ANNALES SCIENTIFIQUES DE L'É.N.S.

GILLES ROBERT

Nombres de Hurwitz et unités elliptiques. Un critère de régularité pour les extensions abéliennes d'un corps quadratique imaginaire

Annales scientifiques de l'É.N.S. 4^e série, tome 11, n° 3 (1978), p. 297-389

<http://www.numdam.org/item?id=ASENS_1978_4_11_3_297_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 11, 1978, p. 297 à 389.

NOMBRES DE HURWITZ ET UNITÉS ELLIPTIQUES

UN CRITÈRE DE RÉGULARITÉ POUR LES EXTENSIONS ABÉLIENNES D'UN CORPS QUADRATIQUE IMAGINAIRE (*)

PAR GILLES ROBERT

RÉSUMÉ. — Soient K un corps quadratique imaginaire et p un idéal premier de K au-dessus du nombre premier p. Concernant le nombre de classes d'idéaux de l'extension abélienne maximale de K de conducteur p, nous démontrons un théorème analogue au résultat suivant, essentiellement dû à Kummer.

PROPOSITION A. — *Soit p un nombre premier $\geqq 5$. Le nombre de classes d'idéaux de l'extension abélienne réelle maximale de* **Q**, *de conducteur p, est premier à p, si, pour chaque entier pair k tel que $0 < k < p-1$, le k-ième nombre de Bernoulli B_k est une unité p-adique.*

TABLE DES MATIÈRES

(*) Thèse présentée à l'Université de Paris-XI et soutenue le 16 novembre 1977.

0. Introduction

Soit p un nombre premier $\geqq 5$. Notons $\mathcal{O}$ l'anneau des entiers du corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-d})$, où d est un entier positif. Regardons $\mathcal{O}$ comme un réseau complexe, et notons $j(\mathcal{O})$ son invariant modulaire. Par la théorie de la multiplication complexe, on sait que le corps $H_0 = K(j(\mathcal{O}))$ est le corps de classes de Hilbert de K, c'est-à-dire l'extension abélienne non ramifiée maximale de K. Soit E une courbe elliptique définie sur H_0 d'invariant $j_E = j(\mathcal{O})$. La courbe E possède des multiplications complexes par $\mathcal{O}$. Désignons par T la réunion de $\{2, 3\}$ et de l'ensemble des nombres premiers q tels que E a mauvaise réduction en au moins un idéal premier de H_0 au-dessus de q. Comme $p \geqq 5$, il est légitime de supposer la courbe E choisie de façon que $p \notin T$ (*cf.* [30], § 6, cor. 1, th. 9). Fixons un idéal premier $\mathfrak{p}$ de K au-dessus de p, et représentons E par une équation de Weierstrass

$$y^2 = 4x_3 - g_2 x - g_3 \tag{0}$$

telle que g_2 et g_3 soient des éléments $\mathfrak{p}$-entiers de H_0 et le discriminant de (0) soit $\mathfrak{p}$-inversible (ce qui est possible puisque $p \notin T$).

Pour tout entier $k \geqq 3$, notons G_k la série d'Eisenstein de poids k, définie sur les réseaux $\mathscr{L} \subset \mathbf{C}$ par

$$G_k(\mathscr{L}) = \sum_{\lambda \in \mathscr{L}}' 1/\lambda^k,$$

où la somme $\sum'$ est prise sur tous les éléments non nuls de $\mathscr{L}$. Pour $k = 2$, on définit G_2 par

$$G_2(\mathscr{L}) = \lim_{\substack{s \to 0 \\ s > 0}} \sum_{\lambda \in \mathscr{L}}' 1/\lambda^2 |\lambda|^{2s}.$$

Les G_k sont homogènes de poids $-k$: pour tout $\rho \in \mathbf{C}^\times$, on a

$$G_k(\rho^{-1}\mathscr{L}) = \rho^k G_k(\mathscr{L}); \tag{1}$$

par suite, seules les séries G_k d'indice k pair sont non nulles.

Soient $L \subset \mathbf{C}$ le réseau associé à l'équation (0), et $\mathfrak{a}$ un idéal entier de K. Considérons les nombres $G_k(\mathfrak{a}^{-1}L)$, $k \geqq 2$. D'après (1), si k n'est pas divisible par l'ordre e du groupe des racines de l'unité de K [1], le nombre $G_k(\mathfrak{a}^{-1}L)$ est nul. D'une façon générale, les nombres $G_k(\mathfrak{a}^{-1}L)$ appartiennent à H_0. Ceci peut être vu ainsi : pour $z \in \mathbf{C}$, posons

$$\sigma(z, \mathfrak{a}^{-1}L) = z \prod_{\lambda \in \mathfrak{a}^{-1}L}' \left(1 - \frac{z}{\lambda}\right) e^{[(z/\lambda) + (1/2)](z/\lambda)^2};$$

c'est la fonction sigma de Weierstrass associée au réseau $\mathfrak{a}^{-1}L$. Notons $\theta(z, \mathfrak{a}^{-1}L)$ le produit

$$\theta(z, \mathfrak{a}^{-1}L) = \Delta(\mathfrak{a}^{-1}L)\, e^{-6G_2(\mathfrak{a}^{-1}L)z^2}\, \sigma^{12}(z, \mathfrak{a}^{-1}L),$$

---

[1] On a $e = 6$ si $K = \mathbf{Q}(\sqrt{-3})$, $e = 4$ si $K = \mathbf{Q}(\sqrt{-1})$ et $e = 2$ sinon.

où $\Delta = (2\pi)^{12}((60\,G_4)^3 - 27\,(140\,G_6)^2)$ est la forme modulaire parabolique de poids 12 usuelle. On a

$$z\frac{\partial}{\partial z}\log\theta(z, \mathfrak{a}^{-1}L) = 12\Big(1 - \sum_{\substack{k>0\\ e\mid k}} G_k(\mathfrak{a}^{-1}L)\,z^k\Big). \tag{2}$$

Par ailleurs, le quotient

$$\theta(z, L; \mathfrak{a}) = \frac{\theta(z, L)^{N(\mathfrak{a})}}{\theta(z, \mathfrak{a}^{-1}L)}, \tag{3}$$

où $N(\mathfrak{a})$ désigne la norme absolue de l'idéal $\mathfrak{a}$, est une fonction elliptique pour le réseau L. Si $\mathscr{P}(z, L) = -(\partial^2/\partial z^2)\log\sigma(z, L)$ est la fonction $\mathscr{P}$ de Weierstrass, il n'est pas difficile de vérifier l'identité

$$\theta(z, L; \mathfrak{a}) = \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)}\prod_{\lambda\in(\mathfrak{a}^{-1}L)/L}{}' \frac{\Delta(L)}{(\mathscr{P}(z, L) - \mathscr{P}(\lambda, L))^6}, \tag{4}$$

où le produit $\prod'$ est pris sur les $N(\mathfrak{a})-1$ éléments non nuls du quotient $(\mathfrak{a}^{-1}L)/L$; on notera que (4) exprime $\theta(z, L; \mathfrak{a})$ comme une fraction rationnelle en $\mathscr{P}(z, L)$ à coefficients dans H_0. Prenons la dérivée logarithmique de (4); il vient

$$z\frac{\partial}{\partial z}\log\theta(z, L; \mathfrak{a}) = -6\,z\frac{\mathscr{P}'(z, L)}{\mathscr{P}(z, L)}\sum_{\lambda\in(\mathfrak{a}^{-1}L)/L}{}'\left[1 - \frac{\mathscr{P}(\lambda, L)}{\mathscr{P}(z, L)}\right]^{-1}, \tag{5}$$

avec $\mathscr{P}'(z, L) = (\partial/\partial z)\,\mathscr{P}(z, L)$. Comme $\mathscr{P}(z, L)$ satisfait l'équation différentielle

$$\mathscr{P}'^2 = 4\mathscr{P}^3 - g_2\mathscr{P} - g_3,$$

où g_2 et g_3 appartiennent à H_0, les coefficients de son développement en série de Laurent au point $z = 0$ appartiennent à H_0; d'après (5), les coefficients du développement de $\partial/\partial z \log\theta(z, L; \mathfrak{a})$ en série de Laurent appartiennent aussi à H_0. Or, on a, d'après (2),

$$z\frac{\partial}{\partial z}\log\theta(z, L; \mathfrak{a}) = 12\Big[N(\mathfrak{a}) - 1 + \sum_{\substack{k>0\\ e\mid k}} (G_k(\mathfrak{a}^{-1}L) - N(\mathfrak{a})\,G_k(L))\,z^k\Big]. \tag{6}$$

Par suite, les différences $G_k(\mathfrak{a}^{-1}L) - N(\mathfrak{a})\,G_k(L)$, et donc les nombres $G_k(\mathfrak{a}^{-1}L)$ eux-mêmes, appartiennent à H_0; en particulier, on a

$$G_2(\mathfrak{a}^{-1}L) - N(\mathfrak{a})\,G_2(L) = \sum_{\lambda\in(\mathfrak{a}^{-1}L)/L}{}' \mathscr{P}(\lambda, L). \tag{7}$$

Il n'est guère plus difficile de montrer que $G_k(\mathfrak{a}^{-1}L) - N(\mathfrak{a})\,G_k(L)$ est $\mathfrak{p}$-entier, pourvu que $2 \leqq k \leqq N(\mathfrak{p}) - 3$ (*cf.* cor. 13, § 3); il en résulte que les nombres $G_k(\mathfrak{a}^{-1}L)$, $2 \leqq k \leqq N(\mathfrak{p}) - 3$, sont eux-mêmes $\mathfrak{p}$-entiers, à condition que l'on ne se trouve pas dans l'une des deux situations suivantes :

(i) p est inerte dans K et $k = p+1$;

(ii) p est ramifié dans K et $k = 2$.

Dans ces deux cas, pour tout élément π de $\mathfrak{p}$, le produit $\pi\, G_k(\mathfrak{a}^{-1} L)$ est $\mathfrak{p}$-entier (*cf.* cor. 14); si $\mathfrak{a}$ est premier à $\mathfrak{p}$ et $\pi \notin \mathfrak{p}^2$, il est même $\mathfrak{p}$-inversible (*cf.* prop. 16, § 3).

Pour $z \in \mathbf{C}$, posons $x(z) = \mathscr{P}(z, L)$ et $y(z) = \mathscr{P}'(z, L)$; l'application ξ :

$$z \mapsto \xi(z) = (x(z), y(z))$$

définit un isomorphisme du tore $\mathbf{C}/L$ sur le groupe $E(\mathbf{C})$ des points complexes de E. Nous identifions $\mathcal{O}$ à l'anneau des endomorphismes de E, de façon qu'à l'élément α de $\mathcal{O}$ corresponde l'endomorphisme de $E(\mathbf{C})$ donné par $\xi(z) \mapsto \xi(\alpha z)$.

Comme $L = \rho\,\mathcal{O}$, avec $\rho \in \mathbf{C}^\times$, le groupe $(\mathfrak{p}^{-1} L)/L$ des points de $\mathfrak{p}$-torsion modulo L est un $(\mathcal{O}/\mathfrak{p})$-module libre de rang 1. En adjoignant à H_0 les coordonnées $x(\tau)$ et $y(\tau)$ des points $\xi(\tau)$, avec $\tau \in \mathfrak{p}^{-1} L$ et $\tau \notin L$, on obtient une extension abélienne $F = H_0(\xi(\mathfrak{p}^{-1} L))$ de H_0; comme il y a bonne réduction en p, son degré est $N(\mathfrak{p}) - 1$. Le corps F contient le corps $H = H_0(x^{e/2}(\mathfrak{p}^{-1} L))$; il résulte de la théorie de la multiplication complexe que ce dernier n'est autre que le corps de classes du rayon modulo $\mathfrak{p}$ de K (*cf.* [31], th. 5.5) et ne dépend donc pas du choix de E.

Soient $h = (H_0 : K)$ le nombre de classes d'idéaux de K, et $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \ldots, \mathfrak{a}_h$, des idéaux entiers de K, premiers à $6\,\mathfrak{p}$, qui forment un système complet de représentants du groupe de classes d'idéaux de K. Notons h_H (resp. h_{H_0}) le nombre de classes d'idéaux de H (resp. H_0); comme on le sait, le quotient h_H/h_{H_0} est entier (*cf.* [6]). *Nous prouvons dans ce travail une condition numérique* (th. 1, ci-dessous) *portant sur les nombres* $G_k(\mathfrak{a}_i^{-1} L)$, $1 \leqq i \leqq h$, $0 < k < N(\mathfrak{p}) - 1$, $k \equiv 0 \pmod{e}$, *qui assure que le quotient* h_H/h_{H_0} *est premier à p.*

Avant d'énoncer ce résultat, introduisons encore quelques notations. Nous désignons par $\mathcal{O}_\mathfrak{p}(H_0)$ l'anneau des éléments $\mathfrak{p}$-entiers de H_0, et posons $\mathfrak{p}(H_0) = \mathfrak{p}\,\mathcal{O}_\mathfrak{p}(H_0)$. Notons $\varkappa$ l'algèbre quotient $\mathcal{O}_\mathfrak{p}(H_0)/\mathfrak{p}(H_0)$; sa dimension, en tant que $(\mathcal{O}/\mathfrak{p})$-espace vectoriel, est égale à h. Lorsque p est inerte dans K, nous munissons $\varkappa \times \varkappa$ de la structure de $(\mathcal{O}/\mathfrak{p})$-espace vectoriel « tordue » définie par

$$\lambda(u, v) = (\lambda u, \lambda^p v), \tag{8}$$

pour tous $\lambda \in \mathcal{O}/\mathfrak{p}$ et $(u, v) \in \varkappa \times \varkappa$. Toujours dans le cas où p est inerte, pour tout entier k tel que $1 \leqq k \leqq N(\mathfrak{p}) - 1$, nous notons $p(k)$ l'entier unique tel que $1 \leqq p(k) \leqq N(\mathfrak{p}) - 1$ et $p(k) \equiv pk \pmod{N(\mathfrak{p}) - 1}$; on a alors $k = p(p(k))$, et pour que $k = p(k)$ il faut et il suffit que $p+1$ divise k. Comme d'habitude, le corps premier à p éléments est noté $\mathbf{F}_p$.

On a (*cf.* th. 28 et 29, § 3) :

THÉORÈME 1. — *Soit p un nombre premier* $\geqq 5$, *non ramifié dans* K, *tel que* $p \notin T$. *Le quotient* h_H/h_{H_0} *est premier à p, si, pour chaque entier k divisible par e, tel que* $0 < k < N(\mathfrak{p}) - 1$, *l'une des trois conditions* A_k, A'_k *ou* B_k *ci-dessous est satisfaite. On notera que ces conditions sont mutuellement exclusives.*

(A_k) *On suppose p décomposé dans* K, *ou bien p inerte dans* K *et k divisible par* $p+1$, $k \neq p+1$. *On demande que les classes modulo* $\mathfrak{p}(H_0)$ *des h nombres* $\mathfrak{p}$-*entiers* $G_k(\mathfrak{a}_i^{-1} L)$, $1 \leqq i \leqq h$, *soient* $\mathbf{F}_p$-*linéairement indépendantes dans* $\varkappa$.

(A'_k) *On suppose p inerte dans* K *et* $k = p+1$. *Soit* $(1, \alpha)$ *une base de* $\mathcal{O}$ *sur l'anneau des entiers rationnels. On demande que les classes modulo* $\mathfrak{p}(H_0)$ *des* $h+1$ *nombres* $\mathfrak{p}$*-entiers* $p\,G_{p+1}(L)$, $\alpha p\,G_{p+1}(L)$ *et* $G_{p+1}(\mathfrak{a}_i^{-1}L) - N(\mathfrak{a}_i)\,G_{p+1}(L)$, $2 \leqq i \leqq h$, *soient* $\mathbf{F}_p$*-linéairement indépendantes dans* $\varkappa$.

(B_k) *On suppose p inerte dans* K *et k non divisible par* $p+1$. *On demande que les classes modulo* $\mathfrak{p}(H_0)\times\mathfrak{p}(H_0)$ *des h couples de nombres* $\mathfrak{p}$*-entiers* $(G_k(\mathfrak{a}_i^{-1}L),\ G_{p(k)}(\mathfrak{a}_i^{-1}L))$, $1 \leqq i \leqq h$, *soient* $(\mathcal{O}/\mathfrak{p})$*-linéairement indépendantes dans* $\varkappa\times\varkappa$ *muni de la structure de* $(\mathcal{O}/\mathfrak{p})$*-espace vectoriel tordue* (8).

Lorsque le nombre de classes d'idéaux h de K est 1, et les coefficients g_2 et g_3 de la représentation (0) de E des entiers rationnels, le théorème **1** se réduit à l'énoncé que nous avons déjà donné dans [29].

Notre démonstration du théorème 1 suit essentiellement la démonstration de la proposition A telle qu'elle est donnée dans [4] (chap. V, § 6). Rappelons que les premiers résultats dans cette direction ont été obtenus par A. P. Novikov [22]; celui-ci a prouvé, pour chacun des corps $K = \mathbf{Q}(\sqrt{-1})$ et $K = \mathbf{Q}(\sqrt{-3})$, une partie du théorème 1 (*cf.* [22] th. 2, et appendice C).

Le rôle de la formule classique, qui exprime le nombre de classes d'idéaux du corps $\mathbf{Q}(\zeta+\zeta^{-1})$, où $\zeta = e^{2\pi i/p}$ est une racine primitive p-ième de l'unité, comme l'indice du groupe des unités circulaires dans le groupe des unités réelles positives de $\mathbf{Q}(\zeta)$, est joué dans notre travail par le corollaire du théorème 16 de [28] (§ 6-4). Le corps $\mathbf{Q}(\zeta+\zeta^{-1})$, qui est l'extension abélienne réelle maximale de $\mathbf{Q}$, de conducteur p, y est remplacé par H et le groupe des unités circulaires par celui des unités elliptiques (*cf.* th. 8, § 1 ci-dessous).

Enfin, rappelons que la première étude systématique des nombres $G_k(\mathfrak{a}^{-1}L)$ semble remonter à A. Hurwitz [12], lorsque $x(z) = \mathscr{P}(z, L)$ et $y(z) = \mathscr{P}'(z, L)$ sont les fonctions qui paramétrisent la courbe elliptique

$$y^2 = 4x^3 - 4x,$$

d'invariant $j(\mathbf{Z}[\sqrt{-1}]) = 1728$. Aussi, désigne-t-on par nombres de Hurwitz les nombres $G_k(\mathfrak{a}^{-1}L)$ associés à l'équation (0). Depuis, ces nombres ont fait l'objet de nombreuses études, dont celles de H. Lang [15], J. U. Manin et M. M. Vishik [20], N. Katz ([13], [14]) et S. Lichtenbaum [18]. En particulier, ces auteurs ont prouvé pour les nombres $k!G_k(\mathfrak{a}^{-1}L)$ des propriétés d'interpolation $\mathfrak{p}$-adique analogues à celles des nombres de Bernoulli; le cas où p est inerte présente des difficultés particulières (*cf.* [14]).

Dans ce travail, nous prouvons également des réciproques partielles du théorème 1. Nous démontrons en particulier les deux théorèmes suivants (*cf.* th. 58 et 61, § 6) :

THÉORÈME 2. — *Soit p un nombre premier décomposé dans* K, $p \notin T$. *Pour que les conditions* A_k *soient vérifiées pour chaque entier k divisible par e tel que* $0 < k < N(\mathfrak{p})-1$, *il faut et il suffit que la p-extension abélienne maximale de* H, *non ramifiée en dehors de* $\mathfrak{p}$, *soit abélienne sur* H_0.

THÉORÈME 3. — *Soit p un nombre premier inerte dans* K, $p \notin T$. *S'il existe un entier k divisible par e, tel que* $p+1 < k$, $p(k) < N(\mathfrak{p})-1$, *pour lequel aucune des conditions* A_k *et* B_k *n'est satisfaite, le quotient* h_H/h_{H_0} *est divisible par p.*

Rappelons ici que l'analogue précis du théorème 2 ci-dessus est bien connu dans le cas cyclotomique; c'est le « critère de Kummer » (*cf.* [7]) :

PROPOSITION B. — *Soit p un nombre premier $\geqq 5$. Pour que les nombres de Bernoulli B_k soient des unités p-adiques pour chaque entier pair k tel que $0 < k < p-1$, il faut et il suffit que la p-extension abélienne maximale de $\mathbf{Q}(e^{2\pi i/p}+e^{-2\pi i/p})$, non ramifiée en dehors de p, soit abélienne sur $\mathbf{Q}$.*

Lorsque le nombre de classes d'idéaux h de K est 1, le théorème 2 se réduit au théorème 1 de J. Coates et A. Wiles [7]. Ceux-ci appuient leur démonstration sur un résultat de S. Lichtenbaum [18], (th. 8.14), prouvé sous l'hypothèse $h = 1$, et emploient des procédés différents des nôtres. Cependant leur travail explicite plusieurs lemmes de la théorie du corps de classes, essentiels à notre preuve du théorème 2.

Par ailleurs, les méthodes de [7] semblent difficiles à généraliser au cas où p ne se décompose pas dans K. En fait, lorsque p est inerte dans K, la situation est assez différente comme le montre le théorème 3. Pour prouver ce dernier nous reprenons des idées de J. Herbrand [11] et utilisons le théorème du miroir de H. W. Leopoldt [17].

Enfin, est-il besoin de préciser que ce que nous démontrons dans ce travail reste bien en deçà des résultats connus dans le cas cyclotomique (*cf.* J. Herbrand [11] et K. Ribet [27]).

CONTENU. — Le paragraphe 1 rassemble les propriétés du groupe des unités elliptiques de H dont nous aurons besoin. Le paragraphe 2 est consacré à la décomposition en composantes simples de certains $\mathbf{F}_p[G]$-modules, où G est le groupe de Galois de l'extension H/H_0. Le paragraphe 3 ramène la démonstration du théorème 1 à la construction d'un homomorphisme φ de $H^\times$ dans le groupe additif de $\varkappa^{(N(\mathfrak{p})-1)/e}$. La construction de φ fait l'objet du paragraphe 5, et s'appuie sur des techniques de groupe formel. Le paragraphe 4 apporte des améliorations importantes aux résultats du paragraphe 3, suivant une suggestion de J.-P. Serre. Enfin, nous poursuivons l'étude de φ dans le paragraphe 6 et en déduisons les théorèmes 2 et 3.

On trouvera en appendice quelques compléments, et des exemples numériques.

1. Nombre de classes d'idéaux des extensions abéliennes de conducteur premier comme indice d'unités

Soit $\mathfrak{p}(K)$ l'idéal maximal de l'anneau des éléments $\mathfrak{p}$-entiers de K. Nous notons $Cl(\mathfrak{p})$ le quotient du groupe des idéaux fractionnaires de K, premiers à $\mathfrak{p}$, par le rayon modulo $\mathfrak{p}$, formé des idéaux principaux (α) tels que $\alpha \equiv 1 \pmod{\mathfrak{p}(K)}$. Pour tout idéal fractionnaire $\mathfrak{b}$ de K, premier à $\mathfrak{p}$, désignons par $(\mathfrak{b}, H/K)$ le symbole d'Artin de $\mathfrak{b}$ sur H. On sait, par la théorie du corps de classes, que l'application $\mathfrak{b} \mapsto (\mathfrak{b}, H/K)$ définit un isomorphisme de $Cl(\mathfrak{p})$ sur le groupe de Galois $\mathscr{G} = G(H/K)$.

Soit $A(\mathfrak{p})$ l'ensemble des couples $(\tau, \mathscr{L})$ formés d'un réseau $\mathscr{L} \subset \mathbf{C}$ tel que

$$\{\lambda \in \mathbf{C} \mid \lambda \mathscr{L} \subset \mathscr{L}\} = \mathcal{O}$$

et d'un point τ de $\mathfrak{p}$-torsion modulo $\mathscr{L}$ non trivial, c'est-à-dire d'un point τ de $\mathfrak{p}^{-1}\mathscr{L}$ n'appartenant pas à $\mathscr{L}$. Nous disons que deux couples $(\tau_1, \mathscr{L}_1)$ et $(\tau_2, \mathscr{L}_2)$ sont *équivalents*, s'il existe $\rho \in \mathbf{C}^\times$ pour lequel $\mathscr{L}_2 = \rho\mathscr{L}_1$ et $\tau_2 - \rho\tau_1 \in \mathscr{L}_2$. L'ensemble $\tau\mathscr{L}^{-1} = \{\alpha \in K \mid \tau\alpha \in \mathscr{L}\}$ est un idéal fractionnaire de K, et le produit $\mathfrak{p}\tau\mathscr{L}^{-1}$ est un idéal entier de K, premier à $\mathfrak{p}$. Notons $C(\tau, \mathscr{L}) \in Cl(\mathfrak{p})$ la classe de $\mathfrak{p}\tau\mathscr{L}^{-1}$. D'après [28] (lemme 4, § 2-2), l'application $(\tau, \mathscr{L}) \mapsto C(\tau, \mathscr{L})$ définit une bijection de $A(\mathfrak{p})$, modulo équivalence, sur $Cl(\mathfrak{p})$.

Soient $(\tau, \mathscr{L}) \in A(\mathfrak{p})$ et $\mathfrak{a}$ un idéal entier de K, premier à $\mathfrak{p}$. Notons $\theta(z, \mathscr{L}; \mathfrak{a})$ la fonction elliptique de la variable complexe z obtenue en substituant $\mathscr{L}$ à L dans la formule (3). Comme $\mathfrak{a}$ est premier à $\mathfrak{p}$, aucun point non trivial de $\mathfrak{p}$-torsion modulo $\mathscr{L}$ n'apparaît dans le diviseur $12(N(\mathfrak{a})\mathscr{L} - \mathfrak{a}^{-1}\mathscr{L})$ de $\theta(z, \mathscr{L}; \mathfrak{a})$. Par suite $\theta(\tau, \mathscr{L}; \mathfrak{a})$ est défini et non nul. De plus, pour tout $\rho \in \mathbf{C}^\times$, on a $\theta(\rho\tau, \rho\mathscr{L}; \mathfrak{a}) = \theta(\tau, \mathscr{L}; \mathfrak{a})$, et, pour tout $\gamma \in \rho\mathscr{L}$,

$$\theta(\tau+\gamma, \rho\mathscr{L}; \mathfrak{a}) = \theta(\tau, \rho\mathscr{L}; \mathfrak{a});$$

par conséquent, il vient :

LEMME 4. — *Soient* $(\tau_1, \mathscr{L}_1)$ *et* $(\tau_2, \mathscr{L}_2) \in A(\mathfrak{p})$ *deux couples équivalents. On a*

$$\theta(\tau_1, \mathscr{L}_1; \mathfrak{a}) = \theta(\tau_2, \mathscr{L}_2; \mathfrak{a}).$$

DÉFINITION 5. — *Pour tout* $C \in Cl(\mathfrak{p})$, *nous posons* $\theta(C, \mathfrak{a}) = \theta(\tau, \mathscr{L}; \mathfrak{a})$, *où* $(\tau, \mathscr{L}) \in A(\mathfrak{p})$ *est tel que* $C(\tau, \mathscr{L}) = C$.

Mais, avec les notations de la proposition 9, paragraphe 4-2 de [28], pour tout idéal entier $\mathfrak{a}$ de K et tout idéal fractionnaire $\mathfrak{b}$ de K, on a l'identité

$$\theta(z, \mathfrak{b}; \mathfrak{a})^{-1} \underset{dfn}{=} \theta^{(12)}(z, \mathfrak{b}; \mathfrak{a}) = L(\mathfrak{b}; \mathfrak{a}) \prod_{\mathfrak{g} \mid \mathfrak{a}} T(\tau(z, \mathfrak{g}), \mathfrak{b}; \mathfrak{a})^{12/e_{\mathfrak{g}}},$$

où les exposants $12/e_{\mathfrak{g}}$ sont des entiers positifs et le produit est pris sur tous les diviseurs entiers $\mathfrak{g}$ de $\mathfrak{a}$; si $(\mathfrak{a}, 6) = (1)$, cette identité n'est autre que celle de la proposition 9, *loc. cit.* Par suite (cf. *loc. cit.*, corollaire de la proposition 9), *pour tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $\mathfrak{p}$, l'invariant $\theta(C, \mathfrak{a})$ appartient à $H^\times$, et pour tout idéal fractionnaire $\mathfrak{b}$ de K premier à $\mathfrak{p}$, on a

$$\theta(C, \mathfrak{a})^{(\mathfrak{b}, H/K)} = \theta(CC_{\mathfrak{b}}, \mathfrak{a}),$$

où $C_{\mathfrak{b}} \in Cl(\mathfrak{p})$ désigne la classe de $\mathfrak{b}$. De plus, si $\mathfrak{b}$ est entier, on déduit de (3) l'identité

$$\theta(CC_{\mathfrak{b}}, \mathfrak{a}) = \theta(C, \mathfrak{a}\mathfrak{b})/\theta(C, \mathfrak{b})^{N(\mathfrak{a})}.$$

Ce qui prouve :

LEMME 6. — *Soient* C *et* $C' \in Cl(\mathfrak{p})$, *et* $\mathfrak{b} \in C'$ *un idéal entier de* K *premier à* $\mathfrak{p}$. *Alors, pour tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $\mathfrak{p}$, *on a*

$$\theta(C, \mathfrak{a})^{(\mathfrak{b}, H/K)} = \theta(CC', \mathfrak{a}) = \theta(C, \mathfrak{a}\mathfrak{b})/\theta(C, \mathfrak{b})^{N(\mathfrak{a})}.$$

En outre, si $(\mathfrak{a}, 6) = (1)$, l'invariant $\theta(C, \mathfrak{a})$ est une puissance 12-ième dans $H^\times$ (*cf.* appendice A); ceci motive la définition suivante du *groupe* Θ *des unités elliptiques de* H :

$$\Theta = \mathscr{E} \cap \Psi,$$

où $\mathscr{E}$ désigne le groupe des unités de $H^\times$ et Ψ le sous-groupe de $H^\times$ engendré par les invariants $\theta(C, \mathfrak{a})$, $\mathfrak{a}$ idéal entier de K premier à $6\mathfrak{p}$ et $C \in Cl(\mathfrak{p})$.

En fait, dans ce texte, le rôle de l'hypothèse $(\mathfrak{a}, 6) = (1)$ est assez secondaire; aussi, chaque fois que cette hypothèse n'est pas rappelée dans un énoncé, celui-ci reste vrai pour $(\mathfrak{a}, 6) \neq (1)$; c'est par exemple le cas de la proposition 7 ci-dessous du théorème 12 (iv), paragraphe 3, du lemme 18, paragraphe 3, de la proposition 46, paragraphe 5, etc. Toutefois, si $(\mathfrak{a}, 6) \neq (1)$, l'invariant $\theta(C, \mathfrak{a})$ n'est pas en général une puissance 12-ième dans H (*cf.* appendice C pour le cas $\mathfrak{a} = (2)$).

Ceci étant précisé, on a *cf.* [25], et [28] (§ 4).

PROPOSITION 7. — *Pour tout entier* $r \geqq 1$, *et tous triplets* $(C_i, \mathfrak{a}_i, m_i)$, $1 \leqq i \leqq r$, *formés d'une classe* $C_i \in Cl(\mathfrak{p})$, *d'un idéal entier* $\mathfrak{a}_i$ *de* K *premier à* $\mathfrak{p}$, *et d'un entier rationnel* m_i, *le produit*

$$\prod_{i=1}^{r} \theta(C_i, \mathfrak{a}_i)^{m_i}$$

appartient à $\mathscr{E}$ *si et seulement si*

$$\sum_{i=1}^{r} m_i(N(\mathfrak{a}_i)-1) = 0.$$

Soit maintenant M un sous-corps de H contenant K. Nous appelons groupe des unités elliptiques de M le groupe

$$\Theta(M) = N_{H/M}\Theta,$$

formé des normes relatives des éléments de Θ. Le groupe $\Theta(M)$ est invariant pour l'action du groupe de Galois $G(M/K)$; et l'on a, d'après le lemme 6 et la proposition 7,

$$\Theta(M) = \mathscr{E}(M) \cap N_{H/M}\Psi,$$

où $\mathscr{E}(M)$ désigne le groupe des unités de M. Posons $M_0 = M \cap H_0$. L'extension M/M_0 est totalement ramifiée en $\mathfrak{p}$, par suite le nombre de classes d'idéaux h_{M_0} de M_0 divise le nombre de classes d'idéaux h_M de M; en effet, soit $\mathscr{H}$ une extension abélienne non ramifiée de M_0; le corps $\mathscr{H}$ M est une extension abélienne non ramifiée de M, de même de degré que $\mathscr{H}/M_0$ puisque $\mathscr{H} \cap M = M_0$.

Soit $\Omega(M)$ le sous-groupe de $\mathscr{E}(M)$ engendré par les trois groupes d'unités ci-dessous :

(α) le groupe $\Theta(M)$;

(β) le groupe $\mu(M)$ des racines de l'unité de M;

(γ) le groupe $\mathscr{E}(M_0)$ des unités de M_0.

D'après [28] (cor. du th. 16, § 6-4), on a :

THÉORÈME 8. — *L'indice de* $\Omega(M)$ *dans* $\mathscr{E}(M)$ *est fini; il est donné par la formule*

$$[\mathscr{E}(M) : \Omega(M)] = 2^a 3^b h_M/h_{M_0},$$

où a et b sont des entiers $\geqq 0$.

Pour le calcul de *a* et *b*, *cf.* appendice A et [28] (§ 6).

2. Représentations du groupe de Galois du corps de classes de rayon sur le corps de classes absolu

Soit $F = H_0(\xi(\mathfrak{p}^{-1}L))$, où ξ désigne l'isomorphisme de $\mathbf{C}/L$ sur $E(\mathbf{C})$ associé à (0). Le groupe $E_\mathfrak{p} = \xi(\mathfrak{p}^{-1}L)$ est le groupe des points de $\mathfrak{p}$-torsion de $E(\mathbf{C})$, et l'action du groupe de Galois $G(F/H_0)$ sur $E_\mathfrak{p}$ définit une injection

$$\sigma : \quad G(F/H_0) \subsetneq (\mathcal{O}/\mathfrak{p})^\times ;$$

l'extension F/H_0 est donc abélienne. Comme $p \notin T$, il résulte du lemme 39 (i) (§ 5), que cette injection est un isomorphisme de $G(F/H_0)$ sur $(\mathcal{O}/\mathfrak{p})^\times$. Soit $\mu(K)$ le groupe des unités de K; comme $p \geqq 5$, nous pouvons identifier $\mu(K)$ à son image dans $(\mathcal{O}/\mathfrak{p})^\times$. L'isomorphisme précédent définit alors, par passage au quotient, un isomorphisme

$$\sigma : \quad G = G(H/H_0) \tilde{\mapsto} (\mathcal{O}/\mathfrak{p})^\times/\mu(K),$$

inverse du symbole d'Artin, dont la e-ième puissance σ^e fournit une injection de G dans $(\mathcal{O}/\mathfrak{p})^\times$ indépendante du choix de E. En particulier, on a $(F : H) = e$ et

$$(H : H_0) = (N(\mathfrak{p})-1)/e,$$

où $e = \#\,\mu(K)$.

Soit k un entier rationnel divisible par e. L'homomorphisme σ^k de G dans $(\mathcal{O}/\mathfrak{p})^\times$ ne dépend que de la classe de k modulo $N(\mathfrak{p})-1$, et les $\#\,G$ homomorphismes σ^k, $e \leqq k \leqq N(\mathfrak{p})-1$, $e \mid k$, sont deux à deux distincts. Par suite, les seules représentations linéaires irréductibles de G sur $\mathcal{O}/\mathfrak{p}$ sont les homomorphismes σ^k, k entier divisible par e. Nous en déduisons facilement la description suivante des représentations linéaires irréductibles de G sur $\mathbf{F}_p$.

LEMME 9. — (i) *Si p se ramifie ou bien se décompose dans* K, *on a* $\mathcal{O}/\mathfrak{p} = \mathbf{F}_p$, *et les représentations linéaires irréductibles de* G *sur* $\mathbf{F}_p$ *sont les homomorphismes* σ^k, $e \mid k$.

(ii) *Si p est inerte dans* K, *le corps* $\mathcal{O}/\mathfrak{p}$ *est une extension de degré* 2 *de* $\mathbf{F}_p$. *Par suite, les représentations linéaires irréductibles de* G *sur* $\mathbf{F}_p$ *sont de degré* 1 *ou* 2.

Or, on a $\sigma^k = \sigma^{pk}$ *si et seulement si l'entier k est divisible par* $p+1$. *Les représentations linéaires de degré* 1 *de* G *sur* $\mathbf{F}_p$ *sont donc les homomorphismes* σ^k, $p+1 \mid k$. *Quant aux représentations linéaires irréductibles de degré* 2 *de* G *sur* $\mathbf{F}_p$, *elles ont pour caractères les sommes*

$$\mathrm{Tr}(\sigma^k) = \sigma^k + \sigma^{pk} = \mathrm{Tr}(\sigma^{pk}), \qquad e \mid k \quad \text{et} \quad k \not\equiv 0 \pmod{p+1}.$$

Comme $\#\,G$ est premier à p, l'algèbre de groupe $\mathbf{F}_p[G]$ est semi-simple. Lorsque χ décrit les caractères irréductibles de G sur $\mathbf{F}_p$, les sommes

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

forment un système primitif d'idempotents orthogonaux de $\mathbf{F}_p[G]$, et on a

$$1 = \sum_\chi 1_\chi .$$

Posons $\mathbf{F}_p[G]_\chi = 1_\chi . \mathbf{F}_p[G]$; c'est un corps fini, et le degré de l'extension $\mathbf{F}_p[G]_\chi/\mathbf{F}_p$ est égal au degré de χ. Un $\mathbf{F}_p[G]$-module $\mathscr{S}$ étant donné, on définit sa χ-composante $\mathscr{S}_\chi$ par $\mathscr{S}_\chi = 1_\chi . \mathscr{S}$. On a

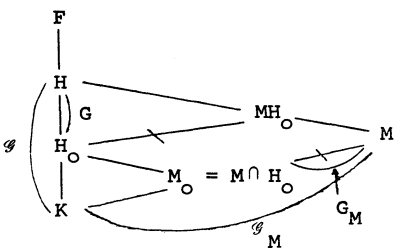
$$\mathscr{S} = \bigoplus_\chi \mathscr{S}_\chi .$$

Rappelons enfin deux conséquences du fait que 1_χ est un idempotent de $\mathbf{F}_p[G]$:

– l'algèbre $\mathbf{F}_p[G]$ agit sur $\mathscr{S}_\chi$ à travers sa χ-composante $\mathbf{F}_p[G]_\chi$.

– la multiplication par 1_χ transforme toute suite exacte de $\mathbf{F}_p[G]$-modules en une suite exacte de $\mathbf{F}_p[G]$-espaces vectoriels.

Soient M un sous-corps de H contenant K, et M_0 l'intersection de M avec H_0. Conformément au schéma suivant, notons G_M (resp. $\mathscr{G}_M$) le groupe de Galois de l'extension M/M_0 (resp. M/K); le groupe G_M est isomorphe au quotient de G par le groupe de Galois $G(H/MH_0)$, et $\mathscr{G}_M$ est le quotient de $\mathscr{G}$ par le groupe de Galois G (H/M).



Soit χ un caractère de G, constant sur $G(H/MH_0)$. Il définit, par passage au quotient, un caractère de G_M, provisoirement noté χ_M. L'application $\chi \mapsto \chi_M$ est un isomorphisme du groupe des caractères de G sur $\mathbf{F}_p$, constants sur $G(H/MH_0)$, avec le groupe des caractères de G_M sur $\mathbf{F}_p$. De plus χ_M est irréductible si et seulement si χ l'est; nous identifions χ et χ_M.

Munissons les quotients $\mathscr{E}^{(p)}(M) = \mathscr{E}(M)/\mathscr{E}(M)^p$, $\Omega^{(p)}(M) = \Omega(M)/\Omega(M) \cap \mathscr{E}(M)^p$ et $\mathscr{S}(M) = \mathscr{E}(M)/\Omega(M)\,\mathscr{E}(M)^p$ de leur structure naturelle de $\mathbf{F}_p[G]$-module (en fait $\mathscr{G}$ laisse stable $\mathscr{E}(M)$ et $\Omega(M)$, ce qui permet de munir $\mathscr{E}^{(p)}(M)$, $\Omega^{(p)}(M)$ et $\mathscr{S}(M)$ d'une structure de $\mathbf{F}_p[\mathscr{G}]$-module; celle-ci n'intervient pas dans ce paragraphe). Soit χ un caractère irréductible de G sur $\mathbf{F}_p$, et considérons les χ-composantes $\mathscr{E}^{(p)}(M)_\chi$, $\Omega^{(p)}(M)_\chi$ et $\mathscr{S}(M)_\chi$ des trois modules précédents. Comme G agit à travers son quotient G_M, on peut supposer que χ est un caractère irréductible de G_M sur $\mathbf{F}_p$ (en effet, si χ n'est pas constant sur $G(H/MH_0)$, on a $\mathscr{E}^{(p)}(M)_\chi = \Omega^{(p)}(M)_\chi = \mathscr{S}(M)_\chi = \{0\}$). La suite de $\mathbf{F}_p[G]$-modules

$$\{0\} \to \Omega^{(p)}(M) \to \mathscr{E}^{(p)}(M) \to \mathscr{S}(M) \to \{0\}$$

est exacte; par conséquent, il en est de même de la suite de $\mathbf{F}_p[G]_\chi$-espaces vectoriels

$$\{0\} \to \Omega^{(p)}(M)_\chi \to \mathscr{E}^{(p)}(M)_\chi \to \mathscr{S}(M)_\chi \to \{0\}. \tag{9}$$

Notons $e(\chi, M)$ (resp. $t(\chi, M)$) la dimension de $\mathscr{E}^{(p)}(M)_\chi$ (resp. $\Omega^{(p)}(M)_\chi$) sur $\mathbf{F}_p[G]_\chi$. D'après (9), on a

$$t(\chi, M) \leqq e(\chi, M).$$

De plus $\Omega(M)$ contient $\mathscr{E}(M_0)$, d'où $\mathscr{S}(M)_1 = \{0\}$, et, d'après (9),

$$t(1, M) = e(1, M).$$

La proposition suivante est alors une conséquence immédiate du théorème 8.

PROPOSITION 10. — *Pour $p \geqq 5$ les quatre propriétés suivantes sont équivalentes :*

(i) $h_M/h_{M_0} \not\equiv 0 \pmod{p}$.

(ii) $\mathscr{S}(M) = \{0\}$.

(iii) *Pour tout caractère irréductible χ de G_M sur $\mathbf{F}_p$, $\chi \neq 1$, on a $\mathscr{S}(M)_\chi = \{0\}$.*

(iv) *Pour tout χ, comme dans* (iii), *on a*

$$t(\chi, M) = e(\chi, M).$$

La dimension $e(\chi, M)$ peut être décrite en fonction du degré de l'extension M_0/K. Notons d'abord que le corps H contient le groupe μ_p des racines p-ièmes de l'unité, pour $p \neq 2$, si et seulement si p ne se décompose pas dans K. L'action de G sur μ_p définit alors un homomorphisme ν de G dans $\mathbf{F}_p^\times$, déterminé par les congruences

$$\nu(((\alpha), H/K)) \equiv N(\alpha) \pmod{p},$$

où α désigne un élément de $\mathcal{O}$ premier à $\mathfrak{p}$. Par suite pour $p \notin T$, on a $\nu = \sigma^2$ si p est ramifié dans K, $\nu = \sigma^{p+1}$ si p est inerte dans K; et ν n'est pas défini si p se décompose dans K. Il vient :

LEMME 11. — *Soient p un nombre premier $\geqq 5$, et χ un caractère irréductible de G_M sur $\mathbf{F}_p$:*

(i) *si $\chi = 1$, on a $e(\chi, M) = (M_0 : K) - 1$;*

(ii) *si M contient μ_p et $\chi = \nu$, on a $e(\chi, M) = (M_0 : K) + 1$;*

(iii) *en dehors des deux cas précédents, on a $e(\chi, M) = (M_0 : K)$.*

Démonstration. — Posons $\mathscr{E}_0(M) = \mathscr{E}(M)/\mu(M)$, $\mathscr{E}_0^{(p)}(M) = \mathscr{E}_0(M)/\mathscr{E}_0(M)^p$ et $\mu^{(p)}(M) = \mu(M)/\mu(M)^p$. La suite exacte de $\mathbf{F}_p[G]$-modules

$$\{0\} \to \mu^{(p)}(M) \to \mathscr{E}^{(p)}(M) \to \mathscr{E}_0^{(p)}(M) \to \{0\}$$

réduit la question à la détermination des dimensions de $\mu^{(p)}(M)_\chi$ et $\mathscr{E}_0^{(p)}(M)_\chi$ sur $\mathbf{F}_p[G]_\chi$.

Le $\mathbf{F}_p[G]$-module $\mu^{(p)}(M)$ est soit nul, soit, si M contient μ_p, isomorphe à μ_p. Dans ce dernier cas ν est défini et

$$\mu^{(p)}(M) = \mu^{(p)}(M)_\nu.$$

Le $\mathbf{F}_p[G]_\chi$-espace vectoriel $\mu^{(p)}(M)_\chi$ est donc de dimension 1 ou 0 suivant que $\chi = \nu$ ou $\chi \neq \nu$.

Désignons par $\mathbf{Z}_p$ l'anneau des entiers p-adiques, et posons $A = \mathscr{E}_0(M) \otimes \mathbf{Z}_p$. Le $\mathbf{Z}_p$-module A est libre de rang $(M : K) - 1$. On sait, d'après le théorème de Dirichlet-Minkowski, qu'il existe une unité $u \in \mathscr{E}(M)$ dont les conjugués par $\mathscr{G}_M$ engendrent un

sous-groupe d'indice fini de $\mathscr{E}(M)$. Par suite, le caractère de la représentation de $\mathscr{G}_M$ dans $\mathscr{E}_0(M)$, et donc dans A, est $r_{M/K}-1$ où $r_{M/K}$ désigne le caractère de la représentation régulière de $\mathscr{G}_M$. Le caractère de la représentation de G_M dans A est donc $(M_0 : K)\, r_{M/M_0}-1$, où r_{M/M_0} désigne le caractère de la représentation régulière de G_M. Or, le caractère irréductible χ de G_M sur $\mathbf{F}_p$ provient, par réduction modulo p, d'un caractère irréductible χ^* de G_M sur $\mathbf{Z}_p$; le caractère χ^* est uniquement déterminé par χ, et χ a même degré que χ^* (l'existence est facile, et l'unicité vient de ce que $\#\, G_M$ est premier à p). Posons

$$1_{\chi^*} = (\#\, G_M)^{-1} \sum_{g \in G_M} \chi^*(g^{-1})\, g.$$

L'action de G sur A en fait un $\mathbf{Z}_p[G]$-module semi-simple, dont la χ^*-composante $A_{\chi^*} = 1_{\chi^*}.A$ est un $\mathbf{Z}_p$-module libre de rang égal au produit de la multiplicité de χ^* dans $(M_0 : K)\, r_{M/M_0}-1$ par le degré de χ^*; d'autre part, ce rang est aussi la dimension du $\mathbf{F}_p$-espace vectoriel

$$A_{\chi^*}/A_{\chi^*}^p \simeq \mathscr{E}_0^{(p)}(M)_\chi,$$

c'est-à-dire le produit de la dimension de $\mathscr{E}_0^{(p)}(M)_\chi$ sur $\mathbf{F}_p[G]_\chi$ par le degré de χ. Cette dernière dimension est donc égale à la multiplicité de χ^* dans $(M_0 : K)\, r_{M/M_0}-1$, soit $(M_0 : K)$ si $\chi \neq 1$, et $(M_0 : K)-1$ si $\chi = 1$; ce qui prouve le lemme ([2]).

3. Où l'on voit comment l'existence de nombres premiers réguliers résulte de la construction d'une dérivée logarithmique tronquée

Soit $p \notin T$, et *fixons* un point τ de $\mathfrak{p}^{-1}L$ n'appartenant pas à L. Notons $C_0 \in C\,l(\mathfrak{p})$ l'image du couple $(\tau, L) \in A(\mathfrak{p})$ par l'application $(\tau, \mathscr{L}) \mapsto C(\tau, \mathscr{L})$ (*cf.* § 1). Pour tous idéaux entiers $\mathfrak{a}$ et $\mathfrak{b}$ de K et tout entier $k > 0$ divisible par e, posons

$$G_k^*(\mathfrak{a}, \mathfrak{b}^{-1}L) = G_k(\mathfrak{a}^{-1}\mathfrak{b}^{-1}L) - N(\mathfrak{a})\, G_k(\mathfrak{b}^{-1}L).$$

En vue d'utiliser la proposition 10, nous construisons un homomorphisme

$$\varphi = (\varphi_k)_{e \leqq k \leqq N(\mathfrak{p})-1,\, e \mid k}$$

de $H^\times$ dans le groupe additif de l'algèbre

$$\varkappa^{(N(\mathfrak{p})-1)/e} = \underbrace{\varkappa \times \ldots \times \varkappa}_{(N(\mathfrak{p})-1)/e \text{ termes}},$$

avec $\varkappa = \mathscr{O}_\mathfrak{p}(H_0)/\mathfrak{p}(H_0)$.

L'homomorphisme φ dépend du choix de L et de celui de classe de τ modulo L; il possède les propriétés suivantes :

THÉORÈME 12. — *Soit k un entier divisible par e, $e \leqq k \leqq N(\mathfrak{p})-1$.*

(i) *Le noyau de φ_k, pour $k \neq N(\mathfrak{p})-1$, ainsi que le noyau de la restriction de $\varphi_{N(\mathfrak{p})-1}$ au groupe $\mathscr{E}$ des unités de* H, *sont stables par $\mathscr{G}$.*

([2]) Ce lemme est aussi vérifié pour $p = 3$, non ramifié dans K.

(ii) *Si* $\sigma^k = \nu$ *et si* $\zeta \in H^\times$ *est une racine primitive p-ième de l'unité, l'image de* ζ *par* φ_k *est inversible dans* $\varkappa$.

(iii) *Pour tous* $u \in H^\times$ *et* $g \in G$, *on a*

$$\varphi_k(u^g) = \sigma^k(g).\varphi_k(u).$$

(iv) *Si* $k \neq N(\mathfrak{p})-1$, *pour tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $\mathfrak{p}$, *on a*

$$\varphi_k(\theta(C_0, \mathfrak{a})) \equiv 12\, G_k^*(\mathfrak{a}, L) (\mathrm{mod}\, \mathfrak{p}(H_0)).$$

L'existence des homomorphismes φ_k reprend une idée déjà développée par Kummer dans le cas cyclotomique (*cf.* par exemple H. Hasse, *Bericht über neuere Untersuchungen and Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, 2e éd. Würzburg-Wien, Physica 1965) : les φ_k sont en quelque sorte des « dérivées logarithmiques modulo $\mathfrak{p}(H_0)$ ». Nous étudions dans ce paragraphe et le suivant quelques conséquences du théorème 12. La construction de φ et la démonstration du théorème 12 sont réservées au paragraphe 5, ci-dessous.

Notons d'abord le corollaire suivant du théorème 12 (iv).

COROLLAIRE 13. — *Soient k comme dans le théorème* 12, $k \neq N(\mathfrak{p})-1$, *et* $\mathfrak{a}$ *un idéal entier de* K *premier à* $\mathfrak{p}$. *Le nombre* $G_k^*(\mathfrak{a}, L)$ *est* $\mathfrak{p}$*-entier.*

Par suite, on a :

COROLLAIRE 14. — *Soient k comme dans le corollaire* 13, *et* $\mathfrak{a}$ *un idéal entier de* K.

(i) *Si* $\sigma^k \neq \nu$, *le nombre* $G_k(\mathfrak{a}^{-1} L)$ *est* $\mathfrak{p}$*-entier.*

(ii) *Si* $\sigma^k = \nu$, *le nombre* $\pi\, G_k(\mathfrak{a}^{-1} L)$ *est* $\mathfrak{p}$*-entier dès que* $\pi \in \mathfrak{p}$.

Démonstration. — Soit α un élément de $\mathcal{O}$ premier à 6 $\mathfrak{p}$. D'après le corollaire 13, le nombre

$$G_k^*((\alpha), L) = (\alpha^k - N(\alpha))\, G_k(L)$$

est $\mathfrak{p}$-entier.

Supposons $\sigma^k \neq \nu$. Si p se décompose dans K le corps H ne contient pas le groupe μ_p; par conséquent, il existe α tel que $\alpha - 1 \in \mathfrak{p}$ et $N(\alpha)-1 \not\equiv 0 \pmod{p}$, d'où $\alpha^k \not\equiv N(\alpha) \pmod{\mathfrak{p}}$. Si p ne se décompose pas dans K, le caractère ν est défini; comme $\sigma^k \neq \nu$, on peut choisir l'entier α de K de façon que

$$\sigma^k((\alpha), H/K) \neq \nu((\alpha), H/K),$$

soit $\alpha^k \not\equiv N(\alpha) \pmod{\mathfrak{p}}$. Par suite $G_k(L)$, et donc $G_k(\mathfrak{a}^{-1} L)$ sont $\mathfrak{p}$-entiers.

Si $\sigma^k = \nu$, d'après le lemme 15 ci-dessous, pour tout $\pi \in \mathfrak{p}$, il existe des éléments α de $\mathcal{O}$ premiers à 6 $\mathfrak{p}$ tels que $\alpha^k - N(\alpha) \equiv \pi \pmod{\mathfrak{p}^2}$. Par suite $\pi\, G_k(L)$, et donc $\pi\, G_k(\mathfrak{a}^{-1} L)$, sont $\mathfrak{p}$-entiers.

LEMME 15. — *Soit p un nombre premier* $\neq 2$ *non décomposé dans* K. *Alors, pour tout* $\pi \in \mathfrak{p}$, *il existe* α *tel que* $\alpha - 1 \in \mathfrak{p}$, $(\alpha, 6) = (1)$ *et* $\alpha^k - N(\alpha) \equiv \pi \pmod{\mathfrak{p}^2}$ *où* $k = 2$ *si p se ramifie dans* K *et* $k = p+1$ *si p est inerte dans* K.

Démonstration. — Supposons d'abord p ramifié, d'où $k = 2$. Notons $D < 0$ le discriminant de K. Comme $p \neq 2$, le nombre $\sqrt{D}$ appartient à $\mathfrak{p}$ et n'appartient pas à $\mathfrak{p}^2$. Soit β' un élément de $\mathcal{O}$ et posons $\alpha = 1+\beta\sqrt{D}$, où $\beta = 6\beta'$ si $p \geqq 5$ et $\beta = 2\beta'$ si $p = 3$. On a $(\alpha, 6) = (1)$, et on vérifie la congruence modulo $\mathfrak{p}^2$:

$$\alpha^2 - N(\alpha) \equiv 2\beta\sqrt{D} \equiv \begin{cases} 12\beta'\sqrt{D}, & p \geqq 5, \\ 4\beta'\sqrt{D}, & p = 3, \end{cases}$$

d'où le lemme dans ce cas.

Supposons maintenant p inerte. On a $k = p+1$. Soit β' un élément de $\mathcal{O}$ et posons $\alpha = 1+\beta^p p$, où $\beta = 6\beta'$ si $p \geqq 5$ et $\beta = 2\beta'$ si $p = 3$. On a $(\alpha, 6) = (1)$, et on vérifie la congruence modulo $\mathfrak{p}^2$:

$$\alpha^{p+1} - N(\alpha) \equiv -\beta p \equiv \begin{cases} -6\beta' p, & p \geqq 5, \\ -2\beta' p, & p = 3 \end{cases}$$

qui complète la démonstration du lemme.

En fait, on a l'analogue suivant du théorème de Von Staudt et Clausen :

PROPOSITION 16. — *Soient k un entier divisible par e, $0 < k < N(\mathfrak{p})-1$, tel que $\sigma^k = \nu$, et $\mathfrak{a}$ un idéal entier de K premier à $\mathfrak{p}$. Alors, si $p \notin T$, le nombre $\pi\, G_k(\mathfrak{a}^{-1} L)$ est $\mathfrak{p}$-inversible pour tout $\pi \in \mathfrak{p}$ tel que $\pi \notin \mathfrak{p}^2$.*

Démonstration. — Distinguons suivant que p est inerte ou ramifié dans K. Si p est inerte, posons

$$\zeta = \frac{\theta(C_0, (1+p\sqrt{D}))}{\theta(C_0, (1-p\sqrt{D}))};$$

si p est ramifié, posons

$$\zeta = \frac{\theta(C_0, (1+\sqrt{D}))}{\theta(C_0, (1-\sqrt{D}))}.$$

Il résulte du lemme 17 ci-dessous et du lemme 6, que ζ est une racine primitive p-ième de l'unité; d'après le théorème 12 (ii), l'image de ζ par φ_k est donc inversible dans $\varkappa$. Or, d'après le théorème 12 (iv), selon que p est inerte ou ramifié dans K, on a respectivement :

$$\varphi_k(\zeta) \equiv 12(G_k^*((1+p\sqrt{D}), L) - G_k^*((1-p\sqrt{D}), L)) \pmod{\mathfrak{p}(H_0)}$$

ou

$$\varphi_k(\zeta) \equiv 12(G_k^*((1+\sqrt{D}), L) - G_k^*((1-\sqrt{D}), L)) \pmod{\mathfrak{p}(H_0)}.$$

Par conséquent, on a $\varphi_k(\zeta) \equiv 24p\sqrt{D}\, G_k(L) \pmod{\mathfrak{p}(H_0)}$ si p est inerte dans K, et $\varphi_k(\zeta) \equiv 48\sqrt{D}\, G_k(L) \pmod{\mathfrak{p}(H_0)}$ si p est ramifié dans K. Ce qui prouve la proposition.

LEMME 17. — *Soit p un nombre premier $\geqq 5$ qui ne se décompose pas dans* K. *Alors, le groupe μ_p des racines p-ièmes de l'unité est contenu dans Θ. Plus précisément, soit $\sqrt{D}$ la racine carrée de partie imaginaire > 0 du discriminant de* K*; il vient :*

(i) *si p est inerte dans* K, *on a*

$$e^{48\pi i/p} = \theta(C, (1+p\sqrt{D}))/\theta(C, (1-p\sqrt{D})),$$

avec $C = C(1/p, \mathcal{O}) \in Cl(\mathfrak{p})$;

(ii) *si p est ramifié dans* K, *on a*

$$e^{48\pi ia/p} = \theta(C, (1+\sqrt{D}))/\theta(C, (1-\sqrt{D})),$$

avec $a = -D/p$ entier premier à p et $C = C(\sqrt{D}/p, \mathcal{O}) \in Cl(\mathfrak{p})$.

Démonstration. — Comme les nombres $\lambda = 1+p\sqrt{D}$ et $\lambda' = 1-p\sqrt{D}$ (resp. $\lambda = 1+\sqrt{D}$ et $\lambda' = 1-\sqrt{D}$) sont conjugués, ils ont même norme. Par suite, le quotient $\theta(C, (\lambda))/\theta(C, (\lambda'))$ est égal à

$$\frac{\theta((1/p)-\sqrt{D}, \mathcal{O})}{\theta((1/p)+\sqrt{D}, \mathcal{O})}$$

(resp. $\theta((\sqrt{D}/p)-(D/p), \mathcal{O})/\theta((\sqrt{D}/p)+(D/p), \mathcal{O})$).

Il suffit alors d'utiliser la formule de transformation des fonctions thêta (*cf.* [28], formule (2), § 1).

Le théorème 12 (iv) a pour autre conséquence le lemme suivant.

LEMME 18. — *Soient k et $\mathfrak{a}$ comme dans le corollaire* 13. *Pour tout $\gamma \in \mathcal{G}$ et tout idéal entier $\mathfrak{b}$ de* K *premier à $\mathfrak{p}$ tel que $\gamma = (\mathfrak{b}, H/K)$, on a*

$$\varphi_k(\theta(C_0, \mathfrak{a})^\gamma) \equiv 12\, G_k^*(\mathfrak{a}, \mathfrak{b}^{-1}L) \pmod{\mathfrak{p}(H_0)}.$$

Démonstration. — Allions le lemme 6 au théorème 12 (iv), il vient

$$\varphi_k(\theta(C_0, \mathfrak{a})^\gamma) \equiv 12(G_k^*(\mathfrak{ab}, L) - N(\mathfrak{a})\, G_k^*(\mathfrak{b}, L)) \pmod{\mathfrak{p}(H_0)}.$$

La congruence annoncée résulte alors de l'identité

$$G_k^*(\mathfrak{a}, \mathfrak{b}^{-1}L) = G_k^*(\mathfrak{ab}, L) - N(\mathfrak{a})\, G_k^*(\mathfrak{b}, L). \quad (10) \qquad \square$$

En particulier, dans le lemme précédent, supposons $\mathfrak{b}$ principal. Soit $\beta \in \mathcal{O}$ un générateur de $\mathfrak{b}$. Si $g = ((\beta), H/K)$, on déduit du lemme 18 la congruence

$$\varphi_k(\theta(C_0, \mathfrak{a})^g) \equiv 12\, \beta^k G_k^*(\mathfrak{a}, L) \pmod{\mathfrak{p}(H_0)},$$

d'où $\varphi_k(\theta(C_0, \mathfrak{a})^g) = \sigma^k(g)\, \varphi_k(\theta(C_0, \mathfrak{a}))$ pour tous $g \in G$. Comme, d'après le lemme 6, les $\theta(C_0, \mathfrak{a})$, lorsque $\mathfrak{a}$ décrit les idéaux entiers de K premiers à $6\,\mathfrak{p}$, engendrent le sous-groupe Ψ de $H^\times$, ceci prouve que (iv) du théorème 12 implique (iii) pour tous les éléments u de Ψ.

Son noyau contenant $H^{\times p}$, l'application φ_k définit un homomorphisme, encore noté φ_k, de $H^\times/H^{\times p}$ dans $\varkappa$. Considérons le sous-groupe

$$\Psi^{(p)} = \Psi/\Psi \cap H^{\times p}$$

de $H^\times/H^{\times p}$. Son image par φ_k est $\varphi_k(\Psi)$, et l'action de $\mathscr{G}$ fait de $\Psi^{(p)}$ un $\mathbf{F}_p[\mathscr{G}]$-module.

Supposons $k \neq N(\mathfrak{p})-1$. Pour tout élément α de $\mathcal{O}_\mathfrak{p}(H_0)$ notons $[\alpha] \in \varkappa$ sa classe modulo $\mathfrak{p}(H_0)$. D'après le théorème 12 (iv), les classes $[G_k^*(\mathfrak{a}, L)]$, lorsque $\mathfrak{a}$ décrit les idéaux entiers de K premiers à 6 $\mathfrak{p}$, engendrent $\varphi_k(\Psi)$ sur $\mathbf{F}_p$. Définissons une action de $\mathscr{G}$ sur $\varphi_k(\Psi)$, compatible avec sa structure $\mathbf{F}_p$-linéaire, en posant

$$[G_k^*(\mathfrak{a}, L)]^\gamma = [G_k^*(\mathfrak{a}, \mathfrak{b}^{-1}L)] \tag{11}$$

pour tout élément γ de $\mathscr{G}$ et tout idéal entier $\mathfrak{b}$ de K premier à $\mathfrak{p}$ tel que $\gamma = (\mathfrak{b}, H/K)$. Comme le théorème 12 (i) nous assure que le noyau de φ_k est stable par $\mathscr{G}$, il résulte du lemme 18 que cette action de $\mathscr{G}$ sur $\varphi_k(\Psi)$ est bien définie : c'est l'unique action qui fait de la restriction de φ_k à $\Psi^{(p)}$ un $\mathbf{F}_p[\mathscr{G}]$-homomorphisme.

Soit χ un caractère irréductible de G sur $\mathbf{F}_p$. Considérons un élément u de $H^\times/H^{\times p}$. D'après le théorème 12 (iii), pour tout entier j divisible par e, $e \leqq j \leqq N(\mathfrak{p})-1$, on a

$$\varphi_j(1_\chi . u) = (\#\, G)^{-1} \Big(\sum_{g \in G} \sigma^j(g)\chi(g^{-1}) \Big) \varphi_j(u).$$

Si le produit scalaire de σ^j et χ est nul, c'est-à-dire si $\sum_{g \in G} \sigma^j(g)\chi(g^{-1}) = 0$, nous avons donc $\varphi_j(1_\chi . u) = 0$. Ceci prouve le lemme suivant.

LEMME 19. — *Soit χ un caractère irréductible de* G *sur* $\mathbf{F}_p$. *Distinguons suivant le degré de χ :*

(i) *si $\chi = \sigma^k$, $e \leqq k \leqq N(\mathfrak{p})-1$, $e \mid k$, l'image de $\Psi_\chi^{(p)}$ par φ_j est $\{0\}$, à moins que $j = k$;*

(ii) *si $\chi = \sigma^k + \sigma^{p(k)}$, $0 < k < N(\mathfrak{p})-1$, $e \mid k$, l'image de $\Psi_\chi^{(p)}$ par φ_j est $\{0\}$, à moins que $j = k$ ou $j = p(k)$.*

DÉFINITION 20. — *Nous notons $\mathscr{L}_\chi$ l'image de $\Psi_\chi^{(p)}$ par φ.*

Selon que $\chi = \sigma^k$ *ou* $\chi = \sigma^k + \sigma^{p(k)}$, il résulte du lemme précédent que $\mathscr{L}_\chi$ est $\mathbf{F}_p$-isomorphe à $\varphi_k(\Psi)$ ou $(\varphi_k, \varphi_{p(k)})(\Psi)$. Si $\chi \neq 1$, c'est-à-dire si $k \neq N(\mathfrak{p})-1$, nous pouvons munir $\varphi_k(\Psi)$ ou $(\varphi_k, \varphi_{p(k)})(\Psi)$, et par suite $\mathscr{L}_\chi$, de la structure de $\mathbf{F}_p[\mathscr{G}]$-module définie par l'identité (11) et par l'identité analogue où k est remplacé par $p(k)$. De cette manière, la restriction de φ à $\Psi_\chi^{(p)}$ devient un $\mathbf{F}_p[\mathscr{G}]$-homomorphisme.

D'après le théorème 12 (iii), toujours selon le degré de χ, l'action d'un élément g de G sur $\varphi_k(\Psi)$ ou sur $(\varphi_k, \varphi_{p(k)})(\Psi)$, est respectivement la multiplication par $\sigma^k(g)$ ou par $(\sigma^k(g), \sigma^{p(k)}(g))$. De plus, l'application $g \mapsto \sigma^k(g)$ définit par $\mathbf{F}_p$-linéarité un isomorphisme de $\mathbf{F}_p[G]_\chi$ sur $\mathbf{F}_p$ (si $\chi = \sigma^k$) ou sur $\mathcal{O}/\mathfrak{p}$ (si $\chi = \sigma^k + \sigma^{p(k)}$); dans ce dernier cas $\mathcal{O}/\mathfrak{p}$ est bien sûr une extension de degré 2 de $\mathbf{F}_p$, et l'isomorphisme conjugué de $\mathbf{F}_p[G]_\chi$ sur $\mathcal{O}/\mathfrak{p}$ est induit par l'application $g \mapsto \sigma^{p(k)}(g)$. Par suite, si $\chi = \sigma^k$, la structure de $\mathbf{F}_p[G]_\chi$-espace vectoriel de $\mathscr{L}_\chi$ n'est autre que sa structure $\mathbf{F}_p$-linéaire, et si

$\chi = \sigma^k + \sigma^{p^{(k)}}$, la structure de $\mathbf{F}_p[G]_\chi$-espace vectoriel de $\mathscr{L}_\chi$ est isomorphe à la structure $(\mathcal{O}/\mathfrak{p})$-linéaire *tordue* de $(\varphi_k, \varphi_{p^{(k)}})(\Psi)$ définie par

$$\lambda(u, v) = (\lambda u, \lambda^p v) \tag{12}$$

pour tous $\lambda \in \mathcal{O}/\mathfrak{p}$ et $(u, v) \in (\varphi_k, \varphi_{p^{(k)}})(\Psi)$.

Soient $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ des idéaux entiers de K premiers à $6\mathfrak{p}$, qui forment un système complet de représentants du groupe de classes d'idéaux de K. A partir des nombres $G_k(\mathfrak{a}_i^{-1} L)$, $1 \leqq i \leqq h$, $0 < k < N(\mathfrak{p}) - 1$, $k \equiv 0 \pmod{e}$, nous allons décrire une famille finie de générateurs effectivement calculables pour chacun des espaces $\mathscr{L}_\chi$, $\chi \neq 1$. Distinguons trois cas :

(*a*) χ est degré 1 et $\chi \neq \nu$;

(*a'*) $\chi = \nu$;

(*b*) χ est de degré 2.

Comme ν est de degré 1, ces trois cas s'excluent mutuellement. Soit k comme dans le lemme 19, $k \neq N(\mathfrak{p}) - 1$. Comme l'homomorphisme $\alpha \mapsto \alpha^k$ de $(\mathcal{O}/\mathfrak{p})^\times$ dans lui-même est le composé de l'application de réciprocité $\alpha \mapsto ((\alpha), H/K)$ et de σ^k, il vient :

Remarque 21. — *Pour que* χ *vérifie* (*a*) *ou* (*a'*), *c'est-à-dire pour que le degré de* χ *soit* 1, *il faut et il suffit que l'homomorphisme* $\alpha \mapsto \alpha^k$ *applique* $(\mathcal{O}/\mathfrak{p})^\times$ *dans* $\mathbf{F}_p^\times$.

En premier lieu, selon que χ est de degré 1 ou 2, rappelons que les classes des nombres $G_k^*(\mathfrak{a}, L)$ modulo $\mathfrak{p}(H_0)$ ou des couples $(G_k^*(\mathfrak{a}, L), G_{p^{(k)}}^*(\mathfrak{a}, L))$ modulo $\mathfrak{p}(H_0) \times \mathfrak{p}(H_0)$, lorsque $\mathfrak{a}$ décrit les idéaux entiers de K premiers à $6\mathfrak{p}$, engendrent respectivement $\varphi_k(\Psi)$ ou $(\varphi_k, \varphi_{p^{(k)}})(\Psi)$ sur $\mathbf{F}_p$. Soient $\mathfrak{a}$ et $\alpha\mathfrak{a}$ deux idéaux entiers de K, avec α élément non nul de K. Considérons l'identité

$$G_k^*(\alpha\mathfrak{a}, L) = \alpha^k G_k^*(\mathfrak{a}, L) + N(\mathfrak{a})(\alpha^k - N(\alpha)) G_k(L), \tag{13}$$

et, si χ vérifie (*b*), l'identité analogue (13') où k est remplacé par $p(k)$. Notons que $G_j^*((1), L) = 0$ pour tout entier $j \geqq 2$ divisible par e. Si χ vérifie (*a*) ou (*a'*) l'identité (13), avec $\mathfrak{a} = (1)$, prouve que la classe de $(\alpha^k - N(\alpha)) G_k(L)$ modulo $\mathfrak{p}(H_0)$ appartient à $\varphi_k(\Psi)$ pour tout élément α de $\mathcal{O}$ premier à $6\mathfrak{p}$. De même, si χ vérifie (*b*), les identités (13) et (13'), avec $\mathfrak{a} = (1)$, prouvent que la classe de

$$((\alpha^k - N(\alpha)) G_k(L), (\alpha^{p^{(k)}} - N(\alpha)) G_{p^{(k)}}(L)) \text{ modulo } \mathfrak{p}(H_0) \times \mathfrak{p}(H_0)$$

appartient à $(\varphi_k, \varphi_{p^{(k)}})(\Psi)$ pour tout élément α de $\mathcal{O}$ premier à $6\mathfrak{p}$.

Si $\chi \neq \nu$, d'après la démonstration du corollaire 14 (i), nous pouvons choisir un tel α de façon que $\alpha^k - N(\alpha) \not\equiv 0 \pmod{\mathfrak{p}}$. De plus, d'après la remarque 21, dans le cas (*a*), la classe de $\alpha^k - N(\alpha)$ modulo $\mathfrak{p}$ appartient à $\mathbf{F}_p$; et, dans le cas (*b*), comme $(k) \equiv pk \pmod{p^2 - 1}$, les classes de $\alpha^k - N(\alpha)$ et $\alpha^{p^{(k)}} - N(\alpha)$ modulo $\mathfrak{p}$ sont des éléments conjugués de $\mathcal{O}/\mathfrak{p}$. Par suite, si χ vérifie (*a*), la classe du nombre $G_k(L)$ appartient au $\mathbf{F}_p$-espace vectoriel $\varphi_k(\Psi)$, et, si χ vérifie (*b*), la classe du couple $(G_k(L), G_{p^{(k)}}(L))$

appartient au $(\mathcal{O}/\mathfrak{p})$-espace vectoriel $(\varphi_k, \varphi_{p\,(k)})(\Psi)$, sa structure $(\mathcal{O}/\mathfrak{p})$-linéaire étant bien sûr celle définie par (12). Considérons alors l'identité

$$G_k(\mathfrak{a}^{-1}L) = N(\mathfrak{a})\,G_k(L) + G_k^*(\mathfrak{a}, L), \tag{14}$$

et, si χ vérifie (*b*), l'identité analogue (14′) où k est remplacé par $p\,(k)$. Compte tenu de ce qui précède, selon que χ vérifie (*a*) ou (*b*), la relation (14) ou les relations (14) et (14′) prouvent que les classes des nombres $G_k(\mathfrak{a}^{-1}L)$ ou des couples $(G_k(\mathfrak{a}^{-1}L), G_{p\,(k)}(\mathfrak{a}^{-1}L))$, lorsque $\mathfrak{a}$ décrit les idéaux entiers de K premiers à $6\,\mathfrak{p}$, engendrent respectivement $\varphi_k(\Psi)$ ou $(\varphi_k, \varphi_{p\,(k)})(\Psi)$ sur $\mathbf{F}_p$. Or, les séries d'Eisenstein G_k et $G_{p\,(k)}$ sont respectivement homogènes de poids $-k$ et $-p\,(k)$, *cf.* introduction formule (1). D'après la remarque 21, ceci implique que les classes des nombres $G_k(\mathfrak{a}_i^{-1}L)$ modulo $\mathfrak{p}(H_0)$ ou des couples $(G_k(\mathfrak{a}_i^{-1}L), G_{p\,(k)}(\mathfrak{a}_i^{-1}L))$ modulo $\mathfrak{p}(H_0)\times\mathfrak{p}(H_0)$, avec $1 \leqq i \leqq h$, engendrent respectivement $\varphi_k(\Psi)$ sur $\mathbf{F}_p$ ou $(\varphi_k, \varphi_{p\,(k)})(\Psi)$ sur $\mathcal{O}/\mathfrak{p}$.

Si $\chi = \nu$, la remarque 21 et l'identité (13), avec $\mathfrak{a} = \mathfrak{a}_i$ pour $1 \leqq i \leqq h$, prouvent que $\varphi_k(\Psi)$ est engendré sur $\mathbf{F}_p$ par les classes modulo $\mathfrak{p}(H_0)$ des nombres $G_k^*(\mathfrak{a}_i^{-1}L)$, avec $2 \leqq i \leqq h$, et $(\alpha^k - N(\alpha))\,G_k(L)$, où α décrit les éléments de $\mathcal{O}$ premiers à $6\,\mathfrak{p}$. D'après le lemme 15, l'espace $\varphi_k(\Psi)$ est donc engendré sur $\mathbf{F}_p$ par les classes des nombres $G_k^*(\mathfrak{a}_i, L)$, avec $2 \leqq i \leqq h$, et $\pi\,G_k(L)$, où π décrit $\mathfrak{p}$.

Nous pouvons résumer ceci dans la proposition suivante.

PROPOSITION 22. — *Soit χ un caractère irréductible de* G *sur* $\mathbf{F}_p$, $\chi \neq 1$. *Alors, pour* $p \notin T$, *on a :*

Cas (*a*). *L'espace* $\mathscr{L}_\chi \simeq \varphi_k(\Psi)$ *est engendré sur* $\mathbf{F}_p$ *par les* h *classes* $[G_k(\mathfrak{a}_i^{-1}L)]$, $1 \leqq i \leqq h$.

Cas (*a*′). *L'espace* $\mathscr{L}_\chi \simeq \varphi_k(\Psi)$ *est engendré sur* $\mathbf{F}_p$ *par les classes* $[\pi\,G_k(L)]$, *où* π *décrit* $\mathfrak{p}$, *et par les* $h-1$ *classes* $[G_k^*(\mathfrak{a}_i, L)]$, $2 \leqq i \leqq h$.

Cas (*b*). *L'espace* $\mathscr{L}_\chi \simeq (\varphi_k, \varphi_{p\,(k)})(\Psi)$ *est engendré sur* $\mathcal{O}/\mathfrak{p}$ *par les* h *couples de classes* $([G_k(\mathfrak{a}_i^{-1}L)], [G_{p\,(k)}(\mathfrak{a}_i^{-1}L)])$, $1 \leqq i \leqq h$.

En particulier, si $\chi \neq \nu$ et $\neq 1$, la proposition précédente fournit un système de h générateurs de $\mathscr{L}_\chi$ sur $\mathbf{F}_p[G]_\chi$. Si $\chi = \nu$, d'après la proposition 16, les classes $[\pi\,G_k(L)]$, lorsque π parcourt $\mathfrak{p}$, forment un $\mathbf{F}_p$-espace vectoriel de dimension 1 ou 2, selon que p est ramifié ou inerte dans K. Par suite, si $\chi = \nu$, la proposition 22 (*a*′) nous fournit, selon que p est ramifié ou inerte dans K, un système de h ou $h+1$ générateurs de $\mathscr{L}_\chi$ sur $\mathbf{F}_p[G]_\chi$.

De plus la formule (11), qui décrit l'action de $\mathscr{G}$ sur les espaces $\mathscr{L}_\chi$, $\chi \neq 1$, a pour conséquence la proposition suivante.

PROPOSITION 23. — *Soit χ comme dans la proposition* 22. *Soient γ un élément de $\mathscr{G}$ et $\mathfrak{b}$ un idéal entier de* K *premier à $\mathfrak{p}$ tel que* $\gamma = (\mathfrak{b}, H/K)$. *Alors, pour* $p \notin T$, *il vient :*

Cas (*a*). *Pour tout idéal entier $\mathfrak{a}$ de* K *premier à $\mathfrak{p}$, la classe* $[G_k(\mathfrak{a}^{-1}L)]$ *appartient à* $\mathscr{L}_\chi$ *et on a*

$$[G_k(\mathfrak{a}^{-1}L)]^\gamma = [G_k(\mathfrak{a}^{-1}\mathfrak{b}^{-1}L)].$$

Cas (a'). *Pour tout élément* π *de* $\mathfrak{p}$, *la classe* $[\pi G_k(L)]$ *appartient à* $\mathscr{L}_\gamma$ *et on a*

$$[\pi G_k(L)]^\gamma = [\pi G_k(\mathfrak{b}^{-1}L)].$$

Cas (b). *Pour tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $\mathfrak{p}$, *le couple* $([G_k(\mathfrak{a}^{-1}L)], [G_{p(k)}(\mathfrak{a}^{-1}L)])$ *appartient à* $\mathscr{L}_\chi$ *et on a*

$$([G_k(\mathfrak{a}^{-1}L)], [G_{p(k)}(\mathfrak{a}^{-1}L)])^\gamma = ([G_k(\mathfrak{a}^{-1}\mathfrak{b}^{-1}L)], [G_{p(k)}(\mathfrak{a}^{-1}\mathfrak{b}^{-1}L)]).$$

Si $\Theta = \Psi \cap \mathscr{E}$ désigne le groupe des unités elliptiques de H, posons

$$\Theta^{(p)} = \Theta/\Theta \cap \mathscr{E}^p = \Theta/\Theta \cap H^{\times p}.$$

C'est un sous-groupe de $\Psi^{(p)}$, stable par $\mathscr{G}$. Comme le montre le lemme suivant, les images par φ de $\Theta^{(p)}$ et $\Psi^{(p)}$ sont essentiellement identiques.

LEMME 24. — *Pour tout caractère irréductible* χ *de* G *sur* $\mathbf{F}_p$, $\chi \neq 1$, *on a*

$$\varphi(\Theta_\chi^{(p)}) = \varphi(\Psi_\chi^{(p)}) = \mathscr{L}_\chi.$$

Démonstration. — Supposons $\chi = \sigma^k$ (resp. $\chi = \sigma^k + \sigma^{p(k)}$), $0 < k < N(\mathfrak{p}) - 1$, $e \mid k$, et soit $\mathfrak{a}$ un idéal entier de K premier à $6\mathfrak{p}$. Il nous suffit de construire un élément ρ de Θ tel que

$$\varphi_k(\rho) = 12[G_k^*(\mathfrak{a}, L)]$$

(resp. $(\varphi_k, \varphi_{p(k)})(\rho) = 12([G_k^*(\mathfrak{a}, L)], [G_{p(k)}^*(\mathfrak{a}, L)])$).

Soit f_χ une application de G dans $\mathbf{Z}$ telle que

(α) Pour tout $g \in G$, $f_\chi(g) \equiv \chi(g) \pmod{p}$.

(β) $\sum_{g \in G} f_\chi(g) = 0$.

Une telle application existe car $\sum_{g \in G} \chi(g) = 0$, puisque $\chi \neq 1$. Posons

$$\rho = \prod_{g \in G} \theta(C_0, \mathfrak{a})^{f_\chi(g^{-1})g}.$$

D'après (β), on a $(\sum_{g \in G} f_\chi(g^{-1}))(N(\mathfrak{a}) - 1) = 0$; par suite, le nombre ρ appartient à Θ (*cf.* prop. 7). D'après (α) et le théorème 12 (iv), lorsque $j = k$ (resp. $j = k$ ou $j = p(k)$), on a

$$\varphi_j(\rho) = 12.\#G.[G_j^*(\mathfrak{a}, L)];$$

ce qui démontre le lemme, puisque $\#G$ est premier à p.

Soient M un sous-corps de H contenant K tel que $(H : M) \not\equiv 0 \pmod{p}$, et M_0 l'intersection de M avec H_0. Posons

$$\Theta^{(p)}(M) = \Theta(M)/\Theta(M) \cap \mathscr{E}(M)^p,$$

où $\Theta(M) = N_{H/M}\Theta$ désigne le groupe des unités elliptiques de M. Munissons $\Theta^{(p)}$ et $\Theta^{(p)}(M)$ de leur structure naturelle de $\mathbf{F}_p[\mathscr{G}]$-module.

D'une manière générale, pour tout $\mathbf{F}_p[\mathscr{G}]$-module $\mathscr{S}$ et tout caractère irréductible χ de G sur $\mathbf{F}_p$, la χ-composante $\mathscr{S}_\chi = 1_\chi.\mathscr{S}$ de $\mathscr{S}$ est un $\mathbf{F}_p[\mathscr{G}]$-module, sur lequel $\mathbf{F}_p[\mathscr{G}]$ agit à travers sa χ-composante $\mathbf{F}_p[\mathscr{G}]_\chi = 1_\chi.\mathbf{F}_p[\mathscr{G}]$ munie de la structure d'algèbre induite par celle de $\mathbf{F}_p[\mathscr{G}]$.

Notons $\mathrm{tr}_{H/M}$ l'élément de $\mathbf{F}_p[\mathscr{G}]$ défini par

$$\mathrm{tr}_{H/M} = (\#\, G(H/M))^{-1} \sum_{g \in G(H/M)} g.$$

On a $\mathrm{tr}_{H/M}.\Theta^{(p)} = \Theta(M)/\Theta(M) \cap \mathscr{E}^p$. Comme $(H : M) \not\equiv 0 \pmod{p}$, il vient $\Theta(M) \cap \mathscr{E}^p = \Theta(M) \cap \mathscr{E}(M)^p$, et par suite

$$\Theta^{(p)}(M) = \mathrm{tr}_{H/M}.\Theta^{(p)}.$$

De même, l'algèbre de groupe $\mathbf{F}_p[\mathscr{G}]$ étant commutative, on a, pour tout caractère irréductible χ de G sur $\mathbf{F}_p$,

$$\Theta^{(p)}(M)_\chi = \mathrm{tr}_{H/M}.\Theta^{(p)}_\chi. \tag{15}$$

Désignons par $\mathscr{K}$ le noyau de la restriction de φ à $\Theta^{(p)}$; d'après le théorème 12 (i), c'est un $\mathbf{F}_p[\mathscr{G}]$-module. Posons

$$\mathscr{L}(\chi, M) = \mathrm{tr}_{H/M}.\mathscr{L}_\chi.$$

Comme $\mathrm{tr}_{H/M}$ est un idempotent de $\mathbf{F}_p[\mathscr{G}]$, la multiplication par $\mathrm{tr}_{H/M}$ transforme toute suite exacte de $\mathbf{F}_p[\mathscr{G}]$-modules en une suite exacte. Par conséquent, d'après (15), le noyau de la restriction de φ à $\Theta^{(p)}(M)_\chi$ est $\mathrm{tr}_{H/M}.\mathscr{K}_\chi$, et, d'après le lemme 24, si $\chi \neq 1$, l'image de $\Theta^{(p)}(M)_\chi$ par φ est $\mathscr{L}(\chi, M)$. Ce qui prouve le lemme suivant.

LEMME 25. — *Soit χ un caractère irréductible de* G *sur* $\mathbf{F}_p$, $\chi \neq 1$. *Alors, l'application* φ *définit un* $\mathbf{F}_p[\mathscr{G}]_\chi$*-homomorphisme de* $\Theta^{(p)}(M)_\chi$ *sur* $\mathscr{L}(\chi, M)$ *dont le noyau est* $\mathrm{tr}_{H/M}.\mathscr{K}_\chi$.

Clairement le $\mathbf{F}_p[\mathscr{G}]$-module $\Theta^{(p)}(M)$ est un sous-module de

$$\Omega^{(p)}(M) = \Omega(M)/\Omega(M) \cap \mathscr{E}(M)^p,$$

où $\Omega(M) = \mu(M)\,\Theta(M)\,\mathscr{E}(M_0)$ est le groupe d'unités de M du théorème 8, paragraphe 1. Comme le montre le lemme suivant, seule la composante de $\Theta^{(p)}(M)$ fixée par G peut être distincte de celle de $\Omega^{(p)}(M)$.

LEMME 26. — *Soit χ comme dans le lemme 25, on a*

$$\Theta^{(p)}(M)_\chi = \Omega^{(p)}(M)_\chi.$$

Démonstration. — Comme $p \geqq 5$, si H contient le groupe μ_p des racines p-ièmes de l'unité, le nombre premier p n'est pas décomposé dans K. Par suite, d'après le lemme 17, si l'on a $\mu_p \subset M$, le groupe Θ, et donc $\Theta(M)$ car $(H : M) \not\equiv 0 \pmod{p}$, contient μ_p. Comme le corps H, de conducteur p, ne contient pas de racine de l'unité d'ordre p^2, on en déduit les inclusions

$$\mu(M) \subset \mu_0(M)\,\Theta(M) \subset \mathscr{E}(M)^p\,\Theta(M),$$

où $\mu_0(M)$ désigne le groupe des racines de l'unité de M d'ordre premier à p. Par conséquent $\Omega^{(p)}(M)$ est isomorphe au $\mathbf{F}_p[\mathscr{G}]$-module

$$A = \Theta(M)\mathscr{E}(M_0)/\Theta(M)\mathscr{E}(M_0) \cap \mathscr{E}(M)^p,$$

a priori intermédiaire entre $\Theta^{(p)}(M)$ et $\Omega^{(p)}(M)$. Considérons la suite exacte de $\mathbf{F}_p[\mathscr{G}]$-modules

$$\{0\} \to \mathscr{E}(M_0)/\mathscr{E}(M_0) \cap \mathscr{E}(M)^p \to A \to B \to \{0\},$$

où le quotient $B = \Theta(M)\mathscr{E}(M_0)/(\Theta(M)\mathscr{E}(M_0) \cap \mathscr{E}(M)^p)\mathscr{E}(M_0)$ est isomorphe au $\mathbf{F}_p[\mathscr{G}]$-module

$$\Theta(M)/\Theta(M) \cap \mathscr{E}(M_0)\mathscr{E}(M)^p.$$

Comme on a $\chi \neq 1$, la χ-composante de $\mathscr{E}(M_0)/\mathscr{E}(M_0) \cap \mathscr{E}(M)^p$ est $\{0\}$ puisque G agit trivialement sur $\mathscr{E}(M_0)$. Il s'ensuit que A_χ est isomorphe à B_χ, d'où

$$\Omega^{(p)}(M)_\chi \simeq (\Theta(M)/\Theta(M) \cap \mathscr{E}(M_0)\mathscr{E}(M)^p)_\chi,$$

c'est-à-dire que $\Omega^{(p)}(M)_\chi$ est isomorphe à un quotient de $\Theta^{(p)}(M)_\chi$. Comme $\Theta^{(p)}(M)$, dont la dimension sur $\mathbf{F}_p$ est finie, est déjà un sous-module de $\Omega^{(p)}(M)$, ceci prouve le lemme.

Dans les conditions des lemmes 25 et 26, l'application φ définit donc un $\mathbf{F}_p[\mathscr{G}]_\chi$-homomorphisme de $\Omega^{(p)}(M)_\chi$ sur $\mathscr{L}(\chi, M)$. Si $e(\chi, M)$, $t(\chi, M)$ et $l(\chi, M)$ désignent respectivement les dimensions de $\mathscr{E}^{(p)}(M)_\chi$, $\Omega^{(p)}(M)_\chi$ et $\mathscr{L}(\chi, M)$ sur $\mathbf{F}_p[G]_\chi$, on a alors, vu que $\Omega^{(p)}(M)$ est un sous-module de $\mathscr{E}^{(p)}(M)$,

$$l(\chi, M) \leqq t(\chi, M) \leqq e(\chi, M);$$

bien sûr ces trois nombres sont nuls si χ n'est pas un caractère de G_M. Supposons donc que χ soit un caractère irréductible de G_M, $\chi \neq 1$, et appelons *défaut de régularité* de l'extension M/M_0 pour χ, l'entier

$$\delta(\chi, M) = e(\chi, M) - l(\chi, M) \geqq 0.$$

On déduit de la suite exacte (9) le lemme suivant.

LEMME 27. — *Soit χ un caractère irréductible de G_M sur $\mathbf{F}_p$, $\chi \neq 1$. On a*

$$\dim_{\mathbf{F}_p[G]\chi} \mathscr{S}(M)_\chi \leqq \delta(\chi, M).$$

Le théorème suivant résulte alors de la proposition 10.

THÉORÈME 28. — *Soient $p \notin T$, et M un sous-corps de H contenant K tel que $(H : M) \not\equiv 0 \pmod p$. Alors, le quotient h_M/h_{M_0} est premier à p, si, pour tout caractère irréductible χ de $G_M = G(M/M_0)$ sur $\mathbf{F}_p$, $\chi \neq 1$, le défaut de régularité $\delta(\chi, M)$ de l'extension M/M_0 est nul.*

Appliquons ce théorème au corps $M = H$. Soit χ un caractère irréductible de $G = G_H$ sur $\mathbf{F}_p$, $\chi \neq 1$. D'après le lemme 11, selon que χ est différent de ν ou non, on a $e(\chi, H) = (H_0 : K) = h$ ou $e(\chi, H) = h+1$. D'autre part, si p se ramifie dans K, que χ soit égal à ν ou non, la proposition 22 fournit un système de h générateurs de $\mathscr{L}(\chi, H) = \mathscr{L}_\chi$ sur $\mathbf{F}_p$; on a donc $\delta(\nu, H) \geqq 1$ et le théorème 28 ne s'applique pas à H. Au contraire, si p ne se ramifie pas dans K, selon que χ est différent de ν ou non, la proposition 22 fournit un système de h ou $h+1$ générateurs de $\mathscr{L}(\chi, H) = \mathscr{L}_\chi$ sur $\mathbf{F}_p[G]_\chi$. Par suite, si p ne se ramifie pas dans K, l'entier $\delta(\chi, H)$ est nul si et seulement si le système de h (si $\chi \neq \nu$) ou $h+1$ (si $\chi = \nu$) générateurs de $\mathscr{L}_\chi$ fourni par la proposition 22 est libre sur $\mathbf{F}_p[G]_\chi$. Lorsque χ décrit les caractères irréductibles de G sur $\mathbf{F}_p$, $\chi \neq 1$, on reconnaît là les conditions A_k, A'_k ou B_k du théorème 1, qui correspondent respectivement au cas (*a*), (*a'*) ou (*b*) de la proposition 22. Nous avons ainsi démontré que le théorème 1 est équivalent au cas $M = H$ du théorème 28, et résulte donc des propriétés de l'application φ énoncées dans le théorème 12.

Plus généralement, supposons que M contienne H_0. Alors, pour tout caractère irréductible χ de G_M sur $\mathbf{F}_p$, on a

$$\mathscr{L}(\chi, M) = \mathrm{tr}_{H/M}\,\mathscr{L}_\chi = \mathscr{L}_\chi = \mathscr{L}(\chi, H);$$

en effet, chaque élément g du sous-groupe $G(H/M)$ de G agit trivialement sur $\mathscr{L}_\chi$, puisque χ est un caractère du quotient G_M de G par $G(H/M)$. Par suite, on a $l(\chi, M) = l(\chi, H)$ et donc $\delta(\chi, M) = \delta(\chi, H)$ puisque $e(\chi, M) = e(\chi, H)$ d'après le lemme 11. Comme on a $\sigma^k(G(H/M)) = \{1\}$ si et seulement si $(H : M)\,e$ divise k, le théorème 28 implique donc la généralisation suivante du théorème 1 aux sous-corps M de H contenant H_0.

THÉORÈME 29. — *Soient $p \notin T$ un nombre premier non ramifié dans* K (3), *et* M *un sous-corps de* H *contenant* H_0. *Alors, le quotient h_M/h_{M_0} est premier à p, si, pour chaque entier k divisible par* $(H : M)\,e$, *tel que* $0 < k < N(\mathfrak{p})-1$, *l'une des conditions* A_k, A'_k *ou* B_k *du théorème* 1 *est satisfaite.*

Enfin, vu le lemme 27, on peut se demander si, pour $\chi \neq 1$, l'entier $\delta(\chi, M)$ est égal à la dimension de $\mathscr{S}(M)_\chi$ sur $\mathbf{F}_p[G]_\chi$, ou, ce qui revient au même, si φ définit un isomorphisme de $\Omega^{(p)}(M)_\chi$ sur $\mathscr{L}(\chi, M)$. Ce n'est pas en général le cas. En effet, l'homomorphisme φ est de nature locale (*cf.* § 5). En particulier φ tue toutes les puissances p-ièmes locales; sa restriction à $\Omega^{(p)}(M)$ se factorise donc à travers le $\mathbf{F}_p[\mathscr{G}]$-module $\overline{\Omega}^{(p)}(M)$, quotient de $\Omega(M)$ par les éléments de $\Omega(M)$ qui sont des puissances p-ièmes locales (pour une définition précise de $\overline{\Omega}^{(p)}(M)$ se rapporter au paragraphe 6). On peut alors énoncer des

---

(3) *Si* $p \notin T$ *se ramifie dans* K, on a $H = H_0(\mu_p)$, et, pour chaque caractère irréductible χ de G sur $\mathbf{F}_p$, différent de $\nu = \sigma^2$ et de 1, on a $\delta(\chi, H) = 0$ si et seulement si le système de h générateurs de $\mathscr{L}(\chi, H) = \mathscr{L}_\chi$ sur $\mathbf{F}_p$, fourni par la proposition 22 (*a*), est libre. De plus, comme 2 et 3 sont les seuls nombres premiers ramifiés dans $\mathbf{Q}(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-3})$ et $p \geqq 5$, *on a* $K \neq \mathbf{Q}(\sqrt{-1})$ *et* $\neq \mathbf{Q}(\sqrt{-3})$, *d'où* $e = 2$. Par suite, *pour tout sous-corps strict* M *de* H *contenant* H_0, le théorème 28 implique :

Le quotient h_M/h_{H_0} est premier à p, si, pour chaque entier k divisible par 2 $(H : M)$, *tel que* $0 < k < p-1$, *les h classes* $[G_k(\mathfrak{a}_i^{-1} L)]$, $1 \leqq i \leqq h$, *sont* $\mathbf{F}_p$*-linéairement indépendantes.*

conditions sur χ, toujours vérifiées si p se décompose dans K, qui assurent que φ définit un isomorphisme de $\bar{\Omega}^{(p)}(M)_\chi$ sur $\mathscr{L}(\chi, M)$ (*cf.* cor. 51, th. 50); mais le noyau de la projection de $\Omega^{(p)}(M)_\chi$ sur $\bar{\Omega}^{(p)}(M)_\chi$ n'est pas toujours trivial (*cf.* appendice B).

4. Généralisation aux corps intermédiaires

Dans ce paragraphe, nous transformons le théorème 28 de façon à l'énoncer en termes d'invariants, indépendants du corps intermédiaire M, et construits à partir des nombres de Hurwitz $G_k(\mathfrak{a}^{-1}L)$. L'idée d'introduire ces invariants est due à J.-P. Serre.

Soit $p \notin T$, et supposons le nombre de classes h de K premier à p. Choisissons une clôture algébrique $\tilde{\mathbf{F}}_p$ de $\mathcal{O}/\mathfrak{p}$. Comme $\#\mathscr{G} = h.\#G$ est premier à p, l'algèbre de groupe $\tilde{\mathbf{F}}_p[\mathscr{G}]$ est semi-simple. Le groupe $\mathscr{G}$ étant commutatif et le corps $\tilde{\mathbf{F}}_p$ algébriquement clos, les caractères irréductibles ω de $\mathscr{G}$ sur $\tilde{\mathbf{F}}_p$ sont les homomorphismes de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ en nombre $\#\mathscr{G}$. Lorsque ω décrit ces homomorphismes, les sommes

$$1_\omega = (\#\mathscr{G})^{-1} \sum_{\gamma \in \mathscr{G}} \omega(\gamma^{-1})\gamma$$

forment un système primitif d'idempotents orthogonaux de $\tilde{\mathbf{F}}_p[\mathscr{G}]$, et on a

$$1 = \sum_\omega 1_\omega .$$

Les ω-composantes $1_\omega.\tilde{\mathbf{F}}_p[\mathscr{G}]$ de $\tilde{\mathbf{F}}_p[\mathscr{G}]$ sont des corps isomorphes à $\tilde{\mathbf{F}}_p$. Un $\tilde{\mathbf{F}}_p[\mathscr{G}]$-module $\mathscr{T}$ étant donné, on définit sa ω-composante $\mathscr{T}_\omega$ par $\mathscr{T}_\omega = 1_\omega.\mathscr{T}$. On a

$$\mathscr{T} = \bigoplus_\omega \mathscr{T}_\omega .$$

Comme 1_ω est un idempotent de $\tilde{\mathbf{F}}_p[\mathscr{G}]$, l'algèbre $\tilde{\mathbf{F}}_p[\mathscr{G}]$ agit sur $\mathscr{T}_\omega$ à travers sa ω-composante $1_\omega.\tilde{\mathbf{F}}_p[\mathscr{G}] \simeq \tilde{\mathbf{F}}_p$, et la multiplication par 1_ω transforme toute suite exacte de $\tilde{\mathbf{F}}_p[\mathscr{G}]$-modules en une suite exacte de $\tilde{\mathbf{F}}_p$-espaces vectoriels.

Notons $k(\omega)$ l'unique entier divisible par e, $e \leqq k(\omega) \leqq N(\mathfrak{p})-1$, tel que $\sigma^{k(\omega)}$ coïncide avec la restriction de ω à G. Pour tout caractère irréductible χ de G sur $\tilde{\mathbf{F}}_p$, la χ-composante $\mathscr{T}_\chi = 1_\chi.\mathscr{T}$ de $\mathscr{T}$ est un $\tilde{\mathbf{F}}_p[\mathscr{G}]$-module, sur lequel $\tilde{\mathbf{F}}_p[\mathscr{G}]$ agit à travers sa χ-composante $\tilde{\mathbf{F}}_p[\mathscr{G}]_\chi = 1_\chi.\tilde{\mathbf{F}}_p[\mathscr{G}]$ munie de la structure d'algèbre induite par celle de $\tilde{\mathbf{F}}_p[\mathscr{G}]$. La ω-composante de $\mathscr{T}_\chi$ est $\{0\}$, à moins que le couple (ω, χ) ne vérifie l'une des deux conditions suivantes, que nous notons $\omega \mid \chi$.

(i) L'image de G par $\sigma^{k(\omega)}$ est contenue dans $\mathbf{F}_p$, et $\chi = \sigma^{k(\omega)}$.

(ii) L'image de G par $\sigma^{k(\omega)}$ n'est pas contenue dans $\mathbf{F}_p$, et $\chi = \sigma^{k(\omega)} + (\sigma^{k(\omega)})^p$.

On a alors

$$\mathscr{T}_\chi = \bigoplus_{\omega \mid \chi} \mathscr{T}_\omega ,$$

ou ω décrit les homomorphismes de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tels que $\omega \mid \chi$.

A partir des modules $\mathscr{L}_\chi$ du paragraphe 3, posons

$$\mathscr{L} = \bigoplus_{\chi \neq 1} \mathscr{L}_\chi,$$

où la somme porte sur tous les caractères irréductibles $\chi \neq 1$ de G sur $\mathbf{F}_p$; c'est un $\mathbf{F}_p[\mathscr{G}]$-module, dont les $\mathscr{L}_\chi$, $\chi \neq 1$, sont les χ-composantes. Soit $\tilde{\mathscr{L}} = \tilde{\mathbf{F}}_p \otimes \mathscr{L}$ le $\tilde{\mathbf{F}}_p[\mathscr{G}]$-module déduit de $\mathscr{L}$ par extension des scalaires de $\mathbf{F}_p$ à $\tilde{\mathbf{F}}_p$. Le lemme suivant est trivial.

LEMME 30. — *Soient ω_1 et ω_2 deux homomorphismes de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$, conjugués sur $\mathbf{F}_p$, c'est-à-dire tels qu'il existe un entier a pour lequel $\omega_2 = \omega_1^q$, avec $q = p^a$. Alors, les $\tilde{\mathbf{F}}_p$-espaces vectoriels $\tilde{\mathscr{L}}_{\omega_1}$ et $\tilde{\mathscr{L}}_{\omega_2}$ sont isomorphes.*

Soit M un sous-corps de H contenant K. Nous identifions de la manière usuelle le groupe des homomorphismes de $\mathscr{G}_M$ dans $\tilde{\mathbf{F}}_p$, au groupe des homomorphismes de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tels que $\omega(G(H/M)) = \{1\}$. Le lemme suivant ramène l'étude des espaces $\mathscr{L}(\chi, M)$, avec $\chi \neq 1$, à celle plus simple des $\tilde{\mathscr{L}}_\omega$; sa démonstration est immédiate.

LEMME 31. — *Pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_p$, on a*

$$\tilde{\mathbf{F}}_p \otimes \mathscr{L}(\chi, M) = \bigoplus_{\omega \mid \chi}^{(M)} \tilde{\mathscr{L}}_\omega,$$

où la somme est prise sur tous les homomorphismes ω de $\mathscr{G}_M$ dans $\tilde{\mathbf{F}}_p$ tels que $\omega \mid \chi$.

Naturellement, ce lemme ne s'applique pas au caractère unité $\chi = 1$ de G. En effet, la composante de $\mathscr{L}$ fixée par G est $\{0\}$, puisque l'on a exclu le caractère $\chi = 1$ de la somme définissant $\mathscr{L}$; on a donc $\tilde{\mathscr{L}}_\omega = \{0\}$ pour tout homomorphisme ω de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que $\omega \mid 1$.

Décrivons maintenant les $\tilde{\mathbf{F}}_p$-espaces vectoriels $\tilde{\mathscr{L}}_\omega$. Pour reconnaître leurs générateurs nous aurons besoin du lemme suivant.

LEMME 32. — *Soient N un $\tilde{\mathbf{F}}_p$-espace vectoriel contenu dans $\tilde{\mathscr{L}}$, et $n_\mathfrak{b} = n(\mathfrak{b}^{-1}L)$ (4), où $\mathfrak{b}$ décrit les idéaux entiers de K premiers à $\mathfrak{p}$, un système générateur de N sur $\tilde{\mathbf{F}}_p$.*

Soit ω un homomorphisme de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$, et supposons que les éléments $n(\mathfrak{b}^{-1}L)$ de N vérifient les identités :

$$\text{(i)} \qquad n(L)^\gamma = n(\mathfrak{b}^{-1}L);$$

$$\text{(ii)} \qquad n(\mathfrak{b}^{-1}L) = \omega(\gamma)\, n(L),$$

où $\gamma = (\mathfrak{b}, H/K)$.

Alors, l'espace N est engendré sur $\tilde{\mathbf{F}}_p$ par $n(L)$ et est stable par $\mathscr{G}$; de plus N est contenu dans $\tilde{\mathscr{L}}_\omega$.

---

(4) L'élément $n_\mathfrak{b} = n(\mathfrak{b}^{-1}L)$ ne dépend que de $\mathfrak{b}$, mais la notation $n(\mathfrak{b}^{-1}L)$ préfigure les quantités $\tilde{G}_\omega(\mathfrak{b}^{-1}L)$ et $[\pi G_k(\mathfrak{b}^{-1}L)]$ auxquelles nous appliquerons ce lemme.

Démonstration. — Que N soit engendré par $n(\mathrm{L})$, (resp. stable par $\mathscr{G}$) résulte clairement de (ii) (resp. (i)). En outre, si nous combinons (i) et (ii), il vient $n(\mathrm{L})^{\gamma} = \omega(\gamma)\, n(\mathrm{L})$ pour tout $\gamma \in \mathscr{G}$; par conséquent, on a $1_{\omega}.n(\mathrm{L}) = n(\mathrm{L})$, ce qui prouve que $n(\mathrm{L})$ appartient bien à $\tilde{\mathscr{L}}_{\omega}$. □

Soit k un entier divisible par e, $0 < k < \mathrm{N}(\mathfrak{p})-1$. Distinguons trois cas.

(α) L'image de G par σ^k est contenue dans $\mathbf{F}_p$, et $\sigma^k \neq \nu$.

(α') $\sigma^k = \nu$.

(β) L'image de G par σ^k n'est pas contenue dans $\mathbf{F}_p$.

Si k vérifie (α) ou (α'), posons $\chi = \sigma^k$. Si k vérifie (β), posons $\chi = \sigma^k + (\sigma^k)^p$. L'application χ est un caractère irréductible de G sur $\mathbf{F}_p$, qui vérifie la condition (*a*), (*a'*) ou (*b*) du paragraphe 3, p. 17 suivant que k vérifie (α), (α') ou (β) (*cf.* remarque 21). Soit ω un homomorphisme de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$, tel que $k(\omega) = k$.

Cas (α). Le $\mathbf{F}_p[\mathscr{G}]$-module $\mathscr{L}_{\chi}$ est alors isomorphe à $\varphi_k(\Psi)$; par suite $\tilde{\mathscr{L}}_{\omega}$ est isomorphe au produit $1_{\omega}.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$. Soit $\mathfrak{b}$ un idéal entier de K premier à $\mathfrak{p}$. D'après le corollaire 14 (i), le nombre $\mathrm{G}_k(\mathfrak{b}^{-1}\mathrm{L})$ est $\mathfrak{p}$-entier. Nous posons

$$\tilde{\mathrm{G}}_{\omega}(\mathfrak{b}^{-1}\mathrm{L}) = 1_{\omega}.1 \otimes \left[\mathrm{G}_k(\mathfrak{b}^{-1}\mathrm{L})\right];$$

c'est un élément de $1_{\omega}.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) \simeq \tilde{\mathscr{L}}_{\omega}$.

Cas (β). Le $\mathbf{F}_p[\mathscr{G}]$-module $\mathscr{L}_{\chi}$ est alors isomorphe à $(\varphi_k, \varphi_{p(k)})(\Psi)$; par suite $\tilde{\mathscr{L}}_{\omega}$ est isomorphe au produit

$$1_{\omega}.\tilde{\mathbf{F}}_p \otimes (\varphi_k, \varphi_{p(k)})(\Psi).$$

En fait, plutôt que de prendre le produit tensoriel sur $\mathbf{F}_p$ comme ci-dessus, nous pouvons le prendre sur $\mathcal{O}/\mathfrak{p}$. Plus précisément, désignons par

$$\tilde{\mathbf{F}}_p \otimes_{\mathcal{O}/\mathfrak{p}} (\varphi_k, \varphi_{p(k)})(\Psi)$$

le produit tensoriel sur $\mathcal{O}/\mathfrak{p}$, de la $\mathcal{O}/\mathfrak{p}$-algèbre $\tilde{\mathbf{F}}_p$ avec $(\varphi_k, \varphi_{p(k)})(\Psi)$, muni de la structure $\mathcal{O}/\mathfrak{p}$-linéaire « tordue » définie par (12). Considérons la surjection naturelle de $\tilde{\mathbf{F}}_p[\mathscr{G}]$-modules

$$1_{\omega}.\tilde{\mathbf{F}}_p \otimes (\varphi_k, \varphi_{p(k)})(\Psi) \to 1_{\omega}.\tilde{\mathbf{F}}_p \otimes_{\mathcal{O}/\mathfrak{p}} (\varphi_k, \varphi_{p(k)})(\Psi). \tag{16}$$

Son noyau est engendré sur $\tilde{\mathbf{F}}_p$ par les différences

$$1_{\omega}.(1 \otimes \alpha x) - 1_{\omega}.(\alpha \otimes x),$$

ou $\alpha \in \mathcal{O}/\mathfrak{p}$ et $x \in (\varphi_k, \varphi_{p(k)})(\Psi)$.

Or, comme k vérifie (β), l'ensemble $\sigma^k(\mathrm{G})$ est un système de générateurs de $\mathcal{O}/\mathfrak{p}$ sur $\mathbf{F}_p$. De plus, l'action d'un élément g de G sur $(\varphi_k, \varphi_{p(k)})(\Psi)$, muni de la structure $\mathcal{O}/\mathfrak{p}$-linéaire (12), est la multiplication par $\sigma^k(g)$. Par suite, le noyau en question est engendré sur $\tilde{\mathbf{F}}_p$ par les différences

$$1_{\omega}.(1 \otimes x^g) - 1_{\omega}.(\sigma^k(g) \otimes x),$$

où $g \in G$, soit encore

$$1_\omega.(1 \otimes x^g) - 1_\omega.(\omega(g) \otimes x) = (g\,1_\omega - \omega(g)\,1_\omega).(1 \otimes x).$$

Comme $\gamma\,1_\omega = \omega(\gamma)\,1_\omega$ pour tout $\gamma \in \mathscr{G}$, et donc pour tout $g \in G$, la surjection (16) est bien un isomorphisme.

Soit $\mathfrak{b}$ un idéal entier de K premier à $\mathfrak{p}$. D'après le corollaire 14 (i), les nombres $G_k(\mathfrak{b}^{-1}L)$ et $G_{p(k)}(\mathfrak{b}^{-1}L)$ sont $\mathfrak{p}$-entiers. Nous posons

$$\tilde{G}_\omega(\mathfrak{b}^{-1}L) = 1_\omega.1 \otimes_{\mathscr{O}/\mathfrak{p}}([G_k(\mathfrak{b}^{-1}L)], [G_{p(k)}(\mathfrak{b}^{-1}L)]);$$

c'est un élément de $1_\omega.\tilde{\mathbf{F}}_p \otimes_{\mathscr{O}/\mathfrak{p}} (\varphi_k, \varphi_{p(k)})(\Psi) \simeq \tilde{\mathscr{L}}_\omega$.

Ayant ainsi défini les nombres $\tilde{G}_\omega(\mathfrak{b}^{-1}L)$ pour tout homomorphisme ω de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que l'entier $k = k(\omega)$ vérifie (α) ou (β), nous pouvons facilement décrire les espaces $\tilde{\mathscr{L}}_\omega$ correspondants. En effet, selon que k vérifie (α) ou (β), la démonstration de la proposition 22 (*a*) ou (*b*) prouve que les nombres $\tilde{G}_\omega(\mathfrak{b}^{-1}L)$, lorsque $\mathfrak{b}$ décrit les idéaux entiers de K premiers à $\mathfrak{p}$, engendrent $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$ ou $1_\omega.\tilde{\mathbf{F}}_p \otimes_{\mathscr{O}/\mathfrak{p}} (\varphi_k, \varphi_{p(k)})(\Psi)$ sur $\tilde{\mathbf{F}}_p$; de plus, on déduit de la proposition 23 (*a*) ou (*b*) les identités

(i) $$\tilde{G}_\omega(L)^\gamma = \tilde{G}_\omega(\mathfrak{b}^{-1}L),$$

(ii) $$\tilde{G}_\omega(\mathfrak{b}^{-1}L) = \omega(\gamma)\,\tilde{G}_\omega(L),$$

où $\gamma = (\mathfrak{b}, H/K)$. Le lemme 32 prouve alors la proposition suivante.

PROPOSITION 33. — *Soient k un entier divisible par e, $0 < k < N(\mathfrak{p}) - 1$, et ω un homomorphisme de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que $k(\omega) = k$.*

Alors, selon que k vérifie (α) ou (β), le $\tilde{\mathbf{F}}_p$-espace vectoriel

$$1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) \simeq \tilde{\mathscr{L}}_\omega \qquad \text{ou} \qquad 1_\omega.\tilde{\mathbf{F}}_p \otimes_{\mathscr{O}/\mathfrak{p}} (\varphi_k, \varphi_{p(k)})(\Psi) \simeq \tilde{\mathscr{L}}_\omega$$

est engendré par $\tilde{G}_\omega(L)$.

Cas (α'). Le $\mathbf{F}_p[\mathscr{G}]$-module $\mathscr{L}_\nu$ est alors isomorphe à $\varphi_k(\Psi)$; par suite $\tilde{\mathscr{L}}_\omega$ est isomorphe au produit $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$.

Comme $\sigma^k = \nu$, le corps H contient le groupe μ_p. Notons ν l'homomorphisme de $\mathscr{G}$ dans $\mathbf{F}_p^\times$ défini par l'action de $\mathscr{G}$ sur μ_p; l'homomorphisme $\tilde{\nu}$ est déterminé par les congruences

$$\tilde{\nu}((\mathfrak{b}, H/K)) \equiv N(\mathfrak{b}) \pmod{p},$$

où $\mathfrak{b}$ désigne un idéal entier de K premier à $\mathfrak{p}$. Clairement ν est la restriction de ν à G; par suite, l'entier k coïncide avec $k(\tilde{\nu})$.

Soit $\pi \in \mathfrak{p}$. D'après le corollaire 14 (ii), pour tout idéal entier $\mathfrak{b}$ de K premier à $\mathfrak{p}$, le nombre $\pi\,G_k(\mathfrak{b}^{-1}L)$ est $\mathfrak{p}$-entier. Or, d'après les propositions 22 (a') et 23 (a'), la classe $[\pi\,G_k(\mathfrak{b}^{-1}L)]$ appartient à $\varphi_k(\Psi)$, et on a

(i) $$[\pi\,G_k(L)]^\gamma = [\pi\,G_k(\mathfrak{b}^{-1}L)],$$

où $\gamma = (\mathfrak{b}, H/K)$. De plus, d'après le corollaire 13, le nombre

$$G_k^*(\mathfrak{b}, L) = G_k(\mathfrak{b}^{-1}L) - N(\mathfrak{b})G_k(L)$$

est $\mathfrak{p}$-entier; par suite, on a

$$\text{(ii)} \qquad [\pi G_k(\mathfrak{b}^{-1}L)] = \tilde{\nu}(\gamma)[\pi G_k(L)].$$

D'après le lemme 32, ceci prouve :

LEMME 34. — *Soit k un entier divisible par e, $0 < k < N(\mathfrak{p})-1$, tel que $\sigma^k = \nu$, et soit $\pi \in \mathfrak{p}$.*

Alors, le nombre $1 \otimes [\pi G_k(L)]$ appartient au $\tilde{\mathbf{F}}_p$-espace vectoriel

$$1_{\tilde{\nu}}.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) = \tilde{\mathscr{L}}_{\tilde{\nu}}.$$

Poursuivons l'étude du cas (α'). Pour tout idéal entier $\mathfrak{b}$ de K premier à $\mathfrak{p}$, posons

$$\tilde{G}_\omega(\mathfrak{b}, L) = 1_\omega.1 \otimes [G_k^*(\mathfrak{b}, L)];$$

si $(\mathfrak{b}, 6\mathfrak{p}) = 1$, c'est donc un élément de $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) \simeq \tilde{\mathscr{L}}_\omega$. Dans la relation (10), substituons $\mathfrak{b}'$ à $\mathfrak{a}$; d'après (11), il vient

$$\text{(17)} \qquad \tilde{G}_\omega(\mathfrak{b}\mathfrak{b}', L) = N(\mathfrak{b}')\tilde{G}_\omega(\mathfrak{b}, L) + \omega((\mathfrak{b}, H/K))\tilde{G}_\omega(\mathfrak{b}', L).$$

Supposons d'abord $\omega = \nu$. On déduit de (17) l'identité

$$\text{(18)} \qquad \tilde{G}_{\tilde{\nu}}(\mathfrak{b}^p, L) = pN(\mathfrak{b})^{p-1}\tilde{G}_{\tilde{\nu}}(\mathfrak{b}, L) = 0.$$

Or, comme $h \not\equiv 0 \pmod{p}$, nous pouvons choisir un système complet de représentants du groupe de classes d'idéaux de K de la forme $\mathfrak{a}_i = \mathfrak{b}_i^p$, $1 \leqq i \leqq h$, où les $\mathfrak{b}_i$ sont des idéaux entiers de K premiers à $6\,\mathfrak{p}$ et $\mathfrak{b}_1 = (1)$. D'après le lemme 34 et la proposition 22 (a'), l'espace $1_{\tilde{\nu}}.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$ est engendré sur $\tilde{\mathbf{F}}_p$ par les nombres $1 \otimes [\pi G_k(L)]$, où π parcourt $\mathfrak{p}$, et $\tilde{G}_{\tilde{\nu}}(\mathfrak{a}_i, L)$, $2 \leqq i \leqq h$; ces derniers sont nuls d'après (18). De plus, la dimension du $\tilde{\mathbf{F}}_p$-espace vectoriel engendré par les nombres $1 \otimes [\pi G_k(L)]$, lorsque π parcourt $\mathfrak{p}$, est 1 ou 2 suivant que p est ramifié ou inerte dans K (*cf.* prop. 16). Ceci prouve la proposition suivante.

PROPOSITION 35. — *Soit k comme dans le lemme* 34. *Le $\tilde{\mathbf{F}}_p$-espace vectoriel $1_{\tilde{\nu}}.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) \simeq \tilde{\mathscr{L}}_{\tilde{\nu}}$ est engendré par les nombres $1 \otimes [\pi G_k(L)]$, lorsque π décrit $\mathfrak{p}$. Sa dimension est 1 si p est ramifié dans* K, *et 2 si p est inerte dans* K.

Supposons maintenant $\omega \neq \tilde{\nu}$. D'après (17), on a

$$\text{(19)} \qquad (\omega - \tilde{\nu})((\mathfrak{b}_0, H/K))\tilde{G}_\omega(\mathfrak{b}, L) = (\omega - \tilde{\nu})((\mathfrak{b}, H/K))\tilde{G}_\omega(\mathfrak{b}_0, L),$$

pour tout couple d'idéaux entiers $\mathfrak{b}_0$ et $\mathfrak{b}$ de K premiers à $\mathfrak{p}$. Or, par construction, les nombres $\tilde{G}_\omega(\mathfrak{b}, L)$, lorsque $\mathfrak{b}$ décrit les idéaux entiers de K premiers à $6\,\mathfrak{p}$, engendrent

l'espace $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$ sur $\tilde{\mathbf{F}}_p$. Soit $\mathfrak{b}_0$ tel que $(\omega - \tilde{\nu})((\mathfrak{b}_0, H/K)) \neq 0$; un tel idéal existe car $\omega \neq \nu$. L'identité (19) montre alors que $\tilde{G}_\omega(\mathfrak{b}_0, L)$ engendre $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi)$ sur $\tilde{\mathbf{F}}_p$. Ce qui prouve :

PROPOSITION 36. — *Soient $k = k(\tilde{\nu})$, et ω un homomorphisme de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que $k(\omega) = k$, $\omega \neq \tilde{\nu}$. Soit $\mathfrak{b}_0$ un idéal entier de K, premier à 6 $\mathfrak{p}$, tel que*

$$(\omega - \tilde{\nu})((\mathfrak{b}_0, H/K)) \neq 0.$$

Alors, le $\tilde{\mathbf{F}}_p$-espace vectoriel $1_\omega.\tilde{\mathbf{F}}_p \otimes \varphi_k(\Psi) \simeq \tilde{\mathscr{L}}_\omega$ est engendré par $\tilde{G}_\omega(\mathfrak{b}_0, L)$.

Comme dans le théorème 28, soit M un sous-corps de H contenant K, et χ un caractère irréductible de G_M sur $\mathbf{F}_p$, $\chi \neq 1$. Notons $\deg \chi$ le degré du caractère χ. Nous cherchons une expression du défaut $\delta(\chi, M)$, où apparaissent les dimensions des $\tilde{\mathbf{F}}_p$-espaces vectoriels $\tilde{\mathscr{L}}_\omega$. D'après le lemme 31, on a

$$l(\chi, M)\deg\chi = \dim_{\mathbf{F}_p} \mathscr{L}(\chi, M) = {}^{(M)}\sum_{\omega \mid \chi} \dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_\omega,$$

où la somme est prise sur tous les homomorphismes ω de G_M dans $\tilde{\mathbf{F}}_p$ tels que $\omega \mid \chi$. Ces homomorphismes sont au nombre de $(M_0 : K)\deg\chi$; par suite, il vient, d'après la définition de $\delta(\chi, M)$ et l'identité précédente,

$$\begin{aligned}\delta(\chi, M)\deg\chi &= (e(\chi, M) - l(\chi, M))\deg\chi \\ &= (M_0 : K)\deg\chi - l(\chi, M)\deg\chi \\ &= {}^{(M)}\sum_{\omega \mid \chi} (1 - \dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_\omega),\end{aligned}$$

chaque fois que $e(\chi, M) = (M_0 : K)$, soit, d'après le lemme 11, chaque fois que M et χ vérifient l'une ou l'autre des deux conditions suivantes :

(i) $\chi \neq \nu$;

(ii) ν n'est pas un homomorphisme de $\mathscr{G}_M$ — autrement dit M ne contient pas μ_p — et $\chi = \nu$.

Si l'on a $\mu_p \subset M$ et $\chi = \nu$, alors, d'après le lemme 11, l'entier $e(\nu, M)$ est égal à $(M_0 : K)+1$, et il vient

$$\begin{aligned}\delta(\nu, M) &= e(\nu, M) - l(\nu, M) \\ &= (M_0 : K) + 1 - l(\nu, M) \\ &= 2 - \dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_{\tilde{\nu}} + {}^{(M)}\sum_{\substack{\omega \mid \nu \\ \omega \neq \tilde{\nu}}} (1 - \dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_\omega).\end{aligned}$$

D'après la proposition 33, si χ est différent de ν, alors, pour tout homomorphisme ω de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que $\omega \mid \chi$, l'entier $1 - \dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_\omega$ vaut 0 ou 1; il vaut 1 si et seulement si $\tilde{\mathscr{L}}_\omega = \{0\}$, c'est-à-dire si $\tilde{G}_\omega(L) = 0$. D'après la proposition 36, si $\chi = \nu$, alors, pour

tout homomorphisme ω de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$ tel que $\omega \mid \nu$, $\omega \neq \tilde{\nu}$, l'entier $1-\dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_\omega$ vaut 0 ou 1; il vaut 1 si et seulement si $\tilde{\mathscr{L}}_\omega = \{0\}$, c'est-à-dire si $\tilde{G}_\omega(\mathfrak{b}_0, L) = 0$, où $\mathfrak{b}_0$ désigne un idéal entier de K, premier à $6\mathfrak{p}$, tel que

$$(\omega - \tilde{\nu})((\mathfrak{b}_0, H/K)) \neq 0.$$

Enfin, d'après la proposition 35, l'entier $2-\dim_{\tilde{\mathbf{F}}_p} \tilde{\mathscr{L}}_{\tilde{\nu}}$ vaut 0 ou 1 selon que p est inerte ou ramifié dans K.

Ceci prouve le théorème suivant.

THÉORÈME 37. — *Soient $p \notin T$ tel que $h \not\equiv 0 \pmod{p}$, et M un sous-corps de H contenant K. Alors, si χ est un caractère irréductible de $G_M = G(M/M_0)$ sur $\mathbf{F}_p$, $\chi \neq 1$, le produit*

$$\delta(\chi, M) \deg \chi$$

est égal au nombre d'homomorphismes ω de $\mathscr{G}_M$ dans $\tilde{\mathbf{F}}_p$ tels que

$$\omega \mid \chi \qquad et \qquad \tilde{\mathscr{L}}_\omega = \{0\},$$

augmenté d'une unité lorsque les trois conditions suivantes sont vérifiées :

(i) *p se ramifie dans K;*

(ii) *M contient μ_p;*

(iii) *$\chi = \nu$.*

En particulier, lorsque ces trois conditions sont vérifiées, le défaut $\delta(\chi, M)$ n'est pas nul.

Combinons ceci avec le théorème 28, il vient :

THÉORÈME 38. — *Soient p et M comme dans le théorème 36. Alors, le quotient h_M/h_{M_0} est premier à p, si les deux conditions suivantes sont vérifiées :*

(i) *Pour tout homomorphisme ω de $\mathscr{G}_M$ dans $\tilde{\mathbf{F}}_p$ tel que*

$$\omega \neq \tilde{\nu} \qquad et \qquad \omega(G_M) \neq \{1\},$$

l'espace $\tilde{\mathscr{L}}_\omega$ est non nul; autrement dit, selon que $\omega \mid \nu$ ou non, l'invariant $\tilde{G}_\omega(\mathfrak{b}_0, L)$ (resp. $\tilde{G}_\omega(L)$) de la proposition 35 (resp. 32) est non nul.

(ii) *Lorsque p se ramifie dans K, le corps M ne contient pas μ_p.*

5. Construction de dérivées logarithmiques tronquées

Introduisons d'abord quelques notations. Soit N une extension algébrique finie de K, d'anneau des entiers $\mathcal{O}(N)$. Pour tout idéal premier $\mathfrak{q}$ de N, nous notons $\mathcal{O}_\mathfrak{q}(N)$ le localisé de $\mathcal{O}(N)$ en $\mathfrak{q}$. L'anneau

$$\mathcal{O}_\mathfrak{p}(N) = \bigcap_{\mathfrak{q} \mid \mathfrak{p}} \mathcal{O}_\mathfrak{q}(N)$$

est l'anneau des éléments $\mathfrak{p}$-entiers de N. Nous notons $\mathfrak{p}(N)$ l'intersection des idéaux maximaux des anneaux locaux $\mathcal{O}_\mathfrak{q}(N)$, $\mathfrak{q} \mid \mathfrak{p}$; c'est un idéal de $\mathcal{O}_\mathfrak{p}(N)$.

Supposons N contenu dans H_0. Comme l'extension N/K est alors non ramifiée, on a $\mathfrak{p}(N) = \mathfrak{p}\,\mathcal{O}_\mathfrak{p}(N)$ en accord avec la notation introduite pour les corps K et H_0. Pour tout idéal premier $\mathfrak{q}$ de N au-dessus de $\mathfrak{p}$, nous notons $\mathfrak{D}_\mathfrak{q}(N)$ le complété $\mathfrak{q}$-adique de $\mathcal{O}_\mathfrak{q}(N)$ et $\mathfrak{m}_\mathfrak{q}(N)$ (resp. $N_\mathfrak{q}$) l'idéal maximal (resp. le corps des fractions) de $\mathfrak{D}_\mathfrak{q}(N)$. Le corps résiduel $\mathfrak{D}_\mathfrak{q}(N)/\mathfrak{m}_\mathfrak{q}(N)$ s'identifie naturellement à $\mathcal{O}(N)/\mathfrak{q}$.

Enfin, considérons l'algèbre $\varkappa = \mathcal{O}_\mathfrak{p}(H_0)/\mathfrak{p}(H_0)$. L'application diagonale de $\mathcal{O}_\mathfrak{p}(H_0)$ dans $\prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{D}_\mathfrak{q}(H_0)$ induit la décomposition suivante de $\varkappa$ en produit de facteurs locaux

$$\varkappa = \mathcal{O}_\mathfrak{p}(H_0)/\mathfrak{p}(H_0) \simeq \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathcal{O}(H_0)/\mathfrak{q}. \tag{20}$$

Nous allons étudier certaines lois de groupes formels attachées à l'équation (0). Étant donné une loi de groupe formel $\mathscr{F}$, définie par une série formelle de deux variables à coefficients dans l'anneau des entiers $\mathfrak{D}$ d'une extension algébrique du corps $\mathbf{Q}_p$ des nombres p-adiques, nous notons $\mathscr{F}(\mathfrak{m})$ le groupe obtenu en munissant l'idéal maximal $\mathfrak{m}$ de $\mathfrak{D}$ de la loi de groupe $\mathscr{F}$.

Soit $t = -2\,x/y$. C'est un paramètre local au point à l'infini de la courbe (0). Comme montré dans [34] (th. 4-2, p. 42), nous avons des développements en séries formelles

$$x = t^{-2}\,a(t), \qquad y = -2\,t^{-3}\,a(t),$$

où $a(t)$ est une série formelle entière en t, à coefficients dans $\mathcal{O}_\mathfrak{p}(H_0)$ et de terme constant 1. De plus, la loi de groupe sur E définit une série formelle de deux variables $A(t_1, t_2)$, à coefficients dans $\mathcal{O}_\mathfrak{p}(H_0)$, telle que

$$\begin{cases} A(t_1, t_2) \equiv t_1 + t_2 \,(\mathrm{mod}\,\deg 2), \\ A(t_1, A(t_2, t_3)) = A(A(t_1, t_2), t_3). \end{cases}$$

Par suite, pour tout idéal premier $\mathfrak{q}$ de H_0 au-dessus de $\mathfrak{p}$, la série $A(t_1, t_2)$ définit une loi de groupe formel sur l'anneau des entiers $\mathfrak{D}_\mathfrak{q}(H_0)$ du corps p-adique $H_{0,\mathfrak{q}}$ complété de H_0 en $\mathfrak{q}$. Notons cette loi $\mathscr{E}_\mathfrak{q}$. Soit $\overline{\mathfrak{D}}$ l'anneau des entiers d'une clôture algébrique $\overline{H}_{0,\mathfrak{q}}$ de $H_{0,\mathfrak{q}}$ et $\overline{\mathfrak{m}}$ son idéal maximal; comme l'équation (0) a bonne réduction modulo $\mathfrak{q}$, l'application

$$t \mapsto P_t = (t^{-2}\,a(t),\ -2\,t^{-3}\,a(t))$$

définit un isomorphisme de $\mathscr{E}_\mathfrak{q}(\overline{\mathfrak{m}})$ sur le groupe $E_{1,\mathfrak{q}}$ des points de $E(\overline{H}_{0,\mathfrak{q}})$, dont la réduction modulo $\overline{\mathfrak{m}}$ est le point à l'infini de la courbe elliptique réduite. Nous notons $P \mapsto t(P)$ l'isomorphisme de $E_{1,\mathfrak{q}}$ sur $\mathscr{E}_\mathfrak{q}(\overline{\mathfrak{m}})$, inverse de l'isomorphisme précédent.

Rappelons d'abord deux lemmes bien connus, mais pour lesquels nous ne connaissons pas de référence appropriée. Soient $\mathfrak{D}_\mathfrak{p}$ le complété $\mathfrak{p}$-adique de l'anneau des entiers $\mathcal{O}$ de K et $\mathfrak{m}_\mathfrak{p}$ son idéal maximal.

A tout $\lambda \in \mathfrak{D}_\mathfrak{p}$ correspond un endomorphisme de $\mathscr{E}_\mathfrak{q}$ défini sur $\mathfrak{D}_\mathfrak{q}(H_0)$, c'est-à-dire une série formelle $[\lambda]_\mathfrak{q}(t)$, à coefficients dans $\mathfrak{D}_\mathfrak{q}(H_0)$, telle que

$$\begin{cases} [\lambda]_\mathfrak{q}(t) \equiv \lambda t \pmod{\deg 2}, \\ A([\lambda]_\mathfrak{q}(t_1), [\lambda]_\mathfrak{q}(t_2)) = [\lambda]_\mathfrak{q}(A(t_1, t_2)). \end{cases}$$

Soit α un élément de $\mathscr{E}_\mathfrak{q}(\overline{\mathfrak{m}})$. Si λ appartient à $\mathscr{O}$, on a

$$[\lambda]_\mathfrak{q}(\alpha) = t(\lambda.P_\alpha), \tag{21}$$

où $\lambda.P_\alpha$ désigne l'image du point $P_\alpha \in E_{1,\mathfrak{q}}$ par l'endomorphisme λ de E. De plus, si $(\lambda_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathfrak{D}_\mathfrak{p}$ de limite λ, on a

$$\lim_{n\to\infty} [\lambda_n]_\mathfrak{q}(\alpha) = [\lambda]_\mathfrak{q}(\alpha).$$

Or, si P_α appartient au groupe $E_\mathfrak{p}^{(\mathfrak{q})}$ des points de $\mathfrak{p}$-torsion de $E(\overline{H}_{0,\mathfrak{q}})$, le produit $\lambda.P_\alpha$ ne dépend que de la classe de λ modulo $\mathfrak{p}$. Par conséquent, il vient :

LEMME 39. — *Soient* $\alpha \in \overline{\mathfrak{m}}$ *et* $P \in E_\mathfrak{p}^{(\mathfrak{q})}$ *tels que* $\alpha = t(P)$. *Alors, pour tout élément* λ *de* $\mathfrak{D}_\mathfrak{p}$, *on a*

$$[\lambda]_\mathfrak{q}(\alpha) = t(\sigma.P), \tag{22}$$

où $\sigma \in \mathscr{O}/\mathfrak{p} = \mathfrak{D}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ *désigne la classe de* λ *modulo* $\mathfrak{m}_\mathfrak{p}$.

En fait, le groupe $E_\mathfrak{p}^{(\mathfrak{q})}$ est contenu dans $E_{1,\mathfrak{q}}$ [5]. Par suite, le noyau de la multiplication par $\mathfrak{m}_\mathfrak{p}$ sur $\mathscr{E}_\mathfrak{q}(\overline{\mathfrak{m}})$ est le groupe $t(E_\mathfrak{p}^{(\mathfrak{q})})$. Choisissons alors un générateur π de $\mathfrak{m}_\mathfrak{p}$ et appliquons le théorème de préparation de Weierstrass à la série $[\pi]_\mathfrak{q}(t)$. Il s'ensuit que les nombres $t(P)$, $P \in E_\mathfrak{p}^{(\mathfrak{q})}$, $P \neq 0$, sont les solutions d'une équation d'Eisenstein :

$$T^{N(\mathfrak{p})-1} + a_1 T^{N(\mathfrak{p})-2} + \ldots + a_{N(\mathfrak{p})-1} = 0, \tag{23}$$

---

[5] En voici une démonstration. On sait que $E(\overline{H}_{0,\mathfrak{q}})$ possède p^2 points de p-torsion, tandis que la courbe elliptique réduite en possède au plus p. Par suite, il existe un point $P \neq 0$ de $E_{1,\mathfrak{q}}$ tel que $p.P = 0$. Posons $\mathfrak{P} = \{\alpha \in \mathscr{O} \mid \alpha.P = 0\}$; c'est un idéal de $\mathscr{O}$ et on a

$$\mathfrak{P} \mid (p) \qquad \text{et} \qquad \mathfrak{P} \neq (1).$$

Comme $E_{1,\mathfrak{q}}$ est stable par $\mathscr{O}$, le groupe $\mathscr{O}.P$ est contenu dans $E_{1,\mathfrak{q}}$. Montrons que $\mathfrak{p}$ divise $\mathfrak{P}$; il en résulte alors que $E_\mathfrak{p}^{(\mathfrak{q})}$ est contenu dans $\mathscr{O}.P$, d'où l'inclusion $E_\mathfrak{p}^{(\mathfrak{q})} \subset E_{1,\mathfrak{q}}$ que nous voulons prouver.

Si p est inerte dans k, on a $\mathfrak{P} = (p) = \mathfrak{p}$. Si p est ramifié dans k, on a $\mathfrak{P} = \mathfrak{p}$ ou $\mathfrak{p}^2$, et $\mathfrak{p}$ divise bien $\mathfrak{P}$. Considérons donc le cas où p est décomposé dans k, et prouvons l'identité $\mathfrak{P} = \mathfrak{p}$. Pour cela, il nous suffit de montrer que l'on a $(\mathfrak{P}, \mathfrak{p}') = (1)$, où $\mathfrak{p}'$ désigne l'idéal conjugué de $\mathfrak{p}$. Soit donc λ un élément de $\mathfrak{p}'$, premier à $\mathfrak{p}$, tel que $\lambda.P = 0$. D'après (21), on a alors

$$[\lambda]_\mathfrak{q}(t(P)) = t(\lambda.P) = 0;$$

comme λ est $\mathfrak{p}$-inversible, il en résulte l'identité $t(P) = 0$, ce qui est absurde et conclut la démonstration. □

où $a_i \in \mathfrak{m}_\mathfrak{q}(H_0)$ pour $1 \leqq i \leqq N(\mathfrak{p})-1$ et où $a_{N(\mathfrak{p})-1}$ engendre $\mathfrak{m}_\mathfrak{q}(H_0)$ dans $\mathfrak{D}_\mathfrak{q}(H_0)$ car $[\pi]_\mathfrak{q}(t) \equiv \pi t \pmod{\deg 2}$. Vu que le groupe $E_\mathfrak{p}^{(\mathfrak{q})}$, comme la courbe E, est défini sur H_0, les coefficients a_i sont des éléments de H_0 indépendants de $\mathfrak{q}$; ils appartiennent donc à $\mathfrak{p}(H_0)$ et $a_{N(\mathfrak{p})-1}$ engendre $\mathfrak{p}(H_0)$ dans $\mathcal{O}_\mathfrak{p}(H_0)$. Si $E_\mathfrak{p}$ désigne le groupe des points de $\mathfrak{p}$-torsion de E(C), et F l'extension de H_0 obtenue par adjonction des coordonnées des points de $E_\mathfrak{p}$, il résulte de l'irréductibilité de l'équation (23) que l'indice de ramification de $\mathfrak{q}$ dans F est divisible par $N(\mathfrak{p})-1 = \#(\mathcal{O}/\mathfrak{p})^\times$. Vu que l'action de $G(F/H_0)$ sur $E_\mathfrak{p}$ définit une injection $G(F/H_0)$ dans $(\mathcal{O}/\mathfrak{p})^\times$ (*cf.* § 2), il vient :

LEMME 40. — *Soit* $p \notin T$.

(i) *L'injection* σ, *définie par l'action de* $G(F/H_0)$ *sur* $E_\mathfrak{p}$, *applique* $G(F/H_0)$ *sur* $(\mathcal{O}/\mathfrak{p})^\times$.

(ii) *Chaque idéal premier* $\mathfrak{q}$ *de* H_0 *au-dessus de* $\mathfrak{p}$ *se ramifie totalement dans* F.

(iii) *Si le discriminant de l'équation* (0) *est* $\mathfrak{p}$-*inversible, alors, pour tout point* $P \neq 0$ *de* $E_\mathfrak{p}$, *le nombre* $t(P)$ *engendre* $\mathfrak{p}(F)$ *dans* $\mathcal{O}_\mathfrak{p}(F)$.

Soit $\mathfrak{q}$ un idéal premier de H_0 au-dessus de $\mathfrak{p}$. D'après le lemme 40 (ii), l'idéal $\mathfrak{q}$ se ramifie totalement dans F. Notons $F_\mathfrak{q}$ le complété $\mathfrak{q}$-adique de F, et désignons respectivement par $\mathfrak{D}_\mathfrak{q}(F)$ et $\mathfrak{m}_\mathfrak{q}(F)$ l'anneau des entiers de $F_\mathfrak{q}$ et son idéal maximal. La restriction de $F_\mathfrak{q}$ à F définit un isomorphisme du groupe de Galois $G(F_\mathfrak{q}/H_{0,\mathfrak{q}})$ sur $G(F/H_0)$ par lequel nous identifions ces deux groupes.

Pour chaque idéal premier $\mathfrak{q}$ de H_0 au-dessus de $\mathfrak{p}$, soit $\varphi_\mathfrak{q} = (\varphi_{k,\mathfrak{q}})_{1 \leqq k \leqq N(\mathfrak{p})-1}$ un homomorphisme de $F_\mathfrak{q}^\times$ dans le groupe additif de l'algèbre

$$(\mathcal{O}(H_0)/\mathfrak{p})^{N(\mathfrak{p})-1} = \underbrace{(\mathcal{O}(H_0)/\mathfrak{p}) \times \ldots \times (\mathcal{O}(H_0)/\mathfrak{p})}_{N(\mathfrak{p})-1 \text{ termes}}.$$

Nous associons aux $\varphi_\mathfrak{q}$, $\mathfrak{q} \mid \mathfrak{p}$, un homomorphisme φ de $H^\times$ dans $\varkappa^{(N(\mathfrak{p})-1)/e}$, défini de la manière suivante. Pour chaque entier k, $1 \leqq k \leqq N(\mathfrak{p})-1$, soit $\varphi_k = \prod_{\mathfrak{q} \mid \mathfrak{p}} \varphi_{k,\mathfrak{q}}$. D'après l'isomorphisme (20), l'application φ_k est un isomorphisme de $\prod_{\mathfrak{q} \mid \mathfrak{p}} F_\mathfrak{q}^\times$ dans $\prod_{\mathfrak{q} \mid \mathfrak{p}} \mathcal{O}(H_0)/\mathfrak{q} \simeq \varkappa$. Plongeons $H^\times$ dans $\prod_{\mathfrak{q} \mid \mathfrak{p}} F_\mathfrak{q}^\times$ par l'application diagonale, et considérons la restriction de φ_k à $H^\times$, encore notée φ_k. L'homomorphisme φ est alors défini par

$$\varphi = (\varphi_k)_{e \leqq k \leqq N(\mathfrak{p})-1,\, e \mid k}.$$

Bien sûr, nous devons maintenant construire des homomorphismes $\varphi_\mathfrak{q}$ comme ci-dessus. Pour cela considérons une uniformisante locale $\Lambda_\mathfrak{q}$ de $\mathfrak{D}_\mathfrak{q}(F)$, c'est-à-dire un générateur de $\mathfrak{m}_\mathfrak{q}(F)$. Nous définissons ici un homomorphisme $\varphi_{\Lambda_\mathfrak{q}} = (\varphi_{k,\Lambda_\mathfrak{q}})_{1 \leqq k \leqq N(\mathfrak{p})-1}$ de $F_\mathfrak{q}^\times$ dans $(\mathcal{O}(H_0)/\mathfrak{q})^{N(\mathfrak{p})-1}$. L'homomorphisme $\varphi_{\Lambda_\mathfrak{q}}$ dépend de l'uniformisante $\Lambda_\mathfrak{q}$; il nous faudra ensuite déterminer $\Lambda_\mathfrak{q}$, pour chaque idéal premier $\mathfrak{q}$ de H_0 au-dessus de $\mathfrak{p}$, de façon que l'homomorphisme φ associé aux $\varphi_\mathfrak{q} = \varphi_{\Lambda_\mathfrak{q}}$ vérifie le théorème 12.

Définissons d'abord $\varphi_{\Lambda_\mathfrak{q}}(u)$ lorsque u est une unité principale de $F_\mathfrak{q}$. Comme $u-1$ appartient à $\mathfrak{m}_\mathfrak{q}(F)$, il existe une série entière $f_u(T)$, non unique, à coefficients dans $\mathfrak{D}_\mathfrak{q}(H_0)$, de terme constant 1, telle que $f_u(\Lambda_\mathfrak{q}) = u$. Posons

$$T\frac{\partial}{\partial T}\log f_u(T) = \sum_{k=1}^{\infty} \alpha_k T^k, \qquad \alpha_k \in \mathfrak{D}_\mathfrak{q}(H_0).$$

D'après le lemme 40, l'extension F_q/H_q est totalement ramifiée de degré $N(\mathfrak{p})-1$; par suite, pour chaque entier k, $1 \leqq k \leqq N(\mathfrak{p})-1$, la classe de α_k modulo $\mathfrak{m}_q(H_0)$ ne dépend pas du choix de la série $f_u(T)$; nous notons cette classe $\varphi_{k,\Lambda_q}(u)$. On vérifie que l'application

$$u \mapsto \varphi_{k,\Lambda_q}(u)$$

est bien un homomorphisme du groupe des unités principales de F_q dans

$$\mathcal{O}(H_0)/\mathfrak{q} = \mathfrak{D}_q(H_0)/\mathfrak{m}_q(H_0).$$

Étendons maintenant φ_{Λ_q} à $F_q^\times$. On a $F_q^\times = \mathfrak{D}_q(F)^\times \times \langle \Lambda_q \rangle$, où $\langle \Lambda_q \rangle$ désigne le groupe multiplicatif engendré par Λ_q. De plus, $\mathfrak{D}_q(F)^\times$ est le produit direct du groupe des unités principales de F_q et du groupe des racines $(q-1)$-ièmes de l'unité de $H_{0,q}$, où q désigne le nombre d'éléments du corps résiduel $\mathcal{O}(H_0)/\mathfrak{q}$; en effet, ces racines de l'unité forment un système de représentants multiplicatifs de

$$(\mathfrak{D}_q(F)/\mathfrak{m}_q(F))^\times = (\mathcal{O}(H_0)/\mathfrak{q})^\times$$

dans $F_q^\times$. Par suite, si l'on pose

$$\varphi_{\Lambda_q}(\Lambda_q) = 0,$$

et, pour toute racine $(q-1)$-ième de l'unité ζ de $H_{0,q}$,

$$\varphi_{\Lambda_q}(\zeta) = 0,$$

l'application φ_{Λ_q} s'étend par multiplicativité à $F_q^\times$ tout entier, d'une manière et d'une seule. On a donc :

PROPOSITION 41. — *L'application φ_{Λ_q}, définie ci-dessus, est un homomorphisme de $F_q^\times$ dans le groupe additif de l'algèbre $(\mathcal{O}(H_0)/\mathfrak{q})^{N(\mathfrak{p})-1}$.*

Le lemme suivant résulte facilement de la définition de φ_{Λ_q}.

LEMME 42. — *Soient k un entier $\geqq 1$, et u une unité principale de F_q telle que*

$$u = 1 + \alpha \Lambda_q^k, \qquad \alpha \in \mathfrak{D}_q(H_0).$$

Alors, pour tout entier j tel que $1 \leqq j \leqq \inf(N(\mathfrak{p})-1, k-1)$, on a

$$\varphi_{j,\Lambda_q}(u) = 0;$$

de plus, si $k \leqq N(\mathfrak{p})-1$, on a

$$\varphi_{k,\Lambda_q}(u) \equiv k\alpha \pmod{\mathfrak{m}_q(H_0)}.$$

En particulier φ_{Λ_q} applique $1+\mathfrak{m}_q(F)^{N(\mathfrak{p})}$ sur $\{0\}$.

Avant de poursuivre donnons une conséquence de ce lemme. Posons $n = 1$ si p se décompose dans K, $n = 2$ si p se ramifie dans K et $n = p+1$ si p est inerte dans K. Si $p \notin T$ et si F_q contient une racine primitive p-ième de l'unité ζ (ce qui est toujours le cas si p

ne se décompose pas dans K, puisque H contient alors μ_p), il résulte du lemme 40 que l'entier n est égal à la valuation de $\zeta-1$ dans F_q. D'après le lemme 42, le nombre $\varphi_{n,\Lambda_q}(\zeta)$ est donc non nul. Ce qui prouve :

COROLLAIRE 43. — *Soient $p \notin T$ et $\zeta \in F_q^\times$ une racine p-ième de l'unité. Alors, on a $\varphi_{n,\Lambda_q}(\zeta) = 0$ si et seulement si $\zeta = 1$.*

Reprenons maintenant l'étude de $\mathscr{E}_q$. L'anneau $\mathfrak{D}_p$ contient le groupe $\mu_{N(p)-1}$ des racines $(N(p)-1)$-ièmes de l'unité. Par conséquent, d'après [19], lemme 4.1.2, il existe une série formelle

$$u_q(t) = t + \sum_{i \geqq 2} \beta_i t^i, \tag{24}$$

non unique, dont les coefficients β_i appartiennent à $\mathfrak{D}_q(H_0)$, telle que

$$u_q \circ [\zeta]_q(t) = \zeta u_q(t) \tag{25}$$

pour tout $\zeta \in \mu_{N(p)-1}$. Soit $A'_q(u_1, u_2)$ l'unique série formelle, à coefficients dans $\mathfrak{D}_q(H_0)$, telle que

$$A'_q(u_q(t_1), u_q(t_2)) = u_q(A(t_1, t_2));$$

nous notons $\mathscr{E}'_q$ la loi de groupe formel définie par $A'_q(u_1, u_2)$. Le développement (24), de u_q en série de puissances de t, est un isomorphisme, défini sur $\mathfrak{D}_q(H_0)$, de $\mathscr{E}_q$ sur $\mathscr{E}'_q$.

Par ailleurs, nous pouvons développer les fonctions $x(z) = \mathscr{P}(z, L)$ et

$$y(z) = \frac{\partial}{\partial z}\mathscr{P}(z, L)$$

en série de puissances de z. Par suite, le paramètre $t = -2\,x/y$ possède un développement en série formelle

$$t = g(z) = z + \sum_{i \geqq 2} \gamma_i z^i, \qquad \gamma_i \in H_0.$$

Ce développement peut être regardé comme un isomorphisme, défini sur $H_{0,q}$, de $\mathbf{G}_a$ sur $\mathscr{E}_q$, où $\mathbf{G}_a$ désigne la loi de groupe formel additif.

Désignons par $I(u_q)$ la série formelle

$$I(u_q) = u_q + \sum_{i \geqq 2} \delta_i u_q^i,$$

dont les coefficients δ_i appartiennent à $H_{0,q}$, telle que

$$I \circ u_q \circ g(z) = z. \tag{26}$$

La série formelle $I(u_q)$ est un isomorphisme, défini sur $H_{0,q}$, de $\mathscr{E}'_q$ sur $\mathbf{G}_a$. Comme $I(u_q) \equiv u_q \pmod{\deg 2}$, cet isomorphisme est l'application logarithme de $\mathscr{E}'_q$ (*cf.* [9], p. 96). On a :

LEMME 44. — *Pour tout $i \geqq 2$, le produit $i\delta_i$ appartient à $\mathfrak{D}_q(H_0)$. De plus, on a $\delta_i = 0$, à moins que $i \equiv 1 \pmod{N(p)-1}$.*

Démonstration. — Comme rappelé dans [8], lemme 7, le premier point est vrai pour l'application logarithme de n'importe quelle loi de groupe formel définie sur un anneau d'entiers p-adiques (*cf.* [9], p. 96).

Démontrons le second point. Soit $\zeta \in \mu_{N(\mathfrak{p})-1}$. D'après (26), on a

$$\zeta \mathrm{I} \circ u_\mathfrak{q} \circ g(z) = \zeta z = \mathrm{I} \circ u_\mathfrak{q} \circ g(\zeta z). \tag{27}$$

Par ailleurs, on a $[\zeta]_\mathfrak{q}(t) \equiv \zeta t \pmod{\deg 2}$ d'où $g(\zeta z) = [\zeta]_\mathfrak{q} \circ g(z)$, puisque $g(z)$ détermine un isomorphisme de $\mathbf{G}_a$ sur $\mathscr{E}_\mathfrak{q}$. On déduit alors de (25) l'identité

$$u_\mathfrak{q} \circ g(\zeta z) = \zeta u_\mathfrak{q} \circ g(z),$$

d'où, d'après (27),

$$\zeta \mathrm{I}(u_\mathfrak{q}) = \mathrm{I}(\zeta u_\mathfrak{q}).$$

Identifions les coefficients de $u_\mathfrak{q}^i$ dans chacun des deux membres de cette dernière identité, il vient $\zeta \delta_i = \zeta^i \delta_i$ pour tout $\zeta \in \mu_{N(\mathfrak{p})-1}$. Par suite, on a $\delta_i = 0$ si $i \not\equiv 1 \pmod{N(\mathfrak{p})-1}$. Le lemme est démontré.

Fixons un point τ de $\mathfrak{p}^{-1}\mathrm{L}$, $\tau \notin \mathrm{L}$, et soit $\mathrm{P} = \xi(\tau)$ le point de $\mathrm{E}_\mathfrak{p}$ image de τ par l'isomorphisme ξ de $\mathbf{C}/\mathrm{L}$ sur $\mathrm{E}(\mathbf{C})$. Pour chaque idéal premier $\mathfrak{q}$ de H_0 au-dessus de $\mathfrak{p}$, posons

$$\Lambda_\mathfrak{q} = u_\mathfrak{q}(t(\mathrm{P})). \tag{28}$$

D'après le lemme 40 (iii), le nombre $t(\mathrm{P})$ engendre $\mathfrak{m}_\mathfrak{q}(\mathrm{F})$; par suite, d'après (24), on a

$$u_\mathfrak{q}(t(\mathrm{P})) \equiv t(\mathrm{P}) \pmod{m_\mathfrak{q}(\mathrm{F})^2}.$$

Le nombre $\Lambda_\mathfrak{q}$ est donc une uniformisante de $\mathfrak{D}_\mathfrak{q}(\mathrm{F})$. Pour tout $g \in \mathrm{G}(\mathrm{F}/\mathrm{H}_0)$, notons $\zeta(g) \in \mathfrak{D}_\mathfrak{p}$ l'unique racine $(\mathrm{N}(\mathfrak{p})-1)$-ième de l'unité dont la classe résiduelle modulo $\mathfrak{m}_\mathfrak{p}$ est $\sigma(g)$. D'après la définition de σ, on a

$$\Lambda_\mathfrak{q}^g = u_\mathfrak{q}(t(\mathrm{P}^g)) = u_\mathfrak{q}(t(\sigma(g).\mathrm{P})),$$

d'où, d'après les identités (22) et (25),

$$\Lambda_\mathfrak{q}^g = u_\mathfrak{q} \circ [\zeta(g)]_\mathfrak{q}(t(\mathrm{P})) = \zeta(g)\Lambda_\mathfrak{q}, \tag{29}$$

pour tout $g \in \mathrm{G}(\mathrm{F}_\mathfrak{q}/\mathrm{H}_{0,\mathfrak{q}}) = \mathrm{G}(\mathrm{F}/\mathrm{H}_0)$.

Nous déduisons de (29) la proposition suivante :

PROPOSITION 45. — *Soit k un entier tel que $1 \leqq k \leqq \mathrm{N}(\mathfrak{p})-1$. Pour tous $u \in \mathrm{F}_\mathfrak{q}^\times$ et $g \in \mathrm{G}(\mathrm{F}/\mathrm{H}_0)$, on a*

$$\varphi_{k,\Lambda_\mathfrak{q}}(u^g) = \sigma^k(g)\varphi_{k,\Lambda_\mathfrak{q}}(u). \tag{30}$$

Démonstration. — Vu la multiplicativité en u de (30), il suffit de vérifier cette identité lorsque u est une unité principale de $\mathrm{F}_\mathfrak{q}$, ou bien un élément du groupe multiplicatif engendré par $\Lambda_\mathfrak{q}$ et par les racines de l'unité de $\mathrm{H}_{0,\mathfrak{q}}$ d'ordre $q-1$.

Ce dernier groupe, d'après (29), est stable par $G(F/H_0)$, et par définition son image par φ_{Λ_q} est $\{0\}$. Donc, si u est le produit d'une puissance de Λ_q par une racine $(q-1)$-ième de l'unité de $H_{0,q}$, les deux membres de (30) sont nuls.

Par ailleurs, soient u une unité principale de F_q et $f_u(T)$ une série entière, à coefficients dans $\mathfrak{D}_q(H_0)$, de terme constant 1, telle que $f_u(\Lambda_q) = u$. Il résulte alors de (29) que, pour tout $g \in G(F/H_0)$, on a $f_{u^g}(\Lambda_q) = u^g$, où $f_{u^g}(T)$ est la série entière, à coefficients dans $\mathfrak{D}_q(H_0)$, de terme constant 1, définie par

$$f_{u^g}(T) = f(\zeta(g)T).$$

L'identité (30), pour u unité principale de F_q, en résulte immédiatement; ce qui conclut la démonstration de la proposition.

Par ailleurs, il vient :

PROPOSITION 46. — *Soient* $\mathfrak{a}$ *un idéal entier de* K *premier à* $\mathfrak{p}$, *et* k *un entier divisible par* e *tel que* $0 < k < N(\mathfrak{p})-1$. *Alors, pour tous* $\tau \in \mathfrak{p}^{-1}L$ *et* $P \in E_{\mathfrak{p}}$ *tels que* $P = \xi(\tau)$ *et* $\tau \notin L$, *on a*

$$\varphi_{k,\Lambda_q}(\theta(C_0, \mathfrak{a})) \equiv 12\, G_k^*(\mathfrak{a}, L) \pmod{\mathfrak{m}_q(H_0)},$$

avec $C_0 = C(\tau, L)$ *et* $\Lambda_q = u_q(t(P))$.

Démonstration. — Posons $\delta = \Delta(L)^{N(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1}L)$; c'est un élément de H_0. En effet, d'après [16] (chap. 12, th. 5), le quotient $\Delta(\mathfrak{a}^{-1}L)/\Delta(L)$ engendre l'idéal $\mathfrak{a}^{12}\mathcal{O}(H_0)$ de H_0, et d'autre part $\Delta(L)$ appartient à H_0 puisque les coefficients de l'équation (0) sont des éléments de H_0. Considérons la fonction elliptique $R_0(z) = \theta(z, L; \mathfrak{a})/\delta$. D'après (4), on a

$$R_0(z) = \prod_{\lambda \in \mathfrak{a}^{-1}L/L}{}' \frac{1}{\mathscr{P}(z, L)^6}\left(1 - \frac{\mathscr{P}(\lambda, L)}{\mathscr{P}(z, L)}\right)^{-6}.$$

Par suite, en posant $x(z) = \mathscr{P}(z, L)$, il vient

$$R_0(z) = R(x(z)),$$

où $R(x)$ désigne la fraction rationnelle de x, à coefficients dans H_0, définie par

$$R(x) = x^{-6(N(\mathfrak{a})-1)} \prod_{\lambda \in \mathfrak{a}^{-1}L/L}{}' (1 - \mathscr{P}(\lambda, L)x^{-1})^{-6}.$$

Comme $\mathfrak{a}$ est premier à $\mathfrak{p}$, les nombres $\mathscr{P}(\lambda, L)$ sont $\mathfrak{p}$-entiers, et l'on déduit de (24) et du développement $x^{-1} = t^2 a(t)^{-1}$, l'existence d'un développement

$$R_1(u_q) = u_q^{12(N(\mathfrak{a})-1)}\left(1 + \sum_{k \geq 1} b_k u_q^k\right) \tag{31}$$

de $R(x)$ en série formelle de u_q, dont les coefficients b_k appartiennent à $\mathfrak{D}_q(H_0)$. Donnons à u_q la valeur $\Lambda_q = u_q(t(P))$, avec $P = \xi(\tau)$; on obtient

$$R_1(\Lambda_q) = R(x(\tau)) = R_0(\tau) = \theta(\tau, L; \mathfrak{a})/\delta = \theta(C_0, \mathfrak{a})/\delta. \tag{32}$$

De plus, $R(x)$ possède un développement en série formelle de z, qui n'est autre que le développement

$$R_0(z) = z^{12(N(\mathfrak{a})-1)}(1+\sum_{k\geqq 1} b'_k z^k), \qquad b'_k \in H_0,$$

de $R_0(z) = R(x(z))$ en série de Taylor au point $z = 0$. Les séries $R_0(z)$ et $R_1(u_\mathfrak{q})$ sont liées par l'identité

$$R_1(u_\mathfrak{q}) = R_0(I(u_\mathfrak{q}));$$

autrement dit, $R_1(u_\mathfrak{q})$ se déduit de la série formelle $R_0(z)$ par la substitution $z = I(u_\mathfrak{q})$. D'après le lemme 44, il s'ensuit que $b'_k = b_k$ pour $0 < k < N(\mathfrak{p})-1$. On déduit alors de (6) la congruence

$$\begin{aligned} z\frac{\partial}{\partial z}\log\left(1+\sum_{k=1}^{N(\mathfrak{p})-2} b_k z^k\right) &\\ \equiv -12(N(\mathfrak{a})-1)+z\frac{\partial}{\partial z}\log\theta(z, L; \mathfrak{a}) &\\ \equiv 12\sum_{\substack{0<k<N(\mathfrak{p})-1 \\ e \mid k}} G_k^*(\mathfrak{a}, L)\, z^k \pmod{z^{N(\mathfrak{p})-1}}. & \end{aligned}$$

D'après (31) et (32), on a donc, pour tout entier k tel que $0 < k < N(\mathfrak{p})-1$,

$$\varphi_{k,\Lambda_\mathfrak{q}}(\theta(C_0, \mathfrak{a})/\delta) \equiv \begin{cases} 0 \pmod{\mathfrak{m}_\mathfrak{q}(H_0)}, & \text{si } k \not\equiv 0 \pmod e \\ 12\,G_k^*(\mathfrak{a}, L) \pmod{\mathfrak{m}_\mathfrak{q}(H_0)}, & \text{si } k \not\equiv 0 \pmod e \end{cases}$$

La proposition résulte alors de ce que $\varphi_{k,\Lambda_\mathfrak{q}}(\delta) = 0$, pour tout entier k tel que $0 < k < N(\mathfrak{p})-1$, comme le prouve le lemme suivant appliqué à l'élément $u = \delta$ de $N = H_{0,\mathfrak{q}}$.

LEMME 47. — *Soient* N *un sous-corps de* $F_\mathfrak{q}$ *contenant* $H_{0,\mathfrak{q}}$, *et n l'ordre du groupe de Galois* $G(F_\mathfrak{q}/N)$. *Alors, il vient :*

(i) $\Lambda_\mathfrak{q}^n$ *est une uniformisante de l'anneau des entiers de* N.

(ii) *Pour tout élément u de* $N^\times$ *et tout entier k*, $1 \leqq k \leqq N(\mathfrak{p})-1$, *tel que* $k \not\equiv 0 \pmod n$, *on a* $\varphi_{k,\Lambda_\mathfrak{q}}(u) = 0$.

Démonstration. — D'après (29), le nombre $\Lambda_\mathfrak{q}^n$ est fixé par tous les éléments de $G(F_\mathfrak{q}/N)$, c'est-à-dire que $\Lambda_\mathfrak{q}^n$ appartient à N. Ceci prouve (i), puisque l'extension $F_\mathfrak{q}/H_{0,\mathfrak{q}}$, et donc $F_\mathfrak{q}/N$, est totalement ramifiée.

Pour (ii), comme l'image par $\varphi_{\Lambda_\mathfrak{q}}$ du groupe multiplicatif engendré par $\Lambda_\mathfrak{q}^n$ et par les racines de l'unité de $H_{0,\mathfrak{q}}$ d'ordre $q-1$ est $\{0\}$, il suffit de prouver que $k \not\equiv 0 \pmod n$ implique $\varphi_{k,\Lambda_\mathfrak{q}}(u) = 0$ lorsque u est une unité principale de N et $1 \leqq k \leqq N(\mathfrak{p})-1$. D'après (i), il existe alors une série entière $g_u(T)$, à coefficients dans $\mathfrak{D}_\mathfrak{q}(H_0)$, de terme constant 1, telle que $g_u(\Lambda_\mathfrak{q}^n) = u$. Posons $f_u(T) = g_u(T^n)$, d'où $f_u(\Lambda_\mathfrak{q}) = u$. Comme

$$T\frac{\partial}{\partial T}\log f_u(T) = n\,T^n\left(\frac{\partial}{\partial T}\log g\right)(T^n),$$

on a bien $\varphi_{k,\Lambda_\mathfrak{q}}(u) = 0$ pour tout entier k tel que $k \not\equiv 0 \pmod{n}$, $1 \leqq k \leqq N(\mathfrak{p})-1$. Le lemme est démontré.

Le corollaire 43 et les propositions 45 et 46 prouvent que l'homomorphisme φ associé aux $\varphi_\mathfrak{q} = \varphi_{\Lambda_\mathfrak{q}}$, avec $\Lambda_\mathfrak{q} = u_\mathfrak{q}(t(P))$ où $P = \xi(\tau)$ est un élément non nul de $E_\mathfrak{p}$, répond aux conditions (ii), (iii) et (iv) du théorème 12, pour $C_0 = C(\tau, L)$.

Vérifions maintenant la condition (i). Soient $\mathfrak{q}$ un idéal premier de H_0 au-dessus de $\mathfrak{p}$, et γ un élément de $\mathscr{G}$. Notons $\mathfrak{q}^\gamma$ l'image de $\mathfrak{q}$ par γ. Désignons par $H_\mathfrak{q}$ le complété $\mathfrak{q}$-adique de H, et notons $\mathfrak{D}_\mathfrak{q}(H)$ l'anneau des entiers de $H_\mathfrak{q}$. D'après le lemme 47 (i), le nombre $\Gamma_\mathfrak{q} = \Lambda_\mathfrak{q}^e$ est une uniformisante de $\mathfrak{D}_\mathfrak{q}(H)$, et, d'après (29), on a, pour tout $g \in G$,

$$\Gamma_\mathfrak{q}^g = \zeta^e(g)\Gamma_\mathfrak{q}. \tag{33}$$

Considérons l'image $\Gamma_\mathfrak{q}^\gamma$ de $\Gamma_\mathfrak{q}$ par γ. Les nombres $\Gamma_\mathfrak{q}^\gamma$ et $\Gamma_{\mathfrak{q}^\gamma}$ sont des uniformisantes de $\mathfrak{D}_{\mathfrak{q}^\gamma}(H)$, et, d'après (33), on a, pour tout $g \in G$,

$$\begin{cases} (\Gamma_{\mathfrak{q}^\gamma})^g = \zeta^e(g)\Gamma_{\mathfrak{q}^\gamma}, \\ (\Gamma_\mathfrak{q}^\gamma)^g = \zeta^e(g)\Gamma_\mathfrak{q}^\gamma, \end{cases} \tag{34}$$

puisque le groupe $\mathscr{G}$ est commutatif. Notons $h(T) = \sum_{i \geqq 1} \eta_i T_i$ l'unique série entière, dont les coefficients η_i sont des racines $(q-1)$-ièmes de l'unité de $H_{0,\mathfrak{q}}$, telle que

$$\Gamma_\mathfrak{q}^\gamma = h(\Gamma_{\mathfrak{q}^\gamma}).$$

D'après (34), on a, pour tout $g \in G$,

$$\zeta^e(g)\,h(\Gamma_{\mathfrak{q}^\gamma}) = (\Gamma_\mathfrak{q}^\gamma)^g = h(\zeta^e(g)\Gamma_{\mathfrak{q}^\gamma}).$$

Les séries entières $\zeta^e(g)\,h(T)$ et $h(\zeta^e(g)\,T)$ prennent donc la même valeur pour $T = \Gamma_{\mathfrak{q}^\gamma}$. Comme leurs coefficients respectifs sont des racines $(q-1)$-ièmes de l'unité, ces séries sont égales, d'où, pour tout $g \in G$,

$$\zeta^e(g)\eta_i = \zeta^{ei}\eta_i, \qquad i \geqq 1.$$

On a donc $\eta_i = 0$, si $ei \not\equiv e \pmod{N(\mathfrak{p})-1}$. Par conséquent, il existe une unique racine $(q-1)$-ième de l'unité $\eta(\gamma, \mathfrak{q}) = \eta_1$ de $H_{0,\mathfrak{q}^\gamma}$ telle que

$$\frac{\Gamma_\mathfrak{q}^\gamma}{\Gamma_{\mathfrak{q}^\gamma}} \equiv \eta(\gamma, \mathfrak{b}) \pmod{\Lambda_{\mathfrak{q}^\gamma}^{N(\mathfrak{p})-1}}. \tag{35}$$

La racine $\eta(\gamma, \mathfrak{q})$ satisfait la proposition suivante.

PROPOSITION 48. — *Soient k un entier tel que $1 \leqq k \leqq N(\mathfrak{p})-1$, et u un élément de $F_\mathfrak{q}^\times$, qui vérifient l'une ou l'autre des deux conditions suivantes :*

(a) $u \in \mathfrak{D}_\mathfrak{q}(H)^\times$;

(b) $u \in F_\mathfrak{q}^\times$ *et* $k \neq N(\mathfrak{p})-1$.

Alors, on a

$$\varphi_{k,\Lambda_{q^\gamma}}(u^\gamma) = \eta(\gamma, \mathfrak{b})^{k/e}(\varphi_{k,\Lambda_q}(u))^\gamma. \tag{36}$$

Démonstration. — Notons d'abord que l'identité (36) a bien un sens; en effet, d'après le lemme 47 (ii), lorsque $k \not\equiv 0 \pmod{e}$ on a

$$\varphi_{k,\Lambda_q}(u) = \varphi_{k,\Lambda_{q^\gamma}}(u^\gamma) = 0,$$

et par suite les deux membres de (36) sont nuls. Ainsi, l'identité (36) ne dépend pas du choix de $\eta(\gamma, \mathfrak{q})^{1/e}$.

Observons ensuite que l'identité (36) est multiplicative en u. Par conséquent, pour démontrer cette identité dans le cas (*a*), il nous suffit de la vérifier lorsque u est une unité principale de $H_\mathfrak{q}$ ou bien une racine $(q-1)$-ième de l'unité de $H_{0,\mathfrak{q}}$. De même, pour démontrer (36) dans le cas (*b*), il nous suffit de vérifier cette identité lorsque $u = \Gamma_\mathfrak{q}$ et d'utiliser (*a*).

Soit donc u une racine $(q-1)$-ième de l'unité de $H_{0,\mathfrak{q}}$. Son image u^γ par γ est alors une racine $(q-1)$-ième de l'unité de $H_{0,\mathfrak{q}^\gamma}$. Par suite, on a

$$\varphi_{\Lambda_\mathfrak{q}}(u) = \varphi_{\Lambda_{\mathfrak{q}^\gamma}}(u^\gamma) = 0,$$

et (36) est vérifiée par u. Soit maintenant u une unité principale de $H_\mathfrak{q}$. Comme $\Gamma_\mathfrak{q}$ est une uniformisante de $\mathfrak{D}_\mathfrak{q}(H)$, il existe une série entière $g_1(T)$, à coefficients dans $\mathfrak{D}_\mathfrak{q}(H_0)$, de terme constant 1, telle que

$$g_1(\Gamma_\mathfrak{q}) = u.$$

Désignons par $g_1^\gamma(T)$ l'image de $g_1(T)$ par γ, et posons

$$g_2(T) = g_1^\gamma \circ h(T), \qquad g_2'(T) = g_1^\gamma(\eta(\gamma, \mathfrak{q})\, T).$$

On a

$$g_2(\Gamma_{\mathfrak{q}^\gamma}) = g_1^\gamma(h(\Gamma_{\mathfrak{q}^\gamma})) = g_1^\gamma(\Gamma_\mathfrak{q}^\gamma) = u^\gamma,$$

et, d'après (35),

$$g_2(\Gamma_{\mathfrak{q}^\gamma}) \equiv g_2'(\Gamma_{\mathfrak{q}^\gamma}) \pmod{\Lambda_{\mathfrak{q}^\gamma}^{N(\mathfrak{p})}}.$$

Posons $v = g_2'(\Gamma_{\mathfrak{q}^\gamma})$; c'est une unité principale de $H_\mathfrak{q}$, et, d'après ce qui précède, on a

$$u^\gamma \equiv v \pmod{\Lambda_{\mathfrak{q}^\gamma}^{N(\mathfrak{p})}}.$$

D'après le lemme 42, les nombres u^γ et v ont donc même image par $\varphi_{\Lambda_{\mathfrak{q}^\gamma}}$. Posons

$$f_u(T) = g_1(T^e) \qquad \text{et} \qquad f_v(T) = g_2'(T^e).$$

On a $f_u(\Lambda_\mathfrak{q}) = u$ et $f_v(\Lambda_{\mathfrak{q}^\gamma}) = v$; et les séries $f_u(T)$ et $f_v(T)$ sont liées par la relation

$$f_v(T) = f_u^\gamma(\eta(\gamma, \mathfrak{q})^{1/e} T), \tag{37}$$

où f_u^γ désigne l'image de f_u par γ. La relation (37) implique l'identité

$$\varphi_{k,\Lambda_{\mathfrak{q}^\gamma}}(v) = \eta(\gamma, \mathfrak{q})^{k/e}(\varphi_{k,\Lambda_\mathfrak{q}}(u))^\gamma,$$

qui est (36) puisque u^γ et v ont même image par $\varphi_{\Lambda_{\mathfrak{q}^\gamma}}$, comme nous l'avons déjà noté. Ce qui prouve (*a*).

Pour en déduire (*b*), il nous suffit maintenant de vérifier (36) lorsque $u = \Gamma_\mathfrak{q}$. Par définition, le membre de droite de (36) est alors nul. De plus, d'après (35), le nombre $u^\gamma = \Gamma_\mathfrak{q}^\gamma$ est le produit de $\Gamma_{\mathfrak{q}^\gamma}$, de $\eta(\gamma, \mathfrak{q})$ et d'un élément de $1 + \mathfrak{m}_\mathfrak{q}(\mathrm{F})^{\mathrm{N}(\mathfrak{p})-1}$, que nous noterons α. L'image de $\Gamma_{\mathfrak{q}^\gamma}$ et de $\eta(\gamma, \mathfrak{q})$ par $\varphi_{\Lambda_{\mathfrak{q}^\gamma}}$ est 0, et, d'après le lemme 42, on a $\varphi_{k,\Lambda_{\mathfrak{q}^\gamma}}(\alpha) = 0$ pour tout entier k tel que $0 < k < \mathrm{N}(\mathfrak{p})-1$. Par conséquent, si on a $k \neq \mathrm{N}(\mathfrak{p})-1$, l'uniformisante $u = \Gamma_\mathfrak{q}$ vérifie (36). Ce qui prouve (*b*), et complète la démonstration de la proposition.

COROLLAIRE 49. — *Soit k un entier divisible par e, tel que $0 < k < \mathrm{N}(\mathfrak{p})-1$ (resp. $k = \mathrm{N}(\mathfrak{p})-1$). Alors, le noyau de la restriction au produit $\prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{H}_\mathfrak{q}^\times$ (resp. $\prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{D}_\mathfrak{q}(\mathrm{H})^\times$) de l'application $\varphi_k = \prod_{\mathfrak{q}\mid\mathfrak{p}} \varphi_{k,\Lambda_\mathfrak{q}}$, avec $\Lambda_\mathfrak{q} = u_\mathfrak{q}(t(\mathrm{P}))$ où P désigne un élément non nul de $\mathrm{E}_\mathfrak{p}$, est stable par $\mathscr{G}$.*

En particulier, l'application φ associée aux $\varphi_\mathfrak{q} = \varphi_{\Lambda_\mathfrak{q}}$, $\mathfrak{q} \mid \mathfrak{p}$, satisfait à la condition (i) *du théorème* 12.

6. Quelques conditions qui assurent l'existence de nombres premiers irréguliers

Soient $p \notin \mathrm{T}$ un nombre premier *non ramifié* dans K, et M un sous-corps de H contenant K tel que $(\mathrm{H} : \mathrm{M}) \not\equiv 0 \pmod{p}$. Soit $\mathfrak{q}_0$ un idéal premier de $\mathrm{M}_0 = \mathrm{M} \cap \mathrm{H}_0$ au-dessus de $\mathfrak{p}$. L'idéal $\mathfrak{q}_0$ se ramifie totalement dans M, et nous notons $\mathrm{M}_{\mathfrak{q}_0}$ la complétion $\mathfrak{q}_0$-adique de M. Pour tout idéal premier $\mathfrak{q}$ de H_0 au-dessus de $\mathfrak{q}_0$, le corps $\mathrm{M}_{\mathfrak{q}_0}$ est aussi l'adhérence de M dans $\mathrm{H}_\mathfrak{q}$.

Soient respectivement $\mathrm{U}_\mathfrak{q}$ et $\mathrm{U}_{\mathfrak{q}_0}(\mathrm{M})$ le groupe des unités de $\mathrm{H}_\mathfrak{q}$ et $\mathrm{M}_{\mathfrak{q}_0}$. Posons $\mathrm{U} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{U}_\mathfrak{q}$ et $\mathrm{U}(\mathrm{M}) = \prod_{\mathfrak{q}_0\mid\mathfrak{p}} \mathrm{U}_{\mathfrak{q}_0}(\mathrm{M})$. Nous plongeons $\mathrm{U}_{\mathfrak{q}_0}(\mathrm{M})$ dans $\prod_{\mathfrak{q}\mid\mathfrak{q}_0} \mathrm{U}_\mathfrak{q}$ par l'application diagonale; le produit de ces injections, lorsque $\mathfrak{q}_0$ décrit les idéaux premiers de M_0 au-dessus de $\mathfrak{p}$, définit un plongement de $\mathrm{U}(\mathrm{M})$ dans U. De même, nous plongeons respectivement $\mathscr{E}$ (resp. $\mathscr{E}(\mathrm{M})$) dans U (resp. $\mathrm{U}(\mathrm{M})$) par l'application diagonale.

Munissons les quotients $\mathrm{U}^{(p)} = \mathrm{U}/\mathrm{U}^p$, $\mathrm{U}^{(p)}(\mathrm{M}) = \mathrm{U}(\mathrm{M})/\mathrm{U}(\mathrm{M})^p$, $\overline{\mathscr{E}}^{(p)} = \mathscr{E}/\mathscr{E} \cap \mathrm{U}^p$ $\overline{\mathscr{E}}^{(p)}(\mathrm{M}) = \mathscr{E}(\mathrm{M})/\mathscr{E}(\mathrm{M}) \cap \mathrm{U}(\mathrm{M})^p$, $\overline{\Omega}^{(p)}(\mathrm{M}) = \Omega(\mathrm{M})/\Omega(\mathrm{M}) \cap \mathrm{U}(\mathrm{M})^p$ et $\overline{\Omega}^{(p)} = \overline{\Omega}^{(p)}(\mathrm{H})$, de leurs structures naturelles de $\mathbf{F}_p[\mathscr{G}]$-modules. Bien sûr $\overline{\Omega}^{(p)}$ est un sous-module de $\overline{\mathscr{E}}^{(p)}$ lui-même contenu dans $\mathrm{U}^{(p)}$, et $\overline{\Omega}^{(p)}(\mathrm{M})$ est un sous-module de $\overline{\mathscr{E}}^{(p)}(\mathrm{M})$ lui-même contenu dans $\mathrm{U}^{(p)}(\mathrm{M})$; de plus, comme on a $(\mathrm{H} : \mathrm{M}) \not\equiv 0 \pmod{p}$, l'injection de $\mathrm{U}(\mathrm{M})$ dans U induit un plongement de $\mathrm{U}^{(p)}(\mathrm{M})$ dans $\mathrm{U}^{(p)}$, de $\overline{\mathscr{E}}^{(p)}(\mathrm{M})$ dans $\overline{\mathscr{E}}^{(p)}$ et de $\overline{\Omega}^{(p)}(\mathrm{M})$ dans $\overline{\Omega}^{(p)}$. Enfin, désignons par $\mathrm{U}_\mathfrak{q}^{(p)}$ le quotient $\mathrm{U}_\mathfrak{q}/\mathrm{U}_\mathfrak{q}^p$; c'est un $\mathbf{F}_p[\mathrm{G}]$-module, et on a $\mathrm{U}^{(p)} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{U}_\mathfrak{q}^{(p)}$.

Posons $n_p = (\mathrm{N}(\mathfrak{p})-1)/(p-1)$. Pour chaque entier k tel que $1 \leqq k \leqq \mathrm{N}(\mathfrak{p})-1$, soit φ_k l'homomorphisme de $\prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{F}_\mathfrak{p}^\times$ dans $\varkappa = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathcal{O}(\mathrm{H}_0)/\mathfrak{q}$ défini dans le paragraphe précédent.

Notre résultat clef est le théorème suivant et son corollaire, d'où nous déduirons successivement le théorème 2 pour les nombres premiers p décomposés dans K, et le théorème 3 pour les nombres premiers p inertes dans K.

THÉORÈME 50. — *Soient p un nombre premier non ramifié dans* K, $p \notin T$, *et χ un caractère irréductible de* G *sur* $\mathbf{F}_p$.

(i) *Si* $\chi = \sigma^k$, *avec* $n_p < k \leqq N(\mathfrak{p})-1$, *l'application* φ_k *définit un isomorphisme de* $U_\chi^{(p)}$ *sur* $\varkappa$.

(ii) *Si* $\chi = \sigma^k + \sigma^{p(k)}$, *avec* $n_p < k$, $p(k) < N(\mathfrak{p})-1$, *l'application* $(\varphi_k, \varphi_{p(k)})$ *définit un isomorphisme de* $U_\chi^{(p)}$ *sur* $\varkappa \times \varkappa$.

(i′) *Supposons que p soit inerte dans* K. *Alors, si* $\chi = \sigma^{n_p} = \nu$, *l'application* φ_k, *avec* $k = n_p = p+1$, *définit une surjection de* $U_\chi^{(p)}$ *sur* $\varkappa$.

Si p se décompose dans K, on a $n_p = 1$, et, d'après le lemme 9, paragraphe 2, tous les caractères irréductibles χ de G sur $\mathbf{F}_p$ vérifient la condition (i) du théorème précédent. Comme, de plus, $\overline{\Omega}^{(p)}$ est un sous-module de $U^{(p)}$, on en déduit le corollaire suivant.

COROLLAIRE 51. — *Soient p et χ comme dans le théorème* 50. *Si p se décompose dans* K, *ou, plus généralement, si χ vérifie l'une des conditions* (i) *ou* (ii) *du théorème* 50 *la restriction de φ à $\overline{\Omega}_\chi^{(p)}$ est injective.*

Démonstration du théorème. — Pour tout entier k tel que $1 \leqq k \leqq N(\mathfrak{p})-1$, on a $\varphi_k = \prod_{\mathfrak{q}\mid\mathfrak{p}} \varphi_{k,\mathfrak{q}}$ avec $\varphi_{k,\mathfrak{q}} = \varphi_{k,\Lambda_\mathfrak{q}}$, où l'uniformisante $\Lambda_\mathfrak{q}$ de $\mathfrak{D}_\mathfrak{q}(F)$ est déterminée par (28). Nous pouvons donc raisonner composante par composante : nous démontrons d'abord que $\varphi_{k,\mathfrak{q}}$ (resp. $(\varphi_{k,\mathfrak{q}}, \varphi_{p(k),\mathfrak{q}})$) définit une surjection de $(U_\mathfrak{q}^{(p)})_\chi$ sur $\mathcal{O}(H_0)/\mathfrak{q}$ (resp. $(\mathcal{O}(H_0)/\mathfrak{q}) \times (\mathcal{O}(H_0)/\mathfrak{q})$).

Au préalable, notons que, sous les hypothèses de (i), (ii) ou (i′), on a toujours $k \not\equiv 0 \pmod{p}$, et, si χ est de degré 2, $p(k) \not\equiv 0 \pmod{p}$. C'est clair pour (i) et (i′) (*cf.* lemme 9, § 2). Plaçons-nous donc sous les hypothèses de (ii); si $p \mid k$ ou $p \mid p(k)$, on a $\chi = \mathrm{Tr}(\sigma^{ap})$, où a est un entier tel que $e < ap < N(\mathfrak{p})-1$; comme p est inerte dans K, on a $n_p = p+1$ et $\chi = \sigma^a + \sigma^{ap}$, avec $a < p < n_p = p+1$; la contradiction avec les hypothèses de (ii) prouve que les entiers k et $p(k)$ sont bien premiers à p.

Supposons d'abord que χ vérifie l'une des conditions (i) ou (i′). Soient s un élément de $\mathcal{O}(H_0)/\mathfrak{q}$, et s_1 un représentant de s dans $\mathfrak{D}_\mathfrak{q}(H_0)$. Le nombre $u = 1+s_1 \Lambda_\mathfrak{q}^k$ est une unité principale de $H_\mathfrak{q}$, et, d'après le lemme 42, on a $\varphi_{k,\mathfrak{q}}(u) = k.s$. Puisque k est p-inversible, il s'ensuit que s appartient bien à $\varphi_{k,\mathfrak{q}}(U_\mathfrak{q}^{(p)}) = \varphi_{k,\mathfrak{q}}((U_\mathfrak{q}^{(p)})_\chi)$.

Supposons maintenant que χ vérifie la condition (ii). Soient (s, s') un élément de $(\mathcal{O}(H_0)/\mathfrak{q}) \times (\mathcal{O}(H_0)/\mathfrak{q})$, et (s_1, s_1') un représentant de (s, s') dans $\mathfrak{D}_\mathfrak{q}(H_0) \times \mathfrak{D}_\mathfrak{q}(H_0)$. Quitte à échanger k et $p(k)$, nous pouvons supposer $k < p(k)$. Le nombre $u = 1+s_1 \Lambda_\mathfrak{q}^k$ est une unité principale de $H_\mathfrak{q}$, et, d'après le lemme 42, on a $\varphi_{k,\mathfrak{q}}(u) = ks$. Posons $a = -(1/k)\varphi_{p(k),\mathfrak{q}}(u)$, et soit a_1 un représentant de a dans $\mathfrak{D}_\mathfrak{q}(H_0)$. Le nombre $u' = 1+(s_1'+a_1)\Lambda_\mathfrak{q}^{p(k)}$ est une unité principale de $H_\mathfrak{q}$, et, d'après le lemme 42, on a $\varphi_{k,\mathfrak{q}}(u') = 0$ et $\varphi_{p(k),\mathfrak{q}}(u') = p(k)(s+a)$. Par suite, on a

$$(\varphi_{k,\mathfrak{q}}, \varphi_{p(k),\mathfrak{q}})(u^{p(k)} u'^k) = k.p(k).(s, s'),$$

et, puisque k et $p(k)$ sont p-inversibles, il s'ensuit que (s, s') appartient bien à

$$(\varphi_{k,\mathfrak{q}}, \varphi_{p(k),\mathfrak{q}})(U_{\mathfrak{q}}^{(p)}) = (\varphi_{k,\mathfrak{q}}, \varphi_{p(k),\mathfrak{q}})((U_{\mathfrak{q}}^{(p)})_\chi).$$

La surjectivité de l'application de $U_\chi^{(p)}$ sur $\varkappa$ (resp. $\varkappa \times \varkappa$) définie par φ_k (resp. $(\varphi_k, \varphi_{p(k)})$) est ainsi prouvée.

Déterminons maintenant la dimension de $U_\chi^{(p)}$ sur $\mathbf{F}_p$. Désignons par ε le sous-groupe de torsion de U, par U_0 le quotient U/ε, et posons $\varepsilon^{(p)} = \varepsilon/\varepsilon^p$, $U_0^{(p)} = U_0/U_0^p$. La suite exacte de $\mathbf{F}_p[G]$-modules

$$\{0\} \to \varepsilon^{(p)} \to U^{(p)} \to U_0^{(p)} \to \{0\},$$

réduit la question à la détermination des dimensions de $\varepsilon_\chi^{(p)}$ et $(U_0^{(p)})_\chi$.

Dans le cas où p est inerte dans K, observons que l'idéal $\mathfrak{p} = (p)$ est principal : par suite, $\mathfrak{p}$ se décompose totalement dans H_0 si bien que le nombre de $\mathfrak{q}$-composantes $U_\mathfrak{q}$ de U est h. Comme on a supposé le nombre premier $p \neq 2$ non ramifié dans K, le groupe U des unités de $H_\mathfrak{q}$ contient le groupe μ_p des racines p-ièmes de l'unité si et seulement si p est inerte dans K; le module $\varepsilon^{(p)}$ est donc égal à $\{0\}$ ou isomorphe au produit de h copies de μ_p, suivant que p est décomposé ou inerte dans K. Comme on a $\mu_p = (\mu_p)_\nu$, il vient $\varepsilon_\chi^{(p)} = \{0\}$ ou $\dim_{\mathbf{F}_p} \varepsilon_\chi^{(p)} = h$, suivant que χ est différent de ν ou non.

Quant à la dimension de $(U_0^{(p)})_\chi$ sur $\mathbf{F}_p$, elle est égale au rang du $\mathbf{Z}_p$-module libre $(U_0)_{\chi^*} = 1_{\chi^*}.U_0$, où 1_{χ^*} désigne l'idempotent de $\mathbf{Z}_p[G]$ attaché au caractère χ^* de G sur $\mathbf{Z}_p$ dont la réduction modulo p est le caractère χ (*cf.* démonstration du lemme 11, § 2). Or, si r_G désigne le caractère de la représentation régulière de G, le caractère de la représentation de G dans U_0 est égal à

$$h(\mathcal{O}/\mathfrak{p} : \mathbf{F}_p)\, r_G.$$

Par suite, le rang de $(U_0)_{\chi^*}$ sur $\mathbf{Z}_p$, qui est le produit de la multiplicité de χ^* dans $h(\mathcal{O}/\mathfrak{p} : \mathbf{F}_p)\, r_G$ par le degré de χ^*, est égal à $h(\mathcal{O}/\mathfrak{p} : \mathbf{F}_p)$ où à $4h$ suivant que le degré de χ^* est 1 ou 2. Comme χ et χ^* ont même degré, on a donc, dans le cas (i),

$$\dim_{\mathbf{F}_p} U_\chi^{(p)} = h(\mathcal{O}/\mathfrak{p} : \mathbf{F}_p) = \dim_{\mathbf{F}_p} \varkappa,$$

et, dans le cas (ii),

$$\dim_{\mathbf{F}_p} U_\chi^{(p)} = 4h = \dim_{\mathbf{F}_p} \varkappa \times \varkappa.$$

Ceci complète la démonstration du théorème.

Dans le cas (i'), c'est-à-dire lorsque p est inerte dans K et χ égal à ν, il résulte de la démonstration précédente que l'on a

$$\begin{aligned}\dim_{\mathbf{F}_p} U_\nu^{(p)} &= \dim_{\mathbf{F}_p} \varepsilon^{(p)} + \dim_{\mathbf{F}_p} (U_0^{(p)})_\nu \\ &= h + 2h = h + \dim_{\mathbf{F}_p} \varkappa.\end{aligned}$$

Par suite, puisque φ_{p+1} applique $U_\nu^{(p)}$ sur $\varkappa$, la restriction de φ_{p+1} à $U_\nu^{(p)}$ possède un noyau N de dimension h sur $\mathbf{F}_p$. Plus précisément, comme μ_p est contenu dans H, donc dans $U_\mathfrak{q}$, [un calcul facile, semblable à celui par lequel on a déterminé la dimension de $U_\nu^{(p)}$

sur $\mathbf{F}_p$, prouve que] la dimension de $(U_q^{(p)})_\nu$ sur $\mathbf{F}_p$ est 3. D'autre part, la dimension de $\mathcal{O}(H_0)/\mathfrak{q} \approx \mathcal{O}/\mathfrak{p}$ est 2; ainsi, la restriction de $\varphi_{p+1,\mathfrak{q}}$ à $(U_q^{(p)})_\nu$ possède un noyau $N_\mathfrak{q}$ de dimension 1 sur $\mathbf{F}_p$, et, bien sûr, on a $N = \prod_{\mathfrak{q}\mid\mathfrak{p}} N_\mathfrak{q}$.

D'après le corollaire 49, paragraphe 5, le noyau N est stable par $\mathcal{G}$; pour tous $u \in N$ et $\gamma \in \mathcal{G}$, considérons alors la représentation $r : \gamma \mapsto r_\gamma$ de $\mathcal{G}$ dans N définie par

$$r_\gamma(u) = u^{\tilde{\nu}(\gamma^{-1})\gamma},$$

où l'homomorphisme $\tilde{\nu}$ est déterminé par l'action de $\mathcal{G}$ sur μ_p. Comme G agit sur N par ν, l'application r_g est l'identité pour tout $g \in G$, si bien que l'on peut regarder r comme une représentation de $G(H_0/K)$ dans N. Comme $G(H_0/K)$ permute transitivement les $\mathfrak{q}$-composantes $N_\mathfrak{q}$ de N et $\dim_{\mathbf{F}_p} N = h = (H_0 : K)$, il s'ensuit que r est la représentation régulière de $G(H_0/K)$. Ce qui prouve :

Remarque 52. — *Si* $h \not\equiv 0 \pmod p$, *le noyau* N *de la restriction de* φ_{p+1} *à* $U_\nu^{(p)}$ *est isomorphe, comme* $\mathbf{F}_p[\mathcal{G}]$*-module, au produit tensoriel*

$$\mu_p \otimes \mathcal{R}_{H_0/K},$$

où μ_p *désigne le* $\mathbf{F}_p[\mathcal{G}]$*-module des racines p-ièmes de l'unité de* H *et* $\mathcal{R}_{H_0/K}$ *la représentation régulière de* $G(H_0/K)$ *sur* $\mathbf{F}_p$.

Par ailleurs, comme dans la démonstration du théorème 50, notons $\varepsilon^{(p)}$ le $\mathbf{F}_p$-espace vectoriel de dimension h, produit des images de μ_p dans chacune des $\mathfrak{q}$-composantes $U_\mathfrak{q}^{(p)}$ de $U^{(p)}$. Clairement $\varepsilon^{(p)}$ est un sous-espace de $U_\nu^{(p)}$ isomorphe, comme $\mathbf{F}_p[\mathcal{G}]$-module, au produit tensoriel $\mu_p \otimes \mathcal{R}_{H_0/K}$. De plus, le corollaire 43 prouve que les sous-espaces N et $\varepsilon^{(p)}$ de $U_\nu^{(p)}$ sont linéairement disjoints, soit

$$N \cap \varepsilon^{(p)} = \{0\};$$

en fait, le module $U_\nu^{(p)}$ est la somme directe de trois copies du $\mathbf{F}_p[\mathcal{G}]$-module $\mu_p \otimes \mathcal{R}_{D/K}$. D'autre part, la ν-composante $\overline{\mathcal{E}}_\nu^{(p)}$ de $\overline{\mathcal{E}}^{(p)}$ est aussi un sous-espace de $U_\nu^{(p)}$, et il serait intéressant de caractériser l'intersection de N avec $\mathcal{E}_\nu^{(p)}$. En particulier, vu le lemme suivant, on peut se demander dans quels cas ces deux sous-espaces sont-ils linéairement disjoints?

LEMME 53. — *Si le nombre de classes d'idéaux* $h = (H_0 : K)$ *de* K *est premier à p, alors, la projection de* $\mathcal{E}/\mathcal{E}^p$ *sur* $\mathcal{E}/\mathcal{E} \cap U^p$ *définit un isomorphisme de* $\mathcal{E}_{\tilde{\nu}}^{(p)}$ *sur* $\overline{\mathcal{E}}_{\tilde{\nu}}^{(p)}$, *et on a*

$$U_{\tilde{\nu}}^{(p)} = N_{\tilde{\nu}} \oplus \overline{\mathcal{E}}_{\tilde{\nu}}^{(p)},$$

où les $\tilde{\nu}$*-composantes* $N_{\tilde{\nu}}$ *et* $\overline{\mathcal{E}}_{\tilde{\nu}}^{(p)}$ *de* N *et* $\overline{\mathcal{E}}^{(p)}$ *sont respectivement de dimension* 1 *et* 2 *sur* $\mathbf{F}_p$.

Démonstration. — Comme $\tilde{\nu}$ est un caractère de degré 1 de $\mathcal{G}$ sur $\mathbf{F}_p$, distinct du caractère unité, et $\mathcal{E}$ contient μ_p [un raisonnement semblable à celui de la démonstration du lemme 11 (§ 2) prouve que] la dimension de $\mathcal{E}_{\tilde{\nu}}^{(p)}$ sur $\mathbf{F}_p$ est 2. D'autre part, on déduit des lemmes 24 et 26 que $\Psi^{(p)}(H)_{\tilde{\nu}}$ et $\Omega^{(p)}(H)_{\tilde{\nu}}$ ont même image par le $\mathcal{G}$-homomorphisme φ_{p+1}; il résulte donc de la proposition 35, que l'image de $\Omega^{(p)}(H)_{\tilde{\nu}}$ par φ_{p+1} est le $\mathbf{F}_p$-espace

vectoriel $\mathscr{L}_{\tilde{\nu}}$ de dimension 2 formé des classes $[\pi\, G_{p+1}(L)]$, lorsque π décrit $\mathfrak{p}$. Puisque $\Omega^{(p)}(H)$ est un sous-module de $\mathscr{E}^{(p)}$, il s'ensuit que φ_{p+1} définit un isomorphisme de $\mathscr{E}^{(p)}_{\tilde{\nu}}$ sur $\mathscr{L}_{\tilde{\nu}}$, qui se factorise à travers $\bar{\mathscr{E}}^{(p)}_{\tilde{\nu}}$. La projection de $\mathscr{E}^{(p)}_{\tilde{\nu}}$ sur $\bar{\mathscr{E}}^{(p)}_{\tilde{\nu}}$ est donc un isomorphisme, et l'on a

$$N_{\tilde{\nu}} \cap \bar{\mathscr{E}}^{(p)}_{\tilde{\nu}} = \{0\},$$

les dimensions des $\tilde{\nu}$-composantes $N_{\tilde{\nu}}$ et $\bar{\mathscr{E}}^{(p)}_{\tilde{\nu}}$ de N et $\bar{\mathscr{E}}^{(p)}$ étant respectivement 1 et 2. L'assertion du lemme résulte alors de ce que la dimension de $U^{(p)}_{\tilde{\nu}}$ sur $\mathbf{F}_p$ est 3.

Le lemme 53 implique le corollaire suivant.

COROLLAIRE 54. — *Soient p un nombre premier inerte dans* K, $p \notin T$, *ne divisant pas h, et* M *un sous-corps de* H *tel que* $K = M \cap H_0$ *et* $\mu_p \subset M$. *Alors, la restriction de* φ *à* $\bar{\mathscr{E}}^{(p)}(M)_\nu$, *et donc à* $\bar{\Omega}^{(p)}(M)_\nu$, *est injective.*

Démonstration. — Comme $K = M \cap H_0$ on a $\mathscr{G} = G.G(H/M)$. Par conséquent, il existe au plus un homomorphisme ω de $\mathscr{G}$ tel que $\omega(G(H/M)) = \{1\}$, dont la restriction à G soit ν. Dans le cas présent, cet homomorphisme est $\tilde{\nu}$; en effet, comme M contient μ_p, on a $\tilde{\nu}(G(H/M)) = \{1\}$ et bien sûr la restriction de $\tilde{\nu}$ à G est ν. Ceci prouve l'inclusion

$$U^{(p)}(M)_\nu \cap N \subset N_{\tilde{\nu}}$$

(cette inclusion est en fait une égalité). Par suite, d'après le lemme 53, on a

$$\bar{\mathscr{E}}^{(p)}(M)_\nu \cap N \subset \bar{\mathscr{E}}^{(p)}(M)_\nu \cap N_{\tilde{\nu}} = \{0\},$$

et le corollaire est démontré.

Le théorème 50, ou plutôt le corollaire 51, a des conséquences intéressantes que nous développons en distinguant deux cas suivant que p est décomposé ou inerte dans K. Il s'agit essentiellement d'énoncés de la forme :

L'existence de caractères $\chi \neq 1$ *de* G_M, *définis et irréductibles sur* $\mathbf{F}_p$, *tels que* $\delta(\chi, M) > 0$, *implique l'existence de p-extensions abéliennes de* M *possédant certaines propriétés de non ramification* (*cf.* th. 58 *et* 61).

Rappelons que l'entier positif $\delta(\chi, M)$ a été introduit immédiatement avant l'énoncé du lemme 27 (§ 3). Pour son calcul, on peut utiliser, si M contient H_0, la proposition 22 (§ 3) (*cf.* démonstration du théorème 29), ou, si $h \not\equiv 0 \pmod{p}$, le théorème 37 (§ 4).

CAS (i) : p DÉCOMPOSÉ DANS K.

Démontrons d'abord les deux lemmes techniques ci-dessous.

LEMME 55. — *Considérons les cinq conditions suivantes :*

(i) *toute* $(\mathbf{Z}/p)$*-extension non ramifiée de* M, *est une extension abélienne de* M_0 *;*

(i') *toute* $(\mathbf{Z}/p)$*-extension de* M, *non ramifiée en dehors de* $\mathfrak{p}$, *est une extension abélienne de* M_0*;*

(ii) *la p-extension abélienne non ramifiée maximale de* M, *est une extension abélienne de* M_0*;*

(ii′) *la p-extension abélienne maximale de* M, *non ramifiée en dehors de* $\mathfrak{p}$, *est une extension abélienne de* M_0;

(iii) $h_M/h_{M_0} \not\equiv 0 \pmod{p}$.

On a (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii), (i′) $\Leftrightarrow$ (ii′), (i′) $\Rightarrow$ (i) *et* (ii′) $\Rightarrow$ (ii).

Démonstration. — Les implications (ii′) $\Rightarrow$ (ii) $\Rightarrow$ (i) et (ii′) $\Rightarrow$ (i′) $\Rightarrow$ (i) sont triviales. Le fait que (i) (resp. (i′)) implique (ii) (resp. (ii′)), est une simple question de représentation de groupes. En effet, soit R la p-extension abélienne non ramifiée maximale de M (resp. la p-extension abélienne maximale de M, non ramifiée en dehors de $\mathfrak{p}$). Le groupe de Galois $G(R/M)$ est de manière naturelle un $\mathbf{Z}_p$-module de type fini; de plus, R est une extension galoisienne de K et donc de M_0, si bien que l'action par conjugaison de $G_M = G(M/M_0)$ fait de $G(R/M)$ un $\mathbf{Z}_p[G_M]$-module. Supposons que R ne soit pas une extension abélienne de M_0, autrement dit que l'action de G_M sur $G(R/M)$ ne soit pas l'action triviale. Comme l'ordre de G_M est premier à p, l'anneau $\mathbf{Z}_p[G_M]$ est semi-simple; il existe donc un caractère irréductible $\chi^* \neq 1$ de G_M sur $\mathbf{Z}_p$ pour lequel la χ^*-composante $G(R/M)_{\chi^*} = 1_{\chi^*}.G(R/M)$ de $G(R/M)$ est non nulle (comme dans la démonstration du lemme 11, § 2, le symbole 1_{χ^*} désigne l'idempotent de $\mathbf{Z}_p[G_M]$ associé à χ^*). Naturellement, la réduction modulo p de χ^* est un caractère irréductible $\chi \neq 1$ de G_M sur $\mathbf{F}_p$, et, comme p se décompose dans K, les caractères χ et χ^* sont de degré 1, autrement dit sont des homomorphismes de G_M. Il s'ensuit que $G(R/M)_{\chi^*}$ possède un quotient Δ d'ordre p sur lequel G_M agit par χ. Le groupe Δ, quotient de $G(R/M)_{\chi^*}$ donc de $G(R/M)$, est le groupe de Galois $G(R'/M)$ d'un sous-corps R′ de R contenant M, et G_M agit sur $G(R'/M)$ par χ; ceci prouve que R′ est une $(\mathbf{Z}/p)$-extension non ramifiée de M (resp. une $(\mathbf{Z}/p)$-extension de M, non ramifiée en dehors de $\mathfrak{p}$), qui n'est pas une extension abélienne de M_0. La contradiction avec (i) (resp. (i′)) prouve que (i) (resp. (i′)) implique bien (ii) (resp. (ii′)).

Montrons enfin l'équivalence de (ii) et (iii). Notons respectivement S_0 et S les p-extensions abéliennes non ramifiées maximales de M_0 et M; les degrés $(S_0 : M_0)$ et $(S : M)$ sont respectivement égaux à la plus grande puissance de p divisant h_{M_0} et h_M. De plus S_0M est une p-extension abélienne non ramifiée de M, d'où $S_0M \subset S$, et on a $(S_0M : M) = (S_0 : M_0)$ puisque $S_0 \cap M = M_0$. Ainsi, la condition (iii) est-elle équivalente à $S = S_0M$. En outre, comme $(M : M_0)$ est premier à p, le corps S_0M est la plus grande p-extension abélienne non ramifiée de M, qui soit une extension abélienne de M_0. Autrement dit, on a $S = S_0M$ si et seulement si la condition (ii) est satisfaite par M. Ceci complète la démonstration du lemme.

Par ailleurs, pour chaque caractère irréductible χ de $G_M = G(M/M_0)$ sur $\mathbf{F}_p$, soit R_χ la p-extension abélienne maximale de M, non ramifiée en dehors de $\mathfrak{p}$, galoisienne sur M_0, dont le groupe de Galois $\Gamma = G(R_\chi/M)$ vérifie les deux conditions suivantes :

(a) Γ est tué par p, autrement dit $\Gamma^p = \{1\}$;

(b_χ) G_M agit sur Γ par χ.

Le groupe $G(R_\chi/M)$ est donc un $\mathbf{F}_p[G_M]_\chi$-espace vectoriel. Comme p est décomposé dans K, le caractère χ est de degré 1 et $G(R_\chi/M)$ est isomorphe à un produit de facteurs $\mathbf{Z}/p$ sur lesquels G_M agit par χ : le corps R_χ est le composé des $(\mathbf{Z}/p)$-extensions de M, non ramifiées en dehors de $\mathfrak{p}$, sur le groupe de Galois desquelles G_M agit par χ.

Il vient :

LEMME 56. — *Soit* M *un sous-corps de* H *contenant* K *tel que* $h_M/h_{M_0} \not\equiv 0 \pmod p$. *Alors, pour tout caractère irréductible* χ *de* G_M *sur* $\mathbf{F}_p$, $\chi \neq 1$, *l'application de réciprocité d'Artin de* M *définit un isomorphisme de* $(U^{(p)}(M)/\overline{\mathscr{E}^{(p)}}(M))_\chi$ *sur* $G(R_\chi/M)$, *où* R_χ *désigne la p-extension abélienne de* M, *non ramifiée en dehors de* p, *définie ci-dessus.*

Démonstration. — Soient S (resp. R) la p-extension abélienne non ramifiée maximale de M (resp. la p-extension abélienne maximale de M, non ramifiée en dehors de p). Désignons par $\overline{\mathscr{E}(M)}$ l'adhérence dans U (M) de l'image de $\mathscr{E}(M)$ par l'application diagonale. D'après la théorie du corps de classes, l'application de réciprocité d'Artin de M définit un isomorphisme du quotient $A = U(M)/\overline{\mathscr{E}(M)}$ sur le groupe de Galois $\Gamma = G(R/S)$. Comme dans la démonstration du lemme précédent, l'action par conjugaison de G_M munit les $\mathbf{Z}_p$-modules de type fini G (R/M) et G (S/M) d'une structure de $\mathbf{Z}_p[G_M]$-modules semi-simples. On a donc les isomorphismes

$$G(R/M) \simeq \prod_{\chi^*} G(R/M)_{\chi^*}$$

$$G(S/M) \simeq \prod_{\chi^*} G(S/M)_{\chi^*},$$

où χ^* décrit les caractères irréductibles de G_M sur $\mathbf{Z}_p$, et $G(R/M)_{\chi^*}$, $G(S/M)_{\chi^*}$ désignent les χ^*-composantes $1_{\chi^*}.G(R/M)$ et $1_{\chi^*}.G(S/M)$ des modules G (R/M) et G (S/M). Les quotients $G(R/M)_{\chi^*}$ et $G(S/M)_{\chi^*}$ de G (R/M) et G (S/M) sont respectivement isomorphes aux groupes de Galois $G(R_{\chi^*}/M)$ et $G(S_{\chi^*}/M)$ des plus grands sous-corps R_{χ^*} et S_{χ^*} de R et S sur lesquels G_M agit par χ^*. Il s'ensuit que $G(R_{\chi^*}/S_{\chi^*})$ est la χ^*-composante $\Gamma_{\chi^*} = 1_{\chi^*}.\Gamma$ de Γ.

Notons χ le caractère irréductible de G_M sur $\mathbf{F}_p$ obtenu par réduction modulo p de χ^*; l'application $\chi^* \mapsto \chi$ est une bijection de l'ensemble des caractères irréductibles de G_M sur $\mathbf{Z}_p$ sur l'ensemble des caractères irréductibles de G_M sur $\mathbf{F}_p$; en particulier, on a $\chi = 1$ si et seulement si $\chi^* = 1$. Supposons $\chi^* \neq 1$. Comme h_M/h_{M_0} est premier à p, le corps M vérifie la condition (ii) du lemme 55; on a donc $S_{\chi^*} = M$, d'où $\Gamma_{\chi^*} = G(R_{\chi^*}/M)$. L'identité

$$G(R_\chi/M) = (\Gamma/\Gamma^p)_\chi = \Gamma_{\chi^*}/\Gamma_{\chi^*}^p$$

en résulte, puisque R_χ est le plus grand sous-corps de R_{χ^*} dont le groupe de Galois $G(R_\chi/M)$ soit tué par p. D'autre part, on a l'isomorphisme de $\mathbf{F}_p[G_M]$-modules

$$\begin{aligned} A/A^p &= (U(M)/\overline{\mathscr{E}(M)})/(U(M)/\overline{\mathscr{E}(M)})^p \simeq U(M)/\overline{\mathscr{E}(M)}\,U(M)^p \\ &\simeq (U(M)/U(M)^p)/(\overline{\mathscr{E}(M)}/\overline{\mathscr{E}(M)} \cap U(M)^p) = U^{(p)}(M)/\overline{\mathscr{E}^{(p)}}(M). \end{aligned}$$

Par conséquent, si $\chi \neq 1$, l'application de réciprocité d'Artin de M définit bien un isomorphisme de $(U^{(p)}(M)/\overline{\mathscr{E}^{(p)}}(M))_\chi = (A/A^p)_\chi = A_{\chi^*}/A_{\chi^*}^p$ sur

$$\Gamma_{\chi^*}/\Gamma_{\chi^*}^p = (\Gamma/\Gamma^p)_\chi = G(R_\chi/M).$$

Le lemme est démontré.

Soient maintenant χ un caractère irréductible de G_M sur $\mathbf{F}_p$, $\chi \neq 1$, et k l'unique entier tel que $\chi = \sigma^k$ et $0 < k < p-1$ (*cf.* lemme 9 (i), § 2). Considérons le diagramme suivant de $\mathbf{F}_p$-espaces vectoriels. Il est exact.

$$\begin{array}{ccccccccc} & & & & & & \{0\} & & \\ & & & & & & \downarrow & & \\ & & & & & & (\bar{\mathscr{E}}^{(p)}(M)/\bar{\Omega}^{(p)}(M))_\chi & & \\ & & & & & & \downarrow & & \\ (38) & & \{0\} \to \bar{\Omega}^{(p)}(M)_\chi & \to & U^{(p)}(M)_\chi & \to & (U^{(p)}(M)/\bar{\Omega}^{(p)}(M))_\chi & \to & \{0\} \\ & & & & & & \downarrow & & \\ & & & & & & (U^{(p)}(M)/\bar{\mathscr{E}}^{(p)}(M))_\chi & & \\ & & & & & & \downarrow & & \\ & & & & & & \{0\} & & \end{array}$$

Comme $\bar{\Omega}^{(p)}(M)$ est un sous-module de $\bar{\Omega}^{(p)}$, il résulte du corollaire 51 que la restriction de φ à $\bar{\Omega}^{(p)}(M)_\chi$ est injective. Or, d'après les lemmes 25 et 26, on a

$$\varphi(\bar{\Omega}^{(p)}(M)_\chi) = \varphi(\Omega^{(p)}(M)_\chi) = \mathscr{L}(\chi, M);$$

par conséquent, les $\mathbf{F}_p$-espaces vectoriels $\bar{\Omega}^{(p)}(M)_\chi$ et $\mathscr{L}(\chi, M)$ sont isomorphes. Comme χ est de degré 1, la dimension de ce dernier est $l(\chi, M)$, d'où

$$\dim_{\mathbf{F}_p} \bar{\Omega}^{(p)}(M)_\chi = l(\chi, M).$$

D'autre part, la dimension de $U^{(p)}(M)_\chi$ sur $\mathbf{F}_p$ est $(M_0 : K)$ (le cas $M = H$ a été traité dans la démonstration du théorème 50; le cas général se traite de manière analogue). De plus, puisque χ est différent de 1, on a, d'après le lemme 11, $e(\chi, M) = (M_0 : K)$. Il s'ensuit que la dimension de $(U^{(p)}(M)/\bar{\Omega}^{(p)}(M))_\chi$ sur $\mathbf{F}_p$ est égale au défaut de régularité

$$\delta(\chi, M) = e(\chi, M) - l(\chi, M) = (M_0 : K) - l(\chi, M)$$

de l'extension M/M_0 pour χ. D'après l'exactitude du diagramme (38), on a donc, pour $\chi \neq 1$,

$$\delta(\chi, M) = \dim_{\mathbf{F}_p}(\bar{\mathscr{E}}^{(p)}(M)/\bar{\Omega}^{(p)}(M))_\chi + \dim_{\mathbf{F}_p}(U^{(p)}(M)/\bar{\mathscr{E}}^{(p)}(M))_\chi. \tag{39}$$

Si h_M/h_{M_0} est premier à p, ce qui équivaut d'après la proposition 10 à supposer le module $\mathscr{S}(M)$ nul, alors, le quotient $\bar{\mathscr{E}}^{(p)}(M)/\bar{\Omega}^{(p)}(M)$ de $\mathscr{S}(M)$ est *a fortiori* nul et l'identité (39) devient

$$\delta(\chi, M) = \dim_{\mathbf{F}_p}(U^{(p)}(M)/\bar{\mathscr{E}}^{(p)}(M))_\chi.$$

Compte tenu de l'interprétation de $(U^{(p)}(M)/\bar{\mathscr{E}}^{(p)}(M))_\chi$ fournie par le lemme 56 (c'est-à-dire par la théorie du corps de classes), ceci prouve la proposition suivante.

PROPOSITION 57. — *Soient p un nombre premier décomposé dans* K, $p \notin T$, *et* M *un sous-corps de* H *contenant* K *tel que* $(H : M) \not\equiv 0 \pmod p$ *et* $h_M/h_{M_0} \not\equiv 0 \pmod p$. *Soient* χ

un caractère irréductible de G_M *sur* $\mathbf{F}_p$, $\chi \neq 1$, *et* R_χ *la p-extension abélienne de* M *définie dans le lemme* 56.

Alors, le groupe de Galois $G(R_\chi/M)$ *est isomorphe à* $(\mathbf{Z}/p)^{\delta(\chi, M)}$, *où* $\delta(\chi, M)$ *désigne le défaut de régularité de l'extension* M/M_0 *pour* χ.

Combinons cette proposition avec le théorème 28 et le lemme 55; il vient :

THÉORÈME 58. — *Soient p comme précédemment, et* M *un sous-corps de* H *contenant* K *tel que* $(H : M) \not\equiv 0 \pmod{p}$. *Alors, les deux conditions suivantes sont équivalentes :*

(α) *la p-extension abélienne maximale de* M, *non ramifiée en dehors de* $\mathfrak{p}$, *est une extension abélienne de* $M_0 = M \cap H_0$.

(β) *pour tout caractère irréductible* $\chi \neq 1$ *de* G_M *dans* $\mathbf{F}_p$, *le défaut de régularité* $\delta(\chi, M)$ *de* M/M_0 *pour* χ *est nul.*

Démonstration. — Supposons que M vérifie (α). Alors, d'après le lemme 55, on a $h_M/h_{M_0} \not\equiv 0 \pmod{p}$. Nous pouvons donc appliquer la proposition 57; mais comme M vérifie (α), on a $R_\chi = M$ pour tout caractère irréductible $\chi \neq 1$ de G_M sur $\mathbf{F}_p$, et donc $\delta(\chi, M) = 0$.

Réciproquement, si $\delta(\chi, M) = 0$ pour tout caractère irréductible $\chi \neq 1$ de G_M sur $\mathbf{F}_p$, il résulte du théorème 28 que le quotient h_M/h_{M_0} est premier à p. Appliquons alors la proposition 57; il s'ensuit que $R_\chi = M$ pour tout caractère irréductible $\chi \neq 1$ de G_M sur $\mathbf{F}_p$, autrement dit M vérifie la condition (i') du lemme 55. D'après ce dernier, M vérifie donc (α).

Notons que le théorème 28, pour p décomposé dans K, résulte de la partie (β) $\Rightarrow$ (α) de ce théorème, puisque (α) implique $h_M/h_{M_0} \not\equiv 0 \pmod{p}$ d'après le lemme 55. Enfin, comme remarqué immédiatement à la suite du théorème 28, lorsque p est décomposé dans K, la condition $\delta(\chi, H) = 0$, avec $\chi = \sigma^k$ et $0 < k < p-1$, est équivalente à la condition A_k du théorème 1. Par conséquent, le théorème 2 est le cas particulier $M = H$ du théorème précédent.

CAS (ii) : p INERTE DANS K.

Soient χ un caractère irréductible de G_M sur $\mathbf{F}_p$, et $\left\{k, p(k)\right\}_i^e$ l'unique paire d'entiers pour laquelle, suivant que χ est de degré 1 ou 2, on a $\chi = \sigma^k = \sigma^{p(k)}$ ou $\chi = \sigma^k + \sigma^{p(k)}$ avec $e \leqq k$, $p(k) \leqq p^2 - 1$ (*cf.* lemme 9, § 2). La dimension du $\mathbf{F}_p[G]_\chi$-espace vectoriel $(U^{(p)}(M)/\bar{\mathscr{E}}^{(p)}(M))_\chi$ est supérieure ou égale à $(M_0 : K) + \varepsilon_1$, où $\varepsilon_1 = 1$ si $\chi = 1$ et $\varepsilon_1 = 0$ sinon; en effet, alors que l'on a dans le cas (i) :

$$\dim_{\mathbf{F}_p} U^{(p)}(M)_\chi = \varepsilon_1 + \dim_{\mathbf{F}_p} \mathscr{E}^{(p)}(M)_\chi,$$

on a dans le cas présent

$$\begin{aligned} \dim_{\mathbf{F}_p} U^{(p)}(M)_\chi &= (\mathscr{O}/\mathfrak{p} : \mathbf{F}_p)(M_0 : K) + \varepsilon_2 \\ &= 2(M_0 : K) + \varepsilon_2 \\ &\geqq (M_0 : K) + \varepsilon_1 + \dim_{\mathbf{F}_p[G]\chi} \mathscr{E}^{(p)}(M)_\chi, \end{aligned}$$

où $\varepsilon_2 = (M_0 : K)$ si $\chi = \nu$ et $\varepsilon_2 = 0$ sinon. Ceci rend inefficace le raisonnement précédent basé sur le diagramme (38).

Cependant, comme p est inerte dans K, le corps H contient le groupe μ_p des racines p-ièmes de l'unité. *Supposons que le corps* M *contienne aussi* μ_p. Alors, d'après la théorie de Kummer, toute $(\mathbf{Z}/p)$-extension N de M est obtenue par adjonction de la racine p-ième d'un élément de M, soit

$$N = M(\sqrt[p]{u_1}), \qquad u_1 \in M^\times.$$

Bien sûr, le corps N ne dépend que de la classe $u \in M^\times/M^{\times p}$ de u_1 modulo $M^{\times p}$; aussi, posons nous $N_u = M(\sqrt[p]{u_1})$. L'application $u \mapsto N_u$ est une bijection de l'ensemble des éléments $u \neq 0$ de $M^\times/M^{\times p}$ sur l'ensemble des $(\mathbf{Z}/p)$-extensions de M. De plus, si u appartient à $\mathscr{E}^{(p)}(M)$, l'extension N_u/M est non ramifiée en dehors de p; elle est partout non ramifiée si u appartient au sous-groupe $\mathscr{E}(M) \cap U(M)^p/\mathscr{E}(M)^p$ de $\mathscr{E}^{(p)}(M)$.

Posons $\pi(M) = \Omega(M) \cap U(M)^p / \Omega(M) \cap \mathscr{E}(M)^p$; c'est un sous-module de $\mathscr{E}(M) \cap U(M)^p/\mathscr{E}(M)^p$. Considérons le diagramme suivant de $\mathbf{F}_p[G]_\chi$-espaces vectoriels. Il est exact.

$$\begin{array}{ccccccccc} & & & & \{0\} & & & & \\ & & & & \downarrow & & & & \\ & & & & \pi(M)_\chi & & & & \\ & & & & \downarrow & & & & \\ (40) & & \{0\} & \to & \Omega^{(p)}(M)_\chi & \to & \mathscr{E}^{(p)}(M)_\chi & \to & \mathscr{S}(M)_\chi \to \{0\} \\ & & & & \downarrow & & & & \\ & & & & \bar{\Omega}^{(p)}(M)_\chi & & & & \\ & & & & \downarrow & & & & \\ & & & & \{0\} & & & & \end{array}$$

La théorie de Kummer nous fournit une interprétation de $\pi(M)_\chi$. Il nous faut d'abord introduire quelques notations. Pour chaque χ comme ci-dessus, nous désignons par χ' le caractère irréductible de G_M sur $\mathbf{F}_p$ défini par

$$\chi'(g) = \nu(g)\chi(g^{-1}), \qquad g \in G_M;$$

c'est le reflet de χ dans le miroir de Leopoldt. On a $(\chi')' = \chi$, $\nu' = 1$, $1' = \nu$ et $\deg \chi = \deg \chi'$. Soit $\mathrm{Ker}(\chi, M) = \{ g \in G_M \mid \chi(\sigma) = \chi(1) \}$, et désignons par M_χ le sous-corps de M, contenant M_0, fixé par $\mathrm{Ker}(\chi, M)$. Notons alors N le composé des extensions N_u de M, lorsque u décrit $\pi(M)_\chi$. D'après la théorie de Kummer, le corps N est une p-extension abélienne non ramifiée de M, dont le groupe de Galois G(N/M) est isomorphe à $\pi(M)_\chi$. De plus, d'après Leopoldt [17], l'extension N/M_0 est galoisienne et l'action par conjugaison de G_M sur G(N/M) est donnée par χ'. Par suite, il existe un unique sous-corps de N, noté $N(M_{\chi'})$, qui contient $M_{\chi'}$ et tel que le groupe de Galois $G(N/M_{\chi'})$ soit isomorphe au produit direct des groupes G(N/M) et $G(N/N(M_{\chi'}))$; on a donc

$$G(N(M_{\chi'})/M_{\chi'}) \simeq G(N/M) \simeq \pi(M)_\chi.$$

D'autre part, désignons par $\bar{\delta}(\chi, M)$ la différence

$$\bar{\delta}(\chi, M) = e(\chi, M) - \dim_{\mathbf{F}_p[G]_\chi} \bar{\Omega}^{(p)}(M)_\chi.$$

Comme $\bar{\Omega}^{(p)}(M)$ est un quotient de $\Omega^{(p)}(M)$, lui-même contenu dans $\mathscr{E}^{(p)}(M)$, l'entier $\bar{\delta}(\chi, M)$ est $\geqq 0$. Si χ n'est pas le caractère unité, il résulte des lemmes 25 et 26 que $\mathscr{L}(\chi, M)$ est l'image de $\bar{\Omega}^{(p)}(M)_\chi$ par φ, d'où l'inégalité

$$\bar{\delta}(\chi, M) \leqq \delta(\chi, M).$$

Bien sûr, si χ vérifie de plus l'une des conditions (i) ou (ii) du théorème 50, c'est-à-dire si $p+1 < k$, $p(k) < p^2-1$, on a

$$\bar{\delta}(\chi, M) = \delta(\chi, M); \tag{41}$$

en effet, puisque $(H : M) \not\equiv 0 \pmod{p}$, le module $\bar{\Omega}^{(p)}(M)$ est contenu dans $\bar{\Omega}^{(p)}$, et la restriction de φ à $\bar{\Omega}^{(p)}_\chi$ est injective d'après le corollaire 51.

Avec ces notations, pour tout χ comme précédemment, on déduit de l'exactitude du diagramme (40) l'identité

$$\dim_{\mathbf{F}_p} \mathscr{S}(M)_\chi + \log_p(N(M_{\chi'}) : M_{\chi'}) = \bar{\delta}(\chi, M).\deg\chi. \tag{42}$$

Or, on a $\mathscr{S}(M_\chi)_\chi = \mathscr{S}(M)_\chi$; par suite, l'identité (42) et la proposition 10 (§ 2) prouvent en particulier :

PROPOSITION 59. — *Soit χ un caractère irréductible de G_M sur $\mathbf{F}_p$. Alors, si $\bar{\delta}(\chi, M) > 0$, l'un au moins des deux nombres h_{M_χ}/h_{M_0} et $h_{M_{\chi'}}$ est divisible par p.*

Nous pourrions déduire de (42) beaucoup plus que l'assertion précédente, si nous connaissions quelque relation entre les groupes $\mathscr{S}(M)_\chi$, $\mathscr{S}(M)_{\chi'}$ d'une part et $G(N(M_\chi)/M_\chi)$, $G(N(M_{\chi'})/M_{\chi'})$ d'autre part. En particulier, on peut se demander si, pour chaque caractère irréductible $\chi \neq 1$ de G_M sur $\mathbf{F}_p$, les groupes $\mathscr{S}(M)_\chi$ et $G(N(M_\chi)/M_\chi)$ sont isomorphes. Une autre question serait : est-il vrai que $N(M_\chi)$ est la p-extension abélienne non ramifiée maximale de M_χ, galoisienne sur M_0, dont le groupe de Galois $G(N(M_\chi)/M_\chi)$ vérifie les conditions (a) et (b_χ) précédant l'énoncé du lemme 56? D'après (42), une réponse affirmative à la première de ces questions impliquerait en particulier l'égalité

$$\bar{\delta}(\chi, M) = \bar{\delta}(\chi', M) \tag{43}$$

pour tout caractère irréductible χ de G_M sur $\mathbf{F}_p$ différent de 1 et ν. Désignons alors par $\{k', p(k')\}$ l'unique paire d'entiers associée au reflet χ' de χ. Les conditions $p+1 < k$, $p(k) < p^2-1$ et $p+1 < k'$, $p(k') < p^2-1$ sont trivialement équivalentes, si bien que l'on devrait avoir, d'après (41) et (43),

$$\delta(\chi, M) = \delta(\chi', M), \tag{44}$$

pour tout χ comme précédemment, tel que $p+1 < k$, $p(k) < p^2-1$. Nous avons vérifié (44) dans un certain nombre de cas (*cf.* appendice B).

En l'absence de tels renseignements, notre ressource est de sommer les identités (42) lorsque χ parcourt les caractères irréductibles de G_M sur $\mathbf{F}_p$. Il vient :

$$\dim_{\mathbf{F}_p} \mathscr{S}(M) + \sum_{\chi} \log_p (N(M_\chi) : M_\chi) = \sum_{\chi} \bar{\delta}(\chi, M).\deg \chi. \tag{45}$$

Posons $a = \dim_{\mathbf{F}_p} \mathscr{S}(M)$ et $b = \sum_{\chi \neq 1} \log_p (N(M_\chi) : M_\chi)$. Vu la définition de $\mathscr{S}(M)$, l'entier p^a divise h_M/h_{M_0}. D'autre part, considérons l'extension N de M composée des corps $N_\chi = M.N(M_\chi)$, pour $\chi \neq 1$. Puisque G_M agit sur $G(N_\chi : M) \simeq G(N(M_\chi) : M_\chi)$ par χ, les extensions N_χ/M sont linéairement disjointes, d'où $G(N/M) = \prod_{\chi \neq 1} G(N_\chi/M)$ et donc $(N : M) = p^b$. De plus, le corps N est une p-extension abélienne non ramifiée de M, et l'unique sous-groupe de $G(N/M)$ sur lequel G_M agit trivialement est $\{1\}$. Soit alors S_0 la p-extension abélienne non ramifiée maximale de M_0; comme remarqué dans la démonstration du lemme 55, le degré $(S_0M : M) = (S_0 : M_0)$ est la plus grande puissance de p qui divise h_{M_0}. Or, les extensions S_0M et N de M sont linéairement disjointes, puisque G_M agit trivialement sur $G(S_0M/M)$; le corps N' composé de N et S_0M est donc une p-extension abélienne non ramifiée de M, et on a

$$(N' : M) = (S_0M : M)(N : M) = (S_0 : M_0)\, p^b.$$

Par suite, le produit $(S_0 : M_0)\, p^b$ divise h_M, c'est-à-dire que p^b divise h_M/h_{M_0}. Or, en utilisant (42) pour $\chi = \nu$, on déduit de (45) l'identité

$$a + b = \dim_{\mathbf{F}_p} \mathscr{S}(M)_\nu + \sum_{\chi \neq \nu} \bar{\delta}(\chi, M).\deg \chi.$$

Il s'ensuit donc :

PROPOSITION 60. — *Soient p un nombre premier inerte dans* K, $p \notin T$, *et* M *un sous-corps de* H *contenant* $K(\mu_p)$ *tel que* $(H : M) \not\equiv 0 \pmod p$. *Alors, on a*

$$p^{c_1} \mid (h_M/h_{M_0}),$$

où c_1 *désigne le plus petit entier supérieur à*

$$\frac{1}{2}\left[\dim_{\mathbf{F}_p} \mathscr{S}(M)_\nu + \sum_{\chi \neq \nu} \bar{\delta}(\chi, M).\deg \chi\right].$$

D'après l'identité (41), on en déduit le théorème suivant.

THÉORÈME 61. — *Soient p et* M *comme dans la proposition* 60. *Alors, on a*

$$p^{c_2} \mid (h_M/h_{M_0}),$$

où c_2 *désigne le plus petit entier supérieur à* $1/2 \sum_{\chi}^{*} \delta(\chi, M).\deg \chi$, *la somme étant prise sur les caractères irréductibles* χ *de* G_M *sur* $\mathbf{F}_p$ *tels que* $p+1 < k$, $p(k) < p^2 - 1$.

Comme remarqué immédiatement à la suite du théorème 28, suivant que

$$\chi = \sigma^k = \sigma^{p(k)}$$

ou

$$\chi = \sigma^k + \sigma^{p(k)}$$

avec

$$p+1 < k,\ p(k) < p^2-1,$$

la condition $\delta(\chi, H) = 0$ est équivalente à la condition A_k ou B_k du théorème 1. Par conséquent, le théorème 3 résulte du cas particulier $M = H$ du théorème précédent.

Pour conclure, considérons le sous-corps $M = K(\mu_p)$ de H. Comme p est inerte dans K, on a $(M : K) = p-1$ et les caractères irréductibles de $G_M = G(K(\mu_p)/K) = \mathcal{G}_M$ sur $\mathbf{F}_p$ sont les homomorphismes σ^k de G dans $\mathbf{F}_p$, tels que l'entier k soit divisible par $p+1$. On a :

PROPOSITION 62. — *Soit $p \notin T$ un nombre premier inerte dans K tel que $h \not\equiv 0 \pmod p$. Alors, pour que le nombre de classes d'idéaux $h_{K(\mu_p)}$ soit premier à p, il faut et il suffit que la condition (a) ci-dessous soit vérifiée.*

(a) Pour chaque entier k divisible par $p+1$, tel que $p+1 < k < p^2-1$, le défaut de régularité $\delta(\sigma^k, K(\mu_p))$, a priori égal à 0 ou 1, est nul.

Démonstration. — D'après le théorème 37 (§ 4), on a $\delta(v, M) = 0$. Par suite, à l'aide du lemme 27 (§ 3), on déduit de la condition (a) l'identité $\mathcal{G}(M) = \{0\}$. La proposition 10 (§ 2) implique alors que l'entier $h_{K(\mu_p)}$ est premier à p.

Réciproquement, si la condition (a) n'est pas vérifiée, alors le théorème 61 ci-dessus nous assure que l'entier $h_{K(\mu_p)}$ est bien divisible par p, ce qui complète la démonstration de la proposition.

APPENDICE

A. Une amélioration de la formule d'indice

D'après H. M. Stark [1], démonstration du lemme 1, il vient :

Lemme A.1. — *Pour toutes classes d'idéaux* $C \in Cl(\mathfrak{p})$ *et tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $6\mathfrak{p}$, *le nombre* $\theta(C, \mathfrak{a})$ *est une puissance d'ordre* 12 *dans* H.

Corollaire A.2. — *Pour tout idéal entier* $\mathfrak{a}$ *de* K *premier à* 6, *le quotient* $\Delta(L)^{N(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1}L)$ *est une puissance d'ordre* 12 *dans* H_0.

Démonstration. — Soit $R \subset \mathfrak{a}^{-1} L/L$. Pour chaque unité α de K, la multiplication par α induit une permutation $\lambda \mapsto \alpha.\lambda$ de $\mathfrak{a}^{-1} L/L$; nous notons $\alpha.R$ l'image de R par cette permutation. Comme $\mathfrak{a}$ est premier à 6, l'entier $N(\mathfrak{a}) = \#(\mathfrak{a}^{-1} L/L)$ est congru à 1 modulo *e*, si bien que l'on peut choisir R de façon que les deux conditions suivantes soient vérifiées :

(i) lorsque α parcourt les unités de K, on a

$$\bigcup_{\alpha} \alpha.R = \mathfrak{a}^{-1} L/L - \{0\};$$

(ii) pour tous couples d'unités α, α' de K, on a $\alpha.R \cap \alpha'.R = \emptyset$ si $\alpha \neq \alpha'$.

Or, on a $\mathscr{P}(\alpha\lambda, L) = \alpha^{-2} \mathscr{P}(\lambda, L)$ pour toute unité α de K. Par suite, le produit

$$\prod'_{\lambda \in \mathfrak{a}^{-1} L/L} (X - \mathscr{P}(\lambda, L))$$

est le carré du polynôme

$$P_{\mathfrak{a}}(X) = \prod_{\lambda \in R} (X^{e/2} - \mathscr{P}(\lambda, L)^{e/2}),$$

indépendant du choix de R. D'après la théorie de la multiplication complexe, les coefficients de $P_{\mathfrak{a}}(X)$ appartiennent à H_0 (*cf.* [28], § 4.2). Par conséquent, pour tout point τ de $\mathfrak{p}$-torsion modulo L, i. e. $\tau \in \mathfrak{p}^{-1} L$, $\tau \notin L$, et tout idéal entier $\mathfrak{a}$ de K premier à $6\mathfrak{p}$, le produit

$$\prod'_{\lambda \in \mathfrak{a}^{-1} L/L} (\mathscr{P}(\tau, L) - \mathscr{P}(\lambda, L))$$

est le carré de l'élément $P_{\mathfrak{a}}(\mathscr{P}(\tau, L))$ de $H = H_0(\mathscr{P}(\tau, L)^{e/2})$, corps de classes de rayon de K de conducteur $\mathfrak{p}$. De plus, la formule (4) (§ 0) implique l'identité

$$\theta(\tau, L; \mathfrak{a}) = \frac{\Delta(L)^{N(\mathfrak{a})}}{\Delta(\mathfrak{a}^{-1} L)} . P_{\mathfrak{a}}(\mathscr{P}(\tau, L))^{-12}, \tag{A.1}$$

où, comme on le sait, le nombre $\theta(\tau, L; \mathfrak{a}) \in H$ est non nul (*cf.* § 1). Par suite, le lemme A.1 nous assure que $\Delta(L)^{N(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1} L)$ est une puissance d'ordre 12 dans H.

Soit alors $\mathfrak{p}_2$ (resp. $\mathfrak{p}_3$) un diviseur premier de 2 (resp. 3) dans K. Pour tout idéal entier $\mathfrak{a}$ de K premier à 6, le quotient $\Delta(L)^{N(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1} L)$ est donc une puissance d'ordre 12 dans chacun des corps de classes de rayon $H^{(2)}$ et $H^{(3)}$ de K de conducteurs respectifs $\mathfrak{p}_2$ et $\mathfrak{p}_3$.

L'assertion du corollaire s'ensuit puisque les degrés $(H^{(2)} : H_0)$ et $(H^{(3)} : H_0)$ divisent respectivement 3 et 4. □

Notons Ψ' le sous-groupe de $H^\times$ engendré par les nombres

$$\delta_\alpha / P_\alpha(\mathscr{P}(\tau, L)),$$

où α parcourt les idéaux entiers de K premiers à $6\mathfrak{p}$, δ_α les éléments de H_0 tels que $\delta_\alpha^{12} = \Delta(L)^{N(\alpha)}/\Delta(\alpha^{-1} L)$, et où τ désigne un point de $\mathfrak{p}$-torsion modulo L *fixé une fois pour toutes*. Si $C_0 \in Cl(\mathfrak{p})$ désigne l'image du couple $(\tau, L) \in A(\mathfrak{p})$ par l'application $(\tau, \mathscr{L}) \mapsto C(\tau, \mathscr{L})$ du paragraphe 1, on a, d'après (A.1),

$$\theta(C_0, \alpha) = (\delta_\alpha / P_\alpha(\mathscr{P}(\tau, L)))^{12}.$$

Par suite, le groupe $(\Psi')^{12}$ est engendré par les nombres $\theta(C_0, \alpha)$, lorsque α parcourt les idéaux entiers de K premiers à $6\mathfrak{p}$; le lemme 6 (§ 1) prouve donc l'égalité

$$(\Psi')^{12} = \Psi,$$

où Ψ est défini comme dans le paragraphe 1.

Posons $\Theta' = \Psi' \cap \mathscr{E}$, et plus généralement, pour tout sous-corps M de H contenant K,

$$\Theta'(M) = N_{H/M} \Theta'.$$

On a donc $\Theta(M) = \Theta'(M)^{12}$, où $\Theta(M)$ est défini comme dans le paragraphe 1. Si $M_0 = M \cap H_0$, soit alors

$$\Omega'(M) = \mu(M).\mathscr{E}(M_0).\Theta'(M);$$

le groupe $\Omega(M)$, défini comme étant le produit $\varepsilon(M).\mathscr{E}(M_0).\Theta(M)$, est donc égal au groupe $\mu(M).\mathscr{E}(M_0).\Omega'(M)^{12}$. En raisonnant comme pour démontrer le corollaire du théorème 16, paragraphe 6.5, de [28], on obtient le théorème suivant.

THÉORÈME A.3. — *Soit p un nombre premier différent de* 2. *L'indice de* $\Omega'(M)$ (*resp.* $\Omega(M)$) *dans* $\mathscr{E}(M)$ *est égal au quotient*

$$\lambda' h_M / h_{M_0} \quad (resp.\ \lambda 12^{(M:K)} h_M / 12^{(M_0:K)} h_{M_0}),$$

où λ' *et* λ *sont des entiers tels que*

$$\lambda' \mid \lambda \mid e_{M_0}/e.$$

COROLLAIRE A.4. — *L'indice de* $\Omega(M)$ *dans* $\Omega'(M)$ *est égal à*

$$\lambda 12^{(M:K)} / \lambda' 12^{(M_0:K)}.$$

Remarque A.5. — *Les entiers* λ' *et* λ *sont premiers à p.*

Démonstration. — C'est clair pour $p \geqq 5$. Si $p = 3$, on a $H = H_0$, et donc $\lambda = 1$, à moins que p ne soit inerte dans K. Dans ce dernier cas, l'entier λ divise 2 puisque e_{H_0} est alors premier à 3.

Par ailleurs, comme dans le paragraphe 5, notons φ l'homomorphisme associé aux $\varphi_q = \varphi_{\Lambda_q}$, avec $\Lambda_q = u_q(t(\mathrm{P}))$ et $\mathrm{P} = \xi(\tau)$; d'après le paragraphe 5, cet homomorphisme répond aux conditions (i) à (iv) du théorème 12 (§ 3).

Reprenant alors la démonstration de la proposition 46 (§ 5), on obtient la proposition suivante.

PROPOSITION A.6. — *Soient p un nombre premier modulo lequel l'équation* (0) *se réduit bien, et* $\mathfrak{p}$ *un diviseur premier de p dans* K. *Alors, pour tout entier k divisible par e, tel que* $0 < k < \mathrm{N}(\mathfrak{p}) - 1$, *et tout idéal entier* $\mathfrak{a}$ *de* K *premier à* $6\mathfrak{p}$, *on a*

$$\varphi_k(\delta_\mathfrak{a}/\mathrm{P}_\mathfrak{a}(\mathscr{P}(\tau, \mathrm{L}))) \equiv \mathrm{G}_k^*(\mathfrak{a}, \mathrm{L}) \pmod{\mathfrak{p}(\mathrm{H}_0)},$$

où $\delta_\mathfrak{a}$ *désigne un quelconque élément de* H_0 *tel que* $\delta_\mathfrak{a}^{12} = \Delta(\mathrm{L})^{\mathrm{N}(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1}\mathrm{L})$.

Vu le théorème A.3 et la remarque A.5, ceci permet d'étendre le théorème 1, ainsi que les théorèmes 28 et 29, au cas où $p = 3$ est inerte dans K; en effet, dans ce cas, on peut toujours trouver une équation de Weierstrass d'invariant égal à $j(\mathscr{O})$, dont les coefficients g_2 et g_3 appartiennent à $\mathscr{O}(\mathrm{H}_0)$, ayant bonne réduction en 3 (*cf.* appendice D).

B. Cas où le corps de base est principal

Il s'agit des 9 (*cf.* [32]) corps quadratiques imaginaires de discriminants respectifs $-D = -3, -4, -7, -8, -11, -19, -43, -67$ et -163. L'anneau des entiers $\mathcal{O} = \mathcal{O}_D$ de chacun de ces corps est principal, c'est-à-dire que l'on a $h = 1$, ou ce qui revient au même $H_0 = K$.

Choisissons les nombres $g_2 = g_{2,D}$ et $g_3 = g_{3,D}$ comme dans le tableau suivant.

Tableau B.I

Valeurs des coefficients de l'équation de Weierstrass E_D

D	g_2	g_3
3.....	0	4
4.....	4	0
7.....	5.7	7^2
8.....	2.3.5	$2^2.7$
11.....	$2^3.3.11$	7.11^2
19.....	$2^3.19$	19^2
43.....	$2^4.5.43$	$3.7.43^2$
67.....	$2^3.5.11.67$	$7.31.67^2$
163.....	$2^4.5.23.29.163$	$7.11.19.127.163^2$

Le discriminant $\Delta_D = g_{2,D}^3 - 27\, g_{3,D}^2$ de l'équation de Weierstrass

$$y^2 = 4x^3 - g_{2,D}x - g_{3,D}$$

est alors égal à $-3^3.2^4$, 2^6, $-2^6.7^3$, $3^6.2^3$ et $-3^6.11^3$ pour les cinq premières valeurs de D, et à $-D^3$ pour les quatre dernières valeurs. Il s'ensuit que l'invariant

$$j_{E_D} = 2^6 3^3 g_{2,D}^3/\Delta_D$$

est égal à l'invariant modulaire $j(\mathcal{O}_D)$ (*cf.* [37], § 125, p. 460-462). Chacune des équations E_D ci-dessus possède donc des multiplications complexes par l'anneau des entiers de $K = \mathbf{Q}(\sqrt{-D})$. Désignons par q_D le nombre premier qui divise D; l'ensemble S_D des nombres premiers pour lesquels E_D a mauvaise réduction est formé de 2 et des diviseurs premiers de Δ_D, soit, si 3 n'est pas inerte dans K (i. e. $D = -3, -8$ ou -11),

$$S_D = \{2, 3\} \cup \{q_D\},$$

et, si 3 est inerte dans K,

$$S_D = \{2\} \cup \{q_D\}.$$

Par suite les équations précédentes ont bonne réduction pour tout nombre premier $p \geqq 5$ non ramifié dans K; de plus, les équations E_4, E_7, E_{19}, E_{43}, E_{67} et E_{163} ont bonne réduction en 3.

Comme les coefficients $g_{2,D}$ et $g_{3,D}$ des équations E_D sont des entiers rationnels, les nombres de Hurwitz $G_k(L)$ associés à celles-ci, pour k entier pair $\geqq 2$, sont des nombres rationnels; en effet, ce sont des éléments de $H_0 = K$ invariants par conjugaison complexe. Pour $k \geqq 8$, les nombres $G_k(L)$ se calculent par récurrence à partir de $G_4(L) = g_{2,D}/60$

TABLEAU B.II

Valeurs de $G_2(L)$

$-D$	-3	-4	-7	-8	-11	-19	-43	-67	-163
$G_2(L)$	0	0	1/2	1/2	2	2	12	2.19	$2^2.181$

et $G_6(L) = g_{3,D}/140$ à l'aide de la formule (D-10). Le tableau ci-dessus donne les valeurs de $G_2(L)$ (*cf.* appendice D).

Soit M un sous-corps de H contenant K. Comme $H_0 = K$, on a, pour tout caractère irréductible $\chi \neq 1$ de $G_M = G(M/K)$ sur $\mathbf{F}_p$,

$$\delta(\chi, M) = \delta(\chi, H),$$

et $\delta(\chi, H)$ ne peut prendre que la valeur 0 ou 1. Cette valeur est donnée par la proposition suivante, qui reprend la proposition 22 (§ 3) pour un corps de base principal, compte tenu du commentaire à la fin de l'appendice A.

PROPOSITION B.1. — *Soient p un nombre premier $\neq 2$, non ramifié dans* K, *et χ un caractère irréductible de* G *sur* $\mathbf{F}_p$, $\chi \neq 1$. *Si χ est de degré* 1 (*resp.* 2), *on désigne par k un entier divisible par e, tel que* $0 < k < N(\mathfrak{p})-1$ *et* $\chi = \sigma^k$ (*resp.* $\chi = \sigma^k + \sigma^{p(k)}$).

Alors, en distinguant entre les trois cas (*a*), (*a'*) *et* (*b*) *de la proposition* 22, *on a :*

Cas (*a*) : χ *de degré* 1, $\chi \neq \nu$.

$$\delta(\chi, H) = \begin{cases} 1, & \text{si } [G_k(L)] = 0, \\ 0, & \text{si } [G_k(L)] \neq 0. \end{cases}$$

Cas (*a'*) : p *inerte dans* K *et* $\chi = \nu$.

$$\delta(\nu, H) = 0 \quad \text{et} \quad [p\,G_{p+1}(L)] \neq 0.$$

Cas (*b*) : χ *de degré* 2.

$$\delta(\chi, H) = \begin{cases} 1, & \text{si } [G_k(L)] = [G_{p(k)}(L)] = 0, \\ 0, & \text{si } [G_k(L)] \neq 0 \quad \text{ou} \quad [G_{p(k)}(L)] \neq 0. \end{cases}$$

Nous allons maintenant démontrer, pour un corps de base K principal ([6]), une variante relative (prop. B.5 et th. B.6, ci-dessous) de la proposition 10 (§ 2), et du théorème 28 (§ 3). Rappelons d'abord quelques notations et résultats de [28].

Pour toute classe $C \in Cl(\mathfrak{p})$, soit $\varphi_{\mathfrak{p}}(C)$ l'entier de H, défini comme dans [28] (§ 2.2, p. 15). D'après [28] (§ 2.3, th. 1, p. 17), pour toute classe $C' \in Cl(\mathfrak{p})$ et tout idéal $\mathfrak{b}$ de C', on a

$$\varphi_{\mathfrak{p}}(C)^{(\mathfrak{b}, H/K)} = \varphi_{\mathfrak{p}}(CC'),$$

et le quotient $\varphi_{\mathfrak{p}}(C)/\varphi_{\mathfrak{p}}(C')$ est une unité de H. Pour tout sous-corps M de H contenant K, notons alors $Cl(M/K)$ le quotient de $Cl(\mathfrak{p})$ correspondant à l'extension M/K. Pour chaque classe $C \in Cl(M/K)$, le produit

$$\varphi_M(C) = \prod_{\hat{C} \in Cl(\mathfrak{p}),\, \hat{C} \subset C} \varphi_{\mathfrak{p}}(C)$$

est donc un entier de M.

Par ailleurs, notons e_M le nombre de racines de l'unité de M. Pour chaque classe $C \in Cl(M/K)$, et tout idéal entier $\mathfrak{a}_C$ de C, premier à $6\mathfrak{p}$, la classe de $N(\mathfrak{a}_C)$ modulo e_M ne dépend que de C. De plus, lorsque $\mathfrak{a}$ parcourt les idéaux entiers, premiers à $6\mathfrak{p}$, de la classe unité de $Cl(M/K)$, les entiers $N(\mathfrak{a})-1$ engendrent l'idéal (e_M) de $\mathbf{Z}$ (*cf.* [28], § 4.1, lemme 6, p. 31). Or, d'après [28] (§ 4.2, prop. 10, p. 35), pour toute classe $C \in Cl(\mathfrak{p})$ et tout idéal entier $\mathfrak{a}$ de K, premier à $\mathfrak{p}$, on a

$$\theta(C, \mathfrak{a})^p = \varphi_{\mathfrak{p}}(C)^{N(\mathfrak{a})}/\varphi_{\mathfrak{p}}(CC_{\mathfrak{a}}),$$

où $C_{\mathfrak{a}} \in Cl(\mathfrak{p})$ désigne la classe de $\mathfrak{a}$. Il s'ensuit :

LEMME B.2. — *Le groupe $\Theta(M)^p$ est l'ensemble des produits $\prod_{C \in Cl(M/K)} \varphi_M(C)^{n_C}$, où les entiers rationnels n_C sont astreints à vérifier les conditions $\Sigma n_C N(\mathfrak{a}_C) \equiv 0 \ (e_H)$ et $\Sigma n_C = 0$.*

Comme $H_0 = K$, le groupe $\Omega(M)$, d'indice fini dans $\mathscr{E}(M)$, est égal au produit $\mu(M)\,\Theta(M)$; par suite le lemme précédent prouve que les nombres $\varphi_M(C)$, $C \in Cl(M/K)$, sont multiplicativement indépendants : en effet, d'après [28] (§ 2.2, remarque p. 18-19), l'idéal $(\varphi_M(C))$ est strictement contenu dans l'anneau des entiers de M.

([6]) Lorsque le corps de base K n'est plus principal, désignons par M et N deux sous-corps de H contenant K tels que

$$M_0 = M \cap H_0 \subset N \subset H.$$

Nous ignorons si l'on a encore $\Omega(M) \cap N = \Omega(N)$ et $\Omega'(M) \cap N = \Omega'(N)$. Toutefois, la proposition B.5 et le théorème B.6 restent vrais, du moins si $p \neq 2$. En effet, on peut démontrer que l'indice de $\Omega(N)$ (resp. $\Omega'(N)$) dans $\Omega(M) \cap N$ (resp. $\Omega'(M) \cap N$) divise le quotient e_{M_0}/e du nombre de racines de l'unité de M_0 par celui de K; d'après la remarque A.5, ces indices sont donc premiers à p. On en déduit alors que l'indice du groupe $\Omega'(N)$ $\mathscr{E}(N)$ dans $\mathscr{E}(M)$ est égal à $\lambda\, h_M/h_N$, où $\lambda = \lambda(M, N)$ est un entier premier à p.

On déduit alors du lemme précédent :

PROPOSITION B.3. — *Soit* K *un corps quadratique imaginaire principal. Pour tous sous-corps* M *et* N *de* H *contenant* K, *tels que* $N \subset M$, *on a*

$$\Omega(M) \cap N = \Omega(N),$$

et par suite

$$\Omega'(M) \cap N = \Omega'(N).$$

Démonstration. — Il s'agit de vérifier l'identité

$$(\mu(M)\Theta(M)) \cap N = \mu(N)\Theta(N),$$

avec $\Theta(N) = N_{M/N}\Theta(M)$; pour cela, il suffit de prouver l'identité

$$\Theta(M)^p \cap N = \Theta(N)^p.$$

Or, le groupe $\Theta(N)^p$ est trivialement contenu dans $\Theta(M)^p \cap N$. Réciproquement, soit u un élément de $\Theta(M)^p \cap N$; d'après le lemme, on a donc

$$u = \prod_{C \in Cl(M/K)} \varphi_M(C)^{m_C},$$

où les entiers rationnels m_C sont tels que $\sum_{C \in Cl(M/K)} n_C = 0$ et $\sum_{C \in Cl(M/K)} m_c N(\mathfrak{a}_C) \equiv 0 (e_M)$. Les nombres $\varphi_M(C)$, $C \in Cl(M/K)$, étant multiplicativement indépendants et permutés transitivement par $G_M = G(M/K)$, l'appartenance de u à N nous assure que l'on a $m_{C_1} = m_{C_2}$, des que les classes C_1 et C_2 de $Cl(M/K)$ sont contenues dans une même classe de $Cl(N/K)$. Si $\hat{C} \in Cl(M/K)$ est contenue dans $C \in Cl(N/K)$, on pose donc $n_C = m_{\hat{C}}$, et il vient

$$u = \prod_{C \in Cl(N/K)} \varphi_N(C)^{n_C},$$

où les entiers rationnels n_C vérifient les relations

$$\sum_{C \in Cl(N/K)} n_C = 0 \qquad \text{et} \qquad (M : N) \cdot \sum_{C \in Cl(N/K)} n_C N(\mathfrak{a}_C) \equiv 0 (e_N).$$

Or, si $H = K$ on a $M = N$ et il n'y a rien à démontrer. Supposons donc $H \neq K$; si p est différent de 2, les entiers e et p sont alors premiers entre eux et on a $e_N = ep^\varepsilon$, où ε est égal à 1 ou 0 suivant que N contient ou non le groupe des racines p-ièmes de l'unité; si $p = 2$, on a $e_N = e$ et l'on pose $\varepsilon = 0$. Avec ces notations, puisque le degré $(M : N)$ est premier à p, les entiers n_C vérifient alors la congruence

$$\sum_{C \in Cl(N/K)} n_C N(\mathfrak{a}_C) \equiv 0 (p^\varepsilon).$$

D'après le lemme, celle-ci prouve que u appartient à $\Theta(N)^p$. En effet, puisque K contient le groupe des racines de l'unité d'ordre e, on a

$$\sum n_C N(\mathfrak{a}_C) = \sum n_C (N(\mathfrak{a}_C) - 1) \equiv 0 (e),$$

si bien que les entiers n_C vérifient les conditions $\Sigma\, n_C = 0$ et $\Sigma\, n_C\, N(\mathfrak{a}_C) \equiv 0\ (e_N)$, caractéristiques des éléments de $\Theta(N)^p$. La proposition est démontrée.

Par ailleurs, on a

$$[\mathscr{E}(M) : \Omega'(M)\mathscr{E}(N)] = [\mathscr{E}(M) : \Omega'(M)]/[\mathscr{E}(N) : \Omega'(M) \cap \mathscr{E}(N)],$$

et, d'après la proposition précédente,

$$[\mathscr{E}(N) : \Omega'(M) \cap \mathscr{E}(N)] = [\mathscr{E}(N) : \Omega'(N)].$$

Or, d'après le théorème A.3, si $p \neq 2$, les indices $[\mathscr{E}(M) : \Omega'(M)]$ et $[\mathscr{E}(N) : \Omega'(N)]$ sont respectivement égaux à h_M et h_N. Ceci prouve le théorème suivant.

THÉORÈME B.4. — *Soient p un nombre premier différent de* 2, *et* K, M, N *comme précédemment. On a*

$$[\mathscr{E}(M) : \Omega'(M)\mathscr{E}(N)] = h_M/h_N.$$

Mais, lorsque χ parcourt les caractères irréductibles de G_M sur $\mathbf{F}_p$, dont la restriction au groupe de Galois G(M/N) n'est pas constante, le quotient $\mathscr{E}(M)/\Omega'(M)\,\mathscr{E}(N)\,\mathscr{E}(M)^p$ est isomorphe à la somme directe

$$\bigoplus_{\chi} (\mathscr{E}(M)/\Omega'(M)\mathscr{E}(M)^p)_\chi.$$

Par suite, si l'on pose $\mathscr{S}(M) = \mathscr{E}(M)/\Omega'(M)\,\mathscr{E}(M)^p$, définition qui coïncide, pour $p \geqq 5$, avec celle donnée dans le paragraphe 2, on obtient la variante suivante de la proposition 10 (§ 2).

PROPOSITION B.5. — *Soit p un nombre premier différent de* 2. *Les deux conditions suivantes sont équivalentes :*

(i) $h_M/h_N \not\equiv 0 \pmod{p}$.

(ii) *Pour tout caractère irréductible* χ *de* G_M *sur* $\mathbf{F}_p$, *non constant sur* G(M/N), *on a*

$$\mathscr{S}(M)_\chi = \{0\}.$$

On en déduit en particulier le théorème suivant, dont le théorème 28 (§ 3), pour un corps de base K principal, est le cas particulier N = K et $p \geqq 5$.

THÉORÈME B.6. — *Soient p un nombre premier* $\neq 2$, *pour lequel l'équation* (0) *a bonne réduction, et* K, M, N *comme dans la proposition* B.3. *Alors, le quotient* h_M/h_N *est premier à p, si, pour tout caractère irréductible* χ *de* G_M *sur* $\mathbf{F}_p$, *non constant sur* G(M/N), *le défaut de régularité* $\delta(\chi, M) = \delta(\chi, H)$ *est nul.*

Venons-en maintenant à des exemples numériques précis d'utilisation de la proposition B.1 et du théorème B.6. Nous distinguons entre les nombres premiers inertes et ceux décomposés dans K.

Nous nous référons librement aux minorations de discriminants obtenues récemment par A. M. Odlyzko et autres. En effet, pour des corps de nombres de discriminant suffisamment petit, celles-ci interdisent l'existence d'extensions non ramifiées de degré trop élevé, (*cf.* G. Poitou [24], § 7, remarque). Pour des tables numériques d'emploi commode, on peut provisoirement se référer à [23].

Enfin, pour $p \neq 2$ inerte dans K, et χ un caractère irréductible de G sur $\mathbf{F}_p$, on pose $N_\chi = N(H_\chi)$, où $N(H_\chi)$ désigne l'extension abélienne non ramifiée de H_χ telle que $G(N(H_\chi)/H_\chi) \simeq \pi(H)_\chi$ (*cf.* § 6, p. 345).

(a) NOMBRES PREMIERS INERTES DANS K, $3 \leqq p \leqq 13$:

— $p = 3$, *inerte dans* $K = \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-19})$, $\mathbf{Q}(\sqrt{-43})$, $\mathbf{Q}(\sqrt{-67})$ *et* $\mathbf{Q}(\sqrt{-163})$.

D'après la proposition B.1, pour chacun de ces corps, excepté $\mathbf{Q}(\sqrt{-43})$, on a $\delta(\chi, H) = 0$ pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_3$; le théorème B.6 implique donc

$$(h_H, 3) = 1$$

lorsque le corps de base K est différent de $\mathbf{Q}(\sqrt{-43})$.

Ici $H = \mathbf{Q}(\sqrt{-1}, \sqrt{-3})$ pour $K = \mathbf{Q}(\sqrt{-1})$; sinon H est une extension cyclique de degré 4 de K qui contient $K(\sqrt{-3})$. Notons que la formule de Dirichlet pour les corps biquadratiques bicycliques (*cf.* [10], § 26), nous assure que le corps $K(\sqrt{-3})$ est principal dès que K l'est : il suffit de vérifier sur une table que le nombre de classes du corps $\mathbf{Q}(\sqrt{3D})$ est bien 1 (*cf.* [4], tables 1 et 2).

Par ailleurs, les minorations de discriminant d'Odlyzko, appliquées à H, impliquent $h_H = 1$ pour $K = \mathbf{Q}(\sqrt{-7})$, $h_H \leqq 2$ pour $K = \mathbf{Q}(\sqrt{-19})$, $h_H \leqq 8$ pour $K = \mathbf{Q}(\sqrt{-43})$ et $h_H \leqq 28$ pour $K = \mathbf{Q}(\sqrt{-67})$. Appliquons ceci au corps $K = \mathbf{Q}(\sqrt{-43})$. D'après la proposition B.1, on a $\delta(\sigma^4, H) = 0$ tandis que $\delta(\sigma^2+\sigma^6, H) = 1$. Le lemme 27 (§ 3), modifié par l'appendice A, implique donc $\mathscr{S}(H)_{\sigma^4} = \{0\}$. Supposons $\mathscr{S}(H)_{\sigma^2+\sigma^6}$ non nul; comme le degré de $\sigma^2+\sigma^6$ est 2, on aurait

$$\dim_{\mathbf{F}_3} \mathscr{S}(H)_{\sigma^2+\sigma^6} = 2,$$

et h_H devrait être divisible par 9. La contradiction avec Odlyzko implique la trivialité de $\mathscr{S}(H)$; la proposition B.5 nous assure donc que l'on a encore

$$(h_H, 3) = 1 \quad (7).$$

---

(7) Pour $K = \mathbf{Q}(\sqrt{-43})$, nous avons étudié de manière un peu détaillée le groupe des unités elliptiques de H.

Rappelons d'abord que $\alpha = 16855 + 4.7.53\sqrt{3.43}$ est l'unité fondamentale, totalement positive, de $\mathbf{Q}(\sqrt{3.43})$. Dans $\mathbf{Q}(\sqrt{-3}, \sqrt{-43})$, l'unité $-\alpha$ est un carré :

$$-\alpha = \delta^2, \qquad \text{avec} \quad \delta = 53\sqrt{-3} + 14\sqrt{-43}.$$

Posons

$$a = \frac{5\sqrt{-43}-11}{2} + \frac{19\sqrt{-3}-\sqrt{3.43}}{2};$$

le nombre

$$\rho = \frac{1}{2}\left[a + \sqrt{-3}\sqrt{159+14\sqrt{3.43}}\right]$$

est racine de l'équation

$$X^2 - aX - \delta = 0.$$

— $p = 5$, *inerte dans* $K = \mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-43})$, $\mathbf{Q}(\sqrt{-67})$ *et* $\mathbf{Q}(\sqrt{-163})$.

En appliquant la proposition B.1, pour chacun des cinq premiers de ces corps et pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_5$, nous avons trouvé $\delta(\chi, H) = 0$, si bien que le théorème B.6 implique

$$(h_M, 5) = 1$$

pour toute extension abélienne M de K de conducteur (5).

Par contre, pour $K = \mathbf{Q}(\sqrt{-163})$, nous avons trouvé $\delta(\nu^2, H) = \delta(\nu^3, H) = 1$ et $\delta(\chi, H) = 0$ pour tous les autres caractères irréductibles $\chi \neq 1$ de G sur $\mathbf{F}_5$. Par suite, d'après le théorème 61 (§ 6), le nombre de classes du corps $\mathbf{Q}(\sqrt{-163}, e^{2\pi i/5})$ est divisible par 5. Notons que ν^2 et ν^3 sont bien reflets l'un de l'autre dans le miroir de Leopoldt. Nous avons étudié ce cas un peu plus précisément dans [28], appendice, p. 67-76. On y a prouvé les isomorphismes

$$\mathscr{S}(H)_{\nu^2} \simeq \mathrm{Gal}(N_{\nu^2}/H_{\nu^2}) \simeq \mathbf{Z}/5$$

et $\mathscr{S}(H)_{\nu^3} \simeq \mathrm{Gal}(N_{\nu^3}/H_{\nu^3}) = \{0\}$; on a ici $H_{\nu^2} = \mathbf{Q}(\sqrt{-163}, \sqrt{5})$ et

$$H_{\nu^3} = \mathbf{Q}(\sqrt{-163}, e^{2\pi i/5}).$$

En particulier, le nombre de classes du corps $\mathbf{Q}(\sqrt{-163}, \sqrt{5})$ est divisible par 5; il est en fait égal à 15 d'après la formule de Dirichlet. Le lemme 27 (§ 3) prouve donc que $\mathscr{S}(H)_{\nu^2}$ est la seule composante non nulle de $\mathscr{S}(H)$. Par suite, d'après la proposition B.5, le nombre de classes des extensions abéliennes M de conducteur (5) de $\mathbf{Q}(\sqrt{-163})$,

---

Si C désigne la classe de l'idéal $((1 + \sqrt{-43})/2)$ dans $Cl(\mathfrak{p}) = Cl(3)$, on a

$$\rho^{36} = \varepsilon \frac{\varphi_H(C^3)^2 \varphi_H(C)}{\varphi_H(C^2)^2 \varphi_H(1)},$$

avec $\varepsilon^2 = 1$. Il s'ensuit que ρ appartient à $\Omega'(H)$.

On vérifie alors que ρ engendre $\Omega'(H)$ modulo torsion en tant que $\mathbf{Z}[G]$-module (ou, de manière équivalente, que ρ^{12} engendre $\Omega(H)$ modulo torsion). Ensuite, comme $N_{H/K}\rho = -1$ n'est pas un carré dans H, on montre que les éléments de $\Omega'(H)$ qui sont des carrés dans H appartiennent à $\Omega'(H)^2$. Le nombre de classes h_H, égal à l'indice $[\mathscr{E}(H) : \Omega'(H)]$ d'après le théorème B.6, est donc impair. Comme on sait déjà que h_H est premier à 3 et inférieur ou égal à 8, on doit donc avoir

$$h_H = 1,5 \text{ ou } 7.$$

Si $\sigma = (((1 + \sqrt{-43})/2), H/K)$, on prouve alors que $h_H = 5$ (resp. 7) si et seulement si le produit $u = \rho(\rho^\sigma)^2 \rho^{\sigma^2}$, qui vérifie

$$u^{36} = \frac{\varphi_H(1)\varphi_H(C)}{\varphi_H(C^2)\varphi_H(C^3)},$$

possède une racine 5-ième (resp. 7-ième) dans H. Un calcul numérique sans difficulté établit qu'il n'en est rien. On a donc $h_H = 1$ et $\mathscr{E}(H) = \Omega'(H)$; en particulier ρ engendre $\mathscr{E}(H)$ modulo torsion en tant que $\mathbf{Z}[G]$-module. □

auxquelles $\sqrt{5}$ appartient, est exactement divisible par 5; leur unique extension abélienne non ramifiée de degré une puissance de 5 est donc $N_{v2}M/M$. Quant aux extensions abéliennes non ramifiées de conducteur (5) de $\mathbf{Q}(\sqrt{-163})$, auxquelles $\sqrt{5}$ n'appartient pas, leur nombre de classes est premier à 5.

– $p = 7$, *inerte dans* $K = \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-11})$, $\mathbf{Q}(\sqrt{-43})$, $\mathbf{Q}(\sqrt{-67})$ *et* $\mathbf{Q}(\sqrt{-163})$.

Pour chacun de ces 6 corps et pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_7$, nous avons trouvé $\delta(\chi, H) = 0$, si bien que le théorème B.6 implique

$$(h_M, 7) = 1,$$

pour toute extension abélienne M de K de conducteur (7).

– $p = 11$, *inerte dans* $K = \mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-67})$ *et* $\mathbf{Q}(\sqrt{-163})$.

Pour les deux premiers de ces corps, nous avons trouvé, en appliquant la proposition B.1,

$$\delta(\chi, H) = 0$$

pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_{11}$; d'après le théorème B.6, on a donc

$$(h_M, 11) = 1,$$

pour toute extension abélienne M de $\mathbf{Q}(\sqrt{-3})$ ou $\mathbf{Q}(\sqrt{-1})$ de conducteur (11).

Quant aux corps $K = \mathbf{Q}(\sqrt{-67})$ et $\mathbf{Q}(\sqrt{-163})$, nous avons respectivement trouvé $\delta(\chi, H) = 0$ pour tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_{11}$ différent de $\sigma^4+\sigma^{44}$ et $\sigma^8+\sigma^{88}$ (resp. $\sigma^6+\sigma^{66}$), tandis que l'on a $\delta(\sigma^4+\sigma^{44}, H) = \delta(\sigma^8+\sigma^{88}, H) = 1$ (resp. $\delta(\sigma^6+\sigma^{66}, H) = 1$). Désignons par H_{σ^8} (resp. H_{σ^6}) le sous-corps d'indice 4 (resp. 3) de H qui contient $K = \mathbf{Q}(\sqrt{-67})$ (resp. $K = \mathbf{Q}(\sqrt{-163})$). Le théorème B.6 nous assure alors que

$$(h_M, 11) = 1,$$

pour toute extension abélienne M de $\mathbf{Q}(\sqrt{-67})$ (resp. $\mathbf{Q}(\sqrt{-163})$) de conducteur (11), ne contenant pas H_{σ^8} (resp. H_{σ^6}). Mais, nous ignorons si les groupes $\mathscr{S}(H)_{\sigma^4+\sigma^{44}}$ et $\mathscr{S}(H)_{\sigma^8+\sigma^{88}}$ (resp. le groupe $\mathscr{S}(H)_{\sigma^6+\sigma^{66}}$) sont nuls ou non, de sorte que, pour le corps H_{σ^8} (resp. H_{σ^6}) et à plus forte raison pour le corps H lui-même, nos méthodes ne nous permettent pas de conclure; notons toutefois que $\sigma^4+\sigma^{44}$ et $\sigma^8+\sigma^{88}$ sont reflets l'un de l'autre dans le miroir de Leopoldt, et que $\sigma^6+\sigma^{66}$ y est son propre reflet.

– $p = 13$, inerte dans $K = \mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-11})$, $\mathbf{Q}(\sqrt{-19})$, $\mathbf{Q}(\sqrt{-67})$ et $\mathbf{Q}(\sqrt{-163})$.

En appliquant la proposition B.1, nous avons trouvé $\delta(\chi, H) = 0$ pour chacun des quatre corps $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-11})$ et $\mathbf{Q}(\sqrt{-67})$ et tout caractère irréductible $\chi \neq 1$ de G sur $\mathbf{F}_{13}$, si bien que le théorème B.6 implique

$$(h_M, 13) = 1$$

pour toute extension abélienne M de conducteur (13) de l'un de ces corps; ceci s'applique en particulier à leur extension abélienne maximale H de conducteur (13) (*cf.* appendice C).

Par contre, pour les corps $K = \mathbf{Q}(\sqrt{-19})$ et $\mathbf{Q}(\sqrt{-163})$ nous avons trouvé $\delta(v^4, H) = \delta(v^9, H) = 1$ (resp. $\delta(v^5, H) = \delta(v^8, H) = 1$) et $\delta(\chi, H) = 0$ pour tous les autres caractères irréductibles $\chi \neq 1$ de G sur $\mathbf{F}_{13}$. Le théorème 61 (§ 6) nous assure donc que 13 divise le nombre de classes des corps $\mathbf{Q}(\sqrt{-19}, e^{2\pi i/13})$ et $\mathbf{Q}(\sqrt{-163}, e^{2\pi i/13})$. Plus précisément, d'après la formule (42) (§ 6), on a, pour $K = \mathbf{Q}(\sqrt{-19})$,

$$\begin{aligned} &\#\mathscr{S}(H)_{v^4} . \# \operatorname{Gal}(N_{v^9}/H_{v^9}) \\ &= \#\mathscr{S}(H)_{v^9} . \# \operatorname{Gal}(N_{v^4}/H_{v^4}) = 13, \end{aligned} \tag{B.1}$$

et, pour $K = \mathbf{Q}(\sqrt{-163})$,

$$\begin{aligned} &\#\mathscr{S}(H)_{v^8} . \# \operatorname{Gal}(N_{v^5}/H_5) \\ &= \#\mathscr{S}(H)_{v^5} . \neq \operatorname{Gal}(N_{v^8}/H_{v^8}) = 13. \end{aligned} \tag{B.2}$$

Ici H_{v^4} (resp. H_{v^8}) est le corps obtenu par adjonction de $\sqrt{-19}$ (resp. $\sqrt{-163}$) à l'extension cubique cyclique A de conducteur 13 de $\mathbf{Q}$. Quant à H_{v^9} (resp. H_{v^5}) c'est le sous-corps d'indice 3 de $\mathbf{Q}(\sqrt{-19}, e^{2\pi i/13})$ qui contient $\mathbf{Q}(\sqrt{-19})$ (resp. le corps $\mathbf{Q}(\sqrt{-163}, e^{2\pi i/13})$).

Mais $\mathscr{E}^{(13)}(A(\sqrt{-19}))$ (resp. $\mathscr{E}^{(13)}(A(\sqrt{-163}))$) s'injecte dans $U^{(13)}(A(\sqrt{-19}))$ (resp. $U^{(13)}(A(\sqrt{-163}))$); en effet A est le sous-corps réel de $A(\sqrt{-19})$ et $A(\sqrt{-163})$, si bien que les groupes $\mathscr{E}^{(13)}(A(\sqrt{-19}))$ et $\mathscr{E}^{(13)}(A(\sqrt{-163}))$ sont isomorphes au quotient $\mathscr{E}/\mathscr{E}^{13}$ du groupe $\mathscr{E}$ des unités de A, et notre assertion résulte alors de ce que 13 est régulier sur $\mathbf{Q}$. Par suite, les groupes $\pi(A(\sqrt{-19}))$ et $\pi(A(\sqrt{-163}))$ sont nuls; ceci prouve la trivialité des extensions N_{v^9}/H_{v^9} (pour $K = \mathbf{Q}(\sqrt{-19})$) et N_{v^5}/H_{v^5} (pour $K = \mathbf{Q}(\sqrt{-163})$). D'après les identités (B.1) et (B.2), on a donc les isomorphismes

$$\mathscr{S}(A(\sqrt{-19}))_{v^4} \simeq \mathbf{Z}/13 \simeq \mathscr{S}(A(\sqrt{-163}))_{v^8},$$

et, d'après la proposition B.5, les nombres de classes des corps $A(\sqrt{-19})$ et $A(\sqrt{-163})$ sont divisibles par 13. En fait, les techniques de H. Hasse [10], en particulier la formule (1) (§ 27, p. 79), et la formule (3) (§ 28, p. 82, *loc. cit.*), permettent de déterminer les nombres de classes relatifs h_* des corps $A(\sqrt{-19})$ et $A(\sqrt{-163})$; on trouve respectivement 13 et 7.13 pour valeurs de h_*. Comme le corps A est principal, on a donc

$$h_{A(\sqrt{-19})} = 13 \qquad \text{et} \qquad h_{A(\sqrt{-163})} = 7.13.$$

On peut de même déterminer le nombre de classes relatif du sous-corps H_{v^9}, qui contient $\mathbf{Q}(\sqrt{-19})$ et est d'indice 3 dans $\mathbf{Q}(\sqrt{-19}, e^{2\pi i/13})$, (resp. du corps $H_{v^5} = \mathbf{Q}(\sqrt{-163}, e^{2\pi i/13})$); on trouve respectivement 3 et $7^3.13.17$ ([8]).

([8]) Pour le premier de ces corps les contributions respectives de χ_9^{19}, $\chi_{13}^6\chi_9^{19}$, et de la classe de conjugaison de χ_{13}^3 (avec les notations de [10]), sont 1/2, 3 et 1/2. Il s'ensuit que l'indice Q est égal à 2 et h_* à 3.

Pour le corps $\mathbf{Q}(\sqrt{-163}, e^{2\pi i/13})$ les contributions de χ_{163}^{81} et $\chi_{13}^6\chi_{163}^{81}$ sont respectivement 1/2 et 17, et celles des classes de conjugaison de χ_{13}, χ_{13}^3, $\chi_{13}^2\chi_{163}^{81}$ et $\chi_{163}^4\chi_{163}^{81}$ (de degrés respectifs 4, 2, 2 et 2) sont 1/13, 1/2, 7^2 et 7.13. Il s'ensuit que l'indice Q est égal à 2 et h_* à $7^3.13.17$.

Par ailleurs, le sous-corps réel maximal B de H_{v^9} est le sous-corps réel cyclique de degré 4 de $\mathbf{Q}(\sqrt{-19}, e^{2\pi i/13})$; son discriminant D est $13^3.19^2$, d'où

$$D^{1/4} = 13^{3/4}.19^{1/2} < 29{,}8425.$$

Les minorations de discriminant d'Odlyzko nous assurent que B ne peut pas posséder d'extension réelle non ramifiée de degré > 9; par suite, le nombre de classes de B est premier à 13. En fait, d'après un calcul que M. N. Gras a bien voulu nous communiquer, le corps B est principal, et donc $h_{B(\sqrt{-19})} = 3$; ainsi, d'après la proposition B.5, le groupe $\mathscr{S}(H_{v^9})$ est nul, et, compte tenu de l'identité (B.1), on a l'isomorphisme

$$\mathrm{Gal}(N_{v^4}/A(\sqrt{-19})) \simeq \mathbf{Z}/13 \simeq \mathscr{S}(A(\sqrt{-19}))_{v^4}.$$

Compte tenu du lemme 27 (§ 3), le groupe $\mathscr{S}(H)_{v^4}$ est donc la seule composante non nulle de $\mathscr{S}(H)$, et la proposition B.5 prouve que le nombre de classes des extensions abéliennes M de conducteur (13) de $\mathbf{Q}(\sqrt{-19})$, qui contiennent le corps A, est exactement divisible par 13; leur unique extension abélienne non ramifiée de degré une puissance de 13 est donc $N_{v^4}M/M$. Quant aux extensions abéliennes de conducteur (13) de $\mathbf{Q}(\sqrt{-19})$ qui ne contiennent pas A, leur nombre de classes est premier à 13.

De même, pour prouver l'isomorphisme présumé

$$\mathrm{Gal}(N_{v^8}/A(\sqrt{-163})) \simeq \mathbf{Z}/13 \simeq \mathscr{S}(A(\sqrt{-163}))_{v^8},$$

ou, ce qui revient au même d'après le lemme 27 (§ 3) et l'identité (B.2), que $\mathscr{S}(H)_{v^8}$ est la seule composante non nulle de $\mathscr{S}(H)$, il suffirait de prouver que le nombre de classes du sous-corps réel maximal (9) de $\mathbf{Q}(\sqrt{-163}, e^{2\pi i/13})$ est premier à 13. Mais, nous n'en savons rien, si bien que la proposition B.5 prouve seulement que le nombre de classes des extensions abéliennes de conducteur (13) de $\mathbf{Q}(\sqrt{-163})$, qui contiennent le corps A, est divisible par 13, tandis que le nombre de classes de celles qui ne contiennent pas A, est premier à 13.

(b) NOMBRES PREMIERS DÉCOMPOSÉS DANS K, $5 \leqq p \leqq 107$ OU $p = 163$.

Nos résultats sont réunis dans le tableau B.III. On y indique, pour chaque corps $K = \mathbf{Q}(\sqrt{-D})$ et chaque nombre premier p décomposé dans K, les entiers k divisibles par e, tels que $0 < k < p-1$, pour lesquels le numérateur du nombre de Hurwitz $G_k(L) \in \mathbf{Q}$ (où $L \subset \mathbf{C}$ désigne le réseau associé à l'équation E_D) est divisible par p, c'est-à-dire pour lesquels on a

$$[G_k(L)] = 0.$$

Par exemple, pour $K = \mathbf{Q}(\sqrt{-43})$ et $p = 67$, on a

$$[G_{30}(L)] = [G_{38}(L)] = [G_{62}(L)] = 0.$$

(9) Son discriminant D est égal à $13^{11}.163^6$, d'où $D^{1/12} = 13^{11/12}.163^{1/2} < 134{,}0321$.

TABLEAU B.III

Nombres premiers irréguliers décomposés dans K

Les croix désignent les couples (K, p), où p est inerte ou ramifié dans K, et les cases blanches les nombres premiers réguliers décomposés dans K.

K \ p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
$Q(\sqrt{-3})$												36 *				
$Q(\sqrt{-1})$																36;56 *
$Q(\sqrt{-7})$																
$Q(\sqrt{-2})$											26;36 *					
$Q(\sqrt{-11})$																
$Q(\sqrt{-19})$					12 *							30				
$Q(\sqrt{-43})$											24					
$Q(\sqrt{-67})$						2	16									
$Q(\sqrt{-163})$											28		12	32		

K \ p	67	71	73	79	83	89	97	101	103	107	163
$Q(\sqrt{-3})$				66 *							
$Q(\sqrt{-1})$											
$Q(\sqrt{-7})$											
$Q(\sqrt{-2})$	18 *					? manque				36	
$Q(\sqrt{-11})$		24									82
$Q(\sqrt{-19})$								78			82
$Q(\sqrt{-43})$	30;38 62			76							
$Q(\sqrt{-67})$		20				22;72					84
$Q(\sqrt{-163})$		58			62						

Précisons trois points :

– Dans les limites du tableau nous n'avons rencontré aucun nombre de Hurwitz $G_k(L)$ comme ci-dessus, dont le numérateur soit divisible par p^2.

– Pour le corps $K = \mathbf{Q}(\sqrt{-7})$, les nombres de Hurwitz $G_k(L)$, avec k entier pair tel que $0 < k < p-1$, sont tous p-inversibles, du moins lorsque p est un nombre premier décomposé dans $\mathbf{Q}(\sqrt{-7})$ inférieur ou égal à 163.

– Lorsque p est « irrégulier pour K », il est parfois possible d'utiliser les minorations de discriminants d'Odlyzko pour prouver que le nombre de classes de H (corps de classes de K pour le rayon modulo $\mathfrak{p}$) est premier à p; il suffit pour cela que D et p ne soient pas trop grands ([10]). Dans ce cas, la proposition 57 (§ 6) affirme l'existence d'extensions abéliennes de degré p de H, non ramifiées en dehors de $\mathfrak{p}$ et sauvagement ramifiées en $\mathfrak{p}$: il y a autant de telles extensions linéairement indépendantes que d'indices k, divisibles par e, vérifiant

$$0 < k < p-1 \qquad \text{et} \qquad [G_k(L)] = 0.$$

Ces couples sont désignés dans le tableau B.III par un astérisque.

([10]) Prenons pour exemple le corps $\mathbf{Q}(\sqrt{-2})$ dans lequel 67 est décomposé. Tous les nombres $G_k(L)$, pour k pair tel que $0 < k < 66$, sont 67-inversibles, à l'exception de $G_{18}(L)$. Par suite, d'après le lemme 27 (§ 3), on a $\mathscr{S}(H)_\chi = \{0\}$ pour tout caractère irréductible χ de $G = \mathrm{Gal}(H/K)$ sur $\mathbf{F}_{67}$ différent de σ^{18}. Désignons par M l'unique sous-corps d'indice 3 de H contenant $\mathbf{Q}(\sqrt{-2})$; c'est une extension de degré 11 de $\mathbf{Q}(\sqrt{-2})$. Son discriminant D vérifie

$$|D|^{1/22} = 8^{1/2}.67^{5/11} < 19{,}1241.$$

Il s'ensuit que l'on a $h_M \leqq 12$: le nombre de classes de M est premier à 67. D'après la proposition B.5, on a donc $\mathscr{S}(M) = \{0\}$, et en particulier

$$\mathscr{S}(H)_{\sigma^{18}} = \mathscr{S}(M)_{\sigma^{18}} = \{0\},$$

de sorte que le groupe $\mathscr{S}(H)$ est nul. La proposition B.5 nous assure que le nombre de classes de H est premier à 67.

C. Remarques sur le travail cité d'A. P. Novikov

Pour chaque corps quadratique imaginaire K, d'anneau des entiers $\mathcal{O}$, A. P. Novikov introduit dans [22] (p. 1075) des invariants $B_m^K \in H_0$, définis pour m entier $\geqq 1$. Dans nos notations, ces invariants vérifient l'identité formelle

$$-\frac{z}{e}\frac{\partial}{\partial z}\log \mathscr{P}'(z, L) = \frac{3}{e} + \sum_{m\geqq 1} B_m^K z^{em}/(m-1)!,$$

où $L \subset \mathbf{C}$ désigne le réseau associé à l'équation de Weierstrass, d'invariant $j(\mathcal{O})$, ainsi choisie :

$$y^2 = 4x^3 - 1, \quad \text{si} \quad K = \mathbf{Q}(\sqrt{-3});$$
$$y^2 = 4x^3 - x, \quad \text{si} \quad K = \mathbf{Q}(\sqrt{-1});$$
$$y^2 = 4x^3 - 3j(j-2^6 3^3)x - j(j-2^6 3^3)^2,$$

avec $j = j(\mathcal{O})$, si $K \neq \mathbf{Q}(\sqrt{-3})$ et $\neq \mathbf{Q}(\sqrt{-1})$.

Or, la fonction elliptique $\mathscr{P}'(z, L)$ admet pour pôles les points de L, chacun d'ordre 3, et pour zéros les points de $(L/2)-L$, chacun d'ordre 1, d'où l'identité

$$\mathscr{P}'(z, L)^{12} = \Delta(L)^3 \theta\left(z, \frac{1}{2}L\right)\Big/\theta(z, L)^4 = \Delta(L)^3/\theta(z, L; (2)).$$

Par suite, d'après la formule (6) (§ 0), on a

$$-\frac{z}{e}\frac{\partial}{\partial z}\log \mathscr{P}'(z, L) = \frac{3}{e} + \sum_{\substack{k>0 \\ e \mid k}} \frac{(2^k-4)}{e} G_k(L) z^k.$$

En identifiant, il vient

$$B_m^K/(m-1)! = \frac{(2^{em}-4)}{e} G_{em}(L).$$

Ainsi, pour $p \geqq 5$ et $e \leqq em \leqq (p-1)-e$, les nombres B_m^K sont des éléments $\mathfrak{p}$-entiers de H_0 (*cf.* [22], lemme 10), et B_m^K est $\mathfrak{p}$-inversible si et seulement si le nombre de Hurwitz $G_{em}(L)$ et l'entier $2^{em}-4$ le sont. De plus, pour $K \neq \mathbf{Q}(\sqrt{-1})$ et $\neq \mathbf{Q}(\sqrt{-3})$, on a $B_1^K = 0$.

Le théorème 2 de [22], qui a inspiré le théorème 1 du présent travail, est plus faible que celui-ci des points de vue suivants :

– il ne concerne que les corps $K = \mathbf{Q}(\sqrt{-1})$ et $K = \mathbf{Q}(\sqrt{-3})$, et les nombres premiers qui s'y décomposent;

– même dans ce cas, la condition obtenue est un peu moins stricte.

Dans le même article, il est énoncé que p divise le nombre de classes h_H du corps de classes H de K pour le rayon modulo $\mathfrak{p}$, pourvu que K soit différent de $\mathbf{Q}(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-3})$ et que p satisfasse les quatre conditions suivantes :

(i) p est inerte dans K;

(ii) p ne divise pas $6\,N_{H_0/K}(j(\mathcal{O})(j(\mathcal{O})-2^6 3^3))$;

(iii) le résidu du nombre 2 a un ordre pair dans le groupe $\mathbf{F}_p^\times$ des résidus modulo p;

(iv) le corps H contient au moins une unité non congrue modulo $\mathfrak{q}^2$ à un élément de H_0, pour un idéal premier convenable $\mathfrak{q}$ de H au-dessus de $\mathfrak{p}$.

(*Cf.* [22] th. 1, p. 1073).

En fait, ceci n'est pas toujours exact; examinons par exemple le cas où le corps K est principal. Notons encore D la valeur absolue du discriminant de K, et $L \subset \mathbf{C}$ le réseau associé à l'équation de Weierstrass E_D. La condition (iv) est relativement facile à vérifier. D'après le lemme 24 (§ 3) et la proposition 22 (*b*), il suffit que le nombre rationnel $G_2(L)$ soit p-inversible. Pour la condition (iii), elle est certainement vérifiée par $p = 13$; en effet, on a

$$2^6 = 64 \equiv -1 \pmod{13},$$

de sorte que la classe de 2 modulo 13 est d'ordre 12. De plus, d'après le tableau I de l'appendice B, aucun des entiers rationnels $j(\mathcal{O}_D) = 2^6 3^3 g_{2,D}^3/\Delta_D$ et $j(\mathcal{O}_D)-2^6 3^3 = 2^6 3^6 g_{3,D}^2/\Delta_D$ n'est divisible par 13. Enfin, le nombre 13 est inerte dans chacun des corps principaux $K = \mathbf{Q}(\sqrt{-D})$, avec D = 7, 8, 11, 19, 67 et 163, si bien que 13 satisfait aux conditions (i) à (iv) pour chacun de ces six corps.

Or, les calculs dont nous avons donné les résultats dans l'appendice B prouvent que l'on a $(h_H, 13) = 1$, lorsque H désigne le corps de classes du rayon modulo (13) de l'un quelconque des quatre corps $\mathbf{Q}(\sqrt{-D})$, avec D = 7, 8, 11 et 67.

D. Méthode de calcul des nombres de Hurwitz

Table des sections :

(*a*) construction d'une équation de Weierstrass d'invariant $j(\mathcal{O})$, ayant bonne réduction en p;

(*b*) formules pour $G_2(\mathfrak{a}^{-1}L)$, $G_4(\mathfrak{a}^{-1}L)$ et $G_6(\mathfrak{a}^{-1}L)$;

(*c*) estimation du dénominateur de $G_2(\mathfrak{a}^{-1}L)$;

(*d*) détermination de L et calcul de $G_2(L)$;

(*e*) calcul de $G_k(\mathfrak{a}^{-1}L)$ à partir des nombres $G_k(L)$ et $\lambda(\mathfrak{a}, L)$;

(*f*) étude de $\lambda(\mathfrak{a}, L)$; équation de Weierstrass minimale;

(*g*) calcul de $\lambda(\mathfrak{a}, L)$;

(*h*) récapitulation et formule de récurrence pour les séries d'Eisenstein G_k, $k \geqq 8$.

(*a*) *Construction d'une équation de Weierstrass, d'invariant égal à $j(\mathcal{O})$, ayant bonne réduction en p.*

Soit K un corps quadratique imaginaire d'anneau des entiers $\mathcal{O}$, et supposons que l'on connaisse l'invariant modulaire $j(\mathcal{O})$ ([11]). Rappelons que la théorie de la multiplication complexe nous dit que $j(\mathcal{O})$ est un entier algébrique de degré égal au nombre de classes d'idéaux h de K; le corps $H_0 = K(j(\mathcal{O}))$ est l'extension abélienne non ramifiée maximale de K. De plus $j(\mathcal{O})$ est réel; en effet, l'anneau $\mathcal{O}$ est stable pour la conjugaison complexe. Par suite, lorsque $h = 1$, l'invariant $j(\mathcal{O})$ est un entier rationnel (*cf.* appendice B), et lorsque $h = 2$, un élément entier du sous-corps quadratique réel de H_0 (*cf.* appendice E).

Il est alors facile de construire une courbe elliptique E, représentée par une équation de Weierstrass

$$y^2 = 4x^3 - g_2 x - g_3,$$

d'invariant $j_E = 2^6 3^3 g_2^3/(g_2^3 - 27 g_3^2)$ égal à $j(\mathcal{O})$, dont les coefficients g_2 et g_3 appartiennent à l'anneau des entiers $\mathcal{O}(H_0)$ de H_0 :

– si $K = \mathbf{Q}(\sqrt{-3})$, on peut prendre $g_2 = 0$ et $g_3 = 4$; l'équation E_3 correspondante a bonne réduction en dehors de 2 et 3;

– si $K = \mathbf{Q}(\sqrt{-1})$, on peut prendre $g_2 = 4$ et $g_3 = 0$; l'équation E_4 correspondante a bonne réduction en dehors de 2;

– enfin, si $K \neq \mathbf{Q}(\sqrt{-3})$ et $\neq \mathbf{Q}(\sqrt{-1})$, c'est-à-dire $j(\mathcal{O}) \neq 0$ et $\neq 2^6 3^3$, on peut prendre $g_2 = 3j(j-2^6 3^3)$ et $g_3 = j(j-2^6 3^3)^2$ avec $j = j(\mathcal{O})$; si D désigne la valeur absolue du discriminant de K, l'équation E_D ainsi définie a bonne réduction en dehors des diviseurs premiers de $N_{H_0/\mathbf{Q}}(6j(j-2^6 3^3))$.

De plus, quel que soit le nombre premier p, il existe une courbe elliptique E, définie sur H_0 et d'invariant j_E égal à $j(\mathcal{O})$, ayant bonne réduction en p (*cf.* [30], § 6, cor. 1,

([11]) Cette hypothèse est très restrictive. En effet, on ne sait calculer $j(\mathcal{O})$ que pour un nombre fini de corps quadratiques imaginaires de petit discriminant (*cf.* [37] et [2] ainsi que [26], [36] et [3]).

p. 507). Il en résulte que, pour tout idéal premier $\mathfrak{q}$ de H_0, le discriminant

$$\Delta = g_2^3 - 27 g_3^2 = 2^6 3^6 j^2 (j - 2^6 3^3)^3$$

de l'équation E_D doit vérifier $v_\mathfrak{q}(\Delta) \equiv 0 \pmod 6$, d'où les congruences

$$v_\mathfrak{q}(j) \equiv 0 \pmod 3, \qquad v_\mathfrak{q}(j - 2^6 3^3) \equiv 0 \pmod 2.$$

Par suite, pour $p \neq 2$ et $\neq 3$, on peut toujours « tordre » les coefficients de l'équation E_D, de façon à lui donner bonne réduction en p, tout en lui conservant sa forme d'équation de Weierstrass à coefficients dans $\mathcal{O}(H_0)$.

Il en est de même pour $p = 3$, à condition que 3 soit inerte dans K. En effet, on a alors

$$v_\mathfrak{q}(j) = 3 \qquad \text{et} \qquad v_\mathfrak{q}(j - 2^6 3^3) \geqq 6,$$

pour tout idéal premier $\mathfrak{q}$ de H_0 au-dessus de 3 ([12]). Or, comme $v_\mathfrak{q}(j - 2^6 3^3)$ est pair, il existe α dans H_0 tel que

$$\begin{cases} 2 v_\mathfrak{q}(\alpha) + v_\mathfrak{q}(j - 2^6 3^3) = 0, & \text{si } \mathfrak{q} \mid 3; \\ v_\mathfrak{q}(\alpha) \geqq 0, & \text{si } (\mathfrak{q}, 3) = 1. \end{cases}$$

Les coefficients « tordus » :

$$\begin{cases} g_2' = g_2 (\alpha 3^{-2})^2 = (j/3^3) \times \alpha^2 (j - 2^6 3^3), \\ g_3' = g_3 (\alpha 3^{-2})^3 = (j/3^3) \times \alpha^3 (j - 2^6 3^3)^2 3^{-3} \end{cases}$$

appartiennent alors à $\mathcal{O}(H_0)$. De plus g_2' est 3-inversible, si bien que le discriminant $\Delta' = (g_2')^3 - 27 (g_3')^2$ l'est aussi : l'équation associée à g_2' et g_3' a bien bonne réduction en 3.

(*b*) *Formules pour* $G_2(\mathfrak{a}^{-1} L)$, $G_4(\mathfrak{a}^{-1} L)$ *et* $G_6(\mathfrak{a}^{-1} L)$.

Désignons toujours par D la valeur absolue du discriminant de K, et supposons connue une équation de Weierstrass

$$E_D : \quad y^2 = 4x^3 - g_2 x - g_3,$$

d'invariant $j = 2^6 3^3 g_2^3/(g_2^3 - 27 g_3^2)$ égal à $j(\mathcal{O})$ et dont les coefficients g_2 et g_3 appartiennent à $\mathcal{O}(H_0)$. Soit $L = \rho\mathcal{O}$, avec $\rho \in \mathbf{C}^\times$, le réseau tel que

$$g_2 = 60 G_4(L) \qquad \text{et} \qquad g_3 = 140 G_6(L).$$

([12]) Soit E une courbe elliptique, définie sur H_0, d'invariant $j = j(\mathcal{O})$, ayant bonne réduction en 3. Comme 3 est inerte dans K, la courbe elliptique réduite modulo n'importe quel idéal premier $\mathfrak{q}$ de H_0 au-dessus de 3 est supersingulière, autrement dit ne possède aucun point d'ordre 3; par suite, on a $v_\mathfrak{q}(j) > 0$. D'après [30], § 6, p. 510, ceci, joint au fait que E a bonne réduction en 3, implique $v_\mathfrak{q}(j - 2^6 3^3) \geqq 6$ et donc $v_\mathfrak{q}(j) = 3$.

Pour $\mathfrak{a}$ idéal entier de K, les formules (5) et (6) (§ 0) impliquent l'identité

$$12\left[N(\mathfrak{a})-1+\sum_{\substack{k>0\\ e\mid k}}(G_k(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_k(L))z^k\right]$$
$$=-6z\frac{\mathscr{P}'(z,L)}{\mathscr{P}(z,L)}\sum_{\lambda\in\mathfrak{a}^{-1}L/L}{}'\left[1-\frac{\mathscr{P}(\lambda,L)}{\mathscr{P}(z,L)}\right]^{-1}.$$

Développons le membre de droite en série de puissances de z jusqu'à l'ordre 6, puis identifions les coefficients de z^2, z^4 et z^6 dans chacun des deux membres. On obtient les formules (*cf.* aussi J. Vélu [35]) :

$$(D.1)\qquad G_2(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_2(L)=\mathscr{P}^{(1)}_{\mathfrak{a},L},$$

$$(D.2)\qquad G_4(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_4(L)=\mathscr{P}^{(2)}_{\mathfrak{a},L}-6(N(\mathfrak{a})-1)G_4(L),$$

$$(D.3)\qquad G_6(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_6(L)=\mathscr{P}^{(3)}_{\mathfrak{a},L}-9G_4(L)\mathscr{P}^{(1)}_{\mathfrak{a},L}-15(N(\mathfrak{a})-1)G_6(L),$$

où l'on a posé $\mathscr{P}^{(i)}_{\mathfrak{a},L}=\sum'_{\lambda\in\mathfrak{a}^{-1}L/L}\mathscr{P}^i(\lambda,L)$ pour $i=1$, 2 et 3, la somme étant prise sur tous les éléments λ non nuls de $\mathfrak{a}^{-1}L/L$.

Ces formules peuvent être utilisées pour calculer les nombres $G_2(\mathfrak{a}^{-1}L)$, $G_4(\mathfrak{a}^{-1}L)$ et $G_6(\mathfrak{a}^{-1}L)$ à partir de $G_2(L)$, $G_4(L)$ et $G_6(L)$, en s'aidant du q-développement de la fonction $\mathscr{P}(z,L)$ ([13]). De même, à condition de choisir pour $\mathfrak{a}$ un idéal principal, la formule (D.1) permet de calculer $G_2(L)$ à partir de $G_4(L)$ et $G_6(L)$.

(*c*) *Estimation du dénominateur de* $G_2(\mathfrak{a}^{-1}L)$.

La somme $\mathscr{P}^{(1)}_{\mathfrak{a},L}$ étant une fonction symétrique des $\mathscr{P}(\lambda,L)$, lorsque λ parcourt les éléments non nuls de $\mathfrak{a}^{-1}L/L$, appartient donc à H_0; par suite, quel que soit l'idéal entier $\mathfrak{a}$ de K, la quantité $2\mathscr{P}^{(1)}_{\mathfrak{a},L}$ doit être un entier algébrique (*cf.* J. W. S. Cassels [5]). D'après (D.1), le produit $2(G_2(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_2(L))$ appartient donc à $\mathscr{O}(H_0)$.

Choisissons alors pour $\mathfrak{a}$ un idéal principal (α) de K. Il vient

$$G_2(\mathfrak{a}^{-1}L)-N(\mathfrak{a})G_2(L)=\alpha(\alpha-\bar{\alpha})G_2(L),$$

([13]) Soit $\mathscr{L}\subset\mathbf{C}$ un réseau de base (w_1,w_2) telle que $\mathrm{Im}(w_2/w_1)>0$, et posons

$$q=e^{2\pi i w_2/w_1},\qquad q_z=e^{2\pi i z/w_1}.$$

Alors, pour tout $z\in\mathbf{C}-\mathscr{L}$, on a

$$(D.4)\qquad \left(\frac{w_1}{2\pi i}\right)^2\mathscr{P}(z,\mathscr{L})=\frac{1}{12}+\sum_{m\in\mathbf{Z}}\frac{q^m q_z}{(1-q^m q_z)^2}-2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n};$$

(*cf.* e. g. [16], chap. 4, § 2, prop. 3).

En fait, comme $z\mapsto\mathscr{P}(z,\mathscr{L})$ admet $\mathscr{L}$ pour réseau de périodes, et est une fonction paire de z, on peut toujours choisir un représentant de z de façon que l'on ait

$$|q|^{1/2}\leqq|q_z|\leqq|q|^{-1/2},$$

si bien que la série (D.4) converge très rapidement et fournit de bons résultats numériques.

où $\bar{\alpha}$ désigne le conjugué de α. Comme le p.p.c.m. des nombres α $(\alpha-\bar{\alpha})$ est l'idéal $(\sqrt{-D})$, il s'ensuit que $2\sqrt{-D}\,G_2(L)$, et donc $2\sqrt{-D}\,G_2(\mathfrak{a}^{-1}L)$, appartient toujours à $\mathcal{O}(H_0)$.

(*d*) *Détermination de* L *et calcul de* $G_2(L)$.

Cas $h = 1$.

Lorsque $K = \mathbf{Q}(\sqrt{-3})$ ou $K = \mathbf{Q}(\sqrt{-1})$, on a alors $G_2(L) = 0$, puisque K possède des unités d'ordre > 2 tandis que la série d'Eisenstein G_2 est homogène de poids -2.

Supposons donc K différent de $\mathbf{Q}(\sqrt{-3})$ et $\mathbf{Q}(\sqrt{-1})$, ce qui équivaut à demander que chacun des nombres $G_4(L)$ et $G_6(L)$ soit non nul. Si $\rho = \rho(L)$ désigne le nombre complexe tel que $L = \rho\,\mathcal{O}$, on déduit alors de l'homogénéité des séries d'Eisenstein G_4 et G_6 la formule suivante pour ρ^2

$$\rho^2 = \left(\frac{G_6(\mathcal{O})}{G_6(L)}\right)\left(\frac{G_4(\mathcal{O})}{G_4(L)}\right)^{-1} = \frac{140}{60}\,\frac{g_2}{g_3}\,\frac{G_6(\mathcal{O})}{G_4(\mathcal{O})}.$$

Les nombres g_2 et g_3 étant donnés et les q-développements de $G_4(\mathcal{O})$ et $G_6(\mathcal{O})$ connus ([14]), cette formule permet de calculer numériquement le nombre transcendant ρ^2, et donc L. Du q-développement de $G_2(\mathcal{O})$ ([14]), on déduit alors la valeur de

$$G_2(L) = \rho^{-2}\,G_2(\mathcal{O}).$$

Enfin, pour déterminer exactement $G_2(L)$, il suffit de se rappeler que $2\sqrt{-D}\,G_2(L)$ appartient à l'anneau des entiers de $H_0 = K$, comme prouvé en (*c*). De plus, les quantités $G_2(\mathcal{O})$, $G_4(\mathcal{O})$ et $G_6(\mathcal{O})$ sont réelles, et les invariants g_2 et g_3, considérés dans l'appendice B, entiers rationnels donc réels; par suite $G_2(L)$ est aussi réel. Suivant que $K = \mathbf{Q}(\sqrt{-2})$ ou $K \neq \mathbf{Q}(\sqrt{-2})$, il s'ensuit que le produit $4\,G_2(L)$ ou $2\,G_2(L)$ est un entier rationnel ([15]).

Cas $h > 1$.

Le raisonnement dans son principe est le même que précédemment.

Pour tout idéal $\mathfrak{a}$ de K, désignons par $(\mathfrak{a}, H_0/K) \in G(H_0/K)$ l'automorphisme d'Artin de l'extension H_0/K associé à $\mathfrak{a}$. Pour tout élément γ de $G(H_0/K)$, soit $L_\gamma \subset \mathbf{C}$ le réseau

---

([14]) Soit $\mathscr{L} \subset \mathbf{C}$ un réseau de base (w_1, w_2), avec $\mathrm{Im}(w_2/w_1) > 0$. Alors, on a

$$\left(\frac{w_1}{2\pi}\right)^2 G_2(\mathscr{L}) = \frac{1}{6\times 2}\left[1-24\sum_{n\geq 1}\frac{nq^n}{1-q^n} - \frac{3}{\pi\,\mathrm{Im}(w_2/w_1)}\right]$$

$$\left(\frac{w_1}{2\pi}\right)^4 G_4(\mathscr{L}) = \frac{1}{30\times 24}\left[1+240\sum_{n\geq 1}\frac{n^3q^n}{1-q^n}\right],$$

$$\left(\frac{w_1}{2\pi}\right)^6 G_6(\mathscr{L}) = \frac{1}{42\times 720}\left[1-504\sum_{n\geq 1}\frac{n^5q^n}{1-q^n}\right],$$

où l'on a posé $q = e^{2\pi i(w_2/w_1)}$ (*cf.* e. g. [16], chap. 4).

Bien entendu, on utilise ici ces formules pour $\mathscr{L} = \mathcal{O}$, et lorsque $h > 1$, pour $\mathscr{L} = \mathfrak{a}^{-1}$, avec $\mathfrak{a}$ idéal de K. □

([15]) Les valeurs trouvées pour $G_2(L)$, sont données dans le tableau B.II.

tel que

$$G_4(L_\gamma) = G_4(L)^\gamma, \qquad G_6(L_\gamma) = G_6(L)^\gamma;$$

d'après (D.1), on a donc

$$G_2(L_\gamma) = G_2(L)^\gamma.$$

Or, d'après la théorie de la multiplication complexe, on a

$$j(\mathcal{O})^{(\mathfrak{a}, H_0/K)} = j(\mathfrak{a}^{-1}),$$

si bien qu'il existe un nombre complexe $\rho(\mathfrak{a}) = \rho(\mathfrak{a}, L)$ non nul tel que

$$L_{(\mathfrak{a}, H_0/K)} = \rho(\mathfrak{a}, L)\mathfrak{a}^{-1}.$$

Soient $\gamma \in G(H_0/K)$ et $\mathfrak{a}$ un idéal de K tels que $(\mathfrak{a}, H_0/K) = \gamma$. Les nombres $g_2^\gamma = 60\, G_4(L_\gamma)$ et $g_3^\gamma = 140\, G_6(L_\gamma)$, ainsi que les q-développements de $G_2(\mathfrak{a}^{-1})$, $G_4(\mathfrak{a}^{-1})$ et $G_6(\mathfrak{a}^{-1})$ étant connus (*cf.* note ci-dessus), les formules suivantes permettent de calculer $\rho(\mathfrak{a})^2$, puis $G_2(L_\gamma) = G_2(L)^\gamma$:

$$\text{(D.5)} \qquad \begin{cases} \rho(\mathfrak{a})^2 = \dfrac{140}{60}\dfrac{g_2^\gamma}{g_3^\gamma}\dfrac{G_6(\mathfrak{a}^{-1})}{G_4(\mathfrak{a}^{-1})}, \\ G_2(L_\gamma) = \rho(\mathfrak{a})^{-2} G_2(\mathfrak{a}^{-1}). \end{cases}$$

Lorsque γ parcourt $G(H_0/K)$, on obtient ainsi un système de h valeurs

$$a_\gamma + ib_\gamma, \qquad \text{avec } a_\gamma \text{ et } b_\gamma \text{ réels},$$

approchant les nombres $G_2(L)^\gamma$; système qu'il suffit ensuite de résoudre sachant que $2\sqrt{-D}\, G_2(L)$ est un entier de H_0.

En fait, *nous n'avons entrepris ce calcul que dans le cas* $h = 2$; le cas $h > 2$ reste à traiter. D'après Gauss, lorsque $h = 2$, il existe un diviseur premier d_+ de D tel que $H_+ = \mathbf{Q}(\sqrt{d_+})$ soit le sous-corps réel de H_0, et on a

$$H_0 = K(\sqrt{d_+}) = \mathbf{Q}(\sqrt{d_+}, \sqrt{-D}).$$

De plus, la classe non triviale de K peut être représentée par un diviseur premier ϑ de D dans K. Posons $\tau = (\vartheta, H_0/K)$: c'est l'automorphisme non trivial de l'extension H_0/K; autrement dit, on a

$$\begin{cases} (\sqrt{d_+})^\tau = -\sqrt{d_+} \\ (\sqrt{-D})^\tau = \sqrt{-D}. \end{cases}$$

Nous choisissons les coefficients g_2 et g_3 de E_D dans l'anneau des entiers $\mathcal{O}(H_+)$: c'est possible, quitte à étendre l'ensemble des nombres premiers où E_D se réduit mal; en effet $j(\mathcal{O})$ appartient à $\mathbf{R} \cap \mathcal{O}(H_0) = \mathcal{O}(H_+)$, comme remarqué en (*a*). Les nombres $G_2(\mathcal{O})$, $G_4(\mathcal{O})$ et $G_6(\mathcal{O})$, ainsi que g_2, g_3 et g_2^τ, g_3^τ sont donc tous réels; de plus, comme $\vartheta \mid D$, l'idéal ϑ

est invariant par conjugaison : les nombres $G_2(\vartheta)$, $G_4(\vartheta)$ et $G_6(\vartheta)$ sont aussi réels. Par suite, les valeurs numériques obtenues pour $G_2(L)$ et $G_2(L)^\tau$ doivent représenter des éléments conjugués de H_+. La valeur exacte de $G_2(L)$ s'en déduit immédiatement : on sait que $2\sqrt{-D}\,G_2(L)$ appartient à $\mathcal{O}(H_0)$, si bien que, pour D impair (resp. pair) le produit $2\sqrt{d_+}\,G_2(L)$ (resp. $4\sqrt{d_+}\,G_2(L)$) doit être un élément entier de H_+.

(*e*) *Calcul de* $G_k(\mathfrak{a}^{-1}L)$ *à partir des nombres* $G_k(L)$ *et* $\lambda(\mathfrak{a}, L)$.

Pour tout idéal $\mathfrak{a}$ de K, désignons par $\lambda(\mathfrak{a}, L)$ le quotient $\rho(\mathfrak{a}, L)/\rho(L)$: c'est le nombre complexe caractérisé par l'identité

$$\mathfrak{a}^{-1}L = \lambda(\mathfrak{a}, L)^{-1}.L_{(\mathfrak{a}, H_0/K)}. \tag{D.6}$$

Cette identité définit $\lambda(\mathfrak{a}, L)$ à multiplication près par une unité de K.

Si l'idéal $\mathfrak{a}$ est principal, le nombre $\lambda(\mathfrak{a}, L)$ est simplement un générateur de $\mathfrak{a}$. En général, d'après (*d*), le nombre $\lambda(\mathfrak{a}, L)$ vérifie les identités suivantes qui le caractérisent :

$$\begin{cases} G_2(\mathfrak{a}^{-1}L) = \lambda(\mathfrak{a}, L)^2.G_2(L)^{(\mathfrak{a}, H_0/K)}, \\ G_4(\mathfrak{a}^{-1}L) = \lambda(\mathfrak{a}, L)^4.G_4(L)^{(\mathfrak{a}, H_0/K)}, \\ G_6(\mathfrak{a}^{-1}L) = \lambda(\mathfrak{a}, L)^6.G_6(L)^{(\mathfrak{a}, H_0/K)}. \end{cases} \tag{D.7}$$

Par suite, la puissance *e*-ième $\lambda(\mathfrak{a}, L)^e$ de $\lambda(\mathfrak{a}, L)$ appartient à H_0; comme $e = 2$ pour $K \neq \mathbf{Q}(\sqrt{-3})$ et $\neq \mathbf{Q}(\sqrt{-1})$, ceci prouve que $\lambda(\mathfrak{a}, L)^2$ appartient à H_0, quel que soit le corps de base K.

En fait, pour tout entier pair $k > 0$, on a

$$G_k(\mathfrak{a}^{-1}L) = \lambda(\mathfrak{a}, L)^k.G_k^{(\mathfrak{a}, H_0/K)}; \tag{D.8}$$

en effet, pour tout entier pair $k \geqq 8$, la série d'Einsenstein G_k s'exprime comme un polynôme à coefficients rationnels en G_4 et G_6 (*cf.* (*h*), formule (D.10)). Ainsi, la détermination de $G_k(\mathfrak{a}^{-1}L)$ se ramène-t-elle à celle des nombres $G_k(L)$ et $\lambda(\mathfrak{a}, L)$.

(*f*) *Étude de* $\lambda(\mathfrak{a}, L)$*; équation de Weierstrass minimale.*

Les nombres $\lambda(\mathfrak{a}, L)$ introduits précédemment possèdent les propriétés formelles suivantes :

(i) *pour tout* $\alpha \in K^\times$, *on a*

$$\lambda(\alpha\mathfrak{a}, L)^e = \alpha^e.\lambda(\mathfrak{a}, L)^e;$$

(ii) *pour tout* $\beta \in H_0^\times$, *on a*

$$\lambda(\mathfrak{a}, \beta^{1/e}L)^e = \lambda(\mathfrak{a}, L)^e.\beta^{(\mathfrak{a}, H_0/K)}/\beta,$$

ou $\beta^{1/e}$ *désigne une racine e-ième de* β*;*

(iii) *pour tout élément* γ *de* $G(H_0/K)$, *on a*

$$\lambda(\mathfrak{a}, L_\gamma)^e = (\lambda(\mathfrak{a}, L)^e)^\gamma;$$

(iv) (*propriété de cocycle*). *Pour tout couple* $\mathfrak{a}$, $\mathfrak{b}$ *d'idéaux de* K, *on a*

$$\lambda(\mathfrak{ab}, L)^e = (\lambda(\mathfrak{b}, L)^e)^{(\mathfrak{a}, H_0/K)} . \lambda(\mathfrak{a}, L)^e.$$

La propriété (i) résulte trivialement de (D.6). Les propriétés (ii) et (iv) se déduisent facilement de (D.7), et il en est de même de (iii) compte tenu de la relation

$$G_k(\mathfrak{a}^{-1} L_\gamma) = G_k(\mathfrak{a}^{-1} L)^\gamma.$$

Ces propriétés permettent de décrire un peu plus précisément les nombres $\lambda(\mathfrak{a}, L)$. Commençons par un résultat d'ordre général.

PROPOSITION D.1. — *Soient* $\mathfrak{a}$ *un idéal de* K, $n_\mathfrak{a}$ *l'ordre de* $(\mathfrak{a}, H_0/K)$ *dans* $G(H_0/K)$ *et* $m_\mathfrak{a}$ *le p.p.c.m de e et* $n_\mathfrak{a}$. *Alors, pour chaque générateur* $\alpha \in K^\times$ *de* $\mathfrak{a}^{n_\mathfrak{a}}$, *il existe* $\beta \in H_0^\times$ *tel que*

$$\lambda(\mathfrak{a}, L)^{m_\mathfrak{a}} = \alpha^{m_\mathfrak{a}/n_\mathfrak{a}} . \beta^{(\mathfrak{a}, H_0/K)}/\beta.$$

Démonstration. — D'après les propriétés (i) et (iv) des nombres $\lambda(\mathfrak{a}, L)$, il vient :

$$\alpha^e = \lambda(\mathfrak{a}^{n_\mathfrak{a}}, L)^e = \prod_{k=1}^{n_\mathfrak{a}} (\lambda(\mathfrak{a}, L)^e)^{(\mathfrak{a}^k, H_0/K)}. \tag{D.9}$$

Posons alors $\eta = (\lambda(\mathfrak{a}, L)^{n_\mathfrak{a}}/\alpha)^{e/\text{p.g.c.d}(e, n_\mathfrak{a})}$; d'après (D.9), on a $\prod_{k=1}^{n_\mathfrak{a}} \eta^{(\mathfrak{a}^k, H_0/K)} = 1$, et l'assertion de la proposition résulte du théorème 90 de Hilbert.

Restreignons-nous maintenant au cas $h = 2$, et adoptons les notations introduites à la fin de (*d*). En particulier $\mathfrak{P}$ désigne un diviseur premier non principal de D dans K, et $\tau = (\mathfrak{P}, H_0/K)$ l'automorphisme non trivial de H_0/K. On a $\mathfrak{P}^2 = (N\mathfrak{P})$, et, d'après la proposition précédente, il existe β_1 et β_2 dans $H_0^\times$ tels que

$$\begin{cases} \lambda(\mathfrak{P}, L)^2 + N(\mathfrak{P})\beta_1^\tau/\beta_1 = 0, \\ \lambda(\mathfrak{P}, L)^2 - N(\mathfrak{P})\beta_2^\tau/\beta_2 = 0. \end{cases}$$

D'après la propriété (ii) des nombres $\lambda(\mathfrak{a}, L)$, il s'ensuit

$$\lambda(\mathfrak{P}, \beta_i^{-1/2} L)^2 = (-1)^i N(\mathfrak{P}), \qquad i = 1, 2.$$

De plus, si g_2 et g_3 appartiennent à $H_+ = \mathbf{Q}(\sqrt{d_+})$, l'identité (D.9), avec $\mathfrak{a} = \mathfrak{P}$ et $\alpha = \pm N\mathfrak{P}$, nous assure que l'on peut choisir β_1 et β_2 dans H_+. Mais, le quotient β_i^τ/β_i ne dépend que la classe de β_i modulo $\mathbf{Q}^\times$, et l'on peut aussi bien choisir β_1 et β_2 entiers dans H_+. Ceci implique la proposition suivante :

PROPOSITION D.2. — *Soient* K *un corps quadratique imaginaire de nombre de classes* 2, *et* $\mathfrak{P}$ *un diviseur premier non principal de* D *dans* K.

Alors, il existe des équations de Weierstrass :

$$E_D^{(i)} : \quad y^2 = 4x^3 - g_2^{(i)} x - g_3^{(i)}, \qquad i = 1, 2,$$

dont les invariants sont égaux à $j(\mathcal{O})$ *et les coefficients* $g_2^{(i)}$ *et* $g_3^{(i)}$ *appartiennent à* $\mathcal{O}(H_+)$, *telles que les réseaux* $L_1 \subset \mathbf{C}$ *et* $L_2 \subset \mathbf{C}$ *respectivement associés à* $E_D^{(1)}$ *et* $E_D^{(2)}$ *vérifient*

$$\lambda(\vartheta, L_1)^2 + N(\vartheta) = 0, \tag{1}$$

$$\lambda(\vartheta, L_2)^2 - N(\vartheta) = 0. \tag{2}$$

De plus, les identités (D.1) et (D.7) nous fournissent un critère commode pour reconnaître si un réseau L vérifie l'une des relations (1) ou (2) de la proposition précédente. Plus précisément, on a :

LEMME D.3. — *Soient* $\vartheta \mid D$ *et* E_D *comme dans la proposition précédente,* $L \subset \mathbf{C}$ *le réseau associé à* E_D *et* $G_2(L) = (m/2) + (n\sqrt{d_+}/2\,d_+)$, *où m et n sont des nombres rationnels tels que* $(2m, 2n) \in \mathbf{Z} \times \mathbf{Z}$.

Alors, quand m est $\neq 0$, *on a* $\lambda(\vartheta, L^2) + N(\vartheta) = 0$ *si et seulement si* $\mathscr{P}^{(1)}_{\vartheta, L} = -m\,N(\vartheta)$; *de même, quand n est* $\neq 0$, *on a* $\lambda(\vartheta, L)^2 - N(\vartheta) = 0$ *si et seulement si*

$$\mathscr{P}^{(1)}_{\vartheta, L} = -n\,N(\vartheta)\frac{\sqrt{d_+}}{d_+}.$$

On peut également prouver le lemme suivant, d'usage plus malaisé.

LEMME D.4. — *Soient* $L \subset \mathbf{C}$ *comme dans le lemme précédent, et* ϑ_1, ϑ_2 *deux diviseurs premiers non principaux distincts* ([16]) *de* D *dans* K.

Si $\mathscr{P}^{(1)}_{\vartheta_1, L} = m$ *et* $\mathscr{P}^{(1)}_{\vartheta_2, L} = n\sqrt{d_+}$, *où m et n sont des nombres rationnels tels que* $(2m, 2n) \in \mathbf{Z} \times \mathbf{Z}$, *alors on a*

$$G_2(L) = -\frac{1}{2}(m\,N(\vartheta_1)^{-1} + n\,N(\vartheta_2)^{-1}\sqrt{d_+}).$$

De plus, si le couple (m, n) *est différent de* $(0, 0)$, *on a*

$$\lambda(\vartheta_i, L)^2 = (-1)^i N(\vartheta_i), \qquad i = 1, 2.$$

Démonstration. — Pour $i = 1, 2$, posons $d_i = N(\vartheta_i)$; et soient a, b, α et β des nombres rationnels tels que $G_2(L) = a + b\sqrt{d_+}$ et $\lambda(\vartheta_1, L)^2 = \alpha + \beta\sqrt{d_+}$. Comme

$$(\sqrt{-d_1\,d_2}) = \vartheta_1\,\vartheta_2,$$

on a

$$\lambda(\vartheta_2, L)^2 = -\frac{d_2}{d_1}\lambda(\vartheta_1, L)^2.$$

([16]) Un tel couple existe pour tous les corps quadratiques imaginaires de nombre de classes 2, à l'exception de ceux tels que $D \equiv 4 \pmod 8$, à savoir $K = \mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(\sqrt{-13})$ ou $\mathbf{Q}(\sqrt{-37})$.

D'après (D.7), la formule (D.1), appliquée à $\alpha = \vartheta_i$, implique les relations

$$\begin{cases} (\alpha+\beta\sqrt{d_+})(a-b\sqrt{d_+})-d_1(a+b\sqrt{d_+}) = m, \\ -(\alpha+\beta\sqrt{d_+})(a-b\sqrt{d_+})-d_1(a+b\sqrt{d_+}) = \dfrac{nd_1}{d_2}\sqrt{d_+}. \end{cases}$$

On en tire le système

$$\begin{cases} a\beta-b\alpha = bd_1, \\ bd_+\beta-a\alpha = ad_1 \end{cases}$$

et les relations

$$\begin{cases} 2ad_1+m = 0 \\ 2bd_2+n = 0 \end{cases}$$

Ces dernières prouvent l'égalité

$$G_2(L) = -\frac{1}{2}(md_1^{-1}+nd_2^{-1}\sqrt{d_+}).$$

Quant au système, on en déduit $\beta = 0$ et $\alpha+d_1 = 0$, c'est-à-dire $\lambda(\vartheta_1, L)^2+d_1 = 0$, pourvu que le déterminant

$$\begin{vmatrix} a & -b \\ bd_+ & -a \end{vmatrix} = -N(a+b\sqrt{d_+})$$

soit non nul, c'est-à-dire $(m, n) \neq (0, 0)$.

Toujours lorsque $h = 2$, le nombre premier d_+ tel que $H_+ = \mathbf{Q}(\sqrt{d_+})$ est égal à 2, 5, 13, 17, 29, 37, 41, 61 ou 89 (*cf.* appendice E), si bien que H_+ est toujours principal. Par suite, parmi les équations de Weierstrass d'invariant $j(\mathcal{O})$, et dont les coefficients g_2 et g_3 appartiennent à $\mathcal{O}(H_+)$, il est possible d'en trouver une telle que son *idéal discriminant*

$$(\Delta) = (g_2^3-27g_3^2)$$

soit *minimal*, pour la relation de division parmi les idéaux entiers de H_+. Bien entendu, deux équations de Weierstrass d'invariant $j(\mathcal{O})$, et dont les coefficients respectifs g_2, g_3 et g_2', g_3' appartiennent à $\mathcal{O}(H_+)$, ont même idéal discriminant si et seulement si il existe une unité $u \in \mathcal{O}^*(H_+)$ telle que

$$g_2' = u^2 g_2 \qquad \text{et} \qquad g_3' = u^3 g_3.$$

Les calculs résumés dans le tableau E.II prouvent alors le résultat suivant.

PROPOSITION D.5. — *Soit* K *un corps quadratique imaginaire de nombre de classes* 2. *Alors, il existe un diviseur premier* $\mathfrak{d}$ *non principal de* D *dans* K, *et une équation de Weierstrass* E_D (*d'invariant égal à* $j(\mathcal{O})$, *et dont les coefficients* g_2 *et* g_3 *appartiennent à*

$\mathcal{O}(H_+)$) *dont l'idéal discriminant est minimal, tels que*

$$\lambda(\mathfrak{9}, L)^2 + N(\mathfrak{9}) = 0,$$

pour le réseau $L \subset \mathbf{C}$ *associé à* E_D.

D'après la propriété (ii) des nombres $\lambda(\mathfrak{a}, L)$, l'idéal $\mathfrak{9}$ et l'équation E_D dont la proposition précédente affirme l'existence, sont uniquement déterminés, au signe de g_3 près. En fait, dans le cas très particulier considéré, la proposition D.5 constitue une réponse à une question plus générale posée par C. J. Moreno dans [21] (chap. X, p. 69), et il serait certainement intéressant d'en posséder une démonstration ne reposant pas sur l'énumération des corps quadratiques imaginaires de nombre de classes 2 ([17]).

Enfin, la remarque suivante résulte aussi du tableau E.II.

Remarque D.6. — *Soient* $\mathfrak{9}$ *et* L *comme dans la proposition précédente.*

Alors, pour chacun des trois corps $K = \mathbf{Q}(\sqrt{-D})$, *avec* $D = 20$, 52 *ou* 148, *on a* $N(\mathfrak{9}) = 2$, *si bien que l'invariant* $\lambda(\mathfrak{9}, L)$, *qui doit vérifier l'identité* $\lambda(\mathfrak{9}, L)^2 + 2 = 0$ *n'appartient pas au corps de classes absolu* H_0 *de* K.

Au contraire, pour les autres corps $K = \mathbf{Q}(\sqrt{-D})$ *de nombre de classes* 2, *l'invariant* $\lambda(\mathfrak{9}, L)$ *appartient à* H_0, *de telle sorte que* $\lambda(\mathfrak{a}, L) \in H_0$ *pour tout idéal* $\mathfrak{a}$ *de* K.

(*g*) *Calcul de* $\lambda(\mathfrak{a}, L)$.

Soit $\mathfrak{a}$ un idéal entier de K. Le principe du calcul de la somme $\mathscr{P}^{(1)}_{\mathfrak{a}, L}$ est semblable à celui du calcul de $G_2(L)$ (*cf.* (*d*)). Plus précisément, soient $\gamma \in G(H_0/K)$ et $\mathfrak{b}$ un idéal de K tel que

$$(\mathfrak{b}^{-1}, H_0/K) = \gamma.$$

Pour $K \neq \mathbf{Q}(\sqrt{-3})$ et $\neq \mathbf{Q}(\sqrt{-1})$, la formule (D.5) nous permet de calculer le nombre $\rho(\mathfrak{b}^{-1})^2 = \rho(\mathfrak{b}^{-1}, L)^2$ défini par

$$\rho(\mathfrak{b}^{-1}, L)\mathfrak{b} = L_\gamma.$$

On calcule ensuite la somme

$$\mathscr{P}^{(1)}_{\mathfrak{a}, \mathfrak{b}} = \sum_{\lambda \in \mathfrak{a}^{-1}\mathfrak{b}/\mathfrak{b}}{}' \mathscr{P}(\lambda, \mathfrak{b})$$

terme à terme, à l'aide du q-développement de la fonction $\mathscr{P}$ (*cf.* (*b*)). Lorsque γ parcourt $G(H_0/K)$, on obtient ainsi h valeurs $\alpha_\gamma + i\beta_\gamma$, avec α_γ et β_γ réels, approchant les nombres

$$\mathscr{P}^{(1)}_{\mathfrak{a}, L_\gamma} = \rho(\mathfrak{b}^{-1})^{-2}\mathscr{P}^{(1)}_{\mathfrak{a}, \mathfrak{b}}.$$

Or, pour tout $\gamma \in G(H_0/K)$, on a

$$\mathscr{P}^{(1)}_{\mathfrak{a}, L_\gamma} = (\mathscr{P}^{(1)}_{\mathfrak{a}, L})^\gamma,$$

([17]) *Cf.* B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Thèse (Harvard University, Jan. 1978), § 15.

si bien que ces nombres sont les conjugués de $\mathscr{P}^{(1)}_{\mathfrak{a},L} \in H_0$ pour l'action de $G(H_0/K)$. Comme on sait que $2\,\mathscr{P}^{(1)}_{\mathfrak{a},L}$ appartient à $\mathscr{O}(H_0)$, il suffit donc de résoudre le système de h valeurs $\alpha_\gamma + i\,\beta_\gamma$, $\gamma \in G(H_0/K)$, approchant les nombres $(\mathscr{P}^{(1)}_{\mathfrak{a},L})^\gamma$, pour en déduire la valeur exacte de $\mathscr{P}^{(1)}_{\mathfrak{a},L}$.

Une fois la somme $\mathscr{P}^{(1)}_{\mathfrak{a},L}$ déterminée, les formules (D.1) et (D.7) nous donnent les valeurs de $G_2(\mathfrak{a}^{-1}L)$ et $\lambda(\mathfrak{a}, L)^2$, pourvu que le nombre $G_2(L)$ soit déjà connu.

QUELQUES CAS PARTICULIERS :

(i) *L'idéal* $\mathfrak{a}$ *est principal.*

Supposons donc $\mathfrak{a} = (\alpha)$, avec $\alpha \in \mathscr{O}(K)$. La formule (D.1) s'écrit alors

$$\alpha(\alpha-\bar{\alpha})\,G_2(L) = \mathscr{P}^{(1)}_{(\alpha),L};$$

par suite, si α et son conjugué complexe $\bar{\alpha}$ sont distincts, la valeur de $\mathscr{P}^{(1)}_{(\alpha),L}$ détermine celle de $G_2(L)$ (et réciproquement).

(ii) *Le nombre de classes h de* K *est égal à* 2.

Pour $K \neq \mathbf{Q}(\sqrt{-5})$, $\neq \mathbf{Q}(\sqrt{-13})$ et $\neq \mathbf{Q}(\sqrt{-37})$, le lemme D.4 fournit un procédé de calcul pour obtenir les valeurs de $G_2(L)$ et $\lambda(\vartheta_i, L)^2$ à partir des sommes $\mathscr{P}^{(1)}_{\vartheta_i,L}$, $i = 1, 2$.

Exemple :

$$K = \mathbf{Q}(\sqrt{-91}), \qquad \mathscr{O} = \mathbf{Z}+\mathbf{Z}\left(\frac{1+\sqrt{-91}}{2}\right), \qquad H_0 = \mathbf{Q}(\sqrt{13}, \sqrt{-7})$$

et

$$g_2 = 2^3.7.(3\sqrt{13}+10), \qquad g_3 = 7^2.11.(2\sqrt{13}+7).$$

L'équation de Weierstrass E_{91}, de coefficients g_2 et g_3, a pour discriminant

$$\Delta = g_2^3 - 27\,g_3^2 = -7^3\left(\frac{\sqrt{13}-3}{2}\right)^6;$$

c'est donc une équation de Weierstrass d'idéal discriminant $(\Delta) = (7^3)$ minimal, et son invariant

$$j_{E_{91}} = 2^6\,3^3\,g_2^3/\Delta = -2^{15}.3^3(3\sqrt{13}+10)^3\left(\frac{3+\sqrt{13}}{2}\right)^6$$

est égal à l'invariant modulaire $j(\mathscr{O})$ (*cf.* Weber [37], § 139, p. 523). Pour $\vartheta_1 \mid 7$ et $\vartheta_2 \mid 13$ on trouve

$$\mathscr{P}^{(1)}_{\vartheta_1,L} = -56 \qquad \text{et} \qquad \mathscr{P}^{(1)}_{\vartheta_2,L} = -4.7.\sqrt{13},$$

d'où

$$G_2(L) = 4+\frac{14\sqrt{13}}{13} \qquad \text{et} \qquad \lambda(\vartheta_1, L)^2+7 = 0, \quad \lambda(\vartheta_2, L)^2-13 = 0.$$

(iii) *il existe un idéal premier* δ *de* K *de norme* 2 *ou* 3.

Le corps de classes de K du rayon modulo δ coïncide alors avec l'extension abélienne non ramifiée maximale H_0 de K. Par suite, l'équation des points de 2-torsion

$$4x^3-g_2x-g_3=0$$

(resp. l'équation des points de 3-torsion

$$3x^4-\frac{3g_2}{2}x^2-3g_3x-\frac{g_2^2}{16}=0\Big)$$

possède au moins une solution dans H_0. De plus, si x_δ désigne l'abscisse d'un point de δ-torsion, on a

$$\mathscr{P}^{(i)}_{\delta,L}=x_\delta^i \qquad \text{ou} \qquad \mathscr{P}^{(i)}_{\delta,L}=2x_\delta^i, \quad i=1,2,3,$$

suivant que δ divise 2 ou 3.

Supposons δ *invariant par conjugaison*, c'est-à-dire 2 (resp. 3) ramifié dans K. Alors, pour $K\neq \mathbf{Q}(\sqrt{-1})$ et $\neq \mathbf{Q}(\sqrt{-3})$, le nombre x_δ est l'unique solution de $4x^3-g_2x-g_3=0$ (resp. $3x^4-(3g_2/2)x^2-3g_3x-(g_2^2/16)=0$) dans H_0; de plus x_δ est réel dès que g_2 et g_3 le sont.

Exemples. – (α) 2 *se ramifie dans* K *et* $\delta \mid 2$.

– $K=\mathbf{Q}(\sqrt{-2})$ principal, et $g_2=2.3.5$, $g_3=2^2.7$ (*cf.* tableau B.I). L'équation des points de 2-torsion est ici

$$4x^3-2.3.5x-2^2.7=(x+2)(4x^2-8x-2.7)=0,$$

d'où $x_\delta=-2$. Par conséquent, on a $G_2(\delta^{-1}L)-2G_2(L)=-2$, et, puisque $\delta=(\sqrt{-2})$, $G_2(L)=1/2$.

– $K=\mathbf{Q}(\sqrt{-58})$, $H_0=\mathbf{Q}(\sqrt{29},\sqrt{-2})$ et

$$g_2=2.5(3^3.11^2+4.7.13\sqrt{29}), \qquad g_3=2^2.3.7.11(3^2.11^2+4.5.13\sqrt{29});$$

(*cf.* tableau E.I). On a

$$4x^3-g_2x-g_3=(x+66)[4x^2-2^3.3.11x-2.7(3^2.11^2+4.5.13\sqrt{29})],$$

d'où $x_\delta=-66$.

– De même pour les corps $K=\mathbf{Q}(\sqrt{-D})$, avec D = 20, 24, 40, 52, 88 et 148, et les équations de Weierstrass E_D définies par la table E.II, on trouve respectivement $x_\delta=-2$, $-\sqrt{2}$, -2, -2, $-11\sqrt{2}$ et -14.

(β) 3 *se ramifie dans* K *et* $\delta \mid 3$.

– $K=\mathbf{Q}(\sqrt{-51})$, $H_0=\mathbf{Q}(\sqrt{17},\sqrt{-3})$ et $g_2=2^2.3(\sqrt{17}+5)$,

$g_3 = 7(15+4\sqrt{17})$ (*cf.* tableau E.II). L'équation des points de 3-torsion est ici

$$x^4-2.3(\sqrt{17}+5)x^2-7(15+4\sqrt{17})x-2.3(21+5\sqrt{17})$$
$$=(x+3)[x^3-3x^2-3(7+2\sqrt{17})x-2(21+5\sqrt{17})]=0,$$

d'où $x_\delta = -3$.

– De même pour les corps $K = \mathbf{Q}(\sqrt{-D})$, avec D = 15, 24, 123 et 267, et E_D définie par le tableau E.II, on trouve respectivement $x_\delta = -3/2$, $-3/2$, -12 et -75.

Cas particulier. – D'après ce qui précède, si $K = \mathbf{Q}(\sqrt{-6})$ et $\delta \mid 2$, $\delta' \mid 3$, on a $\mathscr{P}^{(1)}_{\delta,L} = -\sqrt{2}$ et $\mathscr{P}^{(1)}_{\delta',L} = -3$. Le lemme D.4 implique donc

$$G_2(L) = \frac{1}{2}\left(1+\frac{\sqrt{2}}{2}\right) \quad \text{et} \quad \lambda(\delta, L)^2 = 2, \quad \lambda(\delta', L)^2 = -3.$$

Supposons maintenant δ *différent de l'idéal conjugué* $\bar{\delta}$, c'est-à-dire 2 (resp. 3) décomposé dans K.

Si g_2 et g_3 sont réels et $\delta\bar{\delta} = (2)$, l'équation $4x^3-g_2x-g_3 = 0$ possède deux solutions complexes conjuguées x_δ et $x_{\bar{\delta}} = \overline{x_\delta}$ dans H_0; sa troisième solution x_2 représente l'abscisse du point propre de 2-torsion et appartient au sous-corps réel de H_0.

Exemple. – $K = \mathbf{Q}(\sqrt{-7})$ et $g_2 = 5.7$, $g_3 = 7^2$ (*cf.* tableau B.I). Les trois solutions de l'équation $4x^3-5.7x-7^2 = 0$, sont

$$x_2 = \frac{7}{2} \quad \text{et} \quad x_\pm = \frac{-7\pm\sqrt{-7}}{4}.$$

Or, le nombre rationnel $G_2(L)$ doit être solution de l'équation

$$\left(\frac{-7+\sqrt{-7}}{2}\right)G_2(L) = G_2(\delta^{-1}L)-2G_2(L) = x_\delta,$$

avec

$$\delta = \left(\frac{1+\sqrt{-7}}{2}\right).$$

Par suite, on a $G_2(L) = 1/2$ et

$$x_\delta = \frac{-7+\sqrt{-7}}{4}, \qquad x_{\bar{\delta}} = \frac{-7-\sqrt{-7}}{4}.$$

Si g_2 et g_3 sont réels et $\delta\bar{\delta} = (3)$, l'équation

$$3x^4-\frac{3g_2}{2}x^2-3g_3x-\frac{g_2^2}{16} = 0$$

possède deux solutions complexes conjuguées x_δ et $x_{\bar{\delta}} = \overline{x_\delta}$ dans H_0; les deux autres solutions engendrent une extension quadratique de H_0.

Exemple. – $K = \mathbf{Q}(\sqrt{-11})$ principal et $g_2 = 2^3.3.11$, $g_3 = 7.11^2$ (*cf.* tableau B.I). L'équation des points de 3-torsion s'écrit

$$x^4 - 2^2.3.11\,x^2 - 7.11^2\,x - 2^2.3.11^2 = (x^2+11\,x+11.3)(x^2-11\,x-2^2.11) = 0,$$

et le facteur $x^2+11\,x+11.3$ admet

$$x_\pm = \frac{-11 \pm \sqrt{-11}}{2}$$

pour racines. Comme précédemment, le nombre rationnel $G_2(L)$ doit être solution de l'équation

$$\left(\frac{-11+\sqrt{-11}}{2}\right) G_2(L) = G_2(\delta^{-1}L) - 3\,G_2(L) = 2\,x_\delta,$$

avec

$$\delta = \left(\frac{1+\sqrt{-11}}{2}\right).$$

Par suite, on a $G_2(L) = 2$ et

$$x_\delta = \frac{-11+\sqrt{-11}}{2}, \qquad x_{\bar{\delta}} = \frac{-11-\sqrt{-11}}{2}.$$

(*h*) *Récapitulation et formule de récurrence pour les séries d'Eisenstein* G_k, $k \geqq 8$.

Comme nous l'avons déjà observé, la formule (D.8) de la section (*e*) ramène le calcul des nombres de Hurwitz $G_k(\mathfrak{a}^{-1}L)$ à celui de $\lambda(\mathfrak{a}, L)$, auquel est consacré la section précédente, et des nombres $G_k(L)$.

Or, les nombres $G_4(L) = g_2/60$ et $G_6(L) = g_3/140$ sont déjà connus par la section (*a*) et nous avons vu dans la section (*d*) comment on peut calculer $G_2(L)$. Il nous reste donc à examiner la question du calcul des $G_k(L)$, pour k entier pair $\geqq 8$. On utilise à cet effet la formule de récurrence

$$\text{(D.10)} \qquad \frac{(k-6)(k+1)(k-1)}{6} G_k = \sum_{\substack{4 \leqq j \leqq k-4 \\ j \text{ pair}}} (j-1)(k-j-1)\,G_j\,G_{k-j},$$

valable pour $k \geqq 8$.

En effet, d'après la formule (2) (§ 0), pour tout réseau $\mathscr{L} \subset \mathbf{C}$, le développement en série de Laurent de $\mathscr{P}(z, \mathscr{L})$ au point $z = 0$ est

$$\text{(D.11)} \qquad \mathscr{P}(z, \mathscr{L}) = \frac{1}{z^2}\Big[1 + \sum_{\substack{k \geqq 4 \\ k \text{ pair}}} (k-1)\,G_k(\mathscr{L})\,z^k\Big].$$

On déduit alors la formule (D.10) en substituant (D.11) dans l'équation différentielle

$$2\frac{\partial^2}{\partial z^2}\mathscr{P}(z, \mathscr{L}) = 12\,\mathscr{P}(z, \mathscr{L})^2 - 60\,G_4(\mathscr{L}),$$

et en identifiant les coefficients de z^{k-4} dans chaque membre.

E. Cas où le corps de base possède exactement deux classes d'idéaux

D'après H. M. Stark [33], il s'agit des dix-huit corps quadratiques imaginaires de discriminants respectifs $-D = -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403$ et -427.

Tableau E.I

Valeur de ε, *unité fondamentale de* $H_+ = \mathbf{Q}(\sqrt{d_+})$ *telle que* $0 < \varepsilon < 1$

d_+	ε	d_+	ε
2.....	$\sqrt{2}-1$	37.....	$\sqrt{37}-6$
5.....	$\frac{1}{2}(\sqrt{5}-1)$	41.....	$5\sqrt{41}-32$
13.....	$\frac{1}{2}(\sqrt{13}-3)$	61.....	$\frac{1}{2}(5\sqrt{61}+39)$
17.....	$\sqrt{17}-4$	89.....	$53\sqrt{89}-500$
29.....	$\frac{1}{2}(\sqrt{29}-5)$		

Si $H_+ = \mathbf{Q}(\sqrt{d_+})$ est le sous-corps quadratique réel de H_0, désignons par ε son unité fondamentale, $0 < \varepsilon < 1$ (*cf.* tableau I), et choisissons les nombres $g_2 = g_{2,D}$ et $g_3 = g_{3,D}$ dans $\mathcal{O}(H_+)$ comme indiqué par le tableau II; on a aussi noté dans cette table la valeur prise par le discriminant $\Delta_D = g_{2,D}^3 - 27\, g_{3,D}^2$ de l'équation de Weierstrass

$$E_D : \quad y^2 = 4x^3 - g_2 x - g_3 .$$

On vérifie que l'invariant $j_{E_D} = 2^6\, 3^3\, g_{3,D}^2/\Delta_D$ de l'équation E_D est égal à l'invariant modulaire $j(\mathcal{O}_D)$ associé à l'anneau des entiers $\mathcal{O}_D$ de $K = \mathbf{Q}(\sqrt{-D})$ (*cf.* W. E. H. Berwick [2], § 4).

Chacune des équations E_D ci-dessus possède donc des multiplications complexes par l'anneau $\mathcal{O}_D$; de plus, son idéal discriminant (Δ_D) est minimal dans $\mathcal{O}(H_+)$ (*cf.* appendice D, (*e*)).

Pour $D \neq 20$, 52 et 148, désignons par q_D le nombre premier divisant D pour lequel $\sqrt{-q_D}$ appartient à H_0; pour $D = 20$, 52 ou 148, posons $q_D = 2$. Alors, d'après le tableau II, si 3 n'est pas inerte dans K, i. e. $D \not\equiv 1 \pmod 3$, l'ensemble S_D des nombres premiers pour lesquels E_D a mauvaise réduction est

$$S_D = \{2, 3\} \cup \{q_D\},$$

et, si 3 est inerte dans K,

$$S_D = \{2\} \cup \{q_D\}.$$

Pour $L \subset \mathbf{C}$ le réseau associé à l'équation E_D et $\mathfrak{P}$ le diviseur premier non principal de D dans K de norme $N(\mathfrak{P})$ donnée par le tableau III, les méthodes de l'appendice D, en particulier le lemme D.3, établissent l'identité

$$N(\mathfrak{P}) + \lambda(\mathfrak{P}, L^2) = 0.$$

Le tableau III indique aussi la valeur trouvée pour $G_2(L)$. Quant aux nombres $G_k(L)$, avec k entier pair $\geqq 8$, ils se calculent par récurrence à partir de $G_4(L) = g_{2,D}/60$ et $G_6(L) = g_{3,D}/140$ à l'aide de la formule (D.10).

TABLEAU E.II

Valeurs des coefficients et du discriminant de l'équation de Weierstrass E_D.

$-D$	g_2	g_3	Δ	d_+
$-15\ldots$	$3\sqrt{5}(4+\sqrt{5})$	$7(3+2\sqrt{5})$	$-2^6.3^3.\varepsilon^2$	5
$-20\ldots$	$3\sqrt{5}(3+2\sqrt{5})$	$2(14+9\sqrt{5})$	$3^6.\varepsilon^3$	5
$-24\ldots$	$3(5+2\sqrt{2})$	$(12+7\sqrt{2})$	$3^3.\varepsilon^2$	2
$-35\ldots$	$2^2.3\sqrt{5}(3+\sqrt{5})7$	$(63+26\sqrt{5})7^2$	$-3^6.7^3.\varepsilon^6$	5
$-40\ldots$	$2\sqrt{5}(4+3\sqrt{5})$	$2^2(7+4\sqrt{5})$	$2^3.\varepsilon^6$	5
$-51\ldots$	$2^2.3(5+\sqrt{17})$	$7(15+4\sqrt{17})$	$-3^3.\varepsilon^2$	17
$-52\ldots$	$5(6+\sqrt{13})$	$2(14+5\sqrt{13})$	ε^3	13
$-88\ldots$	$5(33+14\sqrt{2})11$	$7(20+11\sqrt{2})11^2$	$11^3.\varepsilon^6$	2
$-91\ldots$	$2^3(10+3\sqrt{13})7$	$11(7+2\sqrt{13})7^2$	$-7^3.\varepsilon^6$	13
$-115\ldots$	$2^2\sqrt{5}(19+9\sqrt{5})23$	$(7.19+2.29\sqrt{5})23^2$	$-23^3.\varepsilon^{18}$	5
$-123\ldots$	$2^3.3.5(8+\sqrt{41})$	$7(3.317+2^5.5\sqrt{41})$	$-3^3.\varepsilon^2$	41
$-148\ldots$	$5(2.3.7^2+29\sqrt{37})$	$2.7(2.7^3+5.29\sqrt{37})$	ε^3	37
$-187\ldots$	$2^2.5\sqrt{17}(13+3\sqrt{17})11$	$(5.7.79+4.13^2\sqrt{17})11^2$	$-11^3.\varepsilon^6$	17
$-232\ldots$	$5(3^3.11^2+4.7.13\sqrt{29})2$	$3.7.11(3^2.11^2+4.5.13\sqrt{29})2^2$	$2^3.\varepsilon^6$	29
$-235\ldots$	$2^2\sqrt{5}.11(31+15\sqrt{5})47$	$3.7(11.31+2.3.5^2\sqrt{5})47^2$	$-47^3.\varepsilon^{30}$	5
$-267\ldots$	$2^2.3.5(5^4+53\sqrt{89})$	$7(3.223.347+2^2.5^3.53\sqrt{89})$	$-3^3.\varepsilon^2$	89
$-403\ldots$	$2^2.5(5.431+9.67\sqrt{13})31$	$7(3.5.4201+2.8707\sqrt{13})31^2$	$-31^3.\varepsilon^{18}$	13
$-427\ldots$	$2^2.5.11(317+3.13\sqrt{61})7$	$23(7^2.1627+2.5.13.79\sqrt{61})7^2$	$-7^3.\varepsilon^6$	61

TABLEAU E.III

Valeurs de $G_2(L)$ *et* $N(\vartheta)$

$-D$	$G_2(L)$	$N(\vartheta) = -\lambda(\vartheta, L)^2$	$-D$	$G_2(L)$	$N(\vartheta) = -\lambda(\vartheta, L)^2$
$-15\ldots$	$\frac{1}{2}\left(1+2\frac{\sqrt{5}}{5}\right)$	3	$-115\ldots$	$11+\frac{23\sqrt{5}}{5}$	23
$-20\ldots$	$\frac{1}{2}\left(1+3\frac{\sqrt{5}}{5}\right)$	2	$-123\ldots$	$4+\frac{38\sqrt{41}}{41}$	3
$-24\ldots$	$\frac{1}{2}\left(1+\frac{\sqrt{2}}{2}\right)$	3	$-148\ldots$	$\frac{1}{2}\left(7+\frac{101\sqrt{37}}{37}\right)$	2
$-35\ldots$	$3+7\frac{\sqrt{5}}{5}$	7	$-187\ldots$	$19+\frac{7.11\sqrt{17}}{17}$	11
$-40\ldots$	$\frac{1}{2}\left(1+4\frac{\sqrt{5}}{5}\right)$	2	$-232\ldots$	$\frac{1}{2}\left(33+\frac{12.37\sqrt{29}}{29}\right)$	2
$-51\ldots$	$1+5\frac{\sqrt{17}}{17}$	3	$-235\ldots$	$3.5^2+\frac{3.47\sqrt{5}}{5}$	47
$-52\ldots$	$\frac{1}{2}\left(1+\frac{7\sqrt{13}}{13}\right)$	2	$-267\ldots$	$5^2+\frac{389\sqrt{89}}{89}$	3
$-88\ldots$	$\frac{1}{4}(34+11\sqrt{2})$	11	$-403\ldots$	$3.71+\frac{5^2.31\sqrt{13}}{13}$	31
$-91\ldots$	$4+14\frac{\sqrt{13}}{13}$	7	$-427\ldots$	$11^2+\frac{7.151\sqrt{61}}{61}$	7

Soient ϑ et L comme dans le tableau III, et supposons que E_D a bonne réduction modulo p, i. e. $p \notin S_D$. Comme $N(\vartheta) \in S_D$, l'automorphisme $(\vartheta, H/K)$ de l'extension H/K est défini et pour chaque $\gamma \in \mathscr{G}$ il existe un unique $g \in G$ tel que

$$\gamma = (\vartheta, H/K)^{\varepsilon} g, \qquad \text{avec} \quad \varepsilon = 0 \text{ ou } 1.$$

Soit k un entier pair, et posons

$$\omega_{i,k}(\gamma) = (-1)^{\varepsilon i} N(\vartheta)^{\varepsilon k/2} \sigma^k(g), \qquad i = 0, 1. \tag{E.1}$$

Trivialement la formule (E.1) définit deux homomorphismes distincts $\omega_{0,k}$ et $\omega_{1,k}$ de $\mathscr{G}$ dans $(\mathscr{O}/\mathfrak{p})^{\times}$ dont la restriction à G est σ^k. Lorsque k varie, ces homomorphismes sont donc au nombre de $\# \mathscr{G}$.

Supposons un instant p non décomposé dans K, et, pour chaque entier pair k, $2 \leqq k \leqq \mathrm{N}(\mathfrak{p})-1$, désignons par k' l'unique entier pair, $2 \leqq k' \leqq \mathrm{N}(\mathfrak{p})-1$, tel que

$$\sigma^{k'} = \nu\sigma^{-k},$$

autrement dit tel que $\sigma^{k'}$ soit l'image de σ^k dans le miroir de Leopoldt. Alors, il vient :

PROPOSITION E.1. — *L'image* $\tilde{\nu}\omega_{i,k}^{-1}$ *de* $\omega_{i,k}$, $i = 0,1$, *dans le miroir de Leopoldt est* $\omega_{i,k'}$ *ou* $\omega_{1-i,k'}$, *suivant que le symbole de Legendre* $(\mathrm{N}\vartheta/p) \equiv (\mathrm{N}\vartheta)^{(p-1)/2} \pmod{p}$ *vaut* 1 *ou* -1.

Démonstration. — Rappelons que le caractère $\tilde{\nu}$ de $\mathcal{G}$ dans $\mathbf{F}_p^\times$, défini par l'action de $\mathcal{G}$ sur le groupe des racines de l'unité d'ordre p, est caractérisé par les congruences

$$\nu((\mathfrak{b}, \mathrm{H/K})) \equiv \mathrm{N}(\mathfrak{b}) \pmod{p},$$

pour tout idéal entier $\mathfrak{b}$ de K premier à $\mathfrak{p}$. Or, pour démontrer la proposition, il suffit de prouver l'identité

$$\tilde{\nu}\omega_{i,k}^{-1}((\vartheta, \mathrm{H/K})) = \left(\frac{\mathrm{N}\vartheta}{p}\right)\omega_{i,k'}((\vartheta, \mathrm{H/K})),$$

qui équivaut donc à la congruence

$$\mathrm{N}(\vartheta)/\mathrm{N}(\vartheta)^{k/2} \equiv \left(\frac{\mathrm{N}\vartheta}{p}\right)\mathrm{N}(\vartheta)^{k'/2} \pmod{p}.$$

Or, si p est ramifié dans K, on a $\nu = \sigma^2$ et donc $k' = p+1-k$; si p est inerte dans K, on a $\nu = \sigma^{p+1}$ et donc $k' \equiv p+1-k \pmod{p^2-1}$, d'où $k'/2 \equiv (p+1-k)/2 \pmod{p-1}$. Par suite, il vient

$$\mathrm{N}(\vartheta)/\mathrm{N}(\vartheta)^{k/2} = \mathrm{N}(\vartheta)^{-(p-1)/2}\mathrm{N}(\vartheta)^{(p+1-k)/2} \equiv \left(\frac{\mathrm{N}\vartheta}{p}\right)\mathrm{N}(\vartheta)^{k'/2} \pmod{p},$$

ce qui prouve l'assertion de la proposition.

Comme $\omega_{0,2} = \tilde{\nu}$ pour p ramifié dans K, et $\omega_{0,p^2-1} = 1$ pour p inerte dans K, la proposition E.1 implique le corollaire suivant.

COROLLAIRE E.2. — *Si* p *est inerte (resp. ramifié) dans* K, *on a*

$$\tilde{\nu} = \omega_{0,p+1} \qquad \textit{ou} \qquad \tilde{\nu} = \omega_{1,p+1}$$

(*resp.* $1 = \omega_{0,p-1}$ *ou* $1 = \omega_{1,p-1}$), *suivant que* $(\mathrm{N}\vartheta/p)$ *vaut* 1 *ou* -1.

Ce cas particulier précisé, considérons maintenant un homomorphisme ω de $\mathcal{G}$ dans une clôture algébrique $\tilde{\mathbf{F}}_p$ de $\mathcal{O}/\mathfrak{p}$: l'homomorphisme ω est donc de la forme $\omega_{i,k}$, avec $i \in \{0, 1\}$ et k entier pair tel que $2 \leqq k \leqq \mathrm{N}(\mathfrak{p})-1$. Tout d'abord, supposons que la restriction de ω à G n'est pas ν, et déterminons le générateur $\tilde{\mathrm{G}}_\omega(\mathrm{L})$ de $\acute{\mathrm{L}}_\omega$ (*cf.* § 4).

Si $\omega_{i,k}(\mathscr{G}) \subset \mathbf{F}_p^\times$ (cas (α) du § 4), le nombre $\tilde{G}_{\omega_{i,k}}$ est la somme

$$(\#\mathscr{G})^{-1}\sum_{\mathfrak{b}}\omega_{i,k}^{-1}((\mathfrak{b}, H/K)).[G_k(\mathfrak{b}^{-1}L)],$$

où $\mathfrak{b}$ parcourt une famille d'idéaux de K premiers à $\mathfrak{p}$ qui forme un système complet de représentants du groupe $Cl(\mathfrak{p})$. Par suite, on a

$$\tilde{G}_{\omega_{i,k}}(L) = \frac{1}{2}([G_k(L)]+(-1)^i N(\vartheta)^{-k/2}[G_k(\vartheta^{-1}L)]).$$

Or, comme $N(\vartheta)+\lambda(\vartheta, L)^2 = 0$, on a d'après la formule (D.8) :

$$G_k(\vartheta^{-1}L) = (-1)^{k/2} N(\vartheta)^{k/2} G_k(L)^\tau,$$

où $\tau = (\vartheta, H_0/K)$ est l'automorphisme non trivial de l'extension H_0/K; ceci prouve la congruence

$$\tilde{G}_{\omega_{i,k}} \equiv \frac{1}{2}(G_k(L)+(-1)^{i+(k/2)} G_k(L)^\tau) \pmod{\mathfrak{p}(H_0)}. \tag{E.2}$$

De même, si $\omega_{i,k}(\mathscr{G}) \not\subset \mathbf{F}_p^\times$ (cas (β) du § 4)), on prouve comme ci-dessus que les deux composantes de $\tilde{G}_{\omega_{i,k}}(L)$ sont les sommes

$$\begin{cases} \frac{1}{2}([G_k(L)]+(-1)^i N(\vartheta)^{-k/2}[G_k(\vartheta^{-1}L)]), \\ \frac{1}{2}([G_{p(k)}(L)]+(-1)^i N(\vartheta)^{-p(k/2)}[G_{p(k)}(\vartheta^{-1}L)]). \end{cases}$$

Or, on a

$$p(k/2) \equiv pk/2 \equiv p(k)/2 \pmod{(p^2-1)/2},$$

et l'on déduit donc de la formule (D.8) la congruence

$$\tilde{G}_{\omega_{i,k}} \equiv \frac{1}{2}(G_k(L), G_{p(k)}(L)) \tag{E.3}$$

$$+(-1)^{i+(k/2)}\frac{1}{2}(G_k(L)^\tau, G_{p(k)}(L)^\tau) \pmod{\mathfrak{p}(H_0)\times\mathfrak{p}(H_0)},$$

car $(-1)^{p(k/2)} = (-1)^{k/2}$ puisque p est impair.

Supposons maintenant p non décomposé dans K, et considérons l'homomorphisme ω de $\mathscr{G}$ dans $\tilde{\mathbf{F}}_p$, différent de $\tilde{\nu}$, et dont la restriction à G est ν (cas (α') du § 4). D'après le corollaire E.2, si p est ramifié dans K, on a donc $\omega = \omega_{1,2}$, et, si p est inerte dans K,

$\omega = \omega_{1,p+1}$ ou $\omega = \omega_{0,p+1}$ suivant que $(N\vartheta/p)$ vaut 1 ou -1. D'autre part, on vérifie immédiatement la congruence

$$\omega((\vartheta, H/K)) + N(\vartheta) \equiv 0 \pmod{p},$$

d'où $(\tilde{\nu}-\omega)((\vartheta, H/K)) \equiv 2N(\vartheta) \pmod{p}$, si bien que $\tilde{G}_\omega(\vartheta, L)$ engendre $\tilde{\mathscr{L}}_\omega$ (*cf.* § 4, prop. 36). Déterminons donc $\tilde{G}_\omega(\vartheta, L)$, avec $\omega = \omega_{i,k}$ comme ci-dessus; par définition, c'est la somme

$$(\#\mathscr{G})^{-1} \sum_{\mathfrak{b}} \omega_{i,k}^{-1}((\mathfrak{b}, H/K))[G_k^*(\vartheta, \mathfrak{b}^{-1}L)],$$

où $\mathfrak{b}$ parcourt une famille d'idéaux de K premiers à $\mathfrak{p}$ qui forme un système complet de représentants de $Cl(\mathfrak{p})$. On a donc

$$\tilde{G}_\omega(\vartheta, L) = \frac{1}{2}([G_k^*(\vartheta, L)] + (-1)^i N(\vartheta)^{-k/2}[G_k^*(\vartheta, \vartheta^{-1}L)]);$$

or, la formule (D.8) implique l'identité

$$G_k^*(\vartheta, \vartheta^{-1}L) = (-1)^{k/2} N(\vartheta)^{k/2} G_k^*(\vartheta, L)^\tau,$$

d'où la congruence

$$\tilde{G}_\omega(\vartheta, L) \equiv \frac{1}{2}(G_k^*(\vartheta, L) + (-1)^{i+(k/2)} G_k^*(\vartheta, L)^\tau) \pmod{\mathfrak{p}(H_0)}.$$

Mais on a

$$G_k^*(\vartheta, L) = G_k(\vartheta^{-1}L) - N(\vartheta) G_k(L) = (-1)^{k/2} N(\vartheta)^{k/2} G_k(L)^\tau - N(\vartheta) G_k(L);$$

il vient donc

$$\tilde{G}_\omega(\vartheta, L) \equiv \frac{1}{2}((-1)^i N(\vartheta)^{k/2} - N(\vartheta)).(G_k(L) + (-1)^{i+(k/2)} G_k(L)^\tau) \pmod{\mathfrak{p}(H_0)}.$$

De plus, on a ici

$$\frac{1}{2}((-1)^i N(\vartheta)^{k/2} - N(\vartheta)) \equiv -N(\vartheta) \pmod{p},$$

de sorte que la somme $G_k(L) + (-1)^{i+(k/2)} G_k(L)^\tau$ est $\mathfrak{p}$-entière, et $\tilde{G}_\omega(\vartheta, L)$ est donné par la congruence

$$\tilde{G}_\omega(\vartheta, L) \equiv -N(\vartheta)(G_k(L) + (-1)^{i+(k/2)} G_k(L)^\tau) \pmod{\mathfrak{p}(H_0)}. \tag{E.4}$$

A l'aide du théorème 37 (§ 4), et compte tenu du commentaire à la fin de l'appendice A, on déduit en particulier des congruences (E.2) à (E.4) la proposition suivante.

PROPOSITION E.3. — *Soient p un nombre premier $\neq 2$ non ramifié dans* K, M *un sous-corps de* H *contenant* K, *et χ un caractère irréductible de $G_M = G(M/M_0)$ sur $\mathbf{F}_p$, $\chi \neq 1$. Si χ est de degré* 1 (*resp.* 2), *on désigne par k un entier pair, tel que $0 < k < N(\mathfrak{p}) - 1$ et $\chi = \sigma^k$ (resp. $\chi = \sigma^k + \sigma^{p(k)}$).*

Alors, en distinguant entre les trois cas (a), (a') et (b) de la proposition 22 (§ 3), *il vient :*

Cas (*a*) : χ de degré 1, $\chi \neq \nu$; *on a :*

(i) $\delta(\chi, M) = 2$ *si* $H_0 \subset M$ *et* $[G_k(L)] = [G_k(L)^\tau] = 0$; *sinon* $\delta(\chi, M) \leqq 1$.

(ii) $\delta(\chi, M) \geqq 1$ *s'il existe* $i \in \{0, 1\}$ *tel que*

$$\omega_{i,k}(G(H/M)) = \{1\} \quad et \quad [G_k(L)] + \varepsilon [G_k(L)^\tau] = 0,$$

avec $\varepsilon = (-1)^{i+(k/2)}$; *sinon* $\delta(\chi, M) = 0$.

Cas (*a'*) : p inerte dans K et $\chi = \nu$. *Soit* $i \in \{0, 1\}$ *tel que* $\tilde{\nu} = \omega_{i,p+1}$. *Alors, on a* $\delta(\nu, M) = 1$ *si* $\omega_{1-i,p+1}(G(H/M)) = \{1\}$ *et* $[G_{p+1}(L) + \varepsilon G_{p+1}(L)^\tau] = 0$, *avec* $\varepsilon = (-1)^{i+(p-1)/2}$; *sinon* $\delta(\nu, M) = 0$.

Cas (*b*) : χ de degré 2; *on a :*

(i) $\delta(\chi, M) = 2$ *si* $H_0 \subset M$ *et* $[G_k(L)] = [G_k(L)^\tau] = [G_{p(k)}(L)] = [G_{p(k)}(L)^\tau] = 0$; *sinon* $\delta(\chi, M) \leqq 1$.

(ii) $\delta(\chi, M) \geqq 1$ *s'il existe* $i \in \{0, 1\}$ *tel que*

$$\omega_{i,k}(G(H/M)) = \{1\}$$

et

$$[G_k(L)] + \varepsilon [G_k(L)^\tau] = [G_{p(k)}(L)] + \varepsilon [G_{p(k)}(L)^\tau] = 0,$$

avec $\varepsilon = (-1)^{i+(k/2)}$; *sinon* $\delta(\chi, M) = 0$.

Exemples. — Nos calculs étant trops incomplets, nous nous contenterons de quelques remarques :

D'après les tableaux E.II et E.III, pour le corps $K = \mathbf{Q}(\sqrt{-267})$, on a les congruences remarquables suivantes :

$$\begin{cases} G_2(L) + G_2(L)^\tau \equiv 0 \pmod{5^2}, \\ G_4(L) + G_4(L)^\tau \equiv 0 \pmod{5^4}, \\ G_6(L) - G_6(L)^\tau \equiv 0 \pmod{5^3}; \text{ etc.} \end{cases}$$

D'après le tableau E.III, pour le corps $K = \mathbf{Q}(\sqrt{-51})$ et le nombre premier 5 décomposé dans K, on a

$$[G_2(L)] = [G_2(L)^\tau] = 1,$$

et par suite $\delta(\sigma^2, H) = 1$, si H désigne le corps de classes du rayon modulo un diviseur premier $\mathfrak{p}$ de 5 dans K. Mais, il est facile d'évaluer le discriminant D du corps H, extension non galoisienne de degré 8 de $\mathbf{Q}$; on trouve

$$|D|^{1/8} = 5^{1/4} 51^{1/2} < 10{,}6790,$$

de sorte que les minorations de discriminant d'Odlyzko impliquent $h_H \leqq 2$. D'après la proposition 57 (§ 6), le corps H possède donc une unique extension abélienne de degré 5 non ramifiée en dehors de $\mathfrak{p} \mid 5$; cette extension est sauvagement ramifiée en $\mathfrak{p}$;

De même, pour le corps $K = \mathbf{Q}(\sqrt{-52})$ et le nombre premier 7 décomposé dans K, on a

$$[G_2(L)] = [G_2(L)^\tau] = 1/2,$$

et par suite $\delta(\sigma^2, H) = 1$, si H désigne le corps de classes du rayon modulo un diviseur premier $\mathfrak{p}$ de 7 dans K. Pour le discriminant D du corps H, extension non galoisienne de degré 12 de $\mathbf{Q}$, on trouve

$$|D|^{1/12} = 7^{1/3} 52^{1/2} < 13{,}7944,$$

de sorte que les minorations de discriminant d'Odlyzko impliquent $h_H \leqq 4$. D'après la proposition 57 (§ 6), le corps H possède donc une (unique) extension abélienne de degré 7 non ramifiée en dehors de $\mathfrak{p} \mid 7$; cette extension est sauvagement ramifiée en $\mathfrak{p}$.

INDEX

Modules galoisiens sur $\mathbf{Z}_p$:	
U, $U(M)$	§ 6, p. 336
$\overline{\mathscr{E}}(M)$	§ 6, p. 342
sur $\mathbf{F}_p$:	
$\varkappa$ (algèbre)	§ 0, p. 300
$\Psi^{(p)}$	§ 3, p. 312
$\Theta^{(p)}$, $\Theta^{(p)}(M)$	§ 3, p. 315
$\Omega^{(p)}(M)$, $\mathscr{E}^{(p)}(M)$	§ 2, p. 306
$U_q^{(p)}$, $U^{(p)}$, $U^{(p)}(M)$	§ 6, p. 336
$\overline{\Omega}^{(p)}$, $\overline{\mathscr{E}}^{(p)}$	§ 6, p. 336
$\overline{\Omega}^{(p)}(M)$, $\overline{\mathscr{E}}^{(p)}(M)$	§ 6, p. 336
$\mathscr{S}(M)$	§ 2, p. 306 et appendice B, p. 356
$\mathscr{L}_\chi$, $\mathscr{L}(\chi, M)$	§ 3, p. 312, p. 316
$\pi(M)$	§ 6, p. 345
sur $\tilde{\mathbf{F}}_p$:	
$\tilde{\mathscr{L}}$	§ 4, p. 320
Lois de groupes formels :	
$A(t_1, t_2)$, $A'_q(u_1, u_2)$	§ 5, p. 326, p. 330
$\mathscr{E}_q$, $\mathscr{E}'_q$	§ 5, p. 326, p. 330
$\mathbf{G}_a$	§ 5, p. 330
Séries formelles :	
t, $a(t)$	§ 5, p. 326
$[\lambda]_q(t)$, $u_q(t)$	§ 5, p. 327, p. 330
$g(z)$	§ 5, p. 330
$I(u_q)$	§ 5, p. 330
Dérivées logarithmiques tronquées :	
φ, φ_k	§ 3, p. 308 et § 5, p. 328
φ_q, $\varphi_{k,q}$	§ 5, p. 328
φ_{Λ_q}, φ_{k,Λ_q}	§ 5, p. 328-329

BIBLIOGRAPHIE

[1] H. M. Stark, *Class Fields and Modular Forms of Weight one* (*Modular Functions of one Variable V*; *Lect. Notes in Math.*, n° 601, 1977, p. 277-287, Springer).

[2] W. E. H. Berwick, *Modular Invariants Expressible in Terms of Quadratic and Cubic Irrationnalities* (*Proc. London Math. Soc.* (2), vol. 28, 1927, p. 53-69).

[3] B. J. Birch, *Weber's Class Invariants* (*Mathematika*, vol. 16, 1969, p. 283-294).

[4] Z. I. Borevitch et I. R. Chafarevitch, *Théorie des nombres*, Gauthier-Villars, 1967 (traduction française).

[5] J. W. S. Cassels, *A Note on the Division Values of $\mathscr{P}(u)$* (*Proc. Cambridge Philos. Soc.*, vol. 45, 1949, p. 167-172).

[6] C. Chevalley, *Relation entre le nombre de classes d'un sous-corps et celui d'un sur-corps* (*C. R. Acad. Sc.*, Paris, t. 191, 2 février 1931, p. 257-258).

[7] J. Coates and A. Wiles, *Kummer's Criterion for Hurwitz Numbers* (*Algebraic Number Theory*, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga, Ed. *Japan Society for the Promotion of Science*, Tokyo, 1977).

[8] J. Coates and A. Wiles. *On the Conjecture of Birch and Swinnerton-Dyer* (*Inventiones math.*, vol. 39, 1977, p. 223-251).

[9] A. FRÖHLICH, *Formal Groups* (*Lect. Notes in Math.*, n° 74, Springer, 1968).
[10] H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
[11] J. HERBRAND, *Sur les classes des corps circulaires* (*Journ. Math. Pures et Appl.*, vol. 11, 9e série, 1932, p. 417-441).
[12] A. HURWITZ, *Über die Entwicklungskoeffizienten der lemniscatischen Funktionen* (*Math. Ann.*, vol. 51, 1899, p. 196-226; Werke II, p. 342-373).
[13] N. KATZ, P-*adic Interpolation of Real Analytic Eisenstein Series* (*Ann. of Math.* (2), vol. 104, 1976, p. 459-571).
[14] N. KATZ, *Formal Groups and p-adic Interpolation* (*Astérisque*, t. 41-42; *J. Arith. de Caen*, 1976, p. 55-65).
[15] H. LANG, *Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrass-schen $\mathcal{P}$-funktion* (*Abh. Math. Sem. Hamburg*, vol. 33, 1969, p. 183-196).
[16] S. LANG, *Elliptic functions*, Addison-Wesley, 1973.
[17] H. W. LEOPOLDT, *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper* (*J. Rein. u. And. Math.*, vol. 199, 1958, p. 165-174).
[18] S. LICHTENBAUM, *On p-adic L-functions associated to elliptic curves*, 1976 (à paraître).
[19] J. LUBIN, *One-Parameter Formal Lie Groups Over p-Adic Integer Rings* (*Ann. of Math.* (2), vol. 80, 1964, p. 464-484).
[20] J. U. MANIN et M. M. VISHIK, *Séries de Hecke p-adiques pour un corps quadratique imaginaire* (en russe) (*Math. Sbor.*, vol. 95, 1974, p. 357-383; *Math. of U.S.S.R. Sbor.*, vol. 24, p. 345-371).
[21] C. J. MORENO, *The Von Staudt-Clausen Phenomenon in Geometry and Arithmetic:* I. *The Values of Zeta Functions*, polycopié, 1972.
[22] A. P. NOVIKOV, *Sur la régularité des idéaux premiers de degré un d'un corps quadratique imaginaire* (*en russe*) (*Isv. Akad. Nauk S.S.S.R.*, vol. 33, 1969, p. 1059-1079; *Math. of U.S.S.R. Isv.*, vol. 3, p. 1001-1018).
[23] A. M. ODLYZKO, *Discriminants bounds*, lettre, 29 nov. 1976.
[24] G. POITOU, *Minorations de discriminants, d'après A. M. Odlyzko* (exp. *Bourbaki*, n° 479, février 1976).
[25] K. RAMACHANDRA, *Some Applications of Kronecker's Limit Formulas* (*Ann. of Math.* (2), vol. 80, 1964, p. 104-148).
[26] S. RAMANUJAN, *Modular Equations and Approximation to* π (*Quart. J. of Math.*, vol. 45, 1914, p. 350-372).
[27] K. RIBET, *A Modular Construction of Unramified p-Extensions of* $\mathbb{Q}(\mu_p)$ (*Inventiones math.*, vol. 34, 1976, p. 151-162).
[28] G. ROBERT, *Unités elliptiques Bull. Soc. math. France, mémoire* 36, 1973).
[29] G. ROBERT, *Régularité des idéaux premiers d'un corps quadratique imaginaire de nombre de classes un* (*Astérisque*, t. 24-25; *J. Arith. de Bordeaux*, 1974, p. 75-80).
[30] J.-P. SERRE and J. TATE, *Good Reduction of Abelian Varieties* (*Ann. of Math.* (2), vol. 88, 1968, p. 492-517).
[31] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions* (*Publ. Math. Soc., Japan*, vol. 11, 1971).
[32] C. L. SIEGEL, *Zum Beweise des Starkschen Satze* (*Invent. math.*, 5, 1968, p. 180-191).
[33] H. M. STARK, *A Transcendance Theorem for Class-Number Problems* (*Ann. of Math.* (2), vol. 94, 1971, p. 190-199).
[34] J. TATE, *Algorithm for Determining the type of a Singular Fiber in an Elliptic Pencil* (*Modular Functions in one Variable*; *Lect. Notes in Math.*, n° 476, 1975, p. 33-52, Springer).
[35] J. VÉLU, Isogénies entre courbes elliptiques (*C. R. Acad. Sc.*, Paris, t. 273, 26 juillet 1971, p. 238-241).
[36] G. N. WATSON, *Singular moduli* (5) and (6) (*Proc. London Math. Soc.* (2), vol. 42, 1936, p. 377-397 et 398-409, parmi toute une série de travaux).
[37] H. WEBER, *Lehrbuch der Algebra* III, Braunschweig, 1908.

(Manuscrit reçu le 23 novembre 1977,
révisé le 5 mai 1978.)

Gilles ROBERT,
39, rue de l'Amiral-Mouchez,
75013 Paris.