

FRANÇOISE BERTRANDIAS

**Sur la structure du p -groupe des classes du corps
cyclotomique $\mathbb{Q}^{(p)}$, d'après Leopoldt**

Séminaire de théorie des nombres de Bordeaux (1968-1969), exp. n° 7, p. 1-10

http://www.numdam.org/item?id=STNB_1968-1969__A7_0

© Université Bordeaux 1, 1968-1969, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LA STRUCTURE DU p -GROUPE DES CLASSES DU
CORPS CYCLOTOMIQUE $\mathbb{Q}^{(p)}$, d'après LEOPOLDT [5]

par

Françoise BERTRANDIAS

- - - - -

1. Description des p -groupes attachés à $\mathbb{Q}^{(p)}$.

1.1. - p désigne un nombre premier $\neq 2$, $\mathbb{Q}^{(p)}$ le corps des racines p -èmes de l'unité, ζ une racine primitive de l'unité. On note $g = \text{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q})$; $\mathbb{Q}_0^{(p)} = \mathbb{Q}(\zeta + \zeta^{-1})$.

Soient : F le groupe des idéaux fractionnaires non nuls de $\mathbb{Q}^{(p)}$, H_0 le sous-groupe des idéaux principaux, et H le sous-groupe des idéaux $\mathcal{U}$, tels qu'il existe un entier m premier à p pour lequel $\mathcal{K}^m$ soit principal.

Le groupe des classes $\mathcal{K} = F/H_0$ est d'ordre fini h ; on sait [1], [3] que si h_0 (resp. h^*) est l'ordre du sous-groupe des classes réelles (resp. relatives, c'est-à-dire dont la norme par rapport à $\mathbb{Q}_0^{(p)}$ est la classe principale), on a l'égalité : $h = h_0 h^*$. Kummer a montré que si p divise h , alors p divise h^* .

Rappelons que si p est premier à h (nombre premier régulier), le théorème de Fermat est vrai pour l'exposant p ; de plus Vandiver a montré que si p est premier à h_0 , l'équation $x^p + y^p = z^p$ ne possède pas de solution en entiers x, y, z non tous nuls et premiers à p .

1.2. - Le p -groupe des classes de $\mathbb{Q}^{(p)}$ est, par définition, le groupe $\mathcal{D} = F/H$. On voit facilement que $\mathcal{D}$ est canoniquement isomorphe au p sous-groupe de Sylow du groupe des classes $\mathcal{K}$.

Le groupe g opère sur F et tout σ de g laisse H globalement invariant ; par passage au quotient, g opère donc sur $\mathcal{D}$. Notons τ l'automorphisme de g "passage à l'imaginaire conjugué", $\mathcal{D}_0$ (resp. $\mathcal{D}^*$) le sous-groupe des éléments d de $\mathcal{D}$ invariants par τ (resp. tels que d, d^τ soit l'élément neutre de $\mathcal{D}$).

On montre : $\mathcal{D} = \mathcal{D}_0 \times \mathcal{D}^*$ (produit direct).

Soient r, r_0 et r^* les rangs respectifs des groupes $\mathcal{D}, \mathcal{D}_0$ et $\mathcal{D}^*$ (le rang d'un p -groupe abélien est par définition le nombre de facteurs d'une décomposition de ce groupe en produit direct de sous-groupes cycliques [2]). Un des résultats de Léopoldt est la double inégalité :

$$r_0 \leq r^* \leq r_0 + \frac{p-3}{2}.$$

L'inégalité $r_0 \leq r^*$, déjà démontré par Hecke [4], a comme corollaire immédiat le résultat de Kummer cité ci-dessus (si p divise h , p divise h^*).

1.3. - Le p -groupe élémentaire des classes de $\mathbb{Q}^{(p)}$ est, par définition, le groupe $\mathfrak{F} = F / F^p H_0$. On voit facilement que $\mathfrak{F}$ est canoniquement isomorphe à $\mathcal{B} / \mathcal{B}^p$ (remarquer que $F^p H_0 = F^p H$). $\mathfrak{F}$ est également isomorphe au sous-groupe des classes d'ordre 1 ou p , mais cet isomorphisme n'est pas canonique. $\mathfrak{F}$ est un p -groupe élémentaire, c'est-à-dire d'exposant p . Le groupe g opère sur $\mathfrak{F}$; on définit les sous-groupes $\mathfrak{F}_0$ et $\mathfrak{F}^*$ de $\mathfrak{F}$ de manière analogue aux sous-groupes $\mathcal{B}_0$ et $\mathcal{B}^*$ de $\mathcal{B}$, et on voit que $\mathfrak{F}_0$ (resp. $\mathfrak{F}^*$) est canoniquement isomorphe à $\mathcal{B}_0 / \mathcal{B}_0^p$ (resp. $\mathcal{B}^* / \mathcal{B}^{*p}$). Par suite les rangs de $\mathfrak{F}$, $\mathfrak{F}_0$, $\mathfrak{F}^*$ sont respectivement égaux à r , r_0 , r^* .

1.4. - E désignant le groupe des unités de $\mathbb{Q}^{(p)}$, le groupe des p classes d'unités est par définition le groupe $\mathcal{E} = E / E^p$. C'est un p -groupe élémentaire de rang $\frac{p-1}{2}$; g opère sur $\mathcal{E}$. Une p classe d'unités $u E^p$ est dite primaire si l'extension $\mathbb{Q}^{(p)}(\sqrt[p]{u}) / \mathbb{Q}^{(p)}$ est non ramifiée; les p -classes primaires forment un sous-groupe $\mathcal{E}_1$ de $\mathcal{E}$.

2. Structure de $\mathbb{Z}_p[g]$ module d'un p -groupe abélien sur lequel g opère.

2.1. - $\mathbb{Q}_p$ et $\mathbb{Z}_p$ désignant respectivement le corps des nombres p -adiques et l'anneau des entiers p -adiques, rappelons [2] que l'algèbre $\mathbb{Q}_p[g]$ est l'ensemble des sommes formelles $\sum_{\sigma \in g} a_{\sigma} \sigma$ ($a_{\sigma} \in \mathbb{Q}_p$), muni des lois internes "naturelles"; cette algèbre possède $p-1$ idempotents 1_{χ} , deux à deux orthogonaux, et tels que :

$$1 = \sum_{\chi \in \hat{g}} 1_{\chi} \quad (\text{où } 1 \text{ est l'élément neutre de } g).$$

En effet $\mathbb{Q}_p$ contient les racines $p-1$ èmes de 1 ; si $\hat{g}$ désigne le groupe des caractères χ de g à valeurs dans $\mathbb{Q}_p$, on montre aisément que la famille $(1_\chi)_{\chi \in \hat{g}}$ définie par :

$$1_\chi = \frac{1}{p-1} \sum_{\sigma \in g} \chi(\sigma^{-1}) \sigma ,$$

répond à la question.

Par suite : $\mathbb{Q}_p[g] = \sum_{\chi \in \hat{g}} \mathbb{Q}_p 1_\chi$ (somme directe).

On en déduit : $\mathbb{Z}_p[g] = \sum_{\chi \in \hat{g}} \mathbb{Z}_p 1_\chi$ (somme directe).

2.2. - Soit U un p -groupe abélien sur lequel g opère. On peut le munir d'une structure de $\mathbb{Z}_p[g]$ module en posant, pour tout u de U et pour tout $x = \sum_{\sigma \in g} a_\sigma \sigma$ ($a_\sigma \in \mathbb{Z}_p$) :

$$u^x = \prod_{\sigma \in g} (u^\sigma)^{\overline{a_\sigma}}$$

où $\overline{a_\sigma}$ est un entier rationnel congru à a_σ modulo p^N , ordre de U .

Soit $U_\chi = U^{1_\chi} = \{u^{1_\chi} \mid u \in U\}$. U_χ est un sous-groupe de U

et on montre (utiliser l'égalité $\sigma 1_\chi = \chi(\sigma) 1_\chi$ pour $\sigma \in g$) :

$$U = \prod_{\chi \in \hat{g}} U_\chi \quad (\text{produit direct}) .$$

On remarque que si $u \in U_\chi$, c'est-à-dire si $u^{1_\chi} = u$, alors $u^\sigma = u^{\chi(\sigma)}$; on peut dire que g opère sur U en élevant à une puissance chaque composante dans le produit direct ci-dessus.

Si le caractère χ est pair, c'est-à-dire si $\chi(\tau) = 1$ (τ est l'automorphisme "passage à l'imaginaire conjugué"), et si u appartient à U_χ , $u^\tau = u^{\chi(\tau)} = u$; si χ est impair, c'est-à-dire $\chi(\tau) = -1$, et si u appartient à U_χ , $u^\tau = u^{-1}$. Par suite un élément u de U est invariant par τ si et seulement si u appartient au sous-groupe $U_0 = \bigcap_{\substack{\chi \in \hat{g} \\ \chi \text{ pair}}} U_\chi$;
 $uu^\tau = e$ si et seulement si u appartient au sous-groupe $U^* = \bigcap_{\substack{\chi \in \hat{g} \\ \chi \text{ impair}}} U_\chi$
 (regarder séparément le cas $p = 3$). (On retrouve donc la décomposition $U = U_0 \times U^*$ en produit direct déjà citée dans le cas particulier $U = \mathcal{A}$).

2.3. - g opère sur le groupe $A = \{\zeta^i \mid 1 \leq i \leq p\}$ des racines $p^{\text{èmes}}$ de 1 contenues dans $\mathbb{Q}^{(p)}$. Comme A est cyclique d'ordre p , il existe un caractère de g , noté χ^* , tel que $A = A_{\chi^*}$; on a, pour tout σ de g , $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$ (si r est un entier rationnel tel que $\zeta^\sigma = \zeta^r$, $\chi^*(\sigma) = \lim_{n \rightarrow \infty} r^{p^n}$ dans $\mathbb{Z}_p$).

Définition. On appellera caractère réciproque d'un caractère χ de g , et on notera $\bar{\chi}$, le caractère défini par :

$$\bar{\chi} = \chi^{-1} \chi^*.$$

On remarque que $\bar{\bar{\chi}} = \chi$; d'autre part, comme $\chi^*(\tau) = -1$, χ^* est impair et donc χ et $\bar{\chi}$ sont l'un pair, l'autre impair.

3. Rangs de p groupes $\mathcal{G}_\chi$, $\mathcal{B}_\chi$, $\mathcal{B}_{\bar{\chi}}$.

3.1. - H. W. Leopoldt démontre les résultats suivants :

THEOREME 1. e_χ et $e_{1,\chi}$ désignent les rangs de $\mathcal{G}_\chi$ et $\mathcal{G}_{1,\chi}$. $e_\chi = 1$ si χ est pair distinct du caractère principal, ou si $\chi = \chi^*$; $e_\chi = 0$ sinon. $\mathcal{G}_{1,\chi}$ est un sous-groupe de $\mathcal{G}_\chi$ et donc $e_{1,\chi} \leq e_\chi$; de plus $e_{1,\chi}^* = 0$.

THEOREME 2. (Spiegelungssatz). r_χ et $r_{\bar{\chi}}$ désignant les rangs de $\mathcal{B}_\chi$ et $\mathcal{B}_{\bar{\chi}}$, on a :

$$e_{1,\chi} \geq r_{\bar{\chi}} - r_\chi \geq -e_{1,\bar{\chi}}.$$

COROLLAIRE 1. Si le caractère χ est pair, on a : $r_\chi \leq r_{\bar{\chi}} \leq r_\chi + 1$.
De plus : $r_{\chi_0} = r_\chi^*$.

COROLLAIRE 2. r_0 et r^* désignant les rangs de $\mathcal{B}_0$ et $\mathcal{B}^*$, on a :

$$r_0 \leq r^* \leq r_0 + \frac{p-3}{2}.$$

Les corollaires se déduisent immédiatement des théorèmes 1 et 2. (et des résultats du § 2.2). La démonstration du théorème 1, qui utilise un résultat de Pollaczek [8], ne sera pas abordé ici ; une démonstration complète figure dans l'exposé de J. J. Payan [6].

Dans ce qui suit, sont exposées les grandes lignes de la démonstration du théorème 2.

Signalons que les résultats de Leopoldt se situent dans le cadre plus général d'une extension K de $\mathbb{Q}^{(p)}$, galoisienne sur $\mathbb{Q}$, de degré premier à p .

3.2. - D'après la théorie du corps de classes, à tout sous groupe H' du groupe F des idéaux non nuls de $\mathbb{Q}^{(p)}$ contenant le sous-groupe H_0 des idéaux principaux est associée une extension abélienne N de $\mathbb{Q}^{(p)}$, non ramifiée ; l'application $\mathcal{U} : H' \rightarrow (\mathbb{Q}^{(p)}/\mathcal{U})$ (symbole d'Artin) réalise un isomorphisme du groupe F/H' sur le groupe $\text{Gal}(N/\mathbb{Q}^{(p)})$. N est galoisienne sur $\mathbb{Q}$ si et seulement si H' est globalement invariant par tout élément σ de g .

Dans la suite on prend $H' = F^p H_0$; $\text{Gal}(N/\mathbb{Q}^{(p)}) \simeq \mathfrak{F}$; N est galoisienne sur $\mathbb{Q}$. Soit $G = \text{Gal}(N/\mathbb{Q})$; G est une extension du groupe $U = \text{Gal}(N/\mathbb{Q}^{(p)})$ par g , extension décomposée car les ordres de U et g sont premiers entre eux ([2]) ; on a $G = U \rtimes \bar{g}$ (produit semi-direct) où $\bar{g} \simeq g$ est un relèvement de g dans G ; on note $\bar{\sigma}$ le relèvement dans $\bar{g}$ d'un élément σ de g . Le groupe g opère sur U par : $u \mapsto \bar{\sigma}^{-1} u \bar{\sigma} = u^\sigma$. On montre que l'isomorphisme par le symbole d'Artin des groupes $\mathfrak{F}$ et U est un isomorphisme de $\mathbb{Z}_p[g]$ modules : en effet un élément u de U provient de la classe $\mathcal{U} F^p H_0$ d'un idéal premier $\mathcal{U}$ par le symbole d'Artin, (c'est-à-dire $u = (\mathbb{Q}^{(p)}/\mathcal{U})$) si et seulement si pour tout entier x de N : $x^u \equiv x^{N(\mathcal{U})} \pmod{\mathcal{U}}$; ceci est équivalent à : $x^{\bar{\sigma}^{-1} u \bar{\sigma}} \equiv x^{N(\mathcal{U})} \pmod{\mathcal{U}^\sigma}$; par l'isomorphisme du symbole d'Artin $\bar{\sigma}^{-1} u \bar{\sigma}$ provient donc de la classe $\mathcal{U}^\sigma F^p H_0$. Comme $\mathfrak{F}$ est engendré par les classes d'idéaux premiers, le résultat s'étend à toutes les classes.

Soit $U = \prod_{\chi \in \hat{g}} U_\chi$ la décomposition de U en produit direct associée à sa structure de g -groupe. On pose $U_\chi^* = \prod_{\substack{\psi \in \hat{g} \\ \psi \neq \chi}} U_\psi$; soit N_χ le sous-corps des invariants de U_χ^* ; U_χ^* étant un sous-groupe invariant U , N_χ est galoisien sur $\mathbb{Q}^{(p)}$ et on a :

$$\text{Gal}(N_\chi / \mathbb{Q}^{(p)}) \simeq U_\chi$$

(isomorphisme de groupes).

3.3. - L'extension $N/\mathbb{Q}^{(p)}$ est abélienne d'exposant p ; $\mathbb{Q}^{(p)}$ contient les racines $p^{\text{èmes}}$ de 1; par la théorie de Kummer, on a :

$$N = \mathbb{Q}^{(p)}(W) \quad ,$$

où $W = \{w \in N^* \mid w^p \in \mathbb{Q}^{(p)}\}$; le groupe des caractères $U = \text{Gal}(N/\mathbb{Q}^{(p)})$ à valeurs dans $\mathbb{Q}^p$ est canoniquement isomorphe au groupe $\mathcal{W} = W/\mathbb{Q}^{(p)*}$, par l'application qui à tout élément $w \in \mathbb{Q}^{(p)*}$ de $\mathcal{W}$ fait correspondre le caractère X_w de U défini par : $X_w(u) = \frac{w^u}{w}$.

Notons $\omega = w \in \mathbb{Q}^{(p)*}$, et : $X_w(u) = \langle \omega, u \rangle$.

Le groupe g opère sur les 3 groupes U , $\mathcal{W}$ et A groupe des racines $p^{\text{èmes}}$ de 1 dans $\mathbb{Q}^{(p)}$; on a la relation :

$$\langle \omega, u^\sigma \rangle = \langle \omega^{\bar{\sigma}^{-1}}, u \rangle^\sigma .$$

D'où :

$$\langle \omega, u^\sigma \rangle = \langle \omega^{\bar{\sigma}^{-1}} \chi^*(\sigma), u \rangle ,$$

(d'après la définition de χ^*).

Quel que soit l'élément λ de $\mathbb{Z}_p$, on a : $\langle \omega, u \rangle^\lambda = \langle \omega^\lambda, u \rangle = \langle \omega, u^\lambda \rangle$;

d'où :

$$\langle \omega, u^\sigma \chi(\sigma^{-1}) \rangle = \langle \omega, u \rangle^\sigma \chi(\sigma^{-1}) = \langle \omega^{\bar{\sigma}^{-1}} \bar{\chi}(\sigma), u \rangle ,$$

et :

$$\prod_{\chi} \langle \omega, u^\sigma \chi(\sigma^{-1}) \rangle = \prod_{\chi} \langle \omega^{\bar{\sigma}^{-1}} \bar{\chi}(\sigma), u \rangle .$$

D'où la relation (spiegelungsrelation) :

$$\langle \omega, u^1 \chi \rangle = \langle \omega^1 \bar{\chi}, u \rangle ,$$

c'est-à-dire $X_w(u^1 \chi) = X_{w^1 \bar{\chi}}(u)$.

Il en résulte : $\mathbb{Q}^{(p)}(W_{\bar{\chi}}) = N_{\chi}$, où $W_{\bar{\chi}}$ est l'image réciproque du sous-groupe $\mathcal{W}_{\bar{\chi}}$ de $\mathcal{W}$ par l'application canonique de W dans $\mathcal{W}$.

En effet, les éléments u de U qui laissent $W_{\overline{\chi}}$ invariant point par point sont caractérisés par : $u(\omega^{1\overline{\chi}})^u = \omega^{1\overline{\chi}}$ pour tout ω de $\mathcal{W}$, c'est-à-dire : $X_{\overline{\chi}}(u) = X_{\overline{\chi}}(u^{1\chi}) = 1$ pour tout w de W ; ce qui équivaut à $u^{1\chi} = e$ élément neutre de U . Autrement dit u laisse $W_{\overline{\chi}}$ invariant point par point si et seulement si u appartient au sous-groupe U_{χ}^* de U , qui est par définition le sous-groupe auquel appartient le corps N_{χ} .

U_{χ} étant isomorphe au groupe $\text{Gal}(N_{\chi}/\mathbb{Q}^{(p)})$, et $\mathcal{W}_{\overline{\chi}}$ au groupe des caractères de ce groupe, on a :

$$\mathcal{W}_{\overline{\chi}} \simeq U_{\chi} \quad (\text{isomorphisme de groupes}) ;$$

comme U et $\mathfrak{F}$ sont isomorphes en tant que $\mathbb{Z}_p[g]$ modules, les groupes U_{χ} et $\mathfrak{F}_{\chi}$ sont isomorphes. On a donc l'isomorphisme de groupes : $\mathcal{W}_{\overline{\chi}} \simeq \mathfrak{F}_{\chi}$.

3.4. - L'extension $N/\mathbb{Q}^{(p)}$ est non ramifiée ; le critère de décomposition de Kummer ([7]) montre que :

$$\mathcal{W}^p \mathcal{O}_{\mathbb{Q}(p)} = \mathcal{A}^p ,$$

où $\mathcal{A}$ est un idéal de $\mathbb{Q}^{(p)}$. L'application φ de $\mathcal{W}$ dans $\mathcal{D}$ définie par : $\mathcal{W}_{\mathbb{Q}^{(p)}}^* \rightarrow \mathcal{A}H$ est un homomorphisme de $\mathbb{Z}_p[g]$ modules ; l'image de $\mathcal{W}_{\overline{\chi}}$ par cette application est donc contenue dans $\mathcal{D}_{\overline{\chi}}$; le noyau de l'application φ restreinte à $\mathcal{W}_{\overline{\chi}}$ est formé de p classes d'unités primaires de $\mathcal{W}_{\overline{\chi}}$, qui appartiennent au groupe $\mathcal{G}_{1,\overline{\chi}}$.

$\mathcal{W}_{\overline{\chi}}$ est un p -groupe élémentaire ; le rang du groupe quotient $\mathcal{W}_{\overline{\chi}}/\text{Ker}\varphi|_{\mathcal{W}_{\overline{\chi}}}$ est donc égal à la différence entre le rang de $\mathcal{W}_{\chi}$ (qui est égal au rang r_{χ} de $\mathfrak{F}_{\chi}$), et le rang de $\text{Ker}\varphi|_{\mathcal{W}_{\overline{\chi}}}$ qui est majoré par le rang $e_{1,\overline{\chi}}$ du groupe $\mathcal{G}_{1,\overline{\chi}}$.

D'où l'inégalité du Spiegelungssatz :

$$r_{\chi} - e_{1, \bar{\chi}} \leq r_{\bar{\chi}}$$

-:-:-:-:-

BIBLIOGRAPHIE

BOREVICH - SHAFAREVICH. - Number theory. Acad. Press. 1966.

MARSCHALL HALL. - The theory of groups, Mac. comp. 1959.

H. HASSE. - Über die Klassenzahl abelschen Zahlkörper, Berlin, 1952.

E. HECKE. - Über nicht-regulären Primzahlen und den Fermatschen Satz. Gött. Nachr. Math. Phys. Kl. (1910), 420-424.

H. W. LEOPOLDT. - Zur struktur der 1-Klassen gruppe galoischen Zahlkörper, J. de Crelle 199 (1958), 165-174.

J. J. PAYAN. - Etude sur un cas particulier du théorème de réciprocité de Leopoldt. Séminaire théorie des nombres, Grenoble, Décembre 1968.

J. J. PAYAN. - Différente et discriminant, Séminaire Théorie des Nombres, Grenoble, Février-Mars 1968.

F. POLLACZEK. - Über die irregulären Kreiskörper der 1 ten und 1^2 ten Einheitswurzeln, Math. Zeit, 21 (1924), 1-36.

-:-:-:-:-