Séminaire Delange-Pisot-Poitou. Théorie des nombres

Gilles Robert

Nombres de Hurwitz et régularité des idéaux premiers

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 1 (1974-1975), exp. n° 21, p. 1-7

<http://www.numdam.org/item?id=SDPP_1974-1975__16_1_A16_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
16e année, 1974/75, n° 21, 7 p.

28 avril 1975

NOMBRES DE HURWITZ ET RÉGULARITÉ DES IDÉAUX PREMIERS

par Gilles ROBERT

Introduction.

Soit p un nombre premier. Le corps $\mathbb{Q}(\mu_p)$, où μ_p est une racine primitive p-ième de l'unité, est la plus grande extension abélienne de $\mathbb{Q}$ de conducteur l'idéal (p). On dit que p est régulier lorsque le nombre de classes $h_{\mathbb{Q}(\mu_p)}$ de $\mathbb{Q}(\mu_p)$ est premier avec p ; cette notion a été introduite par KUMMER en liaison avec ses recherches sur l'équation de Fermat.

Soit $K = \mathbb{Q}\sqrt{-d}$ un corps quadratique imaginaire (d entier > 0 sans facteurs carrés). Soit $\mathfrak{p}$ un idéal premier de K au-dessus de (p). Notons $H_{\mathfrak{p}}$ la plus grande extension abélienne de K de conducteur $\mathfrak{p}$. Le corps $H_{\mathfrak{p}}$ est, comme $\mathbb{Q}(\mu_p)$, un corps de nombres, et nous dirons que $\mathfrak{p}$ est régulier lorsque le nombre de classes $h_{H_{\mathfrak{p}}}$ de $H_{\mathfrak{p}}$ est premier avec p.

Nous voulons énoncer ici une condition numérique A qui implique la régularité de $\mathfrak{p}$.

1. Groupe des unités elliptiques.

Soit H la plus grande extension abélienne non ramifiée de K, c'est un sous-corps de $H_{\mathfrak{p}}$. Notons S l'anneau des entiers de K : le groupe de Galois $\mathrm{Gal}(H/K)$ est isomorphe au groupe de classes d'idéaux de S (on a donc $H = K$ si S est principal), et $G = \mathrm{Gal}(H_{\mathfrak{p}}/H)$ est isomorphe à un quotient du groupe multiplicatif $(S/\mathfrak{p})^*$.

Notons Ω le sous-groupe du groupe U de toutes les unités de $H_{\mathfrak{p}}$ construit dans [2] (Corollaire du théorème 16, §6). Les éléments du groupe Ω sont les valeurs singulières de fonctions elliptiques modulaires définies sur H, et Ω possède les propriétés suivantes :

THÉORÈME 1.

(i) Le groupe Ω est invariant par $\mathrm{Gal}(H_{\mathfrak{p}}/k)$.

(ii) Le groupe Ω contient le groupe des unités de H.

(iii) L'indice de Ω dans U est fini ; il est donné par la formule

$$(U:\Omega) = 2^{\alpha}\, 3^{\beta}\, h_{H_{\mathfrak{p}}}/h_H ,$$

où α et β sont des entiers ≥ 0 que nous savons calculer, et où $h_{H_{\mathfrak{p}}}$ (resp. h_H) désigne le nombre de classes du corps $H_{\mathfrak{p}}$ (resp. H).

Supposons que $p \neq 2$, $\neq 3$ et que p ne divise pas h_H, ce qui n'exclut qu'un nombre fini de p lorsque K est fixé. Nous déduisons de (iii) le corollaire suivant :

COROLLAIRE 1. - Pour que l'idéal $\mathfrak{p}$ soit régulier, il faut et il suffit que l'indice $(U:\Omega)$ soit premier avec p.

Considérons le p-groupe quotient $\Lambda = U/\Omega U^p$. Pour que $(U:\Omega)$ soit premier avec p, il faut et il suffit que $\Lambda = (1)$. Comme Ω est stable par $G=Gal(H_p/H)$ d'après (i), le p-groupe Λ possède une structure de $\underset{\sim}{F}_p[G]$-module, où $\underset{\sim}{F}_p$ désigne le corps premier à p éléments.

Vu que l'ordre de G divise $N(\mathfrak{p}) - 1 = \mathrm{card}(S/\mathfrak{p})^*$, les sommes

$$1_\chi = \sum_{g\in G} \chi(g^{-1})\, g/(G:1) ,$$

définies pour tout caractère irréductible χ de G dans $\underset{\sim}{F}_p$, appartiennent à $\underset{\sim}{F}_p(G)$. Les éléments 1_χ forment un système complet d'idempotents primitifs et orthogonaux de $\underset{\sim}{F}_p(G)$, par conséquent nous avons

$$\Lambda = \bigoplus_\chi \Lambda_\chi \text{ , où } \Lambda_\chi = \Lambda . 1_\chi .$$

Comme Ω contient les unités de H d'après (ii), le facteur Λ_1 est trivial, d'où le résultat suivant :

COROLLAIRE 2. - Pour que l'idéal $\mathfrak{p}$ soit régulier, il faut et il suffit que les facteurs Λ_χ soient triviaux pour tout caractère $\chi \neq 1$.

La condition A que nous voulons énoncer se réduit ainsi à un nombre fini de conditions A_χ, pour $\chi \neq 1$, telles que

$$A_\chi \Longrightarrow \Lambda_\chi = (1) .$$

2. Nombres de Hurwitz.

1° Les conditions A_χ font appel aux nombres de Hurwitz $s_{2k}(\Gamma)$, $k \geq 1$, associés à des réseaux $\Gamma \subset \underset{\sim}{C}$ tels que $S\Gamma \subset \Gamma$.

Soit $\Gamma = \underset{\sim}{Z}w_1 + \underset{\sim}{Z}w_2$, avec $\mathrm{Im}(w_1/w_2) > 0$, un réseau complexe. On pose, pour $k \geq 2$,

$$s_{2k}(\Gamma) = \left(\frac{2\pi i}{w_2}\right)^{2k} \left[- b_{2k}/(2k)! + \frac{2}{(2k-1)!} \sum_{n>0} \sigma_{2k-1}(n)\, q^n \right] ,$$

et

$$s_2(\Gamma) = \left(\frac{2\pi i}{w_2}\right)^{2} \left[- b_2/2 + 2 \sum_{n>0} \sigma_1(n)\, q^n + 1/4\pi\ \mathrm{Im}(w_1/w_2) \right] ,$$

où $q = \exp(2\pi i w_1/w_2)$, $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$, et b_{2k} désigne le nombre de Bernoulli d'indice $2k$.

Les formes s_{2k}, $k \geq 1$, sont invariantes par $SL_2(\underset{\sim}{Z})$; par conséquent, les nombres $s_{2k}(\Gamma)$ que nous venons de définir ne dépendent pas du choix de la base

(w_1 , w_2) de Γ ; de plus, s_{2k} est homogène de poids $2k$, c'est-à-dire que, pour tout nombre complexe $\lambda \neq 0$, nous avons l'identité

$$s_{2k}(\Gamma) = \lambda^{2k} s_{2k}(\lambda\Gamma) .$$

2° Lorsque Γ est stable pour la multiplication par S , c'est-à-dire lorsque $S\Gamma \subset \Gamma$, il est bien connu que l'invariant modulaire $j(\Gamma)$ appartient au corps H . Nous pouvons donc, sans restreindre la généralité, choisir un multiple de Γ tel que les invariants $3s_4(\Gamma)$ et $5s_6(\Gamma)$ soient des éléments p-entiers de H .

Pour tout idéal entier $\mathfrak{a}$ non nul de K , définissons les quantités $s_{2k}(\mathfrak{a} , \Gamma)$, $k \geq 1$, par

$$s_{2k}(\mathfrak{a} , \Gamma) = N(\mathfrak{a})\, s_{2k}(\Gamma) - s_{2k}(\mathfrak{a}^{-1}\Gamma) ,$$

où $N(\mathfrak{a})$ désigne le nombre d'éléments de l'anneau résiduel $S/\mathfrak{a}$.

Posons $a = 2$ si p est invariant pour la conjugaison complexe, et $a = 1$ sinon. Nous avons le résultat suivant :

PROPOSITION.

(i) Les sommes $s_{2k}(\mathfrak{a} , \Gamma)$ appartiennent à H .

(ii) Si $v_p(s_{2k}(\mathfrak{a} , \Gamma))$ désigne la p-valuation de $s_{2k}(\mathfrak{a} , \Gamma)$, normalisée par $v_p(p) = 1$, et $[2k/(p^a - 1)]$ la partie entière du quotient $2k/(p^a - 1)$, nous avons l'inégalité

$$v_p(s_{2k}(\mathfrak{a} , \Gamma)) + [2k/(p^a - 1)] \geq 0 .$$

Cette proposition peut se démontrer en considérant la loi de groupe p-adique formel, attachée au tore $\mathbb{C}/\Gamma$, qui est de hauteur 1 ou 2 suivant que $a = 1$ ou 2 .

Nous utiliserons les conséquences suivantes de la proposition :

COROLLAIRE 1. - Lorsque $0 < 2k < p^a - 1$, les sommes $s_{2k}(\mathfrak{a} , \Gamma)$ sont des éléments p-entiers de H .

COROLLAIRE 2. - Les nombres de Hurwitz $s_{2k}(\mathfrak{a}^{-1}\Gamma)$ appartiennent à H , et nous avons l'inégalité

$$v_p(s_{2k}(\mathfrak{a}^{-1}\Gamma)) + [2k/(p^a - 1)] + \nu_{2k} \geq 0 ,$$

où $\nu_{2k} = \inf_{\alpha \in S} v_p(N(\alpha) - \alpha^{2k})$.

Cette dernière inégalité résulte de la proposition et de l'identité

$$s_{2k}((\alpha) , \Gamma) = N(\alpha)\, s_{2k}(\Gamma) - s_{2k}(\alpha^{-1}\Gamma) = (N(\alpha) - \alpha^{2k}) s_{2k}(\Gamma) .$$

Les entiers ν_{2k} ne dépendent que de la classe de $2k$ modulo $N(p) - 1$; on a $\nu_{2k} = 1$ lorsque p est ramifié et $2k \equiv 2 \bmod p - 1$, ou lorsque p est de degré 2 et $2k \equiv p + 1 \bmod p^2 - 1$; dans tous les autres cas, $\nu_{2k} = 0$.

3. Les conditions numériques A_χ .

1° La possibilité d'exprimer les conditions A_χ à l'aide des sommes $s_{2k}(\alpha , \Gamma)$ résulte du fait que les combinaisons linéaires finies

$$\sum m_\alpha \, s_{2k}(\alpha , \Gamma) , \qquad k \geq 1 ,$$

avec $\sum m_\alpha = 0$ et m_α entier rationnel, apparaissent comme coefficients du développement en série de Taylor des dérivées logarithmiques de certaines fonctions elliptiques, celles-là mêmes dont les valeurs singulières sont les éléments du groupe d'unités Ω de H_p introduit précédemment. Cette idée se trouve déjà ébauchée dans le travail d'A. P. NOVIKOV [1].

2° Rappelons d'abord la description classique des caractères du groupe $G = \mathrm{Gal}(H_p/H)$.

Notons e l'ordre du groupe des unités de $K = \mathbb{Q}\sqrt{-d}$ (on sait que $e = 2$ si $d \neq 1$ et $\neq 3$, et que $e = 4$ ou 6 suivant que $d = 1$ ou 3). Lorsque $p \neq 2$ et $\neq 3$, l'isomorphisme de réciprocité d'Artin identifie G au quotient du groupe multiplicatif $(S/\mathfrak{p})^*$ par son sous-groupe cyclique d'ordre e .

Les caractères irréductibles $\chi \neq 1$ de $(S/\mathfrak{p})^*$ dans $\mathbb{F}_p$, triviaux sur le sous-groupe cyclique d'ordre e , sont de deux sortes :

(i) Les caractères χ_k de degré 1 définis par

$$\chi_k(\alpha) = \alpha^k ,$$

où $\alpha \in (S/\mathfrak{p})^*$, et k est un entier tel que $0 < k < N(\mathfrak{p}) - 1$ et $e \mid k$ ou $(p + 1) \mid k$ suivant que $N(\mathfrak{p}) = p$ ou p^2 .

(ii) Lorsque $N(\mathfrak{p}) = p^2$, les caractères $\chi_{k,k'}$ de degré 2 définis par

$$\chi_{k,k'}(\alpha) = \alpha^k + \alpha^{k'} ,$$

où $\alpha \in (S/\mathfrak{p})^*$, et où k et k' sont des entiers tels que $0 < k < k' < p^2 - 1$, $e \mid k$, $e \mid k'$ et $pk \equiv k' \mod p^2 - 1$.

3° Nous supposons désormais que p n'est pas ramifié. Cette nouvelle restriction qui s'ajoute aux précédentes ($p \neq 2$, $\neq 3$ et $p \nmid h_H$) n'exclut à nouveau qu'un ensemble fini de nombres premiers p . Nous avons alors $N(\mathfrak{p}) = p$ ou p^2 suivant que $a = 1$ ou 2 , soit $N(\mathfrak{p}) = p^a$.

Notons $\mathrm{Cl}(K)$ le groupe de classes d'idéaux de l'anneau S , et $h = \deg(H/K)$ le nombre d'éléments de $\mathrm{Cl}(K)$. Soient $\mathfrak{a}_1 = (1)$, $\mathfrak{a}_2 , \ldots , \mathfrak{a}_h$ des idéaux entiers de K premiers avec $\mathfrak{p}$ formant un système complet de représentants de $\mathrm{Cl}(K)$.

Soit k un entier tel que $0 < k < N(\mathfrak{p}) - 1$ et $e \mid k$ ou $(p + 1) \mid k$ suivant que $N(\mathfrak{p}) = p$ ou p^2 . Les restes modulo $\mathfrak{p}$ des solutions $(\lambda_1, \lambda_2, \ldots, \lambda_h) \in S \times S \times \ldots \times S = S^h$ de la congruence

$$\lambda_1 \, p^{\nu_k} \, s_k(\Gamma) + \sum_{i=2}^{h} \lambda_i \, s_k(\mathfrak{a}_i^{-1} \, \Gamma) \equiv 0 \mod \mathfrak{p}$$

forment un $\underset{\sim}{F}_p$-espace vectoriel dont la dimension $d_k(\Gamma)$ ne dépend pas du choix du système de représentants $a_1 , a_2 , \dots , a_h$ de $Cl(K)$. Nous avons le résultat suivant :

THÉORÈME 2. - *Pour tout caractère* χ_k *de degré* 1 *du groupe* $G = Gal(H_p/H)$, *le p-rang de* Λ_{χ_k} *est majoré par* $d_k(\Gamma)$.

D'une manière analogue, supposons que $N(p) = p^2$, et soient k et k' deux entiers tels que $0 < k < k' < p^2 - 1$, et $e|k$, $e|k'$ et $pk \equiv k' \mod p^2 - 1$. Les restes modulo p des solutions $(\lambda_1 , \lambda_2 , \dots , \lambda_h) \in S^h$ des congruences

$$\begin{cases} \lambda_1 s_k(\Gamma) + \sum_{i=2}^{h} \lambda_i s_k(a_i^{-1} \Gamma) \equiv 0 \mod p \\ \lambda_1^p s_{k'}(\Gamma) + \sum_{i=2}^{h} \lambda_i^p s_{k'}(a_i^{-1} \Gamma) \equiv 0 \mod p \end{cases}$$

forment un $\underset{\sim}{F}_p$-espace vectoriel dont la dimension $d_{k,k'}(\Gamma)$ ne dépend pas du choix du système de représentants $a_1 , a_2 , \dots , a_h$ de $Cl(K)$. Nous avons le résultat suivant :

THÉORÈME 3. - *Pour tout caractère* $\chi_{k,k'}$ *de degré* 2 *du groupe* $G = Gal(H_p/H)$, *le p-rang de* $\Lambda_{\chi_{k,k'}}$ *est majoré par* $d_{k,k'}(\Gamma)$.

Dans le cas où $h = 1$, nous avons déjà énoncé ces résultats dans [3].

4. Analogie avec la théorie cyclotomique

1° Soit Ψ le groupe des unités circulaires de $\underset{\sim}{Q}(\mu_p)$. Le groupe Ψ est un sous-groupe du groupe V des *unités réelles* de $\underset{\sim}{Q}(\mu_p)$, dont les éléments sont les valeurs singulières de fonctions circulaires rationnelles, qui possède les propriétés suivantes :

THÉORÈME 4.

(i) *Le groupe* Ψ *est invariant par* $Gal(\underset{\sim}{Q}(\mu_p)^+/\underset{\sim}{Q})$, *où* $\underset{\sim}{Q}(\mu_p)^+$ *désigne le sous-corps réel maximal de* $\underset{\sim}{Q}(\mu_p)$.

(ii) *L'indice de* Ψ *dans* V *est fini ; il est donné par la formule*

$$(V:\Psi) = h_{\underset{\sim}{Q}(\mu_p)^+} ,$$

où $h_{\underset{\sim}{Q}(\mu_p)^+}$ *désigne le nombre de classes du corps* $\underset{\sim}{Q}(\mu_p)^+$.

Il s'agit là de résultats bien connus. Le nombre $h_{\underset{\sim}{Q}(\mu_p)^+}$ est un diviseur de $h_{\underset{\sim}{Q}(\mu_p)}$, et on sait exprimer, à l'aide des nombres de Bernoulli, une condition (B) qui implique que $h_{\underset{\sim}{Q}(\mu_p)^+}$ est premier avec p . *Nous nous proposons de rappeler les grandes lignes de la construction de la condition* (B) *pour mettre en évidence son parallélisme avec la construction précédente.*

Considérons le p-groupe quotient $\mathcal{Y} = V/\Psi V^p$. Comme Ψ est stable par $G = Gal(\underset{\sim}{Q}(\mu_p)^+/\underset{\sim}{Q})$ d'après (i), le p-groupe $\mathcal{Y}$ possède une structure de $\underset{\sim}{F}_p[G]$-

module. Comme l'ordre de G divise $p-1$, nous pouvons décomposer ψ selon les caractères irréductibles χ de G dans $\mathbb{F}_p$. Nous avons

$$\psi = \bigoplus_\chi \psi_\chi \text{ , où } \psi_\chi = \psi.1_\chi \text{ .}$$

D'après (ii), pour que $h_{\mathbb{Q}(\mu_p)^+}$ soit premier avec p, il faut et il suffit que $\psi = (1)$; on en déduit comme précédemment le résultat suivant :

COROLLAIRE. - Pour que $(h_{\mathbb{Q}(\mu_p)^+}, p) = 1$ il faut et il suffit que les facteurs ψ_χ soient triviaux pour tout caractère $\chi \neq 1$.

La condition B se réduit ainsi à un nombre fini de conditions B_χ, pour $\chi \neq 1$, telles que

$$B_\chi \Longrightarrow \psi_\chi = (1) \text{ .}$$

2° La propriété suivante des nombres de Bernoulli b_k, k pair, est également bien connue :

PROPOSITION. - Si $p-1 \nmid k$, le nombre rationnel b_k est p-entier.

La possibilité d'exprimer les conditions B_χ à l'aide des nombres de Bernoulli résulte du fait que les combinaisons linéaires finies

$$\sum m_\alpha \alpha^k b_k/k! \text{ , } \quad k \text{ pair,}$$

avec $\sum m_\alpha = 0$, α et m_α entiers rationnels, apparaissent comme coefficients du développement en série de Taylor des dérivées logarithmiques de certaines fonctions circulaires, celles-là mêmes dont les valeurs singulières sont les éléments du groupe d'unités circulaires Ψ de $\mathbb{Q}(\mu_p)$.

Lorsque $p \neq 2$, l'isomorphisme de réciprocité d'Artin identifie G au quotient du groupe multiplicatif $(\mathbb{Z}/p)^*$ par $\{-1, +1\}$. Les caractères irréductibles $\chi \neq 1$ de $(\mathbb{Z}/p)^*$ dans $\mathbb{F}_p$ tels que $\chi(-1) = 1$ sont les caractères χ_k de degré 1, définis par

$$\chi_k(\alpha) = \alpha^k \text{ ,}$$

où $\alpha \in (\mathbb{Z}/p)^*$, et k est un entier pair tel que $0 < k < p-1$. Nous avons le résultat suivant :

THÉORÈME 5. - Soit χ_k un caractère $\neq 1$ du groupe $G = \mathrm{Gal}(\mathbb{Q}(\mu_p)^+/\mathbb{Q})$, si $\psi_{\chi_k} \neq (1)$, alors $p \mid b_k$.

Notons encore que les techniques p-adiques utilisées pour démontrer les théorèmes 2 et 3 et pour démontrer le théorème 5 sont essentiellement identiques.

3° Un phénomène très remarquable de la théorie cyclotomique est que la conjonction B des conditions B_χ, $\chi \neq 1$, que nous venons de décrire, non seulement implique que $(h_{\mathbb{Q}(\mu_p)^+}, p) = 1$, mais se trouve aussi être équivalente à la régula-

rité du nombre premier p , c'est-à-dire que

$$B = \bigcup_{\chi \neq 1} B_\chi \iff (h_{\mathbb{Q}(\mu_p)} , p) = 1 .$$

Il pourrait être intéressant d'examiner si une telle réciproque existe pour la condition $A = \bigcup_{\chi \neq 1} A_\chi$ énoncée plus haut.

BIBLIOGRAPHIE

[1] NOVIKOV (A. P.). - Sur la régularité des idéaux premiers de degré 1 d'un corps quadratique imaginaire [en russe], Izv. Akad. Nauk SSSR, Serija Mat., t. 33, 1969, p. 1059-1079 ; [en anglais] Math. USSR-Izvestija, t. 3, 1969, p. 1001-1018.

[2] ROBERT (G.). - Unités elliptiques et formules pour le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire, Bull. Soc. math. France, Mémoire 36, 1973, 77 p.

[3] ROBERT (G.). - Régularité des idéaux premiers d'un corps quadratique imaginaire de nombre de classes 1 , "Journées arithmétiques [1974.Bordeaux]", Astérisque 24-25, 1975, p. 75-80.

On trouvera une bibliographie plus détaillée dans [2].

(Texte reçu le 21 juillet 1975)

Gilles ROBERT
99 rue Raymond Losserand
75014 PARIS