfrak{X}$. On confondra désormais la Γ_p-classe $\varkappa''$ de $\varkappa$ avec le caractère $\overline{\varkappa}''$. On a alors les formules

$$\varkappa'' = \sum_{\psi \in \varkappa''} \psi \ ,$$

$$\varkappa'' = \mathrm{Tr}_{\mathbb{Q}_p^{(g_\varkappa)}/\mathbb{Q}_p}(\varkappa) \ ,$$

$$e_{\varkappa''} = \frac{1}{g} \sum_{\sigma \in G} \varkappa''(\sigma^{-1})\sigma$$

3) Remarque concernant le degré de généralité des formules obtenues. Supposons un instant que G soit un groupe fini quelconque et k un corps de caractéristique 0 . Soit $\mathfrak{X}$ l'ensemble des caractères absolument irréductibles de G , c'est-à-dire irréductibles sur une clôture algébrique $\overline{k}$ de k . Précisons (sans justification) que cet ensemble ne dépend pas de k . Si $\varkappa$ appartient à $\mathfrak{X}$, on désigne par $k(\varkappa)$ le corps obtenu en adjoignant à k les valeurs $\varkappa(\sigma)$, σ parcourant G . Ce corps est appelé le corps des valeurs de $\varkappa$. (On reconnait , dans les cas particuliers qui nous intéressaient : $k = \mathbb{Q}$ ou $\mathbb{Q}_p$ et $k(\varkappa) = \mathbb{Q}^{(g_\varkappa)}$ ou $\mathbb{Q}_p^{(g_\varkappa)}$)

Posons $\varkappa' = \mathrm{Tr}_{k(\varkappa)/k}(\varkappa)$. On a le résultat suivant :

Si l'algèbre $k[G]$ est décomposée , alors $\varkappa'$ est un caractère irréductible de G sur k et tout caractère irréductible de G sur k s'obtient de cette façon .

Précisons que l'algèbre $k[G]$ est dite décomposée si elle est isomorphe à un produit d'anneaux de matrices à coefficients dans des corps commutatifs .

Il est clair que si G est commutatif , $k[G]$ est décomposée .

Signalons encore le résultat suivant : Si G est un groupe d'ordre premier à p , l'algèbre $\mathbb{Q}_p[G]$ est décomposée . Ce résultat et plus généralement les caractères p-adiques sont utilisés dans [6] .

III

Etude de certains $\mathbb{Z}[G]$-modules .

Les notations sont les mêmes que précédemment . En particulier G est toujours un groupe abélien fini .

1) Ordres de $\mathbb{Q}[G]$. Soit $\varkappa'$ appartenant à $\mathfrak{X}'$. On a mis en évidence dans I , un isomorphisme entre $\mathbb{Q}[G]e_{\varkappa'}$ et $\mathbb{Q}^{(g_{\varkappa'})}$. Dans cet isomorphisme , l'anneau des entiers de $\mathbb{Q}^{(g_{\varkappa'})}$ correspond à $\mathbb{Z}[G]e_{\varkappa'}$.

Posons $\mathcal{O} = \bigoplus_{\varkappa' \in \mathfrak{X}'} \mathbb{Z}[G]e_{\varkappa'}$. Ce sous-anneau de $\mathbb{Q}[G]$ est l'ordre maximum de $\mathbb{Q}[G]$. Si $d_{\varkappa'}$ désigne le discriminant de $\mathbb{Q}^{(g_{\varkappa})}$, le discriminant de $\mathcal{O}$ (c'est-à-dire le discriminant d'une $\mathbb{Z}$-base de G) sera $d(\mathcal{O}) = \prod_{\varkappa' \in \mathfrak{X}'} d_{\varkappa'}$.

L'anneau $\mathbb{Z}[G]$ est aussi un ordre de $\mathbb{Q}[G]$. Son discriminant est g^g et l'indice de $\mathbb{Z}[G]$ dans $\mathcal{O}$ est donné par :

$$g^g = (\mathcal{O} : \mathbb{Z}[G])^2 \, d(\mathcal{O}) \ .$$

2) Extension de l'anneau des scalaires de $\mathbb{Z}$ à $\mathbb{Q}$. Soit M un $\mathbb{Z}[G]$-module. Dans tout ce qui suit on suppose que M est libre de type fini sur $\mathbb{Z}$.

Définition de $\mathbb{Q}M$. On suppose que M est noté additivement . Si (m, a) et (n, b) appartiennent à $M \times \mathbb{Z}^*$, considérons la relation d'équivalence définie par $(m, a) \sim (n, b)$ si et seulement si $bm = an$. La classe de (m, a) sera notée m/a . En posant $(m/a) + (n/b) = (an+bm)/ab$ et

$(ab^{-1})(n/c) = an/bc$, on définit sur l'ensemble quotient une structure de $\mathbb{Q}$-espace vectoriel . Nous le noterons $\mathbb{Q}M$. (Si M est un $\mathbb{Z}[G]$-module noté multiplicativement : $M^{\mathbb{Q}}$) . La dimension de $\mathbb{Q}M$ sur $\mathbb{Q}$ est égale à la dimension de M sur $\mathbb{Z}$. En posant $\sigma(m/a) = (\sigma m)/a$, pour tout σ de G , $\mathbb{Q}M$ devient un $\mathbb{Q}[G]$-module . L'application $m \to m/1$ réalise une injection de M dans $\mathbb{Q}M$. On considérera M comme une partie de $\mathbb{Q}M$.

Remarque . $\mathbb{Q}M$ est donc déduit de M par extension de l'anneau des scalaires à $\mathbb{Q}$. On aurait pu poser $\mathbb{Q}M = \mathbb{Q} \otimes_{\mathbb{Z}} M$.

Interprétation du théorème de Dirichlet . Soient $K/\mathbb{Q}$ une extension abélienne finie , G son groupe de Galois , E le groupe des unités de K , T le sous-groupe de torsion de E , c'est-à-dire l'ensemble des racines de 1 contenues dans K . Posons $M = E/T$. Il s'agit d'un $\mathbb{Z}[G]$-module et c'est un $\mathbb{Z}$-module libre de type fini . La proposition suivante décrit la structure de $\mathbb{Q}[G]$-module de $M^{\mathbb{Q}}$. (M est un $\mathbb{Z}[G]$-module multiplicatif , d'où la notation $M^{\mathbb{Q}}$.)

Proposition III a . Soit α le caractère de $M^{\mathbb{Q}}$. Si K est réel , α est la somme des caractères irréductibles de G sur $\mathbb{Q}$ différents du caractère unité (noté 1) . C'est-à-dire que $M^{\mathbb{Q}}$ est isomorphe au $\mathbb{Q}[G]$-module (additif) :

$$\bigoplus_{\substack{\chi' \in \mathfrak{X}' \\ \chi' \neq 1}} \mathbb{Q}[G]\, e_{\chi'} \quad .$$

Si K est imaginaire , α est la somme des caractères irréductibles de G sur $\mathbb{Q}$, différents de 1 et tels que $\operatorname{Ker} \chi$ contiennent la conjugaison complexe σ_∞ . C'est-à-dire que $M^{\mathbb{Q}}$ est isomorphe au $\mathbb{Q}[G]$-module :

$$\bigoplus_{\substack{\chi' \in \mathfrak{X}' \\ \sigma_\infty \in \operatorname{Ker} \chi' \\ \chi' \neq 1}} \mathbb{Q}[G]\, e_{\chi'} \quad .$$

démonstration

Supposons K réel . Soient $t = [K:\mathbb{Q}]$ et ℓ le plongement logarithmique de E

$$\ell : E \to \mathbb{R}^t$$

défini par $\ell(\varepsilon) = (\operatorname{Log} |\varepsilon^\sigma|)_{\sigma \in G}$. On sait (Théorème de Dirichlet) que ℓ a pour noyau T et pour image un sous-groupe discret de $\mathbb{R}^t$ de

rang t-1 inclus dans l'hyperplan de $\mathbb{R}^t$ d'équation $\sum_{\sigma \in G} x_\sigma = 0$. Soit U le sous-groupe de $\mathbb{R}^t$ formé des points de la forme $(\lambda, \lambda, \ldots, \lambda)$, λ parcourant $\mathbb{Z}$. Considérons $\ell(E) \oplus U$; c'est un sous-groupe discret de $\mathbb{R}^t$ de rang t . D'autre part munissons $\mathbb{R}^t$ de la structure de G-module ainsi définie : $\tau(x_\sigma)_{\sigma \in G} = (x_{\tau\sigma})_{\sigma \in G}$. On voit alors que ℓ est un G-homomorphisme et U un sous-G-module de $\mathbb{R}^t$. Soit $\{e_1, e_2, \ldots, e_t\}$ une $\mathbb{Z}$-base de $\ell(E) \oplus U$.

Soit σ appartenant à G et soit A_σ la matrice à coefficients entiers définissant l'action de G sur $\ell(E) \oplus U$, c'est-à-dire $(e_1^\sigma, \ldots, e_t^\sigma) = (e_1, \ldots, e_t)A$. Comme $\{e_1, \ldots, e_t\}$ est une base de $\mathbb{R}^t$ la trace de A ne change pas si on remplace $\{e_1, \ldots, e_t\}$ par une base quelconque de $\mathbb{R}^t$. Choisissant alors la base canonique , on en déduit que la trace de A_σ est 0 si σ est différent de 1 et t si $\sigma = 1$.

L'application $\sigma \longrightarrow \operatorname{Tr} A_\sigma$ est le caractère du $\mathbb{Q}[G]$-module $\mathbb{Q}(\ell(E) \oplus U)$. Il est clair que $\mathbb{Q}(\ell(E) \oplus U) = \mathbb{Q}\ell(E) \oplus \mathbb{Q}U$ et que le caractère de ce dernier $\mathbb{Q}[G]$-module est 1 . Le caractère α cherché est donc défini par :

$$\star \quad \begin{cases} \alpha(\sigma) = -1 & \text{si } \sigma \neq 1 \\ \alpha(\sigma) = t-1 & \text{si } \sigma = 1 \ . \end{cases}$$

On vérifie alors que $\alpha = \sum_{\substack{\varkappa' \in \mathfrak{X}' \\ \varkappa' \neq 1}} \varkappa'$.

Si maintenant K est imaginaire , on pose $t = [K:\mathbb{Q}]/2$. On choisit comme indices des composantes de $\mathbb{R}^t$ les éléments du groupe quotient $G/\{1, \sigma_\infty\}$. Le principe de la démonstration reste le même . Le caractère α sera donné par les relations :

$$\star\star \quad \begin{cases} \alpha(\sigma) = -1 & \text{si } \sigma \neq 1 \text{ et } \sigma \neq \sigma_\infty \\ \alpha(\sigma) = t-1 & \text{si } \sigma = 1 \text{ ou } \sigma = \sigma_\infty \ . \end{cases}$$

On vérifie alors que l'on a $\alpha = \sum \varkappa'$, cette somme étant étendue aux éléments de $\mathfrak{X}'$, différents de 1 et tels que Ker $\varkappa$ contienne σ_∞ .

Remarque . Si $K/\mathbb{Q}$ est seulement galoisienne finie , les formules $\star$ et $\star\star$ donnant le caractère α de $M^{\mathbb{Q}}$ sont encore vraies .

3) $\mathbb{Z}[G]$-modules simples et complets . Les $\mathbb{Z}[G]$- modules considérés sont toujours des $\mathbb{Z}$-modules libres de type fini .

Définitions . Soit donc M un tel $\mathbb{Z}[G]$-module . Si $\mathbb{Q}M$ est un $\mathbb{Q}[G]$-module simple , on dira que M est $\mathbb{Z}[G]$-module simple . Si $\varkappa'$ est le caractère de $\mathbb{Q}M$, on dira aussi que $\varkappa'$ est le caractère du $\mathbb{Z}[G]$- module M . L'ensemble des x de $\mathcal{O}$ tels que $xM \subset M$ forme un ordre de $\mathbb{Q}[G]$ noté $\mathcal{O}_M$

$$\mathcal{O}_M = \{ x \; ; \; x \in \mathcal{O} \; ; \; xM \subset M \} \; .$$

On a donc : $\mathbb{Z}[G] \subset \mathcal{O}_M \subset \mathcal{O}$. On dira que M est complet si $\mathcal{O}_M = \mathcal{O}$.

Proposition III b . Soit M un $\mathbb{Z}[G]$-module . Il existe un plus petit module complet contenant M (contenu dans $\mathbb{Q}M$) noté M^* et appelé l'enveloppe de M . Il existe un plus grand module complet contenu dans M , noté M_* , et appelé le noyau de M . Les indices $(M^* : M)$ et $(M : M_*)$ sont finis .

démonstration

Posons $M^* = \mathcal{O}M$. (Il s'agit de la partie de $\mathbb{Q}M$ ainsi définie : $\mathcal{O}M = \{ xm \; ; \; x \in \mathcal{O} \; , \; m \in M \}$) . C'est un $\mathbb{Z}[G]$-module , contenant M , complet et c'est le plus petit module complet contenant M . D'autre part une somme de $\mathbb{Z}[G]$-modules complets est complète . Définissons donc M_* comme la somme des sous-modules complets de M .

On a $g\mathcal{O} \subset \mathbb{Z}[G]$; donc $gM^* = g\mathcal{O}M \subset \mathbb{Z}[G]M \subset M$. L'inclusion $gM^* \subset M$ prouve que $(M^* : M)$ est fini .
D'autre part gM^* est complet , d'où $gM^* \subset M_*$.
On en déduit l'inclusion $gM \subset M_*$. Ceci prouve que $(M : M_*)$ est fini .

Proposition III c . Tout $\mathbb{Z}[G]$-module simple est complet .

démonstration

Supposons que M soit un $\mathbb{Z}[G]$-module simple , et soit ψ' son caractère . Pour tout $\varkappa'$ différent de ψ' on a donc $e_{\varkappa'}\mathbb{Q}M = 0$; d'où $e_{\varkappa'}M = 0$. Quel que soit m appartenant à M , on aura donc : $m = \left(\sum_{\varkappa' \in \mathfrak{X}'} e_{\varkappa'} \right) m = e_{\psi'}m$. D'où $M = e_{\psi'}M$ et $M = \mathcal{O}M$.

Proposition III d . Tout $\mathbb{Z}[G]$-module complet est somme directe de $\mathbb{Z}[G]$-modules simples .

démonstration

Soit M un $\mathbb{Z}[G]$-module complet . On a donc $M = \bigoplus_{\chi' \in \Xi'} e_\chi, M$ et e_χ, M est un $\mathcal{O}$-module . C'est aussi un $e_\chi, \mathcal{O}$-module . Or $e_\chi, \mathcal{O}$ est isomorphe à l'anneau des entiers de $\mathbb{Q}^{(g_\chi,)}$; c'est donc un anneau de Dedekind . Le module e_χ, M sera donc isomorphe à une somme directe (externe) d'idéaux de $e_\chi, \mathcal{O}$, c'est-à-dire : $e_\chi, M = \bigoplus_i M^i_{\chi,}$. En posant $e_\psi, x = 0$ pour tout ψ' différent de χ' et tout x de $M^i_{\chi,}$, on définit sur $M^i_{\chi,}$ une structure de $\mathcal{O}$-module . De plus $\mathbb{Q}M^i_{\chi,} = \mathbb{Q}\, e_\chi, \mathcal{O} = \mathbb{Q}[G]\, e_\chi,$ est un $\mathbb{Q}[G]$-module simple . On a donc décomposé M en somme directe de $\mathbb{Z}[G]$-modules simples .

Proposition III e . Soit χ' un caractère irréductible de G sur $\mathbb{Q}$. Les classes de $\mathbb{Z}[G]$-modules simples , isomorphes , de caractère χ' , correspondent bijectivement aux classes d'idéaux du corps cyclotomique $\mathbb{Q}^{(g_\chi,)}$.

démonstration

Soient M_1 et M_2 deux $\mathbb{Z}[G]$-modules simples de caractère χ'. On a donc $M_1 = e_\chi, M_1$ et $M_2 = e_\chi, M_2$. Les $\mathbb{Z}[G]$-modules M_1 et M_2 sont isomorphes si et seulement si M_1 et M_2 sont isomorphes en tant que $e_\chi, \mathcal{O}$-modules . Or $e_\chi, \mathcal{O}$ est un anneau de Dedekind et M_1 et M_2 sont donc isomorphes (en tant que $e_\chi, \mathcal{O}$-modules) à des idéaux $\mathfrak{a}_1$ et $\mathfrak{a}_2$ de $e_\chi, \mathcal{O}$. On sait que ces idéaux sont isomorphes si et seulement si ils se trouvent dans la même classe .

IV

Caractères résiduels .

1) Définitions . On désigne par $(\mathbb{Z}/f\mathbb{Z})^*$ le groupe multiplicatif des classes résiduelles modulo f , premières à f . On notera $\mathfrak{X}_f$ son dual , c'est-à-dire le groupe des homomorphismes de $(\mathbb{Z}/f\mathbb{Z})^*$ dans le groupe des nombres complexes de module 1 . Un élément de $\mathfrak{X}_f$ sera appelé un caractère résiduel modulo f . Enfin un sous-groupe de $\mathfrak{X}_f$ sera appelé un groupe de caractères résiduels modulo f .

On suppose que f divise g . On notera Π_{fg} l'application

$$\Pi_{fg} : (\mathbb{Z}/g\mathbb{Z})^* \longrightarrow (\mathbb{Z}/f\mathbb{Z})^*$$

qui associe à la classe de y modulo g , la classe de y modulo f . Cette application est un homomorphisme surjectif , Π_{ff} est l'identité et si g divise h , on a $\Pi_{fg} \circ \Pi_{gh} = \Pi_{fh}$.

D'autre part , on notera i_{fg} l'application

$$i_{fg} : \mathfrak{X}_f \to \mathfrak{X}_g$$

qui fait correspondre $\varkappa \circ \Pi_{fg}$ à $\varkappa$. Il s'agit d'un homomorphisme injectif , i_{ff} est l'identité et on a $i_{gh} \circ i_{fg} = i_{fh}$.

Supposons maintenant que f et f' soient deux diviseurs de g. Soient d et m le PGCD et le PPCM de f et f' . On vérifie que :

$$\operatorname{Ker} \Pi_{fg} \cdot \operatorname{Ker} \Pi_{f'g} = \operatorname{Ker} \Pi_{dg}$$
$$\operatorname{Ker} \Pi_{fg} \cap \operatorname{Ker} \Pi_{f'g} = \operatorname{Ker} \Pi_{mg} .$$

On en déduit :

$$i_{fg}(\mathfrak{X}_f) \cap i_{f'g}(\mathfrak{X}_{f'}) = i_{dg}(\mathfrak{X}_d)$$
$$i_{fg}(\mathfrak{X}_f) \cdot i_{f'g}(\mathfrak{X}_{f'}) = i_{mg}(\mathfrak{X}_m) .$$

Soit $\mathfrak{X}$ un groupe de caractères résiduels modulo g . Il existe donc un plus petit entier f tel que $\mathfrak{X}$ soit inclus dans $i_{fg}(\mathfrak{X}_f)$. On appellera cet entier le conducteur de $\mathfrak{X}$. On le notera $f_{\mathfrak{X}}$. Si $\varkappa$ est un caractère résiduel modulo g , on appellera conducteur de $\varkappa$, le conducteur du sous-groupe de $\mathfrak{X}_g$ engendré par $\varkappa$. On le notera $f_{\varkappa}$.

Remarques . Si g divise h , le conducteur de χ (resp. $\mathfrak{X}$) coïncide avec le conducteur de $i_{gh}(\chi)$ (resp. $i_{gh}(\mathfrak{X})$) .
D'autre part , le conducteur de $\mathfrak{X}$ est le P P C M des conducteurs des ca - ractères appartenant à $\mathfrak{X}$.

2) Correspondance entre extensions abéliennes de $\mathbb{Q}$ et groupes de caractères .

Rappelons que le groupe de Galois de $\mathbb{Q}^{(f)}/\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/f\mathbb{Z})^*$. Cet isomorphisme permute avec la projection Π_{fg} et la res - triction des automorphismes de $\mathbb{Q}^{(g)}$ à $\mathbb{Q}^{(f)}$. C'est-à-dire que , si f divise g , le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}^{(g)}/\mathbb{Q}) & \cong & (\mathbb{Z}/g\mathbb{Z})^* \\ \downarrow & & \downarrow \Pi_{fg} \\ \mathrm{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q}) & \cong & (\mathbb{Z}/f\mathbb{Z})^* \end{array}$$

Définition de θ_f . Soit K un sous-corps de $\mathbb{Q}^{(f)}$. Soit H le sous-grou- pe de $(\mathbb{Z}/f\mathbb{Z})^*$ correspondant à $\mathrm{Gal}(\mathbb{Q}^{(f)}/K)$.
Soit $\mathfrak{X}$ l'orthogonal de H , c'est-à-dire :

$$\mathfrak{X} = H^{\perp} = \{ \chi , \chi \in \mathfrak{X}_f ; \chi(H) = 1 \} .$$

L'application θ_f est l'application qui associe le groupe de caractères $\mathfrak{X}$ au corps K .

Proposition IV a . L'application θ_f ainsi définie est une bijection entre l'ensemble des sous-corps de $\mathbb{Q}^{(f)}$ et l'ensemble des groupes de carac - tères résiduels modulo f .
Si K correspond à $\mathfrak{X}$, les conducteurs de K et $\mathfrak{X}$ sont égaux et $\mathfrak{X}$ est ca- noniquement isomorphe au dual de $\mathrm{Gal}(K/\mathbb{Q})$ que nous noterons $\mathrm{Gal}(K/\mathbb{Q})^{\wedge}$.
Supposons que K_1 corresponde à $\mathfrak{X}_1$. On a alors $K_1 \subset K$ si et seulement si $\mathfrak{X}_1 \subset \mathfrak{X}$. Supposons que cette condition soit vérifiée . Alors dans l'iso- morphisme :

$$\mathfrak{X} \cong \mathrm{Gal}(K/\mathbb{Q})^{\wedge}$$

$\mathfrak{X}_1$ correspond à $\mathrm{Gal}(K/K_1)^{\perp}$.

Enfin , si d divise f , $i_{df}(\mathfrak{X}_d)$ correspond par θ_f à $\mathbb{Q}^{(d)}$ et $i_{df} \circ \theta_d$ est la restriction de θ_f à l'ensemble des sous-corps de $\mathbb{Q}^{(d)}$.

démonstration

L'application de l'ensemble des sous-groupes de $(\mathbb{Z}/f\mathbb{Z})^*$ dans l'ensemble des sous-groupes de $\mathfrak{X}_f$ qui à H fait correspondre son orthogonal $H^\perp$ est une bijection qui renverse l'ordre . L'application θ_f est composée de cette bijection et de la correspondance de Galois . Il s'agit donc d'une bijection qui conserve l'ordre .

L'orthogonal de $\mathrm{Ker}\ \Pi_{df}$ est $i_{df}(\mathfrak{X}_d)$ et $\mathrm{Ker}\ \Pi_{df}$ correspond galoisiennement à $\mathbb{Q}^{(d)}$. Comme le conducteur de K est le plus petit entier d tel que $\mathbb{Q}^{(d)}$ contienne K , on en déduit que les conducteurs de $\mathfrak{X}$ et K sont égaux .

On déduit de l'isomorphisme $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/f\mathbb{Z})^*/H$ un isomorphisme $\mathrm{Gal}(K/\mathbb{Q})^\wedge \cong ((\mathbb{Z}/f\mathbb{Z})^*/H)^\wedge$.
D'autre part , en vertu des propriétés de dualité classiques , on a un isomorphisme : $((\mathbb{Z}/f\mathbb{Z})^*/H)^\wedge \cong H^\perp$.
En composant on obtient donc $\mathrm{Gal}(K/\mathbb{Q})^\wedge \cong \mathfrak{X}$.

Soit maintenant K_1 un sous-corps de K , H_1 le sous-groupe de $(\mathbb{Z}/f\mathbb{Z})^*$ correspondant à $\mathrm{Gal}(\mathbb{Q}^{(f)}/K_1)$ et $\mathfrak{X}_1$ l'orthogonal de H_1 . Dans l'isomorphisme $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/f\mathbb{Z})^*/H$ le sous-groupe (K/K_1) correspond à H_1/H . D'autre part dans l'isomorphisme $((\mathbb{Z}/f\mathbb{Z}^*)/H)^\wedge \cong H^\perp$, le sous-groupe $(H_1/H)^\perp$ correspond à $H_1^\perp$. On en déduit que $\mathfrak{X}_1 = H_1^\perp$ correspond à $\mathrm{Gal}(K/K_1)^\perp$ dans l'isomorphisme $\mathfrak{X} \cong \mathrm{Gal}(K/\mathbb{Q})^\wedge$.

3) Limites inductives et projectives . Nous allons énoncer à nouveau les définitions et propriétés déjà citées , mais en nous plaçant cette fois « à la limite » . Nous ne donnerons pas de démonstration . D'ailleurs , ce langage ne sera pas utilisé dans la suite .

Soit A l'extension abélienne maximale de $\mathbb{Q}$ et G son groupe de Galois . En vertu du théorème de Kronecker-Weber , A est la réunion des corps cyclotomiques et G est la limite projective du système : $((\mathbb{Z}/f\mathbb{Z})^*, \Pi_{ff'})$ introduit en IV 1 . Soit $\Pi_f : G \longrightarrow (\mathbb{Z}/f\mathbb{Z})^*$ la projection de G sur $(\mathbb{Z}/f\mathbb{Z})^*$. On rappelle que G est un groupe topologique, un système fondamental de voisinages de 1 étant formé des $\mathrm{Ker}\ \Pi_f$.

Soit X l'ensemble des homomorphismes continus de G dans le groupe des nombres complexes de module 1 . Le groupe X est la limite inductive du système : $(\mathfrak{X}_f , i_{ff'})$.

On pourrait alors définir un caractère résiduel $\varkappa$ comme un élément de X . Le conducteur de $\varkappa$ est le plus petit entier f tel que $\mathrm{Ker}\ \Pi_f$ soit inclus dans $\mathrm{Ker}\ \varkappa$. Un groupe de caractères résiduels pourrait alors être défini comme un sous-groupe fini $\mathfrak{X}$ de X et son conducteur comme le plus petit entier f tel que $\mathrm{Ker}\ \Pi_f$ soit inclus dans $\bigcap_{\varkappa \in \mathfrak{X}} \mathrm{Ker}\,\varkappa$.

A toute extension abélienne finie $K/\mathbb{Q}$ on peut associer l'orthogonal $\mathfrak{X}$ de $\mathrm{Gal}(A/K)$, c'est-à-dire :

$$\mathfrak{X} = \{\varkappa\ ;\ \varkappa \in X\ ;\ \varkappa(\mathrm{Gal}(A/K)) = 1\}\ .$$

Il s'agit d'un sous-groupe fini de X . On obtient ainsi une correspondance biunivoque θ de l'ensemble des extensions abéliennes finies de $\mathbb{Q}$ dans l'ensemble des sous-groupes finis de X . Cette correspondance est d'ailleurs la limite des θ_f .

4) Identifications . Notations définitives . Si f divise g nous identifierons désormais $\mathfrak{X}_f$ à un sous-groupe de $\mathfrak{X}_g$. Cela implique que si $\varkappa$ est donné comme un caractère résiduel modulo g , c'est-à-dire comme une application de $(\mathbb{Z}/g\mathbb{Z})^*$ dans le groupe des nombres complexes de module 1 , alors $\varkappa(y)$ est défini pour tout entier y premier au conducteur $f_\varkappa$ de $\varkappa$. Pour plus de commodité nous poserons $\varkappa(y) = 0$ si y n'est pas premier à $f_\varkappa$. Nous dirons le plus souvent caractère au lieu de caractère résiduel .

Remarque . Un caractère résiduel est donc un caractère de Dirichlet modulo son conducteur .

Soit $K/\mathbb{Q}$ une extension abélienne finie . Compte-tenu du théorème de Kronecker-Weber , il existe un corps cyclotomique $\mathbb{Q}^{(f)}$ contenant K . Soit $\mathfrak{X}$ le groupe des caractères associé à K par θ_f . En vertu de la proposition IV a , l'application θ_f est la restriction de θ_g (si f divise g) et $\mathfrak{X}$ ne dépend pas de f . On appellera les éléments de $\mathfrak{X}$ les caractères de K et $\mathfrak{X}$ sera appelé le groupe des caractères de K . On confondra également ce groupe $\mathfrak{X}$ avec le dual de $\mathrm{Gal}(K/\mathbb{Q})$.

Soit $\varkappa$ un caractère de K . Il correspond par θ_f au sous-groupe engendré par $\varkappa$, un sous-corps de K , que l'on notera $K_\varkappa$, et qui est cyclique sur $\mathbb{Q}$. Le corps $K_\varkappa$ peut aussi être défini de la façon suivante: Le noyau de $\varkappa$ est $\mathrm{Gal}(K/K_\varkappa)$. Il faut remarquer que, malgré la notation , $K_\varkappa$ ne dépend que du caractère $\varkappa$.

Enfin , K étant fixé , l'application $\varkappa \to K_\varkappa$ induit une bijection de $\mathfrak{X}'$, ensemble des Γ-classes de $\mathfrak{X}$, sur l'ensemble des sous-corps cycliques de K .

On notera indifféremment $K_\varkappa$ ou $K_{\varkappa'}$.

Nous dirons qu'un caractère $\varkappa$ est pair (resp. impair) si $\varkappa(-1) = 1$ (resp. -1) ($\varkappa$ étant un caractère résiduel modulo f , -1 désigne la classe de -1 modulo f) .
Un caractère $\varkappa$ est pair si et seulement si $K_\varkappa$ est réel . Un corps K abélien sur $\mathbb{Q}$ est réel si et seulement si tous ses caractères sont pairs .

5) Ramification . Décomposition . Soit $K/\mathbb{Q}$ une extension abélienne , $\mathfrak{X}$ son groupe de caractères et p un nombre premier . On désignera par $K_T^{(p)}$ et $K_Z^{(p)}$ les corps d'inertie et de décomposition de p dans $K/\mathbb{Q}$. Soit $\mathfrak{X}_T^{(p)}$ et $\mathfrak{X}_Z^{(p)}$ leurs groupes de caractères .

Proposition IV b . Le groupe $\mathfrak{X}_T^{(p)}$ est l'ensemble des caractères $\varkappa$ de K tels que $\varkappa(p) \neq 0$. Le groupe $\mathfrak{X}_Z^{(p)}$ est l'ensemble des caractères $\varkappa$ de K tels que $\varkappa(p) = 1$. Si e_p , f_p , g_p sont les trois paramètres habituels caractérisant la décomposition de p dans K , on a :

$$e_p = (\mathfrak{X} : \mathfrak{X}_T^{(p)}) \; ; \quad f_p = (\mathfrak{X}_T^{(p)} : \mathfrak{X}_Z^{(p)}) \quad \text{et} \quad g_p = (\mathfrak{X}_Z^{(p)} : 1) \; .$$

démonstration

Soit K_1 un sous-corps de K et $\mathfrak{X}_1$ son groupe de caractères. Le conducteur de K_1 est le P P C M des conducteurs de ses caractères. D'autre part p est non ramifié dans K_1 si et seulement si p ne divise pas le conducteur de K_1 . Comme $K_T^{(p)}$ est le plus grand sous-corps de K dans lequel p est non ramifié, on a donc $\mathfrak{X}_T^{(p)} = \{\varkappa \; ; \varkappa \in \mathfrak{X} \; ; \varkappa(p) \neq 0\}$.

Soit f le conducteur de $K_T^{(p)}$. La classe de p modulo f engendre dans $(\mathbb{Z}/f\mathbb{Z})^*$ le groupe de décomposition D de p dans $\mathbb{Q}^{(p)}/\mathbb{Q}$. Le corps de décomposition cherché , $K_Z^{(p)}$ est le corps invariant par D. Son groupe de caractères est donc l'orthogonal de D . D'où :

$$\mathfrak{X}_Z^{(p)} = \{ \varkappa \; ; \varkappa \in \mathfrak{X} \; ; \varkappa(p) = 1 \} \; .$$

6) Caractères du corps des genres . K est toujours une extension abélienne finie de $\mathbb{Q}$ et $\mathfrak{X}$ son groupe de caractères . Rappelons que le corps des genres de K est le plus grand corps K_G tel que K_G/K soit non ramifié pour les idéaux et $K_G/\mathbb{Q}$ soit abélienne .
Pour avoir plus de détails sur cette notion on pourra voir [3] et [4].

Soit f un multiple quelconque du conducteur de K , et soit $f = \prod_p p^{u_p}$ la décomposition de f en produit de nombres premiers . Le groupe $\mathfrak{X}_f$ est produit direct des $\mathfrak{X}_{p^{u_p}}$. Considérons alors la projection:

$$\mathfrak{X}_f \longrightarrow \mathfrak{X}_{p^{u_p}} .$$

Cette projection permute avec les injections canoniques i_{fg} .

Soit $\mathfrak{X}^{[p]}$ l'image de $\mathfrak{X}$ par cette projection .
Cette image ne dépend donc pas de f et elle est réduite à 1 si p ne divise pas le conducteur de K . Nous poserons alors $\mathfrak{X}^* = \prod_p \mathfrak{X}^{[p]}$.

Propriété IV c . Le groupe des caractères du corps des genres de K est $\mathfrak{X}^*$.

démonstration

Si $\varkappa$ appartient à $\mathfrak{X}_f$, soit $\varkappa^{[p]}$ l'image de $\varkappa$ par la projection $\mathfrak{X}_f \longrightarrow \mathfrak{X}_{p^{u_p}}$. On a donc $\varkappa = \prod_p \varkappa^{[p]}$ et le conducteur de $\varkappa^{[p]}$ est la p-composante du conducteur de $\varkappa$. En particulier p ne divise pas le conducteur de $\varkappa$ si et seulement si le caractère $\varkappa^{[p]}$ est égal à 1 . Le noyau de la projection $\mathfrak{X}_f \longrightarrow \mathfrak{X}_{p^{u_p}}$ est donc l'ensemble :

$$\{\varkappa \; ; \; \varkappa \in \mathfrak{X}_f \; ; \; \varkappa(p) \neq 0\} .$$

Considérons alors la restriction de cette projection à $\mathfrak{X}$. Son noyau est donc $\mathfrak{X}_T^{(p)}$ et son image $\mathfrak{X}^{[p]}$ a pour ordre l'indice de ramification de p dans K (Proposition IV b) .

Soient K^* l'extension abélienne de $\mathbb{Q}$ ayant pour groupe de caractères $\mathfrak{X}^*$. Appliquons le résultat ci-dessus à K et K^* . On a $\mathfrak{X}^{[p]} = \mathfrak{X}^{*[p]}$ pour tout p . Les indices de ramifications de p dans K et K^* sont les mêmes . L'extension K^*/K est donc non ramifiée pour les idéaux .

Réciproquement , soit K_1 un corps tel que K_1/K soit non ramifiée pour les idéaux et , $K_1/\mathbb{Q}$ abélienne . Soit $\mathfrak{X}_1$ son groupe de caractères . On a donc $|\mathfrak{X}_1^{[p]}| = |\mathfrak{X}^{[p]}|$ d'où $\mathfrak{X}_1^{[p]} = \mathfrak{X}^{[p]}$, pour tout p . En effectuant le produit on aura donc :

$$\mathfrak{X}_1 \subset \prod_p \mathfrak{X}_1^{[p]} = \mathfrak{X}^* \ .$$

Ce qui prouve que K_1 est inclus dans K^* . Nous avons montré que K^* est le corps des genres de K .

Exemple des corps quadratiques . Soit d un entier sans facteur carré. On peut l'écrire sous la forme $d = u p_1 p_2 \dots p_r$ avec u = 1, -1, 2 ou -2 et p_i premier congru à 1 modulo 4 .

Propriété : Le corps des genres de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Q}(\sqrt{u}, \sqrt{p_1}, \dots, \sqrt{p_r})$.

démonstration

Nous supposerons que d est pair . On a donc $u = \pm 2$. Nous poserons $q_i = |p_i|$. On a donc $|d| = 2 q_1 \dots q_r$. On vérifie , c' est élémentaire,que $\mathbb{Q}(\sqrt{d})$ est inclus dans $\mathbb{Q}^{(D)}$, où D est la valeur absolue du discriminant de $\mathbb{Q}(\sqrt{d})$. On a donc $D = 8 q_1 \dots q_r$.

Soit $\mathfrak{X}$ le groupe des caractères de $\mathbb{Q}(\sqrt{d})$. C'est un groupe d'ordre 2 . Le groupe $\mathfrak{X}^{[q_i]}$ est d'ordre 2 et c'est un sous-groupe de $\mathfrak{X}_{q_i}$. Il correspond à ce groupe de caractères le corps cyclotomique $\mathbb{Q}^{(q_i)}$ qui n'admet qu'un seul sous-corps quadratique $\mathbb{Q}(\sqrt{p_i})$ avec $p_i = \pm q_i$ et $p_i \equiv 1 \ (4)$. D'autre part $\mathfrak{X}^{[2]}$ est d'ordre 2 et c'est un sous-groupe de $\mathfrak{X}_8$. Il correspond à ce groupe de caractères le corps cyclotomique $\mathbb{Q}^{(8)}$ qui contient trois sous-corps quadratiques $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$. Soit $\mathbb{Q}(\sqrt{v})$ le corps quadratique correspondant à $\mathfrak{X}^{[2]}$. On a donc

$v = -1$, 2 ou -2 . Le groupe $\mathfrak{X}^*$ est égal à $\mathfrak{X}^{[2]}\,\mathfrak{X}^{[q_1]} \ldots \mathfrak{X}^{[q_r]}$.
Le corps des genres de $\mathbb{Q}(\sqrt{d})$ sera donc $\mathbb{Q}(\sqrt{v}\,,\sqrt{p_1}\,,\ldots,\sqrt{p_r})$. Comme $\mathbb{Q}(\sqrt{d})$ doit être inclus dans le corps des genres , on en déduit que $v = u$.

Si d est impair , même démonstration .

V

Décomposition du p-Sylow du groupe des classes des extensions abéliennes de degré premier à p .

1) Caractères d'extensions dont le corps de base est quelconque .
Dans le paragraphe précédent nous avons introduit , $K/\mathbb{Q}$ étant une extension abélienne, les caractères de K . De tels caractères pouvaient être considérés , soit comme des caractères du groupe $(\mathbb{Z}/f\mathbb{Z})^*$, f étant un multiple du conducteur de K , soit comme des caractères de G , groupe de Galois de $K/\mathbb{Q}$. Le premier aspect est lié au fait que l'extension considérée a pour corps de base $\mathbb{Q}$. Nous allons supprimer cette condition et nous ne retiendrons plus que le deuxième aspect . Enonçons les choses complètement :

Définitions . Soient K/k une extension abélienne de corps de nombres , G son groupe de Galois , $\mathfrak{X}$ le groupe des caractères complexes de G. Un élément de $\mathfrak{X}$ sera appelé un caractère de l'extension K/k et le groupe $\mathfrak{X}$, le groupe des caractères de K/k . (Un caractère de $K/\mathbb{Q}$ était nommé précédemment caractère de K) .

Soit K_1 un corps intermédiaire de K/k et $\mathfrak{X}_1$ l'orthogonal de $\mathrm{Gal}(K/K_1)$ c'est-à-dire :

$$\mathfrak{X}_1 = \{\, \chi \,,\, \chi \in \mathfrak{X} \,;\, \chi(\mathrm{Gal}(K/K_1)) = 1 \,\} \ .$$

Soit $\theta_{K/k}$ l'application qui associe $\mathfrak{X}_1$ à K_1 .

Proposition V a . L'application $\theta_{K/k}$ ainsi définie est une bijection entre l'ensemble des corps intermédiaires de K/k et l'ensemble des sous-groupes de $\mathfrak{X}$. Cette bijection conserve l'ordre . Si K_1 correspond à $\mathfrak{X}_1$, alors $\mathfrak{X}_1$ est canoniquement isomorphe au dual de $\mathrm{Gal}(K_1/k)$. Si l'on convient d'identifer ces deux quantités , alors $\theta_{K_1/k}$ apparait comme la restriction de $\theta_{K/k}$.

La démonstration de cette proposition est contenue dans la démonstration de la proposition IV a . (Il est clair que $\theta_{\mathbb{Q}(f)/\mathbb{Q}}$ est l'application θ_f du paragraphe IV) . On pourrait , comme précédemment « passer à la limite » en utilisant l'extension abélienne maximale de k .

2) Décomposition du p-Sylow du groupe des classes . Soit p un nombre premier . Nous allons utiliser les caractères p-adiques définis en III . Soit K/k une extension abélienne de degré premier à p . Soient G son groupe de Galois , $\mathfrak{X}$ son groupe de caractères et g son degré . Si $\varkappa$ appartient à $\mathfrak{X}$, l'idempotent $e_{\varkappa''}$ appartient à $\mathbb{Z}_p[G]$ et tout $\mathbb{Z}_p[G]$-module H , noté multiplicativement , se décomposera en produit direct de sous-modules : $H = \prod_{\varkappa'' \in \mathfrak{X}''} H^{e_{\varkappa''}}$. Il en est ainsi du p-Sylow $\mathfrak{H}_K$ du groupe des classes d'idéaux de K . Nous avons donc

$$\mathfrak{H}_K = \prod_{\varkappa'' \in \mathfrak{X}''} \mathfrak{H}_K^{e_{\varkappa''}} \quad .$$

Soit maintenant K_1 un corps intermédiaire de l'extension K/k. Soient G_1 , $\mathfrak{X}_1$ et g_1 le groupe de Galois , le groupe des caractères et le degré de l'extension K_1/k .

Soit $\mathfrak{H}_{K_1}$ le p-Sylow du groupe des classes de K_1 .

Introduisons l'application $j : \mathfrak{H}_{K_1} \longrightarrow \mathfrak{H}_K$, déduite de l'injection canonique du groupe des idéaux de K_1 dans le groupe des idéaux de K .

Si $\varkappa$ appartient à $\mathfrak{X}_1$, il faut signaler l'existence d'une ambiguité dans la notation $e_{\varkappa''}$ qui peut désigner

soit : $\frac{1}{g} \sum_{\sigma \in G} \varkappa''(\sigma^{-1})\sigma$, soit : $\frac{1}{g_1} \sum_{\sigma \in G_1} \varkappa''(\sigma^{-1})\sigma$.

Remarquons que $\varkappa''(\sigma) = \varkappa''(\tau)$ dès que $\sigma\tau^{-1}$ appartient à $\mathrm{Gal}(K/K_1)$ et que dans l'homomorphisme :

$$\mathbb{Q}[G] \longrightarrow \mathbb{Q}[G_1]$$

déduit de l'homorphisme de restriction de G à G_1 , l'un de ces éléments est l'image de l'autre . Il s'en suit que $\mathfrak{H}_{K_1}^{e_{\varkappa''}}$ est bien défini .

Proposition V b . L'application j est un homomorphisme injectif . L'image $j(\mathfrak{H}_{K_1})$ de j est le sous-groupe de $\mathfrak{H}_K$ formé des éléments de $\mathfrak{H}_K$ invariants par $\mathrm{Gal}(K/K_1)$.
Si $\varkappa$ est un caractère de K_1 , on a :

$$j\left(\mathfrak{H}_{K_1}^{e_{\varkappa''}}\right) = \mathfrak{H}_K^{e_{\varkappa''}} \quad .$$

démonstration

Soit $Cl(\mathfrak{a})$ un élément de $\mathfrak{H}_{K_1}$, appartenant au noyau de j . Nous aurons donc $\mathfrak{a} A_K = \alpha A_K$, avec α dans K . D'une part $\mathfrak{a}^{g/g_1}$ est principal et est engendré par $N_{K/K_1}(\alpha)$ et d'autre part il existe un entier u tel que $\mathfrak{a}^{p^u}$ soit principal . On en déduit donc que $\mathfrak{a}$ est principal .

Soit maintenant $\mathfrak{a}$ un idéal de K tel que $Cl(\mathfrak{a})$ soit invariant par $\mathrm{Gal}(K/K_1)$. L'idéal $\mathfrak{a}^{g/g_1}$ est l'étendu de $N_{K/K'}(\mathfrak{a})$. Donc , $Cl(\mathfrak{a}^{g/g_1})$ se trouve dans l'image de j . Il en sera de même de $Cl(\mathfrak{a})$, puisque g/g_1 est premier à p .

On déduit de l'inclusion $j(\mathfrak{H}_{K_1}) \subset \mathfrak{H}_K$, l'inclusion :

$$j\left(\mathfrak{H}_{K_1}^{e_{\varkappa''}}\right) = j\left(\mathfrak{H}_{K_1}\right)^{e_{\varkappa''}} \subset \mathfrak{H}_K^{e_{\varkappa''}} \quad .$$

D'autre part , on a : $\tau e_{\varkappa''} = e_{\varkappa''}$ pour tout τ de $\mathrm{Gal}(K/K_1)$.
Cela montre que tout élément de $\mathfrak{H}_K^{e_{\varkappa''}}$ est invariant par $\mathrm{Gal}(K/K_1)$.

Remarque . On a aussi : $N_{K/K_1}\left(\mathfrak{H}_K^{e_{\varkappa''}}\right) = \mathfrak{H}_{K_1}^{e_{\varkappa''}}$, si $\varkappa$ est un caractère de K_1 et $N_{K/K_1}\left(\mathfrak{H}_K^{e_{\psi''}}\right) = 1$, si ψ est un caractère de K n'appartenant pas à $\mathfrak{x}_1$.

démonstration

La première assertion est une conséquence immédiate de

l'égalité $j\left(\mathfrak{Q}_{K_1}^{e_{\varkappa''}}\right) = \mathfrak{Q}_K^{e_{\varkappa''}}$. Pour démontrer la deuxième , on peut introduire $e = (1/[K:K_1]) \sum_{\sigma \in Gal(K/K_1)} \sigma$.

On a : $e = \sum_{\varkappa \in \mathfrak{X}_1} e_\varkappa = \sum_{\varkappa'' \in \mathfrak{X}_1''} e_{\varkappa''}$ et $h^{e[K:K_1]} = j(N_{K/K_1}(h))$,

pour h de $\mathfrak{Q}_K$. Si ψ est un caractère de K n'appartenant pas à $\mathfrak{X}_1$, nous aurons alors $e_\psi e = 0$; d'où $\mathfrak{Q}_K^{e_\psi''} \subset Ker(N_{K/K_1})$.

Conséquence de la proposition V b . Si on identifie $\mathfrak{Q}_{K_1}^{e_{\varkappa''}}$ et son image par j , on voit que $\mathfrak{Q}_K^{e_{\varkappa''}}$ ne dépend finalement pas de K . Posons $\mathfrak{Q}_K^{e_{\varkappa''}} = \mathfrak{Q}(\varkappa'')$. Nous avons montré que le p-Sylow du groupe des classes d'idéaux de K se décompose en produit direct : $\mathfrak{Q}_K = \prod_{\varkappa'' \in \mathfrak{X}''} \mathfrak{Q}(\varkappa'')$.

Pour tout corps K_1 intermédiaire de l'extension K/k , la décomposition du p-Sylow du groupe des classes d'idéaux de K_1 sera :

$$\mathfrak{Q}_{K_1} = \prod_{\varkappa'' \in \mathfrak{X}_1''} \mathfrak{Q}(\varkappa'') \quad .$$

Remarquons enfin que chaque facteur $\mathfrak{Q}(\varkappa'')$ est facteur direct du p-Sylow du groupe des classes d'au moins un corps intermédiaire L tel que L/k soit cyclique ; à savoir le corps L tel que $Gal(K/L) = Ker\ \varkappa$.

Ces considérations sont à la base de [6] . Dans cet article, Leopoldt exhibe , sous certaines hypothèses , une involution $\varkappa'' \to \overline{\varkappa}''$ de $\mathfrak{X}''$ et compare les groupes $\mathfrak{Q}(\varkappa'')$ et $\mathfrak{Q}(\overline{\varkappa}'')$.

Exemple . Soit $K/\mathbb{Q}$ une extension abélienne complexe et soit K_o le sous-corps de K réel maximal . Soient $\mathfrak{D}$ le groupe des classes d'idéaux de K, $\mathfrak{D}_o$ le groupe des classes d'idéaux de K_o et $\mathfrak{D}^*$ le noyau de l'application N_{K/K_o} déduite de la norme relative à K/K_o . Rappelons que $\mathfrak{D}_o$ et $\mathfrak{D}^*$ s'appellent respectivement groupe des classes réelles et relatives de K. Un résultat classique concernant ces groupes (Hasse- Uber die Klassenzahl abelscher Zahlkörper - Berlin 1952) est que : N_{K/K_o} est surjective et induit un isomorphisme : $\mathfrak{D}/\mathfrak{D}^* \cong \mathfrak{D}_o$. Cet isomorphisme peut « se décomposer » en considérant les p-Sylow de chacun de ces groupes . Pour tout p impair , on peut le déduire de la proposition V b .

En effet posons $k = K_o$; désignons par G le groupe de Galois de K/k . Il ne possède que deux éléments : $G = \{1,\sigma\}$. Soit 1 et ψ les deux caractères complexes de G . Les idempotents correspondants sont : $e_1 = \frac{1}{2}(1+\sigma)$ et $e_\psi = \frac{1}{2}(1-\sigma)$. Si p est un nombre premier impair , la Γ_p-conjugaison de $\mathfrak{X}$ coïncide avec l'égalité . Soit $\mathfrak{H}_K$ le p-Sylow de $\mathfrak{D}$. En vertu de la proposition V b , $\mathfrak{H}_K$ est donc produit direct de deux sous-groupes :

$$\mathfrak{H}_K = \mathfrak{H}(1)\mathfrak{H}(\psi) .$$

Le premier : $\mathfrak{H}(1)$, s'identifie au p-Sylow de $\mathfrak{D}_o$ et le deuxième est le p-Sylow de $\mathfrak{D}^*$ (Remarque suivant la proposition V b) .

Bibliographie

[1] BOURBAKI N. :
Eléments de Mathématiques - Algèbre - Chapitre 8 .
(Hermann - 1958) .

[2] CURTIS C.W. - REINER I. :
Representation theory of finite groups and associative algebras .
(Interscience Publishers - 1962) .

[3] HASSE H. :
A Supplement to Leopoldt's Theory of Genera in abelian Number Fields .
(Journal of Number Theory, 1 (1969) p. 4-7 .

[4] LEOPOLDT H.W. :
Zur Geschlechtertheorie in abelschen Zahlkörpern .
(Math. Nachr. 9 (1953) p. 351-362 .

[5] LEOPOLDT H.W. :
Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper .
(Abh. Deutsche Akad. Wiss. Berlin Math. 2 (1954) .

[6] LEOPOLDT H.W. :
Zur Struktur der ℓ-Klassengruppe galoischer Zahlkörper.
(Journ. für die reine und ang. Math. 199 (1958) 165-174) .

[7] RIBENBOIM P. :
L'arithmétique des corps .
(Hermann - 1972) .

[8] SERRE J.P. :
Représentations linéaires des groupes finis .
(Hermann - 1971) .