

Progress in Mathematics



Séminaire de Théorie des Nombres, Paris 1987–88

Edited by
Catherine Goldstein



Birkhäuser

B

Progress in Mathematics

Volume 81

Series Editors

J. Oesterlé

A. Weinstein

Séminaire de Théorie des Nombres, Paris 1987–88

Edited by
Catherine Goldstein

1990

Birkhäuser
Boston · Basel · Berlin

Catherine Goldstein
Mathématique, Bâtiment 425
Université de Paris-Sud
Centre d'Orsay
91405 Orsay Cédex
France

“The Library of Congress has cataloged this
serial publication as follows:”.

Séminaire Delange-Pisot-Poitou.

Séminaire de théorie des nombres/Séminaire Delange-Pisot-Poitou. — 1979-80. — Boston: Birkhäuser, 1981—

v.;24 cm. — (Progress in mathematics)

Annual.

English and French.

Continues: Séminaire Delange-Pisot-Poitou. Séminaire Delange-Pisot-Poitou: [exposés]

I. Numbers, Theory of—Periodicals. I. Title. II. Series: Progress in mathematics (Boston, Mass.)

QA 24.S37a 512'.7'05—dc19 85-648844

Library of Congress [8510] AACR 2 MARC-S

CIP-Kurztitelaufnahme der Deutschen Bibliothek
Séminaire de Théorie des Nombres:
Séminaire de Théorie des Nombres. – Boston ; Basel ;
Berlin : Birkhäuser
Teilw. auf d. Haupttitels. auch : Séminaire Delange-Pisot-Poitou
1987/88. Paris 1987-88. – 1990.
(Progress in mathematics ; Vol. 81)
ISBN-13:978-1-4612-8032-3 e-ISBN-13:978-1-4612-3460-9
DOI: 10.1007/978-1-4612-3460-9

NE: GT

Printed on acid-free paper.

© Birkhäuser Boston, 1990

Softcover reprint of the hardcover 1st edition 1990

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the copyright owner.

Permission to photocopy for internal or personal use, or the internal or personal use of specific clients, is granted by Birkhäuser Boston, Inc., for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of \$0.00 per copy, plus \$0.20 per page is paid directly to CCC, 21 Congress Street, Salem, MA 01970, U.S.A. Special requests should be addressed directly to Birkhäuser Boston, Inc., 675 Massachusetts Avenue, Cambridge, MA 02139, U.S.A.
3458-4/90 \$0.00 + .20

ISBN-13:978-1-4612-8032-3

Camera-ready text provided by the editor.

Les textes qui suivent sont pour la plupart des versions écrites de conférences données pendant l'année 1987-88 au Séminaire de Théorie des Nombres de Paris. Ce séminaire est organisé par la R.C.P. 08 303 du C.N.R.S. qui regroupe des arithméticiens de plusieurs universités et est dotée d'un conseil éditorial et scientifique. Ont été aussi adjoints certains textes dont la mise à la disposition d'un large public nous a paru intéressante. Les papiers proposés ici exposent soit des résultats nouveaux, soit des synthèses originales de questions récentes ; ils ont en particulier tous fait l'objet d'un rapport.

Ce recueil doit bien sûr beaucoup à tous les participants du séminaire et à ceux qui ont accepté d'en réviser les textes. Il doit surtout à Monique Le Bronnec qui s'est chargée comme toujours du secrétariat et de la frappe définitive du manuscrit ; son efficacité et sa très agréable collaboration ont été cruciales dans l'élaboration de ce livre.

Pour le conseil éditorial et
scientifique

C. GOLDSTEIN

CONTENTS

Comportement statistique du nombre de facteurs premiers des entiers <i>M. Balazard</i>	1
Sur les minorations géométriques des régulateurs <i>A.-M. Bergé et J. Martinet</i>	23
Deformations of Galois Representations associated to the cusp form Δ <i>N. Boston</i>	51
Multiplicative functions $ g \leq 1$ and their convolutions : an overview <i>P.D.T.A. Elliott</i>	63
Arithmetic of 3 and 4 branch point covers. A bridge provided by noncongruence subgroups of $SL_2(\mathbb{Z})$ <i>M. Fried</i>	77
Minoration de hauteurs et analyse diophantienne sur les courbes elliptiques <i>M. Hindry</i>	119
Rang P -adique d'unités : un point de vue torique <i>M. Laurent</i>	131
Le groupe des classes ambiges (au sens strict) <i>S. Louboutin</i>	147
Sur l'arithmétique des corps de nombres p -rationnels <i>A. Movahhedi et T. NGuyen Quang Do</i>	155

Algebraic independence of certain power series <i>K. Nishioka</i>	201
Représentations p -adiques, périodes et fonctions <i>L. p-adiques</i> <i>B. Perrin-Riou</i>	213
Raising the levels of Modular Representations <i>K. A. Ribet</i>	259
Matrices dont les coefficients sont des formes linéaires <i>D. Roy</i>	273
Some new Hasse principles for conic bundle surfaces <i>P. Salberger</i>	283
Valeurs des formes quadratiques indéfinies irrationnelles (d'après G.A. Margulis) <i>J.-C. Sikorav</i>	307
P -adic heights on abelian varieties <i>Yuri G. Zarhin</i>	317
Erratum : "Diagonale de fractions rationnelles" (STNP 1986–87) <i>G. Christol</i>	343
Erratum : "On the arithmetic of conic bundle surfaces" (STNP 1985–86) <i>P. Salberger</i>	347
Liste des conférenciers	349

Séminaire de Théorie des Nombres

Paris 1987-88

**COMPORTEMENT STATISTIQUE DU NOMBRE
DE FACTEURS PREMIERS DES ENTIERS
M. BALAZARD**

I.— Introduction.

Si n est un entier positif, on note $\Omega(n)$ le nombre de facteurs premiers de n , comptés avec leurs multiplicités :

$$(1) \quad \Omega(n) = \sum_{p^\alpha | n} 1 = \sum_{p^\alpha \parallel n} \alpha$$

où p désigne un nombre premier générique et α un entier positif générique. La fonction arithmétique Ω est complètement additive, c'est-à-dire que $\Omega(ab) = \Omega(a) + \Omega(b)$, quels que soient les entiers naturels a et b .

Dans cet exposé, nous étudions le comportement local de Ω . Posons :

$$(2) \quad \nu_x(\Omega(n) = k) = \frac{1}{x} \sum_{\substack{n \leq x \\ \Omega(n)=k}} 1$$

où x est un entier positif tendant vers l'infini, et k un entier positif. Dans (2), ν_x désigne la probabilité uniforme sur l'ensemble des entiers $1, 2, \dots, x$; comme $2^{\Omega(n)} \leq n$, on a $\nu_x(\Omega(n) = k) = 0$ pour $k > \frac{\log x}{\log 2}$ et il suffit d'étudier (2) pour $k \leq \frac{\log x}{\log 2}$.

Depuis le début de notre siècle, de nombreux auteurs ont donné des équivalents asymptotiques ou des majorations pour $\nu_x(\Omega(n) = k)$. Nous résumons ci-dessous ces travaux ; pour ne pas alourdir cette présentation, nous omettons les termes d'erreurs effectifs connus pour les résultats (6) et (10).

$$(3) \quad \nu_x(\Omega(n) = k) \sim (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \quad \text{quand } x \rightarrow +\infty,$$

pour tout k fixé (Landau 1900, cf. [11]).

$$(4) \quad \nu_x(\Omega(n) = k) \leq c_0 \left(\frac{10}{9}\right)^{-k} (\log x)^{-1} S_{k-1} \left(\frac{10}{9} (\log \log x + c_1)\right)$$

uniformément pour $x \geq 3$ et $k \geq 1$, où c_0 et c_1 sont des constantes positives absolues et $S_{k-1}(X) = \sum_{i=0}^{k-1} \frac{X^i}{i!}$ est la $(k-1)$ -ième somme partielle de la série exponentielle (Hardy et Ramanujan 1917, cf. [8]). Signalons qu'une inégalité fausse $(\nu_x(\Omega(n) = k) \leq c_0 (\log x)^{-1} (\log \log x + c_1)^{k-1} / (k-1)!$ a parfois été utilisée imprudemment à la place de (4).

$$(5) \quad \nu_x(\Omega(n) = k) \sim (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \quad \text{quand } x \rightarrow +\infty$$

et $|k - \log \log x| \leq B (\log \log x)^{\frac{1}{2}}$ où B est positif, arbitraire mais fixé (Erdős 1948, cf. [5]).

$$(6) \quad \nu_x(\Omega(n) = k) \sim F \left(\frac{k-1}{\log \log x} \right) (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \quad \text{quand } x \rightarrow +\infty,$$

uniformément pour $1 \leq k \leq (2-\epsilon) \log \log x$, où $\epsilon > 0$ est fixé et

$$F(z) = \frac{1}{\Gamma(z+1)} \prod_p \left(1 - \frac{1}{p}\right)^z \left(1 - \frac{z}{p}\right)^{-1} \quad (\text{Sathe--Selberg 1953--54, cf. [19]}).$$

$$(7) \quad \nu_x(\Omega(n) = k) \sim C (\log x) 2^{-k} \quad \text{quand } x \rightarrow +\infty,$$

uniformément pour $(2+\epsilon) \log \log x \leq k \leq B \log \log x$ où ϵ et B sont positifs et fixés et $C = \frac{1}{4} \prod_{p \geq 3} \left(1 + \frac{1}{p(p-2)}\right)$ (Selberg 1954, cf. [19]).

$$(8) \quad \nu_x(\Omega(n) = k) \leq c_2 (\log x) k^4 2^{-k}$$

uniformément pour $x \geq 3$ et $k \geq 1$, où c_2 est une constante positive absolue (Erdős–Sárközy 1980, cf. [6]).

$$(9) \quad \nu_x(\Omega(n) = k) \leq c_3(\log x)(\log \log x)^{\frac{1}{2}} 2^{-k}$$

uniformément pour $x \geq 3$ et $k \geq 1$, où c_3 est une constante positive absolue (Norton 1981, cf. [14]).

$$(10) \quad \nu_x(\Omega(n) = k) \sim C 2^{-k} \log(x 2^{-k}) \text{ quand } x 2^{-k} \rightarrow +\infty,$$

uniformément pour $k \geq (2+\epsilon)\log \log x$, $\epsilon > 0$ étant fixé (Nicolas 1984, cf. [13]). Signalons des travaux récents d'Azzouza, donnant des majorations explicites de $\nu_x(\Omega(n) = k)$, et utilisant la démonstration du théorème de Nicolas.

Le rapprochement entre les lois de répartition des fonctions arithmétiques et les lois probabilistiques classiques est l'un des objectifs de la théorie probabiliste des nombres. Ainsi (6) montre que, pour $k \leq (2-\epsilon)\log \log x$, $\Omega(n)$ se comporte à peu près comme une variable de Poisson de paramètre $\log \log x$ et (10) indique une loi locale à peu près géométrique de raison $\frac{1}{2}$ pour $k \geq (2+\epsilon)\log \log x$.

Il est naturel de s'interroger sur ce brusque changement de nature des formules asymptotiques pour $\nu_x(\Omega(n) = k)$. La solution du problème est donnée par la considération d'une nouvelle loi probabiliste simple.

II.— La loi Poisson—géométrique.

Considérons une loi de Poisson de paramètre $\lambda \geq 0$, définie par la formule

$$(11) \quad p_k = e^{-\lambda} \frac{\lambda^{k-1}}{(k-1)!} \quad k = 1, 2, \dots,$$

et une loi géométrique de raison r :

$$(12) \quad g_k = (1-r)r^k \quad k = 0, 1, 2, \dots$$

Nous appelons loi Poisson—géométrique de paramètre λ et de raison r le produit de convolution :

$$(13) \quad (p * g)_k = \sum_{j=1}^k p_j g_{k-j} = e^{-\lambda} (1-r) r^{k-1} S_{k-1}(\lambda/r)$$

où, comme pour (4), S_{k-1} est la $(k-1)$ -ième somme partielle de la série exponentielle.

Afin d'obtenir l'ordre de grandeur de $(p * g)_k$, rappelons les résultats classiques suivants :

- i) si $k \leq (1-\epsilon)X$, $S_k(X) \asymp \frac{X^k}{k!}$ pour $X \rightarrow +\infty$, $\epsilon > 0$ fixé
- ii) si $k \geq (1+\epsilon)X$, $S_k(X) \sim e^X$ pour $X \rightarrow +\infty$, $\epsilon > 0$ fixé
- iii) si $k = X + t\sqrt{X}$, $S_k(X) \sim \frac{e^X}{\sqrt{2\pi}} \int_{-\infty}^t \exp(-u^2/2) du$ uniformément pour $|t| \leq B$, $B > 0$ fixé.

Le lecteur intéressé trouvera des résultats beaucoup plus précis dans [15].

Ainsi, si r est fixé et λ grand, on a :

$$(14) \quad (p * g)_k \asymp e^{-\lambda} \frac{\lambda^{k-1}}{(k-1)!} (1-r) \text{ si } k \leq (1-\epsilon) \frac{\lambda}{r}$$

$$(15) \quad (p * g)_k \asymp e^{\lambda(\frac{1}{r}-1)} (1-r) r^{k-1} \text{ si } k > (1+\epsilon) \frac{\lambda}{r},$$

avec une transition gaussienne, donnée par iii), entre ces deux zones.

La loi Poisson-géométrique a donc un comportement double : (14) évoque plutôt une loi de Poisson de paramètre λ et (15) une loi géométrique de raison r . En rapprochant (14) et le résultat de Sathe-Selberg (6), (15) et le résultat de Nicolas (10), et compte-tenu également de l'inégalité de Hardy et Ramanujan (4), le théorème suivant semble naturel.

THEOREME 1 (Balazard, Delange, Nicolas 1988). *Uniformément par rapport à k, on a :*

$$(16) \quad \nu_x(\Omega(n) = k) \sim f(\min(2, \frac{k-1}{\log \log y})) \frac{2^{-k}}{\log y} S_{k-1}(2 \log \log y)$$

$$\text{quand } y = x 2^{-k} \rightarrow +\infty, \text{ où } f(z) = \frac{2^{1-z}}{\Gamma(z+1)} \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^z \left(1 - \frac{z}{p}\right)^{-1}.$$

Ce théorème est annoncé, sous une forme plus précise, dans [4]. Sa démonstration complète se trouve dans [2] ; le paragraphe suivant en contient les principales idées. Il montre que la loi locale de $\Omega(n)$ pour $1 \leq n \leq x$ est en gros une loi Poisson-géométrique de "paramètre" $\log \log y$ et de raison $\frac{1}{2}$ ($\log \log y$ dépend de k , mais assez faiblement : on a $0 \leq \log \log x - \log \log y \leq \log \frac{1}{\epsilon}$ si $k \leq (1-\epsilon) \frac{\log x}{\log 2}$). Observons que la fonction f est continue et strictement positive sur $[0,2]$, et que $f(2) = C$.

En utilisant pour $S_k(X)$ des estimations plus précises que i) et ii) ci-dessus, on peut retrouver le résultat de Sathe-Selberg (6) et celui de Nicolas (10) à partir du théorème 1. Combiné avec iii), il donne pour la *zone critique* $k \sim 2 \log \log x$ un nouveau résultat, observé pour la première fois par Delange :

COROLLAIRE. *Pour tout $B > 0$ fixé, on a :*

$$(17) \quad \nu_x(\Omega(n) = k) \sim C 2^{-k} \log x \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t \exp(-u^2/2) du \text{ quand } x \rightarrow +\infty,$$

$$\text{uniformément pour } -B \leq t = \frac{k-2 \log \log x}{\sqrt{2 \log \log x}} \leq B.$$

III.— Interprétation probabiliste et plan de la démonstration du théorème 1.

La loi locale d'une somme de deux variables aléatoires indépendantes est le produit de convolution de leurs lois locales respectives. La signification du théorème 1 est que dans l'écriture

$$(18) \quad \Omega(n) = v_2(n) + \Omega'(n),$$

les fonctions arithmétiques $v_2(n)$ ($=$ valuation 2-adique de n) et $\Omega'(n)$ ($=$ nombre de facteurs premiers impaires de n) se comportent pour $n \leq x$ comme deux variables aléatoires indépendantes. La loi locale de v_2 est approximativement géométrique de raison $\frac{1}{2}$ et celle de Ω' approximativement de Poisson de paramètre $\log \log x$. Bien entendu, la même analyse montre que la loi de Ω' a une composante géométrique prépondérante de raison $\frac{1}{3}$ mais celle-ci s'avère négligeable par rapport à la loi de v_2 .

La démonstration du théorème 1 utilise cette même idée : séparer dans $\Omega(n)$ les deux quantités $v_2(n)$ et $\Omega'(n)$. Si n est entier ≥ 1 , écrivons $n = 2^\alpha m$ avec $\alpha = v_2(n)$ et m impair. Nous avons :

$$\begin{aligned} n \leq x \text{ et } \Omega(n) = k &\Leftrightarrow 2^\alpha m \leq x \text{ et } \alpha + \Omega(m) = k \\ &\Leftrightarrow 2^{k-\Omega(m)} m \leq x, \Omega(m) \leq k \text{ et } \alpha = k - \Omega(m). \end{aligned}$$

Par conséquent, $x \nu_x(\Omega(n) = k)$ est exactement le nombre d'entiers m impairs tels que $m 2^{-\Omega(m)} \leq x 2^{-k}$ et $\Omega(m) \leq k$. En notant $\psi(m) = m 2^{-\Omega(m)}$, $y = x 2^{-k}$, la lettre m désignant dans toute la suite un entier générique impair, nous avons :

$$(19) \quad x \nu_x(\Omega(n) = k) = \sum_{\substack{\psi(m) \leq y \\ \Omega(m) \leq k}} 1.$$

Cette formule est dûe à Halász et a déjà été utilisée par Nicolas pour démontrer (10). Elle peut aussi servir au calcul numérique rapide de $x \nu_x(\Omega(n) = k)$ pour de grandes valeurs de x .

La démonstration de Nicolas pour (10) est élémentaire mais nous pouvons utiliser à partir de (19) des méthodes d'analyse complexe. La formule de Cauchy nous donne en effet :

$$(20) \quad x \nu_x(\Omega(n) = k) = \frac{1}{2\pi i} \int_{|z|=r} \sum_{\psi(m) \leq y} z^{\Omega(m)} \frac{z^{-k-1}}{1-z} dz$$

où $r < 1$ est arbitraire, la circonférence $|z| = r$ étant parcourue une fois dans le sens positif.

On est ainsi amené à chercher une estimation précise de la somme $\sum_{\psi(m) \leq y} z^{\Omega(m)}$. Cette estimation est obtenue par la méthode d'intégration complexe exposée par Selberg dans [19]. La fonction génératrice $\sum_m \frac{z^{\Omega(m)}}{m \psi(m)^s}$ se factorise en $\zeta(s) z^{2s} G(s, z)$, la fonction $G(s, z)$ étant holomorphe pour $|z| < \frac{3}{2}$, $\operatorname{Re} s > \max(\frac{1}{2}, \frac{\log|z|}{\log \frac{3}{2}})$. La nouveauté est ici la dépendance en la variable s de l'exposant de la fonction ζ (cf. également [1]). On obtient finalement :

$$(21) \quad \sum_{\psi(m) \leq y} z^{\Omega(m)} = z f(2z) y (\log y)^{2z-1} + O_R(y (\log y)^{2\operatorname{Re} z - 2} (\log \log y))$$

uniformément pour $|z| \leq R < \frac{3}{2}$ et $y \geq 3$, où f est définie dans l'énoncé du théorème 1.

D'après (20) et (21), $x \nu_x(\Omega(n) = k)$ est somme de deux termes $\frac{y}{\log y} T_1$ et $\frac{y}{\log^2 y} (\log \log y) T_2$ avec :

$$T_1 = \frac{1}{2\pi i} \int_{|z|=r} \frac{f(2z)}{1-z} z^{-k} (\log y)^{2z} dz$$

et

$$T_2 = \frac{1}{2\pi i} \int_{|z|=r} O_R\left(\left|\frac{z^{-k-1}}{1-z}\right| (\log y)^{2\operatorname{Re} z}\right) dz.$$

Les méthodes connues d'évaluation asymptotique d'intégrales complexes (méthodes de Laplace, du col, des résidus) peuvent alors être employées avec succès pour estimer T_1 et T_2 . Au prix de calculs assez fins (voir [2], pages 103–109) on peut montrer que :

$$T_1 \sim f(2r) S_{k-1}(2 \log \log y) \text{ et } T_2 = o(T_1)$$

quand $y \rightarrow +\infty$, uniformément en k , où $r = \frac{S_{k-2}(2 \log \log y)}{S_{k-1}(2 \log \log y)}$ (on peut supposer $k \geq 2$).

Pour terminer la démonstration du théorème 1, on montre que

$$(22) \quad 2r \sim \min(2, \frac{k-1}{\log \log y}), \quad y \rightarrow +\infty$$

uniformément pour $k \geq 2$ (voir le paragraphe VI ci-dessous).

Bien entendu, les méthodes utilisées permettent d'évaluer les termes d'erreurs précisant les équivalences asymptotiques ci-dessus.

IV.— Cas d'autres fonctions.

La fonction $\Omega(n)$ est un exemple de fonction complètement additive valant 0 ou 1 en chaque nombre premier. De façon générale, une telle fonction s'écrit :

$$(23) \quad \Omega_E(n) = \sum_{\substack{p^{\nu} \parallel n \\ p \in E}} \nu,$$

E désignant un ensemble quelconque de nombres premiers. Le problème du comportement statistique de $\Omega_E(n)$ pour $1 \leq n \leq x$ a été étudié notamment par Halász, Sárközy et Norton ; il intervient dans de nombreuses questions de théorie analytique des nombres, notamment dans des situations où l'ensemble E peut dépendre de x (cf. [7]).

Dans [3] nous avons comparé la loi locale $\nu_x(\Omega_E(n) = k)$ avec la loi Poisson—géométrique de raison $\frac{1}{p_1}$ et de paramètre $E_1(y)$, où :

$$p_1 = \min E; \quad E_1(u) = \sum_{\substack{p_1 < p \leq u \\ p \in E}} \frac{1}{p}; \quad y = x p_1^{-k},$$

et nous obtenons le résultat suivant :

THEOREME 2. Posons $t = \min(p_1, \frac{k}{E_1(y)})$. Il existe des constantes positives absolues c_i ($4 \leq i \leq 9$) telles que

$$\nu_x(\Omega_E(n) = k) \leq c_4 p_1^{-k} \exp(c_5 t - E_1(y)) S_k(p_1 E_1(y))$$

pour tout $x \geq 1$, tout E et tout entier naturel k ;

$$\nu_x(\Omega_E(n) = k) \geq c_6 p_1^{-k} \exp(-c_7 t \log(1+t) - E_1(y)) S_{k-1}(p_1 E_1(y))$$

pour tout $x \geq 1$, tout E et tout entier $k \geq 1$ tels que

$$E_1(y) \geq c_8 t \log(1+t) + c_9.$$

On peut aussi compter une seule fois chaque diviseur premier de n et considérer la fonction

$$\omega(n) = \sum_{p|n} 1.$$

Pour cette fonction, le résultat de Sathe et Selberg est

$$(24) \quad \nu_x(\omega(n) = k) \sim G\left(\frac{k-1}{\log \log x}\right) (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!}$$

quand $x \rightarrow +\infty$, uniformément pour $1 \leq k \leq B \log \log x$ où B est positif et fixé (mais quelconque) et $G(z) = \frac{1}{\Gamma(z+1)} \prod (1 - \frac{1}{p})^z (1 + \frac{z}{p-1})$ Hensley a montré (cf. [9]) que (24) est vraie si et seulement si $k = o((\log \log x)^2 (\log \log \log x)^{-2})$. Récemment, Hildebrand et Tenenbaum ont donné une formule asymptotique pour $\nu_x(\omega(n) = k)$ valable pour $k \ll \log x (\log \log x)^{-2}$ cf. [10]. L'intervalle des valeurs de k pour lesquelles $\nu_x(\omega(n) = k) \neq 0$ est $0 \leq k \leq (1+o(1)) \log x (\log \log x)^{-1}$. Le traitement analytique de ce problème est nettement plus difficile que la démonstration de notre théorème 1 et nécessite l'emploi d'une méthode du col en deux variables complexes (cf. également [20]).

V.— Questions d'unimodalité.

Une suite (u_k) de réels ≥ 0 , définie pour k appartenant à un intervalle de \mathbb{Z} , est dite unimodale s'il existe $k_0 \in \mathbb{Z} \cup \{-\infty, +\infty\}$ tel que $u_k \leq u_{k+1}$ pour $k < k_0$, et $u_k \geq u_{k+1}$ pour $k \geq k_0$. L'article [12] de P. Medgyessy présente de façon agréable les faits fondamentaux concernant l'unimodalité des suites. Illustrons ces faits par les exemples suivants :

- 1) La loi de Poisson de paramètre λ , $p_k = e^{-\lambda} \frac{\lambda^{k-1}}{(k-1)!}$ définie pour $k \geq 1$, est unimodale. Son sommet est atteint en $k_0 = \lfloor \lambda \rfloor + 1$ (et aussi en $k_0 = \lambda$ si λ est entier).
- 2) La loi géométrique de raison r , $g_k = (1-r)r^k$, définie pour $k \geq 0$, est unimodale. Son sommet est atteint en $k = 0$.
- 3) Plus généralement, toute loi positive et log-concave (c'est-à-dire vérifiant $u_k^2 \geq u_{k-1} u_{k+1} > 0$ pour tout k) est unimodale.
- 4) Le produit de convolution de deux lois unimodales ne l'est pas forcément. Posons $u_0 = \frac{2}{3}$, $u_1 = u_2 = \frac{1}{6}$ et $u_k = 0$ si $k \neq 0, 1, 2$. Il est facile de vérifier que $u * u$ n'est pas unimodale. En revanche, le produit de convolution de deux lois positives et log-concaves est positif, log-concave et donc aussi unimodal. Ainsi la loi Poisson-géométrique est unimodale, ce qui n'est pas évident directement.
- 5) Soit x un réel. Pour tout entier k , soit u_k la somme des inverses des entiers positifs n vérifiant

$$p \mid n \Rightarrow p \leq x ; n \text{ sans facteur carré} ; \omega(n) = k .$$

La suite (u_k) est unimodale. En effet

$$P(z) = \sum_k u_k z^k = \prod_{p \leq x} \left(1 + \frac{z}{p}\right)$$

et $P(z)(1-z) = u_0 + (u_1 - u_0)z + (u_2 - u_1)z^2 + \dots$

Or une version de la règle de Descartes affirme que si toutes les racines d'un polynôme à coefficients réels sont réelles, le nombre de racines positives est

égal au nombre de changements de signe dans la suite des coefficients du polynôme. Appliqué au polynôme $P(z)(1-z)$, cet énoncé montre qu'il y a un unique changement de signe dans la suite $u_0, u_1 - u_0, u_2 - u_1, \dots$ donc que la suite (u_k) est unimodale.

En 1948, Erdős a montré dans [5] que les suites

$$\sum_{\substack{n \leq x \\ \omega(n)=k}} \frac{1}{n}, \quad \sum_{\substack{n \leq x \\ \omega(n)=k}} \frac{\mu(n)^2}{n}, \quad \sum_{\substack{n \leq x \\ \Omega(n)=k}} \frac{1}{n}$$

sont unimodales si x est assez grand et conjecturé qu'il en est de même pour les suites

$$\sum_{\substack{n \leq x \\ \omega(n)=k}} 1, \quad \sum_{\substack{n \leq x \\ \omega(n)=k}} \mu(n)^2, \quad \sum_{\substack{n \leq x \\ \Omega(n)=k}} 1.$$

Nous confirmons cette conjecture pour cette dernière suite.

THEOREME 3. *Si x est assez grand, la loi locale $\nu_x(\Omega(n) = k)$ est unimodale.*

Démonstration : Si $k \geq \frac{\log x}{\log 3}$ et si $n \leq x$ vérifie $\Omega(n) = k + 1$, alors n est pair sinon $n \geq 3^{\Omega(n)} > x$; l'entier $\frac{n}{2}$ est lui aussi $\leq x$ et vérifie $\Omega(n) = k$. Cela prouve que :

$$(25) \quad \text{si } k \geq \frac{\log x}{\log 3}, \quad \nu_x(\Omega(n) = k + 1) \leq \nu_x(\Omega(n) = k).$$

Il nous suffit donc de montrer l'unimodalité de $\nu_x(\Omega(n) = k)$ pour $k < \frac{\log x}{\log 3}$. Avec cette condition, $y = x 2^{-k} > x^{1-(\log 2)/(\log 3)}$ donc $y \rightarrow +\infty$, uniformément par rapport à k , et

$$(26) \quad 0 \leq \log \log x - \log \log y \leq \log \frac{\log 3}{\log(3/2)}.$$

La formule asymptotique (16) nous donne

$$(27) \quad \frac{\nu_x(\Omega(n)=k+1)}{\nu_x(\Omega(n)=k)} \sim \frac{f(t_2)}{f(t_1)} \frac{\log y}{2\log(y/2)} \frac{S_k(2\log\log(y/2))}{S_{k-1}(2\log\log y)}$$

quand $y \rightarrow +\infty$, uniformément par rapport à k , où :

$$t_1 = \min(2, \frac{k-1}{\log\log y}) ; \quad t_2 = \min(2, \frac{k}{\log\log(y/2)}).$$

Comme $t_1 - t_2$ tend vers 0 quand $y \rightarrow +\infty$, uniformément par rapport à k , et comme f est continue et positive sur $[0,2]$, on peut supprimer le rapport $\frac{f(t_2)}{f(t_1)}$ dans (27).

D'autre part, le théorème des accroissements finis donne :

$$0 \leq S_k(2\log\log y) - S_k(2\log\log(y/2)) \leq S_{k-1}(2\log\log y) \cdot 2 \log \frac{\log y}{\log(y/2)},$$

donc on peut réécrire (27) sous la forme :

$$(28) \quad \frac{\nu_x(\Omega(n)=k+1)}{\nu_x(\Omega(n)=k)} \sim \frac{1}{2} \frac{S_k(2\log\log y)}{S_{k-1}(2\log\log y)} \\ \sim \max\left(\frac{1}{2}, \frac{\log\log y}{k}\right) \text{ d'après (22),}$$

quand $y \rightarrow +\infty$, uniformément par rapport à $k \geq 1$.

Compte tenu de (26), on obtient donc :

$$(29) \quad \frac{\nu_x(\Omega(n)=k+1)}{\nu_x(\Omega(n)=k)} \sim \max\left(\frac{1}{2}, \frac{\log\log x}{k}\right)$$

quand $x \rightarrow +\infty$, uniformément par rapport à k , $1 \leq k < \frac{\log x}{\log 3}$.

Cela prouve que si $\delta \in]0,1[$ est fixé et $x \geq x_0(\delta)$, alors

$$\nu_x(\Omega(n) = k+1) > \nu_x(\Omega(n) = k) \quad \text{si } k \leq (1-\delta)\log\log x$$

$$\text{et} \quad \nu_x(\Omega(n) = k+1) < \nu_x(\Omega(n) = k) \quad \text{si } k \geq (1+\delta)\log\log x.$$

Pour compléter la démonstration, il nous reste à prouver l'unimodalité de $\nu_x(\Omega(n)=k)$ dans le domaine

$$(1-\delta)\log\log x < k < (1+\delta)\log\log x.$$

Dans la formule de Sathe–Selberg (6), on sait que le rapport des deux termes de l'équivalence asymptotique est $1 + O_\epsilon\left(\frac{1}{\log\log x}\right)$. On obtient donc :

$$\frac{\nu_x(\Omega(n)=k+1)}{\nu_x(\Omega(n)=k)} = \frac{\log\log x}{k} \left(1 + O_\epsilon\left(\frac{1}{\log\log x}\right)\right)$$

pour $1 \leq k \leq (2-\epsilon)\log\log x$.

Cela prouve que

$$\nu_x(\Omega(n)=k+1) > \nu_x(\Omega(n)=k) \quad \text{si } k \leq \log\log x - C$$

$$\text{et} \quad \nu_x(\Omega(n)=k+1) < \nu_x(\Omega(n)=k) \quad \text{si } k \geq \log\log x + C$$

où C est une constante absolue inconnue.

Finalement, il reste à démontrer l'unimodalité de $\nu_x(\Omega(n)=k)$ dans le domaine $|k - \log\log x| < C$. Pour cela, nous allons préciser le $O\left(\frac{1}{\log\log x}\right)$ de la formule de Sathe–Selberg à l'aide du lemme suivant.

LEMME. Soit $H(z)$ une fonction holomorphe pour $|z| \leq R$. Posons

$$H(z)e^{tz} = \sum_{k=0}^{+\infty} a_k(t)z^k \quad \text{pour } |z| \leq R.$$

Nous avons alors :

$$(30) \quad a_k(t) = \frac{t^k}{k!} \left\{ H(\rho) - \frac{1}{2} \frac{\rho H''(\rho)}{t} + O\left(\frac{M}{t^2}\right) \right\}$$

uniformément pour $t > 0$ et $0 \leq k \leq Rt$, où $\rho = \frac{k}{t}$ et

$$M = \max_{|s| \leq R} (|s H''(s)|) + \max_{|s| \leq R} (|s^2 H^{(4)}(s)|).$$

Démonstration du lemme : Par la formule de Cauchy, on a

$$a_k(t) = \frac{1}{2\pi i} \int_{|z|=\rho} H(z) e^{tz} z^{-k-1} dz$$

où la circonférence $|z| = \rho$ est parcourue une fois dans le sens positif, $\rho \leq R$ étant pour l'instant arbitraire.

Utilisons maintenant la formule de Taylor pour $H(z)$:

$$(31) \quad H(z) = H(\rho) + H'(\rho)(z-\rho) + H''(\rho) \frac{(z-\rho)^2}{2} + H'''(\rho) \frac{(z-\rho)^3}{6} + R(z, \rho)$$

$$\text{où } R(z, \rho) = \frac{1}{6} \int_{\rho}^z (z-s)^3 H^{(4)}(s) ds.$$

Les cinq termes du second membre de (31) donnent pour contribution à $a_k(t)$ respectivement :

$$\begin{aligned} & H(\rho) \frac{t^k}{k!}; \\ & H'(\rho) \left\{ \frac{t^{k-1}}{(k-1)!} - \rho \frac{t^k}{k!} \right\} = 0 \text{ si } \rho = \frac{k}{t}; \\ & \frac{1}{2} H''(\rho) \left\{ \frac{t^{k-2}}{(k-2)!} - 2\rho \frac{t^{k-1}}{(k-1)!} + \rho^2 \frac{t^k}{k!} \right\} = -\frac{1}{2} \rho H''(\rho) \frac{t^{k-1}}{k!} \text{ si } \rho = \frac{k}{t}; \\ & \frac{1}{6} H'''(\rho) \left\{ \frac{t^{k-3}}{(k-3)!} - 3\rho \frac{t^{k-2}}{(k-2)!} + 3\rho^2 \frac{t^{k-1}}{(k-1)!} - \rho^3 \frac{t^k}{k!} \right\} = \frac{1}{3} \rho H'''(\rho) \frac{t^{k-2}}{k!} \text{ si } \rho = \frac{k}{t}; \\ & \frac{1}{2\pi i} \int_{|z|=\rho} R(z, \rho) e^{tz} z^{-k-1} dz. \end{aligned}$$

Notons I cette dernière intégrale. Nous avons la majoration :

$$|R(z, \rho)| \leq A |z-\rho|^4$$

où $A = \frac{1}{24} \max_{|s| \leq R} |H^{(4)}(s)|$. Par conséquent :

$$\begin{aligned} |I| &\leq \frac{A}{2\pi} \int_{-\pi}^{\pi} (2\rho \sin \frac{\theta}{2})^4 e^{t\rho} \cos \theta \rho^{-k} d\theta \\ &\leq \frac{A}{2\pi} \rho^{4-k} e^{t\rho} \int_{-\infty}^{\infty} \theta^4 e^{-t\rho c\theta^2} d\theta \quad (c \text{ constante } > 0 \text{ absolue}) \\ &\ll A \rho^{\frac{3}{2}-k} \frac{e^{t\rho}}{t^{5/2}} \ll A \frac{t^k}{k!} \frac{\rho^2}{t^2} \quad \text{si } \rho = \frac{k}{t}, \end{aligned}$$

d'après la formule de Stirling.

En regroupant ces estimations on obtient bien l'énoncé du lemme.

Pour utiliser ce lemme, rappelons la formule servant de point de départ pour la démonstration du résultat de Sathe—Selberg (6) :

$$(32) \quad \sum_{n \leq x} z^{\Omega(n)} = z F(z) x(\log x)^{z-1} + Q(x,z)$$

où $|Q(x,z)| = O_R(x(\log x)^{\operatorname{Re} z - 2})$ pour $x \geq 3$ et $|z| \leq R$, R étant < 2 .

Ecrivons $F(z)(\log x)^z = \sum_{k=0}^{+\infty} a_k (\log \log x) z^k$ pour $|z| < 2$.

La formule de Cauchy et (32) nous donnent

$$(33) \quad \nu_x(\Omega(n) = k) = (\log x)^{-1} a_{k-1} (\log \log x) + \frac{1}{2\pi i} \int_{|z|=\rho} x^{-1} Q(x,z) z^{-k-1} dz$$

pour tout $\rho < 2$.

Choisissons $R = \frac{3}{2}$ et supposons $k-1 \leq \frac{3}{2} \log \log x$. En prenant $\rho = \frac{k-1}{\log \log x}$, la contribution de l'intégrale de (33) peut être majorée comme dans la démonstration du lemme :

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{|z|=\rho} x^{-1} Q(x,z) z^{-k-1} dz \right| &\ll (\log x)^{-2} \rho^{-k} \int_{-\pi}^{\pi} e^{\rho \cos \theta} \log \log x d\theta \\ &\ll \rho^{-k} (\log x)^{\rho-2} (\rho \log \log x)^{-\frac{1}{2}} \\ &\ll \frac{(\log \log x)^{k-1}}{(k-1)!} (\log x)^{-2} \log \log x . \end{aligned}$$

Par conséquent, (30) et (33) donnent

$$(34) \quad \nu_x(\Omega(n)=k) = (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \left\{ F(\rho) - \frac{1}{2} \frac{\rho F''(\rho)}{\log \log x} + O((\log \log x)^{-2}) \right\}$$

pour $x \geq 3$ et $0 \leq k-1 \leq \frac{3}{2} \log \log x$, où $\rho = \frac{k-1}{\log \log x}$.

En supposant maintenant que $-C < \Delta_k = k - \log \log x < C$, on obtient :

$$\nu_x(\Omega(n)=k) = (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \left\{ 1 + \frac{F'(1)(\Delta_k - F''(1)/2)}{\log \log x} + O((\log \log x)^{-2}) \right\}$$

et

$$\begin{aligned} \nu_x(\Omega(n)=k+1) &= (\log x)^{-1} \frac{(\log \log x)^k}{k!} \left\{ 1 + \frac{F'(1)\Delta_k - F''(1)/2}{\log \log x} + O((\log \log x)^{-2}) \right\} \\ &= (\log x)^{-1} \frac{(\log \log x)^{k-1}}{(k-1)!} \left\{ 1 + \frac{\Delta_k(F'(1)-1) - F''(1)/2}{\log \log x} + O((\log \log x)^{-2}) \right\} \end{aligned}$$

Par soustraction :

$$\begin{aligned} \nu_x(\Omega(n)=k+1) - \nu_x(\Omega(n)=k) &= (\log x)^{-1} \frac{(\log \log x)^{k-2}}{(k-1)!} \{ F'(1) - \Delta_k + \\ &\quad + O((\log \log x)^{-1}) \} . \end{aligned}$$

Ainsi, il existe une constante absolue $D > 0$, telle que

$$\nu_x(\Omega(n)=k+1) > \nu_x(\Omega(n)=k) \quad \text{si } k < \log \log x + F'(1) - \frac{D}{\log \log x} = A_x$$

et

$$\nu_x(\Omega(n)=k+1) < \nu_x(\Omega(n)=k) \quad \text{si } k > \log \log x + F'(1) - \frac{D}{\log \log x} = B_x .$$

Pour x assez grand, l'intervalle $[A_x, B_x]$ contient au plus un entier. S'il n'en contient pas, l'unimodalité est démontrée et $\nu_x(\Omega(n)=k)$ atteint son maximum pour $k = [A_x] + 1 = [B_x] + 1$. Si $[A_x, B_x]$ contient un entier k_0 , l'unimodalité reste acquise mais on ne connaît pas la position du maximum : suivant que $\nu_x(\Omega(n)=k_0+1) - \nu_x(\Omega(n)=k_0)$ est positif, négatif ou nul, ce maximum est atteint pour $k = k_0 + 1$, $k = k_0$ ou les deux.

Remarques.

1°) Notons $k(x)$ le plus petit entier k tel que $\nu_x(\Omega(n)=k)$ soit maximal.

La démonstration du théorème 3 permet de conclure que $k(x)$ est une fonction non-décroissante de x , pour x assez grand. De plus on a $\nu_x(\Omega(n)=k(x)) = \nu_x(\Omega(n)=k(x)+1)$ pour une infinité d'entiers x . Ces observations sont dues à P. Erdős : nous laissons au lecteur les raisonnements très simples qui y mènent.

2°) Il serait intéressant de connaître le plus petit x_0 pour lequel la suite $(\nu_x(\Omega(n)=k))$ est unimodale si $x \geq x_0$. Il faudrait pour cela expliciter numériquement la formule de Selberg (32) et obtenir un algorithme efficace pour tester l'unimodalité de cette suite pour les premières valeurs de x .

3°) Concernant la fonction ω , la même démonstration que celle du théorème 3 et les résultats de Hildebrand et Tenenbaum prouvent que $\nu_x(\omega(n)=k)$ est unimodale dans le domaine $k \ll (\log x)(\log \log x)^{-2}$. Pour conclure, il manque un argument, peut-être élémentaire, permettant de montrer que :

$$\nu_x(\omega(n)=k+1) \leq \nu_x(\omega(n)=k) \text{ si } k \gg (\log x)(\log \log x)^{-2}.$$

4°) Concernant la fonction Ω_E , nous posons la question suivante : existe-t-il une constante absolue K telle que si $\sum_{\substack{p \leq x \\ p \in E}} \frac{1}{p} \geq K$, alors $\nu_x(\Omega(n)=k)$

est unimodale ?

Pour d'autres résultats d'unimodalité en théorie des nombres, le lecteur peut consulter les articles d'Odlyzko et Richmond [16], [17] et [18].

V.— Démonstration de (22).

Il s'agit de montrer que

$$(35) \quad \frac{S_{k-1}(X)}{S_k(X)} \sim \min(1, \frac{k}{X}),$$

quand $X \rightarrow +\infty$, uniformément pour $k \geq 1$.

Observons d'abord que $\frac{S_{k-1}(X)}{S_k(X)} \leq \min(1, \frac{k}{X})$.

$$\begin{aligned} \text{Pour } k < X \text{ on a } S_k(X) &\leq \frac{X^k}{k!} \left(1 + \frac{k}{X} + \frac{k^2}{X^2} + \dots\right) \\ &= \frac{X^k}{k!} \frac{1}{1 - \frac{k}{X}} \end{aligned}$$

et d'autre part

$$S_k(X) = \frac{1}{2\pi i} \int_{|z|=\rho} e^{zX} \frac{z^{-k-1}}{1-z} dz \quad \text{pour tout } \rho < 1.$$

En écrivant $\frac{1}{1-z} = \frac{1}{1-\rho} + \frac{z-\rho}{(1-\rho)^2} + \frac{(z-\rho)^2}{(1-z)(1-\rho)^2}$, l'intégrale est somme de trois termes. Le premier vaut $\frac{1}{1-\rho} \frac{X^k}{k!}$; le deuxième est nul si $\rho = \frac{k}{X}$ et le troisième est

$$\ll \frac{X^k}{k!} \frac{\rho}{X(1-\rho)^3} \text{ si } \rho = \frac{k}{X},$$

par la méthode de Laplace et la formule de Stirling, comme dans la démonstration du théorème 3.

Ainsi

$$(36) \quad S_k(X) = \frac{1}{1-\rho} \frac{X^k}{k!} \left(1 + O\left(\frac{\rho}{X(1-\rho)^2}\right)\right)$$

uniformément pour $X > 0$ et $\rho = \frac{k}{X} < 1$.

Soit maintenant $\epsilon > 0$. D'après (36) il existe une constante $B_1(\epsilon) > 0$ telle que

$$S_{k-1}(X) \geq \frac{1}{1 - \frac{k-1}{X}} \frac{X^{k-1}}{(k-1)!} (1-\epsilon)$$

$$\text{si } k \leq X - B_1(\epsilon) \sqrt{X}.$$

Par conséquent

$$\begin{aligned} \frac{S_{k-1}(X)}{S_k(X)} &\geq \frac{k}{X} \frac{X-k}{X-k+1} (1-\epsilon) \\ &\leq \frac{k}{X} (1-2\epsilon) \quad \text{si } k \leq X - B_2(\epsilon) \sqrt{X}. \end{aligned}$$

D'autre part la formule de Stirling montre que $\frac{X^k}{k!} \ll \frac{e^X}{\sqrt{X}}$ pour tout k et

iii) (§ II) montre que

$$S_k(X) \gg_\epsilon e^X \quad \text{si } k > X - B_2(\epsilon) \sqrt{X}.$$

$$\begin{aligned} \text{Ainsi : } \frac{S_{k-1}(X)}{S_k(X)} &= 1 - \frac{X^k/k!}{S_k(X)} \geq 1 + O_\epsilon \left(\frac{1}{\sqrt{X}} \right) \\ &\geq (1-2\epsilon) \min \left(1, \frac{k}{X} \right) \end{aligned}$$

si $X \geq X_0(\epsilon)$ et $k > X - B_2(\epsilon) \sqrt{X}$.

$$\text{Finalement, } \frac{S_{k-1}(X)}{S_k(X)} \geq (1-2\epsilon) \min \left(1, \frac{k}{X} \right)$$

si $X \geq X_0(\epsilon)$ et pour tout $k \geq 1$: (35) est démontrée. Bien entendu, on peut rendre cette démonstration effective et fournir un terme d'erreur uniforme pour (35).

BIBLIOGRAPHIE

- [1] R. Balasubramanian et K. Ramachandra.— *On the number of integers n such that $nd(n) \leq x$* , Acta Arith. 49 (1988), 313–322.
- [2] M. Balazard.— *Sur la répartition des valeurs de certaines fonctions arithmétiques additives*, Thèse (Université de Limoges 1987).
- [3] M. Balazard.— *Remarques sur un théorème de G. Halasz et A. Sarközy*, Prépublication.
- [4] M. Balazard, H. Delange et J.-L. Nicolas.— *Sur le nombre de facteurs premiers des entiers*, C.R.A.S. 306 série I (1988), 511–514.
- [5] P. Erdős.— *On the integers having exactly k prime factors*, Ann. of Math. 49 (1948), 53–66.
- [6] P. Erdős et A. Sárközy.— *On the number of prime factors of integers*, Acta Sci. Math. 42 (1980), 237–246.
- [7] R.R. Hall et G. Tenenbaum.— *Divisors*, Cambridge University Press, 1988.
- [8] G.H. Hardy et S. Ramanujan.— *The normal number of prime factors of an integer*, Quarterly J. Math. 48 (1917), 76–92.
- [9] D. Hensley.— *The distribution of round numbers*, Proc. London Math. Soc. 54 (1987), 412–444.
- [10] A. Hildebrand et G. Tenenbaum.— *On the number of prime factors of an integer*, Duke Math. J. 56 (1988), 471–501.
- [11] E. Landau.— *Sur quelques problèmes relatifs à la distribution des nombres premiers*, Bull. Soc. Math. France 28 (1900), 25–38.
- [12] P. Medgyessy.— *On the unimodality of discrete distributions*, Period. Math. Hung. 2 (1972) 245–257.

- [13] J.-L. Nicolas.— *Sur la distribution des entiers ayant une quantité fixée de facteurs premiers*, Acta Arith. 44 (1984), 191–200.
- [14] K.K. Norton.— *On the number of restricted prime factors of an integers III*, L'Ens. Math. 28 (1982) 31–52.
- [15] K.K. Norton.— *Estimates for partial sums of the exponential series*, J. of Math. An. and Ap. 63 (1978), 265–296.
- [16] A.M. Odlyzko and L.B. Richmond.— *On the unimodality of high convolutions of discrete distributions*, Annals of Prob. 13 (1985), 299–306.
- [17] A.M. Odlyzko and L.B. Richmond.— *On the unimodality of some partition polynomials*, Europ. J. Comb. 3 (1982), 69–84.
- [18] A.M. Odlyzko and L.B. Richmond.— *On the compositions of an integer*, in : Combinatorial Mathematics VII, Springer Lecture Notes 829.
- [19] A. Selberg.— *Note on a paper by L.G. Sathe*, J. Indian Math. Soc. 18 (1954), 83–87.
- [20] G. Tenenbaum.— *La méthode du col en théorie analytique des nombres*, Sémin. Théorie des Nombres de Paris (1986–87), Birkhäuser (1988).

Michel Balazard
 Département de Mathématiques
 Faculté des Sciences
 123, rue A. Thomas
 87060 LIMOGES CEDEX

*Séminaire de Théorie des Nombres
Paris 1987-88*

SUR LES MINORATIONS GÉOMÉTRIQUES DES RÉGULATEURS

A.-M. BERGÉ et J. MARTINET^(*)

1.— Introduction.

Les démonstrations géométriques du théorème de Dirichlet sur les unités des corps de nombres conduisent naturellement à des majorations du régulateur en fonction de la signature et du discriminant du corps. Dans une série d'articles, dont l'article posthume [13], Robert Remak s'est intéressé aux minorations géométriques du régulateur, avec comme but une version pour régulateurs du théorème d'Hermite. Et en effet il est exact (cf. Remak) qu'il n'y a, à isomorphisme près et à condition bien entendu d'écartier les corps de type C.M., qu'un nombre fini de corps de régulateur inférieur à une borne donnée.

Comme dans le cas des discriminants, les méthodes analytiques se sont aussi avérées très fécondes pour l'étude de ce problème (Zimmert, [17]; Friedman, [6]). C'est alors le quotient R/w (R : régulateur; w : nombre des racines de l'unité) qui apparaît naturellement. Les minima absolus de R et R/w ont ainsi été obtenus.

Dans cet exposé nous analysons de près les méthodes géométriques introduites par Remak, et nous les appliquons aux extensions K/K' dans lesquelles le corps de nombres K' et la ramification dans K de ses places réelles sont fixés. Nous obtenons, pour une extension K/K' primitive, une minoration du quotient $\frac{R_K}{R_{K'}}$ de la forme :

$$Q_{K/K'} \frac{R_K}{R_{K'}} \geq \frac{1}{C_2} \left(\log \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'})}{C_3} \right)^{C_1}$$

($Q_{K/K'}$ est l'*indice de Hasse*, cf. § 2, et $\mathfrak{d}_{K/K'}$ est le discriminant relatif de l'extension). La constante prépondérante est C_1 , que nous pouvons prendre égale à la différence des rangs des groupes des unités de K et de K' , choix

vraisemblablement optimal (cf. Silverman, [16], p. 438). Ensuite vient C_2 (notée C dans la suite), fonction de la ramification des places infinies dans K'/\mathbb{Q} et K/K' . Cusick ([4]) a testé dans certains cas (avec $K' = \mathbb{Q}$) la qualité des constantes C_1 et C_2 , prouvant parfois leur caractère optimal. Nous montrons cependant ici que la constante C_2 peut souvent être améliorée par des considérations géométriques : nous donnons en effet des *formules explicites* faisant intervenir non seulement la classe de similitude du réseau des logarithmes des unités, ce qui usuel en géométrie des nombres, mais aussi la position de ce réseau. C'est ainsi que la présence d'automorphismes dans l'extension K/K' considérée permet parfois d'obtenir de meilleures constantes C_2 ; nous avons par là été amenés à introduire, à la façon de Korkine et Zolotareff, une notion de réseaux *extremes pour un groupe d'automorphismes*, notion qui présente un intérêt intrinsèque en géométrie des nombres. Signalons enfin que des méthodes issues de la transcendance permettent de traiter les extensions imprimitives (cf. [16]).

Après un court § 2 consacré aux notations et un § 3 à des calculs de discriminants de réseaux, nous exposons au § 4 la méthode de Remak qui fait apparaître la constante C_3 (notée M dans l'article). Les *formules explicites* et les minorations de régulateur qui en résultent font l'objet du § 5. Nous montrons au § 6 comment ces minorations peuvent parfois être améliorées en tenant compte de la forme et de la position du réseau des logarithmes. Dans le § 7, nous énonçons des résultats relatifs aux réseaux admettant un groupe d'automorphismes donné et nous les appliquons à des extensions galoisiennes. Le § 8 est consacré à des exemples. L'article s'achève par un court paragraphe relatif à la constante C_3 .

2.— Notations.

Soit K un corps de nombres de signature (r_1, r_2) et de degré $n = r_1 + 2r_2$. On note S l'ensemble des \mathbb{Q} -isomorphismes de K dans \mathbb{C} , et \mathcal{L}_K (ou \mathcal{L}) l'homomorphisme de K^* dans \mathbb{R}^S qui à $x \in K^*$ associe le vecteur $\sum_{\sigma \in S} \text{Log} |\sigma x| e_\sigma$, où (e_σ) désigne la base canonique de \mathbb{R}^S . Son noyau est le sous-groupe μ_K des racines de l'unité de K , et son image est dense dans le sous-espace V_K de \mathbb{R}^S de dimension $r_1 + r_2$ formé des vecteurs ayant

mêmes composantes sur e_σ et $e_{\bar{\sigma}}$. L'ensemble $\mathcal{L}(E_K)$ (E_K est le groupe des unités de K) est un réseau de l'hyperplan V'_K de V_K d'équation $\Sigma x_\sigma = 0$.

Pour $\sigma \in S$, on pose $i_\sigma = 1$ si $\sigma(K) \subset \mathbb{R}$, et $i_\sigma = 2$ sinon. On note en outre \tilde{S} un système de représentants des éléments de S à conjugaison complexe près (donc, $|\tilde{S}| = r_1 + r_2$). Soit E un sous-groupe de E_K de rang maximum $r = r_1 + r_2 - 1$, et soit $\epsilon_1, \dots, \epsilon_r$ une famille d'unités génératrices de E . La valeur absolue d'un déterminant d'ordre r extrait de la matrice $(i_\sigma \log |\sigma(\epsilon_j)|)_{(1 \leq j \leq r, \sigma \in S)}$ s'appelle *le régulateur* de E et se note $R_K(E)$, et l'on écrit simplement R_K si $E = E_K$. Soit K' un sous-corps de K . On définit de même n' , r'_1 , r'_2 , r' , S' , \tilde{S}' , et l'on pose $m = [K : K']$; on a $n' = r'_1 + 2r'_2$, $r' = r'_1 + r'_2 - 1$ et $n = mn'$. Pour tout $\sigma' \in \tilde{S}'$, soit en outre $r_1(\sigma')$ (resp $r_2(\sigma')$) le nombre de places de K réelles (resp. imaginaires) au-dessus de σ' ; on a $m = r_1(\sigma') + 2r_2(\sigma')$ (resp. $m = r_2(\sigma')$) si σ' est réelle (resp. imaginaire). On note $\rho_{K/K'}$ (ou ρ) la somme $\sum_{\sigma' \text{ réel}} r_2(\sigma')$: c'est le nombre de places imaginaires de K qui sont au-dessus d'une place réelle de K' ; on a $\rho = r_2 - mr'_2$.

2.1.— DEFINITION. *On appelle indice de Hasse de K sur K' l'entier $Q_{K/K'}$, ordre du sous-groupe de torsion de $E_K/\mu_K E_K$. On appelle régulateur relatif de K/K' le nombre réel $R_{K/K'} = Q_{K/K'} R_K / R_{K'}$.*

Si K est de type C.M. de sous-corps réel maximal K' , et dans ce cas seulement, $E_K/\mu_K E_K$ est un groupe de torsion; son ordre (1 ou 2) a été étudié par Hasse dans [8]. La proposition suivante est immédiate :

2.2.— PROPOSITION. *On a $Q_{K/K'} = [\mathcal{L}(E_K) \cap \mathbb{R}\mathcal{L}(E_{K'}) : \mathcal{L}(E_{K'})]$.*

Les indices $Q_{K/K'}$ et $[\mu_K : \mu_{K'}]$ joueront un rôle mineur dans la suite, à cause de la proposition suivante dont la démonstration est également laissée au lecteur :

2.3.— PROPOSITION. *Soit L un corps de nombres, soit q un entier positif et soit \mathcal{E} l'ensemble des extensions primitives (i.e. sans sous-extension non triviale) de L , de degré q , contenues dans une clôture algébrique donnée de L . Alors, à un nombre fini d'exceptions près, on a $\mu_N = \mu_L$ et $Q_{N/L} = 1$ pour $N \in \mathcal{E}$.*

Donnons pour terminer ce paragraphe quelques notations relatives aux discriminants des corps et des réseaux. Étant donné $\theta \in K$, nous notons $d_{K/K'}(\theta)$ le discriminant de $\{1, \theta, \dots, \theta^{m-1}\}$ dans K/K' , et $\mathfrak{d}_{K/K'}$ désigne le discriminant relatif de K/K' , idéal entier de K' . Si $K = \mathbb{Q}$, on écrit simplement $d_K(\theta)$ au lieu de $d_{K/\mathbb{Q}}(\theta)$; on a alors $\mathfrak{d}_{K/\mathbb{Q}} = (d_K)$.

Soit Λ un réseau relatif de dimension q d'un espace euclidien. On définit le *discriminant* $\Delta(\Lambda)$ de Λ comme la valeur absolue du déterminant d'une base de Λ dans une base orthonormée du sous-espace qu'il engendre. On note $\|\Lambda\|$ (*la norme de* Λ) la norme d'un vecteur minimal de Λ , et l'on pose $\gamma_q(\Lambda) = \|\Lambda\|^2 \Delta(\Lambda)^{-2/q}$ et $\gamma_q = \text{Sup } \gamma_q(\Lambda)$; γ_q est *la constante d'Hermite*.

3.— Régulateurs et réseaux des logarithmes.

On munit \mathbb{R}^S de sa structure euclidienne canonique. Les régulateurs R_K et $R_{K'}$ s'expriment en fonction des discriminants des réseaux $\mathcal{L}(E_K)$ et $\mathcal{L}(E_{K'})$:

$$3.1.— \text{PROPOSITION. } \Delta(\mathcal{L}(E_{K'}))^2 = m^{r'} n' 2^{-r'_2} R_{K'}^2.$$

Démonstration : Le sous-espace $\mathbb{R}\mathcal{L}(E_{K'})$ de \mathbb{R}^S engendré par $\mathcal{L}(E_{K'})$ est défini par les relations $x_\sigma = x_\tau$ si σ et τ sont au-dessus d'un même plongement ou de 2 plongements imaginaires conjugués de K' , et $\sum_\sigma x_\sigma = 0$.

Posons, pour $\sigma' \in \tilde{S}'$, $e_{\sigma'} = \frac{1}{2} \sum_{\tau \mid \sigma'} (e_\tau + e_{\bar{\tau}})$, et soit $\sigma'_0 \in \tilde{S}'$. Les r' vecteurs $(e'_{\sigma'}, -e'_{\sigma'_0})$, $\sigma' \in \tilde{S}' - \{\sigma'_0\}$ constituent une base de $\mathbb{R}\mathcal{L}(E_{K'})$ et $\mathcal{L}(E_{K'})$ est l'ensemble des vecteurs

$$\mathcal{L}(\epsilon') = \sum_{\sigma' \in S' - \{\sigma'_0\}} i_{\sigma'} \log |\sigma' \epsilon'| \cdot (e'_{\sigma'}, -e'_{\sigma'_0}),$$

$\epsilon' \in E_{K'}$. On a donc $\Delta(\mathcal{L}(E_{K'})) = R_{K'} \cdot \delta$, où δ est le déterminant de la base $(e'_{\sigma'}, -e'_{\sigma'_0})$ dans une base orthonormée de $\mathbb{R}\mathcal{L}(E_{K'})$ et vérifie donc

$\delta^2 = \det_{(\sigma', \tau')} [(e'_{\sigma'}, -e'_{\sigma'_0}) \cdot (e'_{\tau'}, -e'_{\sigma'_0})]$; un calcul immédiat montre que $(e'_{\sigma'}, -e'_{\sigma'_0})$ est égal à $\frac{m}{i_{\sigma'_0}} + \frac{m}{i_{\sigma'}} \text{ si } \tau' = \sigma' \text{ et à } \frac{m}{i_{\sigma'_0}}$ sinon. Par conséquent

δ^2 est le déterminant de la matrice carrée d'ordre r' dont les termes diagonaux sont $x_0 + x_1, \dots, x_0 + x_{r'}$, et les autres termes x_0 , où l'on a posé $x_0 = \frac{m}{i_{\sigma'_0}}$ et

$x_i = \frac{m}{i_{\sigma'}}$ après avoir indexé les places σ' par l'ensemble $1, 2, \dots, r'$. Or on montre facilement :

3.2.—LEMME (Remak). *Le déterminant d'une telle matrice est égal à*

$$\sum_{i=0}^{i=r'} \prod_{j \neq i} x_j.$$

On en tire $\delta^2 = m^{r'} \frac{\sum_{\sigma'} i_{\sigma'}}{\prod_{\sigma'} i_{\sigma'}} = m^{r'} \cdot n' \cdot 2^{-r'_2}$, ce qui achève la

démonstration de 3.1.

En appliquant 3.1 au cas où $K' = K$, on trouve :

3.3.—COROLLAIRE. $\Delta(\mathcal{L}(E_K))^2 = n \cdot 2^{-r_2} \cdot R_K^2$.

Pour interpréter le quotient $R_K/R_{K'}$, on remarque maintenant que, étant donnés un réseau relatif Λ et un sous-groupe Λ' de Λ , on a l'égalité immédiate $\Delta(\Lambda')^{-1}\Delta(\Lambda) = Q(\Lambda, \Lambda')^{-1}\Delta(p(\Lambda))$, $Q(\Lambda, \Lambda')$ désignant l'ordre du sous-groupe de torsion de Λ/Λ' et p la projection orthogonale sur le supplémentaire orthogonal de $\mathbb{R}\Lambda'$ dans $\mathbb{R}\Lambda$. En utilisant 2.1, 3.1 et 3.3, on obtient l'énoncé suivant :

3.4.— THEOREME. *Soit p la projection orthogonale dans $\mathbb{R}\mathcal{L}(E_K)$ sur le supplémentaire orthogonal de $\mathbb{R}\mathcal{L}(E_{K'})$. On a :*

$$\Delta(p(\mathcal{L}(E_K))) = (m^{r'-1} 2^{r_2-r'_2})^{-\frac{1}{2}} \cdot R_{K/K'}.$$

4.— La méthode de Remak.

On considère ici encore une extension K/K' de corps de nombres.

Soit σ' un plongement de K' dans \mathbb{C} , et soit $\theta \in K^*$. Nous ordonnons les conjugués $\theta_i = \theta_{i, \sigma'}$ de θ au-dessus de σ' de façon que l'on ait $|\theta_1| \leq |\theta_2| \leq \dots \leq |\theta_m|$, $\theta_{i, \sigma'} = \overline{\theta_{i, \tau'}}$ si $\sigma' = \tau'$ et que deux θ_i imaginaires conjugués soient obtenus pour un couple d'indices consécutifs lorsque σ' est réel. On pose

$$4.1. \quad \Delta_{\sigma'}(\theta) = \prod_{i < j} (\theta_j - \theta_i).$$

On a donc l'égalité $\Delta_{\sigma'}(\theta)^2 = d_{\sigma K/\sigma' K'}(\theta)$, où σ désigne un prolongement à K de σ' . L'idée fondamentale de Remak consiste à écrire

$$4.2. \quad \Delta_{\sigma'}(\theta) = \prod_{i < j} \left(1 - \frac{\theta_i}{\theta_j}\right) \prod_{k=1}^m \theta_k^{k-1}$$

et à majorer le produit

4.3.

$$M_{\sigma'}(\theta) = \prod_{i < j} \left| 1 - \frac{\theta_i}{\theta_j} \right|^2$$

qui ne dépend que de θ et de σ' .

Soient z_1, z_2, \dots, z_m des nombres complexes non nuls tels que $|z_1| \leq |z_2| \leq \dots \leq |z_m|$; on a évidemment $\prod_{i < j} \left| 1 - \frac{z_i}{z_j} \right|^2 \leq 2^{m(m-1)}$, ce qui permet de définir

4.4

$$M_m = \sup \prod_{i < j} \left| 1 - \frac{z_i}{z_j} \right|^2,$$

la borne supérieure étant prise sur l'ensemble des suites z_1, \dots, z_m ainsi ordonnées. Plus généralement, à chaque décomposition $m = u_1 + 2u_2$, on associe la constante M_{u_1, u_2} définie en se limitant aux suites (z_1, \dots, z_m) comportant u_1 nombres réels et u_2 couples de nombres complexes conjugués (z_i, z_{i+1}) . On a évidemment

4.5.

$$M_{u_1, u_2} \leq M_m$$

et Remak ([13], p. 253; cf. § 9) montre l'inégalité

4.6.

$$M_m \leq m^m.$$

En posant

4.7.

$$M(\theta) = \prod_{\sigma' \in S'} M_{\sigma'}(\theta),$$

on obtient l'égalité $\left| \prod_{\sigma'} \Delta_{\sigma'}(\theta) \right|^2 = M(\theta) \prod_{i, \sigma'} |\theta_{i, \sigma'}|^{2(i-1)}$

d'où l'on déduit

4.8.— PROPOSITION. $|N_{K'/\mathbb{Q}}(d_{K/K'}(\theta))| = M(\theta) \prod_{i, \sigma'} |\theta_{i, \sigma'}|^{2(i-1)}$.

En utilisant les constantes $M_{r_1(\sigma'), r_2(\sigma')}$, on obtient tout de suite des majorations de $M(\theta)$ en fonction seulement de la ramification à l'infini dans K/K' et K'/\mathbb{Q} (on a par exemple $M(\theta) \leq m^n$, cf. § 9).

4.9.— Notation : On note M un majorant de $M(\theta)$ ne dépendant que de la ramification à l'infini dans K/K' et K'/\mathbb{Q} .

4.10.— PROPOSITION. Soit θ un entier primitif de K/K' . Alors :

$$N_{K'/\mathbb{Q}}(\mathfrak{d}_{K/K'}) \leq M \prod_{i, \sigma'} |\theta_{i, \sigma'}|^{2(i-1)}$$

En effet, on a $N_{K'/\mathbb{Q}}(\mathfrak{d}_{K/K'}) \leq |N_{K'/\mathbb{Q}}(d_{K/K'}(\theta))|$.

La méthode de Remak consiste alors à interpréter, lorsque θ est une unité primitive de K/K' , le logarithme du second membre de ces relations comme le produit scalaire du vecteur projection $p(\mathcal{L}(\theta))$ avec un vecteur de \mathbb{R}^s , ce qui permet de le majorer, par des méthodes de géométrie des nombres, en fonction du discriminant $\Delta(p(\mathcal{L}(E_K)))$, donc du régulateur relatif $R_{K/K'}$ (cf. 3.4). C'est l'objet du paragraphe 5 ci-dessous.

5.— Minorations des régulateurs.

Nous écartons désormais le cas trivial où $r = r'$ (i.e., $K = K'$ ou K/K' de type C.M., cf. 5.12). Soit ϵ une unité de K . On écrit les plongements $\sigma \in S$ sous forme de couples (i, σ') , avec $\sigma' \in S'$ et $1 \leq i \leq m$, tels que $|\epsilon_{i, \sigma'}| \leq |\epsilon_{i+1, \sigma'}|$ pour $i < m$, et vérifiant en outre les conventions du début du paragraphe 4.

5.1.— Notations. On pose $v(\epsilon) = \sum_{i, \sigma'} (i-1)e_{i, \sigma'}$, et l'on note $w(\epsilon)$ la projection de $v(\epsilon)$ sur $\mathbb{R}\mathcal{L}(E_K)$.

Dans l'égalité $\text{Log}(\prod_{i, \sigma'} |\epsilon_{i, \sigma'}|^{i-1}) = v(\epsilon) \cdot \mathcal{L}(\epsilon)$ (produit scalaire dans \mathbb{R}^S), on peut, puisque $\mathcal{L}(\epsilon) \in \mathbb{R} \mathcal{L}(E_K)$, remplacer $v(\epsilon)$ par $w(\epsilon)$. Comme $v(\epsilon)$ (et donc aussi $w(\epsilon)$) est orthogonal à $\mathbb{R} \mathcal{L}(E_{K'})$, on a

$$\text{Log}(\prod_{i, \sigma'} |\epsilon_{i, \sigma'}|^{i-1}) = v(\epsilon) \cdot \mathcal{L}(\epsilon) = w(\epsilon) \cdot \mathcal{L}(\epsilon) = w(\epsilon) \cdot p(\mathcal{L}(\epsilon)),$$

où p désigne toujours la projection orthogonale parallèlement à $\mathbb{R} \mathcal{L}(E_{K'})$. La proposition suivante est alors immédiate :

5.2.— PROPOSITION.

- (i) On a $\text{Log}(\prod_{i, \sigma'} |\epsilon_{i, \sigma'}|^{i-1}) = w(\epsilon) \cdot p(\mathcal{L}(\epsilon))$;
- (ii) Posons $a_i = i - \frac{m+1}{2}$; la composante de $w(\epsilon)$ sur $e_{i, \sigma'}$ est égale à a_i si (i, σ') est réel ou si σ' est imaginaire, et à $\frac{a_i + a_{i+1}}{2} = i - \frac{m}{2}$ si (i, σ') et $(i+1, \sigma')$ sont imaginaires conjugués;
- (iii) On a $\|w(\epsilon)\|^2 = \frac{n(m^2-1)}{12} - \frac{\rho}{2}$.

5.3.— Remarque. Lorsque ϵ parcourt E_K , les composantes de $w(\epsilon)$ au-dessus de chaque $\sigma' \in S'$ sont permutées; le vecteur $w(\epsilon)$ parcourt donc un sous-ensemble fini W de \mathbb{R}^n qui, une fois K' fixé, ne dépend que de la ramification dans K des places réelles de K' .

5.4.— Notation. On note $\varphi(\epsilon) \in [0, \pi]$ l'angle des vecteurs $w(\epsilon)$ et $p(\mathcal{L}(\epsilon))$ lorsque $p(\mathcal{L}(\epsilon)) \neq 0$.

5.5.— PROPOSITION. Soit $\epsilon \in E_K$ telle que $p(\mathcal{L}(\epsilon)) \neq 0$. Alors $\cos \varphi(\epsilon) > 0$.

Démonstration : Il s'agit de montrer l'inégalité $\prod_{i=1}^m x_i^{i-1} > 1$ dans laquelle on a posé $x_i = \prod_{\sigma'} |\epsilon_{i, \sigma'}|$; on a $x_i \leq x_{i+1}$, l'égalité n'ayant lieu que si l'on a $|\epsilon_{i+1, \sigma'}| = |\epsilon_{i, \sigma'}|$ pour tout $\sigma' \in S'$. Ecrivons

$\prod x_i^{i-1} = (x_2 \dots x_m)(x_3 \dots x_m) \dots (x_{m-1} x_m)x_m$; compte tenu de la relation $\prod_i x_i = 1$ et des inégalités $x_i \leq x_{i+1}$, chaque facteur $(x_j \dots x_m)$ est ≤ 1 , d'où $\prod x_i^{i-1} \geq 1$, l'égalité n'étant possible que si tous les x_i sont égaux à 1; mais alors $|\epsilon_{i,\sigma'}|$ ne dépend pas de i , quel que soit σ' , de sorte que $\mathcal{L}(\epsilon)$ appartient à $\mathbb{R}\mathcal{L}(E_K)$, C.Q.F.D.

Désormais, nous supposons que ϵ engendre K sur K' . Il en résulte en particulier que $p(\mathcal{L}(\epsilon))$ est un vecteur non nul du réseau $p(\mathcal{L}(E_K))$, réseau de dimension $r - r' > 0$. On a donc, par définition même de la constante d'Hermite :

$$\left\| p(\mathcal{L}(\epsilon)) \right\| = \frac{\left\| p(\mathcal{L}(\epsilon)) \right\|}{\left\| p(\mathcal{L}(E_K)) \right\|} \cdot \gamma_{r-r'}(p(\mathcal{L}(E_K)))^{\frac{1}{2}} \cdot \Delta(p(\mathcal{L}(E_K)))^{1/(r-r')}.$$

En appliquant maintenant le théorème 3.4 et les propositions 4.8 et 5.2 (i) et (iii), on obtient la *formule explicite* suivante, dans laquelle $R_{K/K'}$ (le régulateur relatif) est défini en 2.1 :

5.6.—THEOREME. Soit ϵ une unité de K qui engendre K sur K' . Alors on a :

$$R_{K/K'} = \frac{1}{C} \left(\log \frac{|N_{K'}/\mathbb{Q}(d_{K/K'}(\epsilon))|}{M(\epsilon)} \right)^{r-r'} \cdot \left(\frac{\gamma_{r-r'}}{\gamma_{r-r'}(p(\mathcal{L}(E_K)))} \right)^{(r-r')/2} \cdot \left(\frac{\left\| p(\mathcal{L}(\epsilon)) \right\|}{\left\| p(\mathcal{L}(E_K)) \right\|} \right)^{-(r-r')} \cdot \frac{1}{\cos^{r-r'} \varphi(\epsilon)}$$

où la constante C , qui ne dépend que des signatures de K et de K' (on a $\rho = r_2 - mr'_2$), est définie par :

$$C = \left[\left(\frac{n(m^2-1)}{3} - 2\rho \right) \gamma_{r-r'} \right]^{(r-r')/2} \cdot m^{-(r'-1)/2} \cdot 2^{-(r_2 - r'_2)/2}.$$

Lorsque $K' = \mathbb{Q}$, on obtient :

5.7.— COROLLAIRE. Soit ϵ une unité primitive de K . Alors :

$$R_K = \frac{1}{C} \cdot \left(\log \frac{|d_{K/\mathbb{Q}}(\epsilon)|}{M(\epsilon)} \right)^r \cdot \left(\frac{\gamma_r}{\gamma_r(\mathcal{L}(\epsilon))} \right)^{r/2} \cdot \left(\frac{\|\mathcal{L}(\epsilon)\|}{\|\mathcal{L}(E_K)\|} \right)^{-r} \cdot \frac{1}{\cos^r \varphi(\epsilon)},$$

où C , qui ne dépend que de la signature de K , est définie par :

$$C = \left[\left(\frac{n(n^2-1)}{3} - 2r_2 \right) \gamma_r \right]^{r/2} \cdot n^{\frac{1}{2}} \cdot 2^{-r_2/2}.$$

En choisissant $p(\mathcal{L}(\epsilon))$ minimal (si $r - r' > 0$), nous obtenons les minorations suivantes, dans lesquelles figure la constante M introduite en 4.9 :

5.8.— THEOREME. Soit K une extension primitive de K' (ou d'une extension quadratique totalement imaginaire de K' lorsque K' est totalement réel). Alors, pourvu que le discriminant relatif ait une norme $> M$, on a :

$$R_{K/K'} \geq \frac{1}{C} \cdot \left(\log \frac{N_{K'/\mathbb{Q}}(\mathfrak{d}_{K/K'})}{M} \right)^{r-r'} \quad (C \text{ est défini en 5.6}).$$

5.9.— COROLLAIRE. Soit K un corps de nombres ne contenant pas d'autre sous-corps que \mathbb{Q} ou un corps quadratique imaginaire, et dont le discriminant soit en valeur absolue $> M$. On a :

$$R_K \geq \frac{1}{C} \cdot \left(\log \frac{|d_K|}{M} \right)^r \quad (\text{où } C \text{ est donné par 5.7}).$$

Ce corollaire rend compte de la minoration de Remak ([13]) à cela près que Remak remplace la constante d'Hermite γ_r par une majoration due à Blichfeldt.

Démonstration de 5.8 : Lorsque $r = r'$, les deux membres de l'inégalité sont égaux (à 1 ou $2^{n'-1}$ selon que $K = K'$ ou que K/K' est de type C.M.) ; nous nous limitons donc désormais au cas $r - r' > 0$, et nous choisissons $\epsilon \in E_K$ telle que $p(\mathcal{L}(\epsilon)) \neq 0$. Cette unité vérifie les hypothèses de 5.6; en outre l'idéal $\mathfrak{d}_{K/K'}$ divise $d_{K/K'}(\epsilon)$, qui est non nul vues les hypothèses faites sur K/K' et sur ϵ . Compte tenu du choix de M , on a donc

$$5.10. \quad \text{Log} \frac{|N_{K'}/\mathbb{Q}(d_{K/K'}(\epsilon))|}{M(\epsilon)} \geq \text{Log} \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'})}{M} > 0$$

d'où, par 5.6, l'inégalité

$$5.11. \quad R_{K/K'} \geq \frac{1}{C} \cdot \left(\text{Log} \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'})}{M} \right)^{r-r'} \cdot \left(\frac{\gamma_{r-r'}}{\gamma_{r-r'}(p(\mathcal{L}(E_K)))} \right)^{(r-r')/2} \cdot \\ \sup_{p(\mathcal{L}(\epsilon)) \neq 0} \left(\frac{\|p(\mathcal{L}(\epsilon))\|}{\|p(\mathcal{L}(E_K))\|} \cos \varphi(\epsilon) \right)^{-(r-r')}.$$

Le second membre de 5.11 est un produit de 4 facteurs. Le troisième, qui ne dépend que de la classe de similitude du réseau $p(\mathcal{L}(E_K))$, est ≥ 1 , avec égalité si et seulement si ce réseau est critique. Le quatrième, qui dépend en outre de la position du réseau, est minoré par 1, comme on le voit en choisissant ϵ telle que $p(\mathcal{L}(\epsilon))$ soit un vecteur minimal de $p(\mathcal{L}(E_K))$, C.Q.F.D.

(Nous verrons au paragraphe 6 comment on peut dans certains cas améliorer la minoration de ce 4ème facteur).

Concluons ce paragraphe par quelques remarques sur les signatures de K et K' correspondant à une dimension $d = r - r'$ donnée. Des relations $r - r' = (m-1)(r'_1 + r'_2) - \rho$ et $\rho = (mr'_1 - r_1)/2 \leq mr'_1/2$ on déduit l'inégalité

$$5.12. \quad \left(\frac{m}{2} - 1 \right) r'_1 + (m-1)r'_2 \leq r - r' (= d).$$

On voit donc que si l'on excepte la possibilité $K = K'$ si $d = 0$ et un nombre fini de signatures pour K et K' avec $m = [K:K'] > 2$, il reste une famille infinie d'extensions quadratiques K/K' où K' est un corps dont la signature (r'_1, r'_2) est soumise aux seules conditions $r'_2 \leq d$ et $r'_1 \geq d - r'_2$; la signature de K est alors déterminée par la relation $\rho = r'_1 + r'_2 - d$, qui entraîne $r_1 = 2(d - r'_2)$ et $r_2 = r'_1 + 3r'_2 - d$ (pour $d = 0$, on trouve bien $K = K'$, ou $r'_2 = 0$ et $r_1 = 0$, i.e. K/K' de type C.M.).

6.— Une amélioration des minorations des régulateurs.

La méthode consiste à minorer la borne supérieure de l'expression $\left[\frac{\|p(\mathcal{L}(\epsilon))\|}{\|p(\mathcal{L}(E_K))\|} \cos(\varphi(\epsilon)) \right]^{-1}$, qui intervient dans 5.11, par le minimum des valeurs

qu'elle prend sur les $(r-r')$ minima successifs du réseau $p(\mathcal{L}(E_K))$. On a vu en 5.3 que les $w(\epsilon)$ décrivent un ensemble W fini de vecteurs, ensemble qui ne dépend que des places à l'infini de K et de K' . En tenant compte du troisième facteur du second membre de 5.11, on est ramené au problème suivant de géométrie des nombres. Soit V un espace euclidien de dimension $d > 0$, et soit $\mathcal{V} = (v_1, \dots, v_d)$ un système de d vecteurs de V de même norme non nulle. A tout réseau Λ de V , de minima successifs $\mu_1 \leq \mu_2 \leq \dots \leq \mu_d$, on associe la fonction

$$6.1. \quad f_{\mathcal{V}}(\Lambda) = \frac{\gamma_d(\Lambda)}{\gamma_d} \min_{i, x_i} \frac{\mu_i^2}{\mu_1^2} \cos^2(v_i, x_i),$$

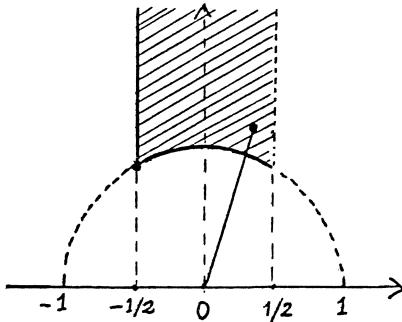
où les vecteurs x_i sont tels que $\|x_i\| = \mu_i$; on a $f_{\mathcal{V}}(\Lambda) \leq 1$. Le problème consiste à déterminer $A_{\mathcal{V}} = \sup_{\Lambda} f_{\mathcal{V}}(\Lambda)$, qui ne dépend que des angles mutuels des vecteurs de \mathcal{V} .

En revenant au problème initial, on appliquera ce qui précède au réseau $\Lambda = p(\mathcal{L}(E_K))$ ($d = r-r'$), en considérant le maximum A de $A_{\mathcal{V}}$ lorsque \mathcal{V} parcourt tous les systèmes de d vecteurs extraits de W . On pourra alors dans l'inégalité du th. 5.9 remplacer la constante $\frac{1}{C}$ par $\frac{1}{C} \cdot A^{-(r-r')/2} \geq \frac{1}{C}$.

Lorsque $d = 1$, on a $f_{\mathcal{V}}(\Lambda) = 1$ quels que soient Λ et \mathcal{V} , et l'on ne peut rien améliorer. La fin de ce paragraphe est consacrée à l'étude de la dimension 2.

Les réseaux Λ de dimension 2 d'un plan euclidien orienté P sont classés à similitude directe près par le point (λ, θ) du domaine dessiné ci-dessous, où $\theta = (x, x')$ et $\lambda = \frac{\|x'\|}{\|x\|}$, x désignant un vecteur minimal de Λ et x' un

vecteur de norme minimale parmi les vecteurs de Λ indépendants de x . On se donne un système $\mathcal{V} = (v, v')$ de deux vecteurs non nuls de même norme dans



P , et l'on pose $\alpha = (v, v') \bmod. 2\pi$. On repère la position de Λ dans P par $\varphi = (v, x)$; en posant $\varphi' = (v', x')$, on a la relation $\varphi' = \varphi + \theta - \alpha$. La fonction $f_{\mathcal{V}}$ sera notée $f_{\mathcal{V}, \alpha}$; elle s'écrit :

$$6.2. \quad f_{\mathcal{V}, \alpha}(\Lambda) = \frac{\gamma_2(\Lambda)}{\gamma_2} \min_{x, x'} (\cos^2 \varphi, \lambda^2 \cos^2 \varphi').$$

On a $f_{\mathcal{V}, \alpha} = f_{\mathcal{V}, \alpha + \pi}$, et l'on se borne au cas où $-\frac{\pi}{2} \leq \alpha \leq \frac{\pi}{2}$. En changeant (x, x') en $(-x, -x')$, on change φ en $\varphi + \pi$ et φ' en $\varphi' + \pi$, et l'on peut supposer que $\varphi \in [-\frac{\pi}{2}, +\frac{\pi}{2}]$.

Sur la classe de similitude d'un réseau Λ donné, $f_{\mathcal{V}, \alpha}(\Lambda)$ est une fonction de φ , dont la borne supérieure est atteinte :

- Lorsque $\lambda |\cos(\theta - \alpha)| \geq 1$, pour $\varphi = 0$, et elle vaut alors $\gamma_2(\Lambda)/\gamma_2$;
- Lorsque $\lambda |\cos(\theta - \alpha)| < 1$, pour un angle φ tel que $\cos \varphi = \lambda |\cos(\varphi + \theta - \alpha)|$, c'est-à-dire $\varphi = \text{Arctg} \frac{\cos(\theta - \alpha) + 1/\lambda}{\sin(\theta - \alpha)}$, et elle vaut alors $\frac{\gamma_2(\Lambda)}{\gamma_2} \cdot \frac{\lambda^2 \sin^2(\theta - \alpha)}{\lambda^2 + 1 - 2\lambda |\cos(\theta - \alpha)|}$.

(Cela se voit en observant que la fonction $f_{\mathcal{V}, \alpha}(\Lambda)$ ne peut être maximum que si $\cos^2 \varphi = 1$ ou $\lambda^2 \cos^2 \varphi' = 1$ ou $\cos^2 \varphi = \lambda^2 \cos^2 \varphi'$.)

Pour obtenir $\sup_{\Lambda} f_{\gamma, \alpha}(\Lambda)$, il est plus commode d'étudier la fonction $f_{\gamma, \alpha}$ pour θ et φ fixés.

Pour $\cos^2 \varphi \leq \lambda^2 \cos^2 \varphi'$, on a $f_{\gamma, \alpha}(\Lambda) = \frac{1}{\gamma_2} \frac{\cos^2 \varphi}{\lambda \sin \theta}$, fonction décroissante de λ , de maximum

$$\frac{1}{\gamma_2} \cdot \frac{\cos^2 \varphi}{\sin \theta \operatorname{Max}\left(1, \frac{\cos \varphi}{|\cos \varphi'|}\right)} .$$

Au contraire, pour $\cos^2 \varphi \geq \lambda^2 \cos^2 \varphi'$, on a $f_{\gamma, \alpha}(\Lambda) = \frac{1}{\gamma_2} \frac{\lambda \cos^2 \varphi'}{\sin \theta}$, fonction croissante de λ , majorée par $\frac{1}{\gamma_2} \cdot \frac{\cos \varphi |\cos \varphi'|}{\sin \theta}$.

Pour $\cos \varphi \geq |\cos \varphi'|$, on a $f_{\gamma, \alpha}(\Lambda) \leq \frac{1}{\gamma_2} \frac{\cos \varphi |\cos \varphi'|}{\sin \theta}$; pour $\cos \varphi \leq |\cos \varphi'|$, on a

$$f_{\gamma, \alpha}(\Lambda) \leq \frac{1}{\gamma_2} \frac{\cos^2 \varphi}{\sin \theta} \leq \frac{1}{\gamma_2} \frac{\cos \varphi |\cos \varphi'|}{\sin \theta} .$$

Dans tous les cas, on a

$$f_{\gamma, \alpha}(\Lambda) \leq \frac{1}{\gamma_2} \frac{\cos \varphi |\cos \varphi'|}{\sin \theta} = \frac{1}{\gamma_2} \frac{|\cos(2\varphi + \theta - \alpha) + \cos(\theta - \alpha)|}{2 \sin \theta} ,$$

fonction de φ qui est un maximum relatif si et seulement si l'on a $2\varphi + \theta - \alpha \equiv 0 \pmod{\pi}$. En effectuant sur Λ la symétrie $\theta \mapsto \pi - \theta$, et en changeant α en $-\alpha$, on peut supposer $\cos(\theta - \alpha) \geq 0$; on a alors $f_{\gamma, \alpha}(\Lambda) \leq \frac{1}{\gamma_2} \frac{1 + \cos(\theta - \alpha)}{2 \sin \theta}$, majorant atteint sur le réseau de rapport λ égal à 1 et de même angle θ que Λ , et pour lequel $\varphi' \equiv -\varphi \equiv \frac{\theta - \alpha}{2} \pmod{\pi}$. Nous avons donc démontré :

6.3.— PROPOSITION. *Sur l'ensemble des réseaux d'angle θ donné, le maximum de f est égal à $\frac{1}{\gamma_2} \frac{1+|\cos(\theta-\alpha)|}{2 \sin \theta}$, et est atteint sur les réseaux engendrés par deux vecteurs de même norme, les valeurs de φ et φ' correspondantes étant*

$$\varphi' \equiv -\varphi \equiv \frac{\theta-\alpha}{2} \text{ ou } \frac{\pi}{2} - \frac{\theta-\alpha}{2} \bmod. \pi$$

selon que $\cos(\theta-\alpha)$ est ≥ 0 ou ≤ 0 .

En étudiant la fonction $\theta \mapsto \frac{1+\cos(\theta-\alpha)}{2 \sin \theta}$ dans le domaine défini par les inégalités $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$ et $\cos(\theta-\alpha) \geq 0$, on montre :

6.4.— PROPOSITION. *Le maximum de $f_{\gamma, \alpha}$ est égal à $\cos^2\left(\frac{\pi}{6} - \frac{|\alpha|}{2}\right)$, atteint uniquement sur les réseaux critiques (réseaux hexagonaux) tels que $\varphi = \frac{\Pi}{6} - \frac{|\alpha|}{2}$ (en fonction de $t = \cos \alpha$, ce maximum vaut $\frac{2+t+\sqrt{3(1-t^2)}}{4}$; t est ≥ 0 , car $\alpha \in [-\frac{\pi}{2}, +\frac{\pi}{2}]$).*

Nous appliquons maintenant la Proposition 6.4 aux minorations du régulateur des extensions K primitives d'un corps K' donné, pour lesquelles $r-r'=2$. La discussion de la fin du paragraphe 5 montre que l'on a ou bien $m=2$, et $r'_2=0,1$ ou 2 (on a alors 3 familles infinies de signatures pour K' paramétrées par $r'_1 \geq 2-r'_2$), ou bien K est une extension cubique de \mathbb{Q} , d'un corps quadratique réel ou imaginaire, ou bien K est une extension quartique de \mathbb{Q} ou d'un corps quadratique réel, ou bien enfin K est une extension de \mathbb{Q} de degré 5 ou 6. La correction est égale à 1 si $m=3$ (les 3 cas) ou si $K'=\mathbb{Q}$ et $m=4$ ou 6. Dans les autres cas, elle est non triviale :

6.5.— THEOREME. *Les notations et hypothèses étant celles du théorème 5.8, et en supposant $r-r'=2$, on a :*

$$R_{K/K'} \geq \frac{1}{AC} \left(\log \frac{N_{K'/\mathbb{Q}} (\mathfrak{d}_{K/K'})}{M} \right)^2, \text{ où}$$

$C = \frac{2}{\sqrt{3}} \left[\frac{n(m^2-1)}{3} - 2\rho \right] m^{-(r'-1)/2} 2^{-(r_2-r'_2)/2}$ et A est donné par les règles suivantes :

(i) Si $m = 2$ et $r'_2 = 0$ ou 2, ou si K est une extension quartique totalement imaginaire d'un corps quadratique réel,

$$A = \frac{2+\sqrt{3}}{4} < 0,934 ;$$

$$(ii) Si m = 2 et r'_2 = 1, A = \frac{7+\sqrt{24}}{12} < 0,992 ;$$

(iii) Si K est un corps de degré 5 à 1 place réelle,

$$A = \frac{89+\sqrt{3021}}{144} < 0,9998$$

(on doit toujours supposer $N_{K'}/\mathbb{Q}^{(\mathfrak{d}_{K/K'})} > M$).

Démonstration : On explicite toutes les valeurs possibles de $|\cos \alpha|$ en utilisant la description des vecteurs $w(\epsilon)$ a priori possibles qui figure au début du paragraphe 5.

7.— Réseaux extrêmes pour un groupe d'automorphismes (énoncés de résultats).

On conserve les notations des paragraphes précédents. Tout automorphisme σ de l'extension K/K' induit une isométrie σ sur chacun des réseaux $\mathcal{L}(E_K)$ et $p(\mathcal{L}(E_K))$ qui respecte les invariants que nous avons introduits (par exemple, $w(\sigma\epsilon) = \sigma w(\epsilon), \dots$). L'existence d'un tel automorphisme permet éventuellement d'améliorer la minoration $\frac{\gamma_{r-r'}}{\gamma_{r-r'}(p(\mathcal{L}(E_k)))} \geq 1$. Cette raison nous a amenés à considérer la généralisation suivante de la notion de réseau extrême introduite par Korkine et Zolotareff :

7.1.— DEFINITION. Soit V un espace euclidien de dimension $d > 0$, soit G un sous-groupe fini du groupe orthogonal $O(V)$, soit R_G l'ensemble des réseaux de V stables par G , et soit \mathcal{S}_G l'ensemble des endomorphismes symétriques de V qui commutent avec chaque élément de G . On dit qu'un réseau $\Lambda \in R_G$ est G -extreme s'il existe $\alpha > 0$ tel que " $u \in \mathcal{S}_G$ et $\|u - id\| < \alpha$ " entraîne " $\gamma_d(u(\Lambda)) \leq \gamma_d(\Lambda)$ ".

Il est clair que les réseaux $\Lambda \in R_G$ en lesquels la fonction γ_d est maximum sont G -extrêmes, et que, lorsque G est réduit à $\{\pm id\}$, on retrouve la notion classique de Korkine et Zolotareff. On peut (comme chez Voronoï) introduire des notions de réseaux G -parfaits et G -eutactiques, et démontrer que G -extreme équivaut à G -parfait et G -eutactique; cela se fait en généralisant le procédé de Barnes ([1]). Les réseaux G -parfaits sont ceux pour lesquels les formes linéaires $w \mapsto x.w(x)$ engendrent le dual de l'espace vectoriel \mathcal{S}_G lorsque x parcourt l'ensemble des vecteurs minimaux du réseau.

7.2.— THEOREME (cf. [3]). *Si Λ est G -parfait, le nombre d'orbites de vecteurs minimaux de Λ sous l'action de $G \cup -G$ est $\geq \dim_R \mathcal{S}_G$.*

[Si $G \subset \{\pm id\}$, on trouve que le nombre de couples $\pm x$ de vecteurs minimaux de Λ est $\geq \frac{d(d+1)}{2}$, résultat dû à Korkine et Zolotareff.]

Nous donnons maintenant les résultats concernant le cas où G est cyclique irréductible sur \mathbb{Q} et d est ≤ 6 . Les notations sont celles de Coxeter–Barnes : A_n , D_n (souvent noté B_n) et E_n proviennent des systèmes de racines du même nom ; le réseau P_6 est défini dans [2] ; C_n désigne le réseau cubique; tous ces réseaux doivent être considérés à similitude près.

7.3.— THEOREME (cf. [3]). *Soit G un sous-groupe cyclique d'ordre q et \mathbb{Q} -irréductible du groupe orthogonal de V , avec $d = \dim V \leq 6$. Alors, $\dim \mathcal{S}_G = 1$ si $d = 1$ et $\frac{d}{2}$ si $d > 1$, et les réseaux vérifiant la condition du théorème 7.2 sont G -extrêmes et sont donnés par la liste suivante :*

- (i) $d = 1 : q = 1$ ou 2 et $\Lambda = A_1$;
- (ii) $d = 2 : q = 3$ ou 6 , et $\Lambda = A_2$, ou $q = 4$, et $\Lambda = C_2$;
- (iii) $d = 4 : q = 5$ ou 10 , et $\Lambda = A_4$, ou $q = 8$ ou 12 , et $\Lambda = D_4$;
- (iv) $d = 6 : q = 7$ ou 14 , et $\Lambda = A_6$ ou P_6 , et $q = 9$ ou 18 , et $\Lambda = E_6$ ou E_6^* (réseau dual de E_6).

On constate que ces réseaux, à l'exception de C_2 , sont extrêmes au sens usuel. Par ailleurs, les réseaux absolument extrêmes (dits *critiques*) en dimension 1,2,4 et 6 sont A_1 , A_2 , D_4 et E_6 . Ainsi, si $q = 5$ ou 7, on a $\gamma_d(\Lambda) < \gamma_d$ lorsque Λ est G -extrême, ce qui permet d'améliorer l'inégalité du paragraphe 5 : on a en effet $\gamma_4(A_4) = 2.5^{-\frac{1}{2}} = 1,337\dots < \gamma_4(D_4) = \sqrt{2}$, et $\gamma_6(A_6) = 2.7^{-1/6} = 1,446\dots < \gamma_6(P_6) = 4.7^{-\frac{1}{2}} = 1,511\dots < \gamma_6 = \gamma_6(E_6) = 2.3^{-1/6} = 1,665\dots$.

7.4.— COROLLAIRE. Soit K/K' une extension cyclique de degré $\ell = 5$ ou 7, K' étant le corps \mathbb{Q} ou un corps quadratique imaginaire. Alors, dans l'inégalité du théorème 5.10, on peut multiplier $\frac{1}{C}$ par $\frac{\sqrt{5}}{2} = 1,118\dots$ si $\ell = 5$ et par $\frac{7\sqrt{7}}{2^3\sqrt{3}} = 1,336\dots$ si $\ell = 7$.

7.5.— REMARQUE. La majoration $\gamma_4(L) \leq 2.5^{-1/4}$ pour un réseau L de dimension 4 muni d'un automorphisme irréductible d'ordre 5 a été trouvée indépendamment par Schoof et Washington ([14]).

Dans le cas des extensions cycliques de degré premier impair de \mathbb{Q} , les constantes C notées C_ℓ que nous donnons, même corrigées par le corollaire 7.4 lorsque $\ell = 5$ ou 7, sont moins bonnes au-delà de $\ell = 3$ que celles trouvées par G. et M.-N. Gras ([7]) en utilisant les unités cyclotomiques : ils montrent que l'on peut remplacer $C_\ell = \left(\frac{\ell(\ell^2-1)}{3}\gamma_{\ell-1}\right)^{(\ell-1)/2}\sqrt{\ell}$ par $C'_\ell = (2(\ell-1))^{\ell-1}$. On trouve $C_3 = C'_3 = 16$, mais $C'_5 = 2^{12} = 4096$ alors que $C_5 = 5200\sqrt{5} = 7155,41\dots$ par 5.7, et que 7.4 donne $C_5^* = 2^8 \cdot 5^2 = 6400$. Nous ignorons quels sont les termes de la formule explicite 5.7 qui sont responsables du remplacement de C_5^* par C'_5 . Notons que, si L est un réseau de norme 1 muni d'un automorphisme σ d'ordre 5 engendré par un vecteur minimal x et ses conjugués σx , $\sigma^2 x$ et $\sigma^3 x$, on a $\Delta(L) = \sqrt{5}(p + \frac{1}{4})$, où $p = (x \cdot \sigma x) \cdot (x \cdot \sigma^2 x) = (x \cdot \sigma x) \cdot (-\frac{1}{2} - x \cdot \sigma x)$ varie entre 0 (et alors, $L = A_4$) et $\frac{1}{16}$ (et alors, $\Delta(L) = \frac{5\sqrt{5}}{16}$). Le quotient $\frac{\Delta(L)}{\Delta(A_4)}$ varie entre 1 et $\frac{5}{4} < \frac{C_5^*}{C'_5} = (\frac{5}{4})^2$.

La constante C_3 est optimale (cf. 8.3). Nous ignorons si C_5 l'est; le seul exemple que nous connaissons de famille paramétrique d'unités (dû à E. Lehmer, [9]) majore $1/C$ par $\frac{71}{2^{16}} > \frac{1}{C_5^2} = \frac{1}{2^{12}}$.

8.— EXEMPLES.

Dans ce paragraphe, nous cherchons à tester la qualité de la constante C qui intervient dans le théorème 5.8. Le principe est, un corps K' étant donné, de chercher des extensions K de K' de ramification à l'infini donnée, à l'aide de polynômes de $\mathbb{Z}_{K'}[X]$ dépendant d'un paramètre $a \in \mathbb{N}$ qui définissent une unité ϵ , et dont le discriminant $D(a)$ tend vers l'infini avec a . Pour assurer que $N_{K'}/\mathbb{Q}(D(a))/N_{K'}/\mathbb{Q}(\mathfrak{d}_{K'/K'})$ soit à croissance assez lente, on n'a guère d'autre ressource que d'imposer l'égalité $(D(a)) = \mathfrak{d}_{K'/K'}$ en sélectionnant les polynômes pour lesquels $D(a)$ est sans facteur carré. C'est le cas (Erdős, [5]) pour une infinité d'entiers a lorsque $D(a)$ est de degré ≤ 3 sauf raison contraire évidente; cette restriction sur le degré est sans doute inutile, mais cela n'a jamais été démontré. En outre, lorsque $r - r'$ est ≥ 2 , on est le plus souvent réduit à chercher des unités indépendantes qui s'obtiennent par translation à partir de ϵ (cf. exemples ci-dessous); l'expérience prouve que ce procédé est trop restrictif en général pour fournir des familles de corps dont les réseaux des unités satisfassent simultanément aux conditions de forme et de position assurant l'optimalité de la constante C .

8.1.— Exemple. $r - r' = 1$. Les facteurs de la formule explicite 5.6 issus de la géométrie des nombres sont triviaux; il suffit donc de choisir une famille d'extensions K_a/K' avec une unité ϵ_a fondamentale modulo $E_{K'}$ et telle que $\text{Log}|N_{K'}/\mathbb{Q}(d_{K_a/K'}(\epsilon_a))|$ soit équivalent à $\text{Log}|N_{K'}/\mathbb{Q}(\mathfrak{d}_{K_a/K'})|$. C'est facile pour $K' = \mathbb{Q}$ et $n = 2$ (prendre par exemple $\epsilon_a = \frac{a+\sqrt{a^2+4}}{2}$). Pour $K' = \mathbb{Q}$ et $n = 3$, Cusik ([4], p. 73) considère la racine ϵ_a réelle de $x^3 - ax^2 - 1$, a entier ≥ -1 , de discriminant $-4a^3 - 27$. Dans ces deux cas, le discriminant du polynôme est sans facteur carré pour une infinité de valeurs de a , et la minoration 5.12 montre que ϵ_a est une unité fondamentale de K_a (on trouve en effet $\frac{|\text{Log}|\epsilon_a||}{R_K} < 2$, d'où $|\text{Log}|\epsilon_a|| = R_K$); les constantes C de 5.12 (respectivement égales à 2 et 3) sont donc optimales.

La théorie de Kummer permet de construire des familles de corps cubiques K_a de corps quadratique associé k fixé. Par exemple, pour $k = \mathbb{Q}(\sqrt{-3})$, on peut prendre $\epsilon_a = -a + \sqrt{a^3 + 1}$, et l'on vérifie (comme ci-dessus) que ϵ_a est une unité fondamentale de $K_a = \mathbb{Q}(\epsilon_a)$ pour tout entier $a \geq 1$ tel que $a^3 + 1$ soit sans facteur carré.

Les constantes C sont sans doute optimales dans bien d'autres situations telles que $r - r' = 1$ (corps quartiques imaginaires, extensions quadratiques de signature mixte d'un corps quadratique...), mais on se heurte au problème des facteurs carrés des valeurs des polynômes de degré ≥ 4 .

8.2.— Exemple. Corps imaginaire à groupe S_3 ($r - r' = 2$). On étudie des extensions K/K' de degré 3, où K est la clôture galoisienne d'un corps cubique L à une place réelle. Si ϵ est une unité fondamentale de L , un calcul assez facile montre que ϵ et $\sigma\epsilon$ (où σ est d'ordre 3 dans $\text{Gal}(K/\mathbb{Q})$) engendrent modulo torsion un sous-groupe E d'indice 1 ou 3 de E_K , et que, si l'indice est 3, $E_K/E_{K'}$ est engendré par ϵ et ϵ' telles que $\epsilon'^3 = \frac{\sigma\epsilon}{\epsilon}$. Les réseaux plans $\mathcal{L}(E)$ et $\mathcal{L}(E_K)$ admettent un automorphisme d'ordre 3 et sont donc hexagonaux (cf. § 7) ; on montre en fait que, dans le cas de l'indice 3, $\mathcal{L}(E_K)$ se déduit de $\mathcal{L}(E)$ par une similitude d'angle $\pi/6$ et de rapport $\frac{1}{\sqrt{3}}$; on a enfin $\varphi(\epsilon) = \pi/6$, et $\varphi(\epsilon') = 0$ dans le cas de l'indice 3. La formule explicite 5.6 donne

$$R_K(E) = \frac{1}{12} \left(\log \left| \frac{N_{K'}/\mathbb{Q}(\epsilon)}{M(\epsilon)} \right|^2 \right)^2 = \frac{1}{3} \left(\log \frac{d_L(\epsilon)}{\sqrt{M(\epsilon)}} \right)^2 = 3R_L^2,$$

d'où, si l'indice est 1, la minoration améliorée

$$R_K \geq \left(\log \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'})}{M} \right)^2, \text{ équivalente à } R_L \geq \frac{1}{6} \log \left| \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'})}{M} \right|;$$

lorsque l'indice est 3, la formule explicite 5.6 donne $R_K = \frac{1}{16} \left(\log \left| \frac{N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'}(\epsilon))}{M(\epsilon)} \right|^2 \right)^2$; la minoration de 5.8 avec $C = 16$ ne peut donc pas être améliorée par des considérations géométriques, et donne l'inégalité

$R_L \geq \frac{1}{4} \log \left| \frac{N_{K'}/\mathbb{Q}}{M} (\mathfrak{d}_{K/K'}) \right|$. La relation $N_{K'}/\mathbb{Q}(\mathfrak{d}_{K/K'}) = (d_L/d_{K'})^2$ montre que, pour une suite de corps cubiques L associés à un corps quadratique imaginaire K' fixé, avec $|d_L| \rightarrow +\infty$, le quotient $R_L/\log|d_L|$ est asymptotiquement minoré par $\frac{1}{3}$ si l'indice est 1 et $\frac{1}{2}$ si l'indice est 3. Dans ce dernier cas, on a asymptotiquement $R_L \sim \log|d_L(\epsilon)|$ et $R_L \geq \frac{1}{2} \log|d_L|$, d'où $|d_L(\epsilon)| \geq (1-o(1))|d_L|^{\frac{1}{2}}$ pour $|d_L| \rightarrow +\infty$. L'indice est donc toujours égal à 1 pour les corps $L = \mathbb{Q}(\sqrt[3]{a^3+1})$ considérés dans l'exemple 1 ($a^3 + 1$ sans facteur carré).

8.3.— Exemple. Corps cubiques réels ($r - r' = 2$) .

L'exemple des corps cubiques K_a définis par les polynômes $x^3 + ax^2 - (a+3)x + 1$ donné par Cusick ([4], § 3) montre que la valeur 16 de la constante C est optimale. Ici, le réseau $\mathcal{L}(E_K)$ est hexagonal (cf. § 7) et l'angle $\varphi(\epsilon_a)$ tend vers 0. Cusick donne également un exemple d'une suite de corps non cycliques pour lesquels $\mathcal{L}(E_K)$ modulo homothéties tend vers le réseau hexagonal avec $\varphi = 0$.

8.4.— Exemple. Corps biquadratique totalement réel.

Soit K' un corps quadratique réel, K une extension quadratique de K' , bicyclique sur \mathbb{Q} ; notons K_1 , K_2 , K' les sous-corps quadratiques, supposés réels, de K , ϵ_1 , ϵ_2 et ϵ' leurs unités fondamentales, et soit E le sous-groupe de E_K qu'elles engendrent. L'indice de Hasse $Q_{K/K'}$ est égal à 1 avec au plus une exception ($K = K'(\sqrt{\epsilon'})$), et l'indice $[E_K : E]$ vaut 1, 2 ou 4. Les vecteurs $\mathcal{L}(\epsilon_1)$, $\mathcal{L}(\epsilon_2)$ et $\mathcal{L}(\epsilon')$ sont deux à deux orthogonaux, de sorte que le réseau $p(\mathcal{L}(E))$ est rectangulaire. Lorsque le réseau $p(\mathcal{L}(E_K))$ est aussi rectangulaire (ce qui est en particulier le cas lorsque l'indice est 1 ou 4), on peut améliorer l'inégalité 5.10 par le facteur $\gamma_2 = \frac{2}{\sqrt{3}}$. Cette correction est encore valable lorsque le réseau $p(\mathcal{L}(E_K))$ est un réseau *rectangulaire centré* (c'est-à-dire lorsque l'une des unités $\epsilon_1\epsilon_2$ ou $\epsilon_1\epsilon_2\epsilon'$ est un carré dans K , avec $[E_K : E] = 2$): on le montre facilement en étudiant les problèmes de majoration du

paragraphe 6 pour les seuls réseaux rectangulaires centrés (le facteur correctif plus général de 6.5 (i) est $\frac{4}{2+\sqrt{3}} < \frac{2}{\sqrt{3}}$). La constante $\frac{C/\sqrt{3}}{2} = 4$ est très vraisemblablement optimale. On s'en rend compte en utilisant le procédé de Cusick ([4], § 6), généralisable à d'autres corps que $K' = \mathbb{Q}(\sqrt{2})$.

8.5.— Exemple. Corps cycliques de degré 4 ($r-r'=2$).

On considère un corps K cyclique de degré 4 sur \mathbb{Q} , contenant un corps quadratique K' donné. Comme $E_K/E_{K'}$ est un module de rang 1 sur $\mathbb{Z}[i]$, il existe $\epsilon \in E_K$ telle que $E_K = \langle E_{K'}, \epsilon, \sigma\epsilon \rangle$, σ désignant un générateur de $\text{Gal}(K/\mathbb{Q})$. Le réseau $p(\mathcal{L}(E_K))$ est carré, d'où, comme dans l'exemple précédent, une amélioration de la minoration 5.10 par un facteur $\frac{2}{\sqrt{3}}$.

8.6.— Exemple. Les réseaux A_r .

Soit n un entier ≥ 2 , soient $0 < a_1 < a_2 < \dots < a_{n-2}$ des entiers fixés, soit $a \in \mathbb{Z}$, et soit $f_a \in \mathbb{Z}[X]$ le polynôme $X(X-a)(X-a_1)\dots(X-a_{n-2}) - 1$. On voit tout de suite que, pour a assez grand, f possède n racines réelles $\epsilon_0, \epsilon_1, \dots, \epsilon_{n-1}$ où $\epsilon_{n-1} \rightarrow +\infty$ et $\epsilon_i \rightarrow a_i$ pour $1 \leq i \leq n-2$ lorsque $a \rightarrow +\infty$. On a $\log |\epsilon_0| \sim -\log a$ et $\log \epsilon_{n-1} \sim \log a$, et $\log \epsilon_i$ a une limite finie non nulle pour $1 \leq i \leq n-2$. Modulo homothétie, le réseau des logarithmes des unités $\epsilon, \epsilon - a_1, \dots, \epsilon - a_{n-2}$ tend vers le réseau ayant dans la base

canonique de \mathbb{R}^{n-1} la matrice $\begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & -1 \\ 1 & 1 & \dots & 1 \end{pmatrix}$; on reconnaît le réseau A_{n-1}

(vecteurs de base de norme $\sqrt{2}$ et d'angles mutuels $\frac{\pi}{3}$). On constate que l'on obtient le réseau critique pour $n \leq 4$; nous n'avons pas d'exemple permettant de trouver des réseaux critiques pour $n \geq 5$. Quant à l'angle $\varphi(\epsilon)$, il est défini par $\cos \varphi = \sqrt{\frac{6(n-1)}{n(n+1)}}$. On a donc $\varphi = 0$ pour $n = 2$ et 3 ; pour $n = 4$, on trouve $\cos \varphi = \frac{3}{\sqrt{10}}$, ce qui rend compte du facteur $\frac{216}{80\sqrt{10}} = \left(\frac{3}{\sqrt{10}}\right)^3$ qui apparaît chez Cusick (loc. cit.) entre la minoration du Théorème 2, p. 63 et l'exemple (17),

p. 71, analogue à notre exemple (Cusick impose les conditions $f_a(0) = 1$, $f_a(2) = -1$). Pour $n = 4$, nous ignorons si la valeur 216 de C est optimale; il est possible que l'inégalité puisse être améliorée par des raisonnements analogues à ceux du § 6.

8.7.— Exemple. Passage du cas totalement réel au cas totalement imaginaire pour une extension C.M.

On se donne une extension K'/K_0 de type C.M. Lorsque K_0 parcourt l'ensemble des extensions totalement réelles de K_0 , et que l'on pose $K = K_0 K'$, la minoration de $R_{K_0}/R_{K_0'}$ que l'on trouve en appliquant 5.10 à K/K' est la même que celle que l'on trouve directement, à un éventuel facteur 2 près dépendant d'indices de groupes d'unités (en l'occurrence, l'entier $\frac{Q_{K_0}/K_0 \cdot Q_{K/K_0}}{Q_{K/K'} \cdot Q_{K'/K_0}}$, qui divise Q_{K/K_0}); les constantes C et les angles $\varphi(\epsilon)$ sont les mêmes dans K_0/K_0' et dans K/K' (pour $\epsilon \in K_0$).

9.— La constante M .

Rappelons les notations du paragraphe 4 : le corps K' étant fixé et σ' désignant un plongement de K' dans \mathbb{C} , on pose, pour un élément θ d'une extension K de K' , $M_{\sigma'}(\theta) = \prod_{i < j} \left| 1 - \frac{\theta_i}{\theta_j} \right|^2$, (formule 4.3; on a $|\theta_1| \leq \dots \leq |\theta_m|$), et $M(\theta) = \prod M_{\sigma'}(\theta)$. On cherche à majorer $M(\theta)$ en fonction de la ramification dans K des places à l'infini de K' lorsque θ est une unité de K .

Dans un premier temps, on se contente d'étudier par des méthodes analytiques le module de la fonction

$$z = (z_1, z_2, \dots, z_m) \mapsto F(z) = \prod_{i < j} \left(1 - \frac{z_i}{z_j} \right)^2$$

dans le domaine D défini par $|z_1| \leq |z_2| \leq \dots \leq |z_m|$ et $|z_2| > 0$ de \mathbb{C}^m , ou dans un domaine plus restreint pour lequel on impose qu'il y ait r_1 variables

réelles et $2r_2$ variables complexes deux à deux conjuguées parmi les m variables z_i . Voici une majoration *universelle* :

9.1.— PROPOSITION (Remak). Pour $z \in D$, on a $|F(z)| \leq m^m$.

Démonstration :

Le principe du maximum appliqué à chacune des variables z_1, \dots, z_m permet de se ramener au cas où $|z_1| = \dots = |z_m| = 1$; on utilise alors l'inégalité (que Schur attribue à Polyà, cf. [15], énoncé IV) : $\prod_{i < j} |z_i - z_j| \leq m^{m/2}$, obtenue

en interprétant le premier membre comme la valeur absolue d'un déterminant de van der Monde, que l'on majore à l'aide de l'inégalité de Hadamard. La majoration est optimale, la borne étant atteinte sur les ensembles semblables à l'ensemble des racines m -ièmes de l'unité, et peut de ce fait être améliorée si et seulement si l'on a $r_1 \geq 3$. Dans le cas où z_1, \dots, z_m sont réels, Pohst conjecture,

et démontre pour $m \leq 11$ ([10], th. IV), l'inégalité $\prod_{i < j} \left(1 - \frac{z_i}{z_j}\right)^2 \leq 4^{[m/2]}$. Le

premier cas non totalement réel dans lequel on puisse améliorer la majoration de Remak par un calcul analytique est $n = 5$, $r_1 = 3$; nous n'avons pas fait les calculs.

Des considérations arithmétiques peuvent permettre d'améliorer les majorations analytiques de $M(\theta)$, au moins lorsque $r - r' = 1$. Le principe consiste à traiter analytiquement le cas où les unités sont supposées grandes, et à examiner ensuite un nombre fini d'exceptions, en déterminant les polynômes correspondants.

9.2.— Exemple. Corps cubiques à une place réelle.

On peut utiliser la majoration $R_K \geq \frac{1}{3} \log \frac{|d_K|}{M_{1,1}}$ avec $M_{1,1} = \frac{23}{a^3} = 9,893\dots$, où α est la racine réelle du polynôme $x^3 - x - 1$; si l'on excepte les corps de discriminant -23 , -31 et -44 , on peut utiliser la majoration $R_K \geq \frac{1}{3} \log \frac{|d_K|}{6}$; enfin, on peut remplacer M par une fonction

$M(d_K)$ tendant vers 4 quand $|d_K|$ tend vers $+\infty$ de façon à avoir l'inégalité

$$R_K \geq \frac{1}{3} \log \frac{|d_K|}{M(d_K)}.$$

9.3.— Exemple. Corps quartiques totalement imaginaires.

Par des arguments analogues à ceux de l'exemple 9.2, mais nécessitant des calculs un peu plus étendus, on montre que l'on a l'inégalité

$$R_K \geq \log \frac{d_K}{M_{0,2}} \text{ avec } M_{0,2} = \frac{229}{|\beta|^8} = 59,395\dots,$$

β désignant une racine de module > 1 de $x^4 + x + 1$. Si l'on excepte les 4 corps de discriminant 229, 257 (plus petits discriminants de corps primitifs) et 392 et 605 (plus petits discriminants de corps imprimitifs ne contenant pas de racine non triviale de l'unité), on peut utiliser la minoration $R_K \geq \frac{1}{4} \log \frac{d_K}{16}$.

L'exemple des corps cubiques réels K_n définis par les polynômes $x^3 - n^2x^2 + 1$, pour lesquels d_{K_n} est vraisemblablement égal à $4n^6 - 27$ pour une infinité d'entiers n , montre que la borne $M = 4$ de Pohst ne peut pas être améliorée lorsque $r = 2$ et $r' = 0$. Noter cependant que, asymptotiquement, la valeur de $C (= \frac{1}{16})$ est à remplacer ici par $\frac{1}{12}$, le rapport $\frac{4}{3}$ étant le carré de $\cos \varphi(\epsilon)$ (le réseau des unités modulo homothétie a ici la *bonne limite*, à savoir le réseau hexagonal). En fait, on peut montrer que la condition " $\varphi(\epsilon) \rightarrow 0$ " entraîne que $M(\epsilon)$ tend vers 1 ; nous n'avons pas recherché de majorations explicites de M en fonction de $\cos \varphi$ autres que la majoration $M \leq 4$.

Manuscrit reçu le 12 octobre 1987

(*) p. 23 : Membres du Laboratoire Associé au C.N.R.S. n° 226.

BIBLIOGRAPHIE

- [1] E.S. Barnes.— *On a theorem of Voronoï*, Proc. Camb. Phil. Soc. 53 (1957), 537–539.
- [2] E.S. Barnes.— *The construction of perfect and extreme forms I*, Acta Arith. 5 (1958), 57–79.
- [3] A.-M. Bergé et J. Martinet.— *Réseaux extrêmes pour un groupe d'automorphismes*, en préparation.
- [4] T.W. Cusick.— *Lower bounds for regulators*, Number Theory, Noordwijkerhout, 1983; Lectures Notes 1068, Springer–Verlag, 1984, 63–73.
- [5] P. Erdős.— *Arithmetical properties of polynomials*, J. London Math. Soc. 28 (1953), 416–425.
- [6] E. Friedman.— *Analytic formulas for the regulator of a number field*, à paraître.
- [7] G. Gras et M.-N. Gras.— *Calcul du nombre de classes et des unités des extensions abéliennes réelles de \mathbb{Q}* , Bull. Sc. Math. 101 (1977), 97–129.
- [8] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper*, Akademie–Verlag, Berlin, 1952; 2ème éd. : 1987.
- [9] E. Lehmer.— *Connections between Gaussian Periods and Cyclic Units*, Math. of Computation, Vol. 50, N° 182 (1988), 535–541.
- [10] M. Pohst.— *Regulatorabschätzungen für total reelle algebraischen Zahlkörper*, J. Number Th. 9 (1977), 459–492.
- [11] R. Remak.— *Elementare Abschätzungen von fundamentale Einheiten und des Regulators eines algebraischen Zahlkörpers*, J. Reine Angew. Math. 165 (1931), 159–179.

- [12] R. Remak.— *Über die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten*, J. Reine Angew. Math. 167 (1932), 360–378.
- [13] R. Remak.— *Über Größenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers*, Compositio Math. 10 (1952), 245–285.
- [14] R. Schoof et L.C. Washington.— *Quintic polynomials and real cyclotomic fields with large class number*, Math. of Computation, Vol. 50, N° 182 (1988), 543–556.
- [15] I. Schur.— *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. I (1918), 377–402; Ges. Abh., Vol. II, N° 32, 213–238.
- [16] J.H. Silverman.— *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory 19 (1984), 437–442.
- [17] R. Zimmert.— *Ideale Kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. 62 (1981), 367–380.

Depuis l'exposé, de nouveaux travaux sur la question sont intervenus.
Voici quelques références :

- A.-M. Bergé et J. Martinet.— *Notions relatives de régulateurs et de hauteurs*, Acta Arith., à paraître.
- A.-M. Bergé et J. Martinet.— *Minorations de hauteurs et petits régulateurs relatifs*, Sémin. Th. des Nombres de Bordeaux, exp. 11, 1987–88 (27 pages).
- E. Friedman et N.P. Skoruppa.— *Relative Regulators and Relative Mellin Transforms*, preprint.

Anne-Marie BERGÉ
et Jacques MARTINET
CeReMaB
351, Cours de la Libération
33405 TALENCE CEDEX

*Séminaire de Théorie des Nombres
Paris 1987-88*

**DEFORMATIONS OF GALOIS REPRESENTATIONS ASSOCIATED
TO THE CUSP FORM Δ**
N. BOSTON

Introduction

In [6] Mazur showed how there is a "versal deformation" parametrising the collection of p -adic representations of a profinite group G lifting a given representation $\bar{\rho} : G \rightarrow GL_2(\mathbb{F}_p)$. Of particular interest are the $\bar{\rho}$ associated to modular forms and elliptic curves in which G is the Galois group of a maximal algebraic extension of \mathbb{Q} unramified outside a finite set S of rational primes containing p .

In [1] techniques were developed that allow many versal deformations to be explicitly calculated. In this paper we show the versatility of these techniques by applying them to a "naturally occurring" family of $\bar{\rho}$, namely the $\bar{\rho}$ associated to the cusp form Δ of weight 12 for $SL_2(\mathbb{Z})$. The problems encountered for varying p are typical of the general theory which will be published elsewhere.

Sections 2, 3 and 4 describe the general machinery for the applications of the last 3 sections.

I would like to thank the Sloan Foundation and IHES for their support during this work.

1.— The Set-up.

Let $\Delta = \Sigma \tau(n) q^n$ be the unique normalised cusp form of weight 12 for $SL_2(\mathbb{Z})$. For each prime number p , there exists [4] a unique semisimple continuous homomorphism $\rho_p : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_p)$ unramified outside p such that if σ_ℓ is a Frobenius element for prime $\ell \neq p$, $\text{tr } \rho_p(\sigma_\ell) = \tau(\ell)$ and $\det \rho_p(\sigma_\ell) = \ell^{11}$.

In this paper we calculate explicit (uni)versal deformations of $\bar{\rho} = \rho_p \pmod{p}$ for 3 different kinds of $\bar{\rho}$, namely where the image of $\bar{\rho}$ is either

- (i) **tame**, i.e. of order prime to p (occurs for $p = 23$ only)
- or (ii) **Borel**, i.e. soluble, of order divisible by p (occurs for $p = 2, 3, 5, 7, 691$ only)
- or (iii) **full**, i.e. contains $SL_2(\mathbb{F}_p)$ (occurs for all other p) [11].

(Since ρ_p may be conjugated by matrices in $GL_2(\mathbb{Q}_p)$, there is leeway in fixing $\bar{\rho}$ for $p = 2, 3, 5$. Here we simply make a suitable choice).

2.– Groups with Normal Sylow p -subgroup.

Let G be a profinite group with normal Sylow p -subgroup P . We assume that P is of finite index in G and (topologically) finitely generated. \bar{P} will denote the maximal elementary p -abelian quotient of P .

I. By Schur–Zassenhaus [10], p. 246, G contains a subgroup A mapping isomorphically onto G/P (and any 2 such subgroups are conjugate by an element of P).

II. By Burnside's basis theorem [5], Satz 4.10, if $x_1, \dots, x_d \in P$ map to generators of \bar{P} , then they generate P .

III. By [1], theorem 2.8, if V is an $\mathbb{F}_p[A]$ -submodule of \bar{P} , then there exists an A -invariant subgroup B of P with $\dim V$ generators mapping onto V .

3.– The Galois Groups

Let K be a finite extension of \mathbb{Q} with Galois group H . Let P be the Galois group over K of a maximal pro- p -extension of K unramified outside primes above p .

Let r_2 be the number of complex places of K . If v is a place of K , then K_v will denote the completion of K at v . If F is a field, set $\delta(F) = 1$ if F contains a nontrivial p th root ζ_p of 1, $\delta(F) = 0$ otherwise.

Let $B = \{x \in K^* : \text{fractional ideal } (x) = I^p, x \in K_v^{*p} \text{ for all } v \mid p\}/K^{*p}$.

PROPOSITION 1 [5] Satz 11.8, [9].— Let $d(P)$ and $r(P)$ denote the generator and relation rank of P respectively, $p > 2$.

- (a) $d(P) = r_2 + 1 + r(P)$,
- (b) $r(P) = (\sum_{v|p} \delta(K_v)) - \delta(K) + \dim B$

Let \bar{E} and \bar{E}_v denote the "global" and "local" units modulo p th powers of K and K_v respectively. If the class number $h(K)$ is prime to p , then global class field theory gives an exact sequence of $\mathbb{F}_p[H]$ -modules :

$$(*) \quad 0 \rightarrow B \rightarrow \bar{E} \rightarrow \bigoplus_{v|p} \bar{E}_v \rightarrow \bar{P} \rightarrow 0.$$

Remark : $(p, h(K(\zeta_p))) = 1$ implies that $B = 0$ [8], p. 103.

Let H_v be a decomposition group of H for a chosen $v|p$ and H_∞ be the group generated by a chosen complex conjugation.

PROPOSITION 2 [2] 1.2.— As $\mathbb{F}_p[H]$ -modules, if H has order prime to p ,

- (a) $\bigoplus_{v|p} \bar{E}_v \cong \mathbb{F}_p[H] \oplus \text{Ind}_{H_v}^H \mu_p(K_v)$,
- (b) $\bar{E} \oplus \mathbb{F}_p \cong (\text{Ind}_{H_\infty}^H) \mathbb{F}_p \oplus \mu_p(K)$.

Notation :

Throughout the rest of this paper, K will denote the fixed field of $\ker \bar{\rho}$ and L a maximal pro- p -extension of K unramified outside primes above p . P , G and H will denote $\text{Gal}(L/K)$, $\text{Gal}(L/\mathbb{Q})$, and $\text{Gal}(K/\mathbb{Q})$ respectively.

4.— Deformation Theory. See also [1], [6].

Let \mathcal{C} be the category of complete noetherian local rings with residue field \mathbb{F}_p . For R in \mathcal{C} define $\Gamma_2(R) := \ker(GL_2(R) \rightarrow GL(\mathbb{F}_p))$. Since $\Gamma_2(R)$ is a pro- p group, all lifts $\rho : G_{\mathbb{Q}} \rightarrow GL_2(R)$ of $\bar{\rho}$ to R (unramified outside p) factor through G . Two such lifts are called *strictly equivalent* if conjugate by an element of $\Gamma_2(R)$.

Define a functor $F : \mathcal{C} \dashrightarrow Sets$ by :

$F(R) := \{\text{strict equivalence class of lifts of } \bar{\rho} \text{ to } R \text{ unramified outside } p\}.$

PROPOSITION 3 [6].— If $\bar{\rho}$ is nontrivial and absolutely irreducible, then F is representable. F always at least has a hull.

This hull is called a *versal deformation* of $\bar{\rho}$ (*universal* if F is representable). The corresponding ring is called the *(uni)versal deformation ring*, $R(\bar{\rho})$.

In [6], p. 30, it is shown that $\text{Krull dim } (R(\bar{\rho})/(p)) \geq 3$ for absolutely irreducible $\bar{\rho}$. The proof there carries over to our Borel cases. In particular, to show $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$, it will suffice to show that $R(\bar{\rho})$ is a quotient of $\mathbb{Z}_p[[T_1, T_2, T_3]]$ since there is a known lift ρ_p of $\bar{\rho}$ to \mathbb{Z}_p .

5.— Tame Case

$p = 23$ (for a deeper study, see [2]).

K is the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$ [11]. $h(K) = 1$ and $B = 0$ [6]. $H \cong S_3$, the symmetric group on 3 letters. By proposition 1, P is free pro- p on 4 generators. By (*) and proposition 2, $\bar{P} \cong 1 \oplus \epsilon \oplus \eta$, where $1, \epsilon, \eta$ are the 3 irreducible abstract $\mathbb{F}[H]$ -modules.

By 2 I, G is a semidirect product of $A \cong S_3$ and P . Pick σ, τ of orders 2 and 3 in A . Then \bar{P} is generated by $\bar{x}, \bar{x}^\tau, \bar{x}^{\tau^2}, \bar{y}$ such that $\bar{x}^\sigma = \bar{x}, \bar{y}^\sigma = \bar{y}^{-1}, \bar{y}^\tau = \bar{y}$. By 2 III, there exist $x, y \in P$ mapping to \bar{x}, \bar{y} such that $x^\sigma = x, y^\sigma = y^{-1}, y^\tau = y$. Then by 2 II x, x^τ, x^{τ^2}, y generate P .

PROPOSITION 4.— $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$. The universal deformation is given by :

$$\sigma \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tau \rightarrow \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix}, x \rightarrow \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}, y \rightarrow \begin{pmatrix} \sqrt[4]{1-3} T_3^2 \\ -3 T_3 \\ \sqrt[4]{1-3} T_3^2 \end{pmatrix}.$$

Proof :

Let R be in \mathcal{C} . By Schur-Zassenhaus the possible restrictions to A of lifts of $\bar{\rho}$ are all strictly equivalent. Indeed we exhaust strict equivalence by fixing lifts on A as above. Then under any lift of $\bar{\rho}$ to R , x and y map to elements of $\Gamma_2(R)$ on which the conjugation action of the images of σ and τ

are as prescribed. The most general possible such give us the above universal deformation.

6.—Borel Cases

$$\underline{p=2}$$

L is a maximal pro-2 extension of \mathbb{Q} unramified outside 2. By [5] 11.5, G is isomorphic to the pro- p group generated by x and y subject only to $x^2 = 1$. Suppose $y \in \ker \bar{\rho}$.

PROPOSITION 5.— $R(\bar{\rho})$ is a quotient of $\mathbb{Z}_p[[T_1, T_2, T_3, T_4]]$ of Krull dimension 4, and is not formally smooth. A versal deformation is given by :

$$x \rightarrow \begin{pmatrix} 1+f & 1 \\ -2f-f^2 & -1-f \end{pmatrix}, \quad y \rightarrow \begin{pmatrix} 1+T_1 & T_2 \\ T_3 & 1+T_4 \end{pmatrix},$$

where f is a power series in T_1, T_2, T_3, T_4 .

Proof :

Consider lifts of $\bar{\rho}$ to the dual numbers $\mathbb{F}_p[\epsilon]$ ($\epsilon^2 = 0$). One calculates that the possibilities for images of x are all strictly equivalent. Strict equivalence has no effect on the image of y (since $\Gamma_2(\mathbb{F}_p[\epsilon])$ is abelian), so y can map to anything in $\Gamma_2(\mathbb{F}_p[\epsilon])$. It follows that $R(\bar{\rho})$ is a quotient of $\mathbb{Z}_p[[T_1, T_2, T_3, T_4]]$.

In a versal deformation x maps to a matrix that by conjugation by a diagonal matrix can be brought to the given form. This does not exhaust strict equivalence, since we can conjugate the image of y by matrices in $\Gamma_2(R(\bar{\rho}))$ fixing the image of x . This forces Krull dim $R(\bar{\rho})$ to be less than 5, so it is 4 by the last paragraph of § 4.

$$\underline{p=3, 5, 7.}$$

L is a maximal pro- p extension of $\mathbb{Q}(\zeta_p)$ unramified outside the prime above p . G therefore has a normal Sylow p -subgroup $Q = \text{Gal}(L/\mathbb{Q}(\zeta_p))$, and so by 2 I, G is a semidirect product of $A \cong \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and Q . By 3,

since p is regular, Q is free pro- p on $(p+1)/2$ generators. By (*) and proposition 2, if $\chi : \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \rightarrow \mathbb{F}_p^*$ is the cyclotomic character, $\epsilon_i \bar{Q} := \{u \in \bar{Q} : u^\alpha = \chi^i(\alpha)u \text{ for all } \alpha \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\}$ has dimension 1 if $i = 0, 1, 3, 5, \dots, p-2$ and dimension 0 otherwise. By 2 III, there exist $x_i \in Q$ ($i = 0, 1, 3, 5, \dots, p-2$) such that $x_i^\alpha = x_i^{\chi^i(\alpha)} (\chi^i(\alpha) \in \mathbb{Z}_p^*$ via the Teichmüller lift) for all $\alpha \in A$, generating Q by 2 II. Let ω be a generator of A .

PROPOSITION 6.— $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$. A versal deformation is given by :

($p = 3$)

$$\omega \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & \chi(\omega) \end{pmatrix}, \quad x_0 \rightarrow \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}, \quad x_1 \rightarrow \begin{pmatrix} \sqrt{1+T_3} & 1 \\ T_3 & \sqrt{1+T_3} \end{pmatrix}$$

($p = 5$)

$$\omega \rightarrow \begin{pmatrix} \chi(\omega) & 0 \\ 0 & \chi^2(\omega) \end{pmatrix}, \quad x_0 \rightarrow \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}, \quad x_1 \rightarrow \begin{pmatrix} 1 & 0 \\ T_3 & 1 \end{pmatrix}, \quad x_3 \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

($p = 7$)

$$\omega \rightarrow \begin{pmatrix} \chi(\omega) & 0 \\ 0 & \chi^4(\omega) \end{pmatrix}, \quad x_0 \rightarrow \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}, \quad x_3 \rightarrow \begin{pmatrix} \sqrt{1+T_3} & 1 \\ T_3 & \sqrt{1+T_3} \end{pmatrix}, \quad x_1, x_5 \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof :

Let R be in \mathcal{C} . As in proposition 4, we can use strict equivalence (and [11]) to fix lifts of $\bar{\rho}$ on A . This does not exhaust strict equivalence since diagonal matrices fix the image of A . Ensuring that x_1 for $p = 3$, x_3 for $p = 5$, and x_3 for $p = 7$ respectively have a 1 in the top right corner then exhausts it, after applying the following lemma to obtain the most general possible images of the x_i 's :

LEMMA.— Let $A \subseteq GL_2(R)$ and $\phi : A \rightarrow \mathbb{Z}_p^*$ be a tame character. Suppose $x \in \Gamma_2(R)$ satisfies $x^g = x^{\phi(g)}$ for all $g \in A$.

(1) If $\phi(A) \neq \{1\}$, then $\det x = 1$.

(2) If $\phi(A) \subseteq \{\pm 1\}$, then $\text{tr } x = 2$. In this case x has the form $\begin{pmatrix} 1+a & b \\ c & 1-a \end{pmatrix}$ with $a, b, c \in m$, the maximal ideal of R , $a^2 + bc = 0$, and then $x^n = \begin{pmatrix} 1+na & nb \\ nc & 1-na \end{pmatrix}$ ($n \in \mathbb{Z}_p$).

Proof : Direct calculation.

$$\underline{p = 691} .$$

Once again G is a semidirect product of $A \cong \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $Q = \text{Gal}(L/\mathbb{Q}(\zeta_p))$. Since p is irregular, Q is not free pro- p [3]. Global class field theory, however, gives an exact sequence of $\mathbb{F}_p[A]$ -modules :

$$\bar{E}_v \rightarrow \bar{Q} \rightarrow \bar{C} \rightarrow 0 ,$$

where \bar{C} is the ideal class group of $\mathbb{Q}(\zeta_p)$ modulo p th powers and \bar{E}_v is the "local" units of $\mathbb{Q}_p(\zeta_p)$ modulo p th powers.

By proposition 2, for $i \neq 1$, $\epsilon_i \bar{E}_v$ has dimension 1, whilst $\epsilon_1 \bar{E}_v$ has dimension 2. Let \bar{x}_i ($i = 0, 1, 2, \dots, p-2$), \bar{y} be the images (possibly trivial) in \bar{Q} of generators (so $\bar{x}_i \in \epsilon_i \bar{Q}$, $\bar{y} \in \epsilon_1 \bar{Q}$). Since Vandiver's conjecture holds for p [12], $\epsilon_i \bar{C}$ has dimension 1 for $i = 491, 679$ (p divides B_{12} and B_{200}) and dimension 0 for all other odd i [13], p. 197. Also $\epsilon_0 \bar{C} = 0$ ([13], p. 102). Lifting to \bar{Q} , let $\bar{z}_{491}, \bar{z}_{679}$ be corresponding elements of $\epsilon_{491} \bar{Q}, \epsilon_{679} \bar{Q}$ respectively. Let $\bar{w}_1, \dots, \bar{w}_k$ be elements of the $\epsilon_i \bar{Q}$ (i even, nonzero) needed to complete a generating set for \bar{Q} .

As in the previous example there exist by 2 III $x_0, x_1, x_2, \dots, x_{p-2}, y, z_{491}, z_{679}, w_1, \dots, w_k \in Q$ such that $x_i^\alpha = x_i^{\chi_i^i(\alpha)}$ for all $\alpha \in A$ etc., mapping to the above generators of \bar{Q} and so by 2 II generating Q . Let w be a generator of A .

PROPOSITION 7.— $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$. A versal deformation is given by

$$\omega \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & \chi^{11}(\omega) \end{pmatrix}, x_0 \rightarrow \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_4 \end{pmatrix}, x_{679} \rightarrow \begin{pmatrix} 1 & T_2 \\ 0 & 1 \end{pmatrix}, x_{11} \rightarrow \begin{pmatrix} 1 & 0 \\ T_3 & 1 \end{pmatrix}, z_{679} \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

all other given generators of Q map to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

T_4 is a power series in T_1, T_2, T_3 , congruent to $T_1 \pmod{(p, T_2, T_3)}$.

Proof :

We proceed as in the previous example, using strict equivalence (and [11]) to fix the image of A and to obtain a 1 in the top right corner of the image of z_{679} . The lemma tells us that under a lift of $\bar{\rho}$ to R in \mathcal{C} the most general possible images of the generators of Q are as given with $T_1, T_2, T_3, T_4 \in m$ (where m is the maximal ideal of R).

Since the \bar{x}_i 's and \bar{y} generate the inertia subgroup at v of \bar{Q} , we can pick x_0, x_{679}, x_{11} to lie in an inertia subgroup I_v of Q ([1], lemma 4.7).

Let $\mathbb{Q}(\zeta_{p^\infty})$ be the cyclotomic \mathbb{Z}_p -extension of $\mathbb{Q}(\zeta_p)$. Let M be a maximal unramified pro- p -extension of $\mathbb{Q}(\zeta_{p^\infty})$ on which $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts as χ^{-11} (via Teichmüller lift). Any lift of $\bar{\rho}$ in which $T_2 = T_3 = 0$ factors through $\text{Gal}(M/\mathbb{Q})$, whose structure is known by Iwasawa theory ([13], p. 199). It is metabelian with $\text{Gal}(M/\mathbb{Q}(\zeta_{p^\infty})) \cong \mathbb{Z}_p$. Thus the image of x_0 in $\text{Gal}(M/\mathbb{Q})$ conjugates the image of z_{679} to some power ("the Iwasawa root") of itself.

It follows that $(1+T_1)/(1+T_4) \equiv 1 \pmod{(p, T_2, T_3)}$.

Full Cases

We investigate only those full cases for which $p > 13$, $\tau(p) \not\equiv 0 \pmod{p}$, $h(K) \not\equiv 0 \pmod{p}$ (one expects this situation to hold for most p).

Let ζ be a generator of \mathbb{F}_p^* . The subgroup of H generated by $\begin{pmatrix} \zeta^{11} & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & \zeta^{11} \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ has order prime to p and so by 2 it lifts isomorphically to a subgroup A of G .

Let $\alpha, \beta, w \in A$ map to the 3 matrices respectively.

Let Q be the Sylow p -subgroup of G such that $\bar{\rho}(Q) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$. The subgroup $\langle \alpha, \beta \rangle$ of A acts on Q . By 2 III, there exists $s \in Q$ such that $\bar{\rho}(s) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $s^\alpha = s^{\zeta^{11}}$, $s^\beta = s^{\zeta^{-11}}$ (where ζ^{11}, ζ^{-11} are lifted by Teichmüller to \mathbb{Z}_p^*).

By (*) and proposition 2, the image of $\text{Ind}_{H_v}^H \mu_p(K_v)$ in \bar{P} is generated as an $\mathbb{F}_p[H]$ -module by one element ; call it \bar{y} . Since $\tau(p) \not\equiv 0 \pmod{p}$, the inertia subgroup of H_v can be chosen to be contained in $\left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\}$ [7]. This inertia subgroup maps onto $\langle \zeta^{11} \rangle \subseteq \mathbb{F}_p^*$ under \det (looking at the maximal abelian subfield of K_v). It follows that the image of α in H lies in H_v . By 2 III there exists $y \in P$ mapping to \bar{y} such that $y^\alpha = y^{\chi(\alpha)}$ (χ the cyclotomic character).

Using (*) and proposition 2, it will be shown elsewhere that \bar{P} is generated as an $\mathbb{F}_p[H]$ -module by \bar{y} , \bar{x} , and a number $\bar{z}_1, \dots, \bar{z}_k$ of extra variables which are taken care of by the lemma (**).

Finally, pick $x, z_1, \dots, z_k \in P$ mapping to $\bar{x}, \bar{z}_1, \dots, \bar{z}_k$. By 2 II, $\alpha, \beta, w, s, x, y, z_1, \dots, z_k$ generate G .

PROPOSITION 8^().** — $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$. *The universal deformation is given by :*

$$\begin{aligned} \alpha &\rightarrow \begin{pmatrix} \zeta^{11} & 0 \\ 0 & 1 \end{pmatrix}, \quad \beta \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & \zeta^{11} \end{pmatrix}, \quad w \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad s \rightarrow \begin{pmatrix} 1 & 1+T \\ 0 & 1 \end{pmatrix}, \quad x \rightarrow \begin{pmatrix} 1+U_1 & U_2 \\ U_3 & 1+U_4 \end{pmatrix}, \\ y, z_i &\rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (i = 1, \dots, k). \end{aligned}$$

Here U_1, U_2, U_3, U_4 are a permutation of T_1, T_2, T_3 together with a variable expressible as a power series in T_1, T_2, T_3 . T is also so expressible.

Proof :

Let R be in \mathcal{C} . Strict equivalence is exhausted by fixing lifts on α, β, w . Under a lift of $\bar{\rho}$ to R , by the lemma of 6, the most general possibility for the image of s under the given conjugation actions of the images of α and β is as given with T in the maximal ideal m of R . By the same lemma the image of y is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let the image of x be as given.

Next, note that $s^p, (ws)^3 \in P$. We shall calculate their images in $GL_2(R/m^2)$ in two ways, where $R = \mathbb{Z}_p[[T, U_1, U_2, U_3, U_4]]$.

$$\text{By direct calculation, } s^p \rightarrow \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, (ws)^3 \rightarrow \begin{pmatrix} 1+T & 2T \\ -2 & T \end{pmatrix}.$$

In terms of x and y , they are both of the form

$$\begin{pmatrix} 1+\Sigma \lambda_i U_i & \Sigma \mu_i U_i \\ \Sigma \nu_i U_i & 1+\Sigma \xi_i U_i \end{pmatrix}, \lambda_i, \mu_i, \nu_i, \xi_i \in \mathbb{F}_p.$$

We therefore get 2 equations, of the form :

$$T \equiv \Sigma \lambda_i U_i \pmod{m^2}$$

$$p \equiv \Sigma \mu_i U_i \pmod{m^2}.$$

The first equation is the reduction mod m^2 of an equation writing T as a power series in the U_i 's. Similarly the second equation allows one of the U_i 's to be written in terms of the others since the equation cannot be simply $p \equiv 0 \pmod{m^2}$ because of the existence of the lift ρ_p of $\bar{\rho}$ to \mathbb{Z}_p .

Remarks :

(1) $p = 11, 13$ and p not ordinary (i.e. $\tau(p) \equiv 0 \pmod{p}$), e.g. $p = 2411$) require better knowledge of H_y .

(2) Using the work of Hida together with 2 III, Mazur has observed that for $p > 13$, $p \neq 691$ ordinary, a natural conjecture, namely that all ordinary lifts of $\bar{\rho}$ are pro-modular, implies that $R(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$. This lends evidence to the suggestion that \bar{C} is at least coprime to the adjoint $\mathbb{F}_p[H]$ -module.

Manuscrit reçu le 15 septembre 1988

(**) p. 59 : (Added August 1989) : Not proven. See forthcoming publication for corrected version.

BIBLIOGRAPHY

- [1] N. Boston.— *Deformation Theory of Galois Representations*, Harvard Ph. D. Thesis, 1987.
- [2] N. Boston and B. Mazur.— *Explicit universal deformations of Galois representations*, to appear in volume 17, Advanced Studies in Pure Mathematics.
- [3] A. Brumer.— *Galois groups of extensions of algebraic number fields with given ramification*, Michigan Math. J. 13 (1966), 33–40.
- [4] P. Deligne.— *Formes modulaires et représentations ℓ -adiques*, Sémin. Bourb. 355 (1969) ; LNM 179 (1971) Berlin–Heidelberg–New York.
- [5] H. Koch.— *Galoissche Theorie der p -Erweiterungen*, Springer–Verlag, Berlin–Heidelberg–New York, 1970.
- [6] B. Mazur.— *Deforming Galois representations*, to appear in the Proceedings of the March 1987 Workshop on *Galois groups over Q* held at MSRI, Berkeley, California.
- [7] B. Mazur and A. Wiles.— *On p -adic analytic families of Galois representations*, Comp. Math. 59 (1986), 231–264.
- [8] J. Neukirch.— *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Inv. Math. 21 (1973), 59–116.
- [9] O. Neumann.— *On p -closed number fields and an analogue of Riemann’s existence theorem*, In *Algebraic Number Fields*, Academic Press., London 1977 (Fröhlich ed.), 625–647.
- [10] D. Robinson.— *A Course in the Theory of Groups*, Springer–Verlag, Berlin–Heidelberg, New York, 1982.

- [11] P. Swinnerton-Dyer.— *On ℓ -adic representations and congruences for coefficients of modular forms*, LNM 350, Springer-Verlag, Berlin-Heidelberg-New York, 1973, 1–55.
- [12] S. Wagstaff.— *The irregular primes to 125000*, Math. Comp. 32 (1978), 583–591.
- [13] L. Washington.— *Introduction to Cyclotomic Fields*, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

N. Boston
Department of Mathematics
University of California
Berkeley CA 94720
U.S.A.

*Séminaire de Théorie des Nombres
Paris 1987-88*

MULTIPLICATIVE FUNCTIONS $|g| \leq 1$ AND THEIR
CONVOLUTIONS : AN OVERVIEW
P.D.T.A. ELLIOTT

In this lecture a multiplicative function g will be defined on the positive integers, assume complex values, and satisfy the relation $g(mn) = g(m)g(n)$ whenever $(m,n) = 1$. I shall assume that $|g(n)| \leq 1$ for all positive n . *Overview* in the title means that there will be few details, but I will indicate the more important ideas. All the results labelled THEOREM are new, due to myself to appear this year or later.

For each function of the above type there are real constants α , A and a slowly-oscillating function $L(u)$, identically one in absolute value, so that

$$(1) \quad x^{-1} \sum_{n \leq x} g(n) = Ax^{i\alpha} L(\log x) + o(1)$$

as $x \rightarrow \infty$. This result was conjectured by Wirsing [11], who could obtain it provided the values of the function g do not essentially fill the complex unit disc. Such an estimate is already decidedly non-trivial, since it contains the celebrated Prime Number Theorem as a straightforward consequence. The full result is due to Halász [8], using Fourier analysis. His argument employs in an essential manner the Euler product representation of the corresponding Dirichlet series $\sum_{n=1}^{\infty} g(n)n^{-s}$. It further gives, and one feels that this is the heart of the matter, that if

$$(2) \quad \limsup_{x \rightarrow \infty} x^{-1} \left| \sum_{n \leq x} g(n) \right| > 0,$$

then for some real τ

$$\operatorname{Re} \sum \frac{1}{p} (1 - g(p)p^{-ir}) < \infty ,$$

the series being taken over all primes p .

Next let $a \geq 1$, b be integers. Then we still have

$$(3) \quad x^{-1} \sum_{n \leq x} g(an+b) = Ax^{\frac{i\alpha}{2}} L(\log x) + o(1) ,$$

with, of course, possibly different A , α and L . Moreover, if

$$(4) \quad \lim_{x \rightarrow \infty} \sup x^{-1} \left| \sum_{n \leq x} g(an+b) \right| > 0 ,$$

then there is a Dirichlet character $(\text{mod } a)$ and a real r for which

$$(5) \quad \operatorname{Re} \sum \frac{1}{p} (1 - g(p)\chi(p)p^{-ir}) < \infty .$$

A natural way to approach (3) seems to be to reduce ourselves to the case $(a,b) = 1$, and to introduce a representation employing the orthogonality of characters :

$$\frac{1}{\phi(a)} \sum_{\chi \pmod{a}} \bar{\chi}(b) \frac{1}{x} \sum_{m \leq x} g(m)\chi(m) .$$

We then apply the result (1) of Halász to each innersumm. This way is not completely clear. For example, a sum of $\phi(a)$ functions of the form given on the right-hand side of (1) will not generally be of the same form. The following remark is very helpful.

If

$$\operatorname{Re} \sum \frac{1}{p} (1 - u_p) , \quad \operatorname{Re} \sum \frac{1}{p} (1 - v_p)$$

converge for complex u_p , v_p of modulus 1, then so does the series

$$\operatorname{Re} \sum \frac{1}{p} (1 - u_p \bar{v}_p) .$$

Applications of the Cauchy–Schwarz inequality will suffice. Applied in our present circumstances it enables us to reduce to the case of a single r , and a class of equivalent characters χ . After (4), the validity of (5) is clear.

In fact the exponent ia is independent of a , and one can arrange for a common function L . A detailed account of these matters may be found in Delange [1], a paper from which I could have profited, had I studied it. I thank him for bringing it to my attention. It does not contain the above remark.

In the study of these sums much of the tangle can be swept away by applying one of the next four theorems.

THEOREM 1. *Let $1 \leq w_0 \leq x$. There is a real $r, |r| \leq (\log x)^{1/19}$, so that*

$$\frac{w}{x} \sum_{\substack{n \leq x/w \\ n \leq x}} g(n) = w^{ir} \frac{1}{x} \sum_{n \leq x} g(n) + O\left(\left(\frac{\log 2w_0}{\log x}\right)^{1/19}\right)$$

uniformly for $1 \leq w \leq w_0$. If g is real-valued, then we may set $r = 0$. The implicit constant is absolute.

THEOREM 2. *For a suitable $\eta(D)$*

$$\frac{1}{x} \sum_{\substack{n \leq x \\ (n, D)=1}} g(n) = \eta(D) \frac{1}{x} \sum_{n \leq x} g(n) + O\left(\left(\frac{(\log \log 3D)^2}{(\log x)^{1/19}}\right)\right)$$

uniformly for $D \geq 1$, D odd, $x \geq 2$.

The form of $\eta(D)$ may be anticipated by considering appropriate Euler products. It may implicitly employ a real r , in the manner of Theorem 1. There is also a version of Theorem 2 for even D . Note that as $x \rightarrow \infty$ the error term in Theorem 1 is asymptotically small so long as w does not get as large as a fixed power of x . The value of the constant $1/19$ can perhaps be improved. At present it seems doomed not to exceed 1.

THEOREM 3.

$$\sum_{\substack{n \leq y \\ n \equiv r \pmod{D}}} g(n) = \frac{1}{\phi(D)} \sum_{\substack{n \leq x \\ (n, D)=1}} g(n) + O\left(y \left(\frac{(\log \log x)}{(\log x)}\right)^{1/8} \frac{\log x}{\log y}\right)$$

uniformly for $y \leq x$, for all $(r, D) = 1$, and all moduli $D \geq 1$ with the possible exceptions of the multiples of a single modulus $D_0 > 1$.

The example of a non-principal Dirichlet character $(\text{mod } 3)$ for g shows that the exceptional moduli may all occur. D_0 may depend upon x and g , but this is not generally too damaging. More important is that the theorem becomes trivial if D gets above $(\log x)^{1/8}$.

Define

$$M(g, x) = \frac{1}{x} \left| \sum_{n \leq x} g(n) \right| .$$

THEOREM 4. *Let χ_1, χ_2 be inequivalent characters, defined to moduli not exceeding M . Then*

$$M(\chi_1, y) M(\chi_2, y) \ll \left(\frac{\log \log x + \log 2M}{\log x} \right)^{1/4} \left(\frac{\log x}{\log y} \right)^2$$

uniformly for $2 \leq y \leq x$, $M \geq 1$.

In short, for characters defined to be small moduli the mean-value of $g\chi$ can only misbehave once. This represents yet another example of the Deuring-Heilbronn phenomenon, save that the exceptional cases actually occur.

It is convenient to insert here

THEOREM 5 *There is a positive constant c_0 so that*

$$\sum_{p \leq x^{1/2} \exp(-(\log x)^{23/24})} \max_{(r, p) = 1} \max_{y \leq x} p \left| \sum_{\substack{n \leq y \\ r \equiv n \pmod{p} \\ r \equiv b \pmod{a}}} g(n) - \frac{1}{p-1} \sum_{\substack{n \leq y \\ (n, p) = 1 \\ r \equiv b \pmod{a}}} g(n) \right|^2 \\ \ll x^2 (\log x)^{-c_0},$$

where the summation over the primes p omits at most $\phi(a)$ moduli.

Once again exceptional moduli can actually occur. The important feature of this theorem is that beyond $|g(n)| \leq 1$ there is no restriction upon the values of g . Although in appearance similar to the well-known theorem of Bombieri–Vinogradov on primes in arithmetic progression, it is the first result of such a completely general nature. For proofs of these results see Elliott [6], [7].

Here we go :

CONJECTURE I. Let g_1, \dots, g_k be $k \geq 1$ multiplicative functions which satisfy $|g_j(n)| \leq 1$ for all n , and let $a_j > 0$, b_j be integers for which

$$\det \begin{pmatrix} a_r & b_r \\ a_t & b_t \end{pmatrix} \neq 0, \quad 1 \leq r < t \leq k.$$

Then there are real constants A , α and a slowly-oscillating function $L(u)$, of absolute value 1, so that

$$x^{-1} \sum_{n \leq x} g_1(a_1 n + b_1) \dots g_k(a_k n + b_k) = A x^{i\alpha} L(\log x) + o(1)$$

as $x \rightarrow \infty$.

As a complement :

CONJECTURE II. *If*

$$\limsup_{x \rightarrow \infty} x^{-1} \left| \sum_{n \leq x} \prod_{j=1}^k g_j(a_j n + b_j) \right| > 0,$$

then there are characters $\chi_j \pmod{a_j}$, reals r_j so that the series

$$\operatorname{Re} \sum \frac{1}{p} (1 - g_j(p) \chi_j(p) p^{-ir_j}), \quad j = 1, \dots, k,$$

converge.

The earlier results amount to the case $j = 1$ of these conjectures.

For the remainder of this lecture I consider the case $k = 2$, and write $a_1 = a$, $b_1 = b$, $a_2 = A$, $b_2 = B$, so that always $aB \neq Ab$ is assumed. A main difficulty should be stated at once. For general multiplicative functions g_j there seems no hope of analytically continuing the Dirichlet series $\sum_{n=1}^{\infty} g_1(an+b)g_2(An+B)n^{-s}$ into the half-plane $\operatorname{Re}(s) < 1$. Indeed, we cannot even do it for a single function g_1 , with $a = 1$, $b = 0$. Worse, there is nothing available to play the rôle of an Euler product.

THEOREM 6. *Assume that for a certain specified constant c , $0 < c < 1$,*

$$x^{-1} \left| \sum_{n \leq x} g_1(an+b)g_2(An+B) \right| \geq 1 - c, \text{ for all } x \geq N.$$

Then there is a constant $x_0(N)$, and further constant c_1, c_2 depending at most upon c , so that if for some Dirichlet character $\chi \pmod{a}$ we have

$$\min_{|r| \leq c_1} \operatorname{Re}(1 - g_1(p)\chi(p)p^{-ir}) \leq c_2,$$

on those primes $p \leq x_0$, then

$$(6) \quad \operatorname{Re} \sum \frac{1}{p} (1 - g_1(p)\chi(p)p^{-ir}) < \infty$$

taken over all primes, holds for some real r .

A similar assertion can be made for g_2 , the character being defined $(\bmod A)$.

Some remarks to clarify this result :

If for some function g_1 or g_2 , with values confined to m^{th} roots of unity, a condition of the type (6) is satisfied, then the assertion of Conjecture I is valid – so we are here dealing with the *hard* case.

The condition on the finitely many primes up to x_0 is a flaw. At the moment the method, surrealistically speaking, cannot tell which Dirichlet character $(\bmod a)$ to favour, and we choose it.

Although one could compute a value for c , it would not presently be significant.

We have \liminf , where we should have \limsup .

To compensate for all this, although it does not show, the method will allow the functions g_j to depend considerably upon x . This is very helpful in applications.

Lightning sketch of the proof. The method is a multiplicative analogue of that given for additive functions in Chapters 6–9 of my (1984/85) Springer book *Arithmetic Functions and Integer Products* [5]. My Paris lecture, *A new inequality in the theory of additive arithmetic functions*, of 1982 [4] is also pertinent.

If complex numbers $w_n, |w_n| = 1$ satisfy $x^{-1} |\sum_{n \leq x} w_n| > 1 - \epsilon > 0$, then for a certain positive absolute constant K , there is a θ , $|\theta| = 1$, so that $x^{-1} \sum_{n \leq x} |w_n - \theta| < 1 - K\epsilon^{1/3}$. We can thus transfer the hypothesis of Theorem 6 to one of the form

$$x^{-1} \sum_{n \leq x} |g_1(an+b) - \theta \overline{g_2(An+B)}| \ll \text{small}.$$

We apply a suitably modified Turán–Kubilius dual (or a version of the Large Sieve) :

$$\sum_{p \leq x^{1/4}} p \left| \sum_{\substack{m \leq x \\ m \equiv 0 \pmod{p}}} d_m - \frac{1}{p} \sum_{m \leq x} d_m \right|^2 \ll x \sum_{m \leq x} |d_m|^2$$

setting $d_m = 0$ unless m is of the form $an + b$, in which case

$$d_m = g_1(m) - \theta \overline{g_2\left(A\left[\frac{m-b}{a}\right] + B\right)}.$$

Applying Theorem 5 we do away completely with the function g_2 , and reach (essentially)

$$\sum_{p \leq x^{1/4}} \frac{1}{p} \sum_{\substack{m \leq x \\ m \equiv 0 \pmod{p} \\ m \equiv b \pmod{a}}} g_1(m) - \frac{1}{x} \sum_{\substack{m \leq x \\ m \equiv b \pmod{a}}} g_1(m) \ll \text{small}.$$

Defining

$$S(y, r) = y^{-1} \sum_{\substack{m \leq y \\ m \equiv r \pmod{a}}} g_1(m)$$

we have (again essentially)

$$(7) \quad \sum_{p \leq x^{1/4}} \frac{1}{p} \left| g_1(p) S\left(\frac{x}{p}, b\bar{p}\right) - S(x, b) \right|^2 \ll \text{small},$$

where $p\bar{p} \equiv 1 \pmod{a}$. We regard this as an approximate functional equation for the $\phi(a)$ unknown functions $S(y, r)$, and vary x to solve it as far as possible, using the fact that the primes p give many interpolation values x/p . In this way we obtain an estimate for the mean-value of g_1 of the type given in Theorem 1, but with the useful uniformity in w reaching up to a fixed power of x . This enables us to factorize out the functions $S(y, r)$ in (7), to obtain (essentially)

$$|M(g_\chi, x)|^2 \sum_{\substack{p \\ p \leq x^{1/4}}} \left| \frac{1}{p} g_1(p) \chi(p) p^{ir} - 1 \right|^2 \ll \text{small ,}$$

for the character χ under consideration. An inductive procedure now completes the proof.

The inequality (8) may be compared with that obtained for the characteristic function of an additive function in my paper of the 1972 meeting in St. Louis, Missouri [2]. The argument given there applies equally well to any multiplicative function g which satisfies $|g(n)| \leq 1$. The present inequality is a far-reaching elaboration, and not at all obvious. Between these works lies 16 years of mathematics.

An appropriate treatment of a related approximate functional equation, itself an analogue of my result for additive functions, and arising in a related manner, may be found in Hildebrand's 1987 paper [9]. A suitable modification of it may be applied here. Indeed, a first version of Theorem 6, involving a single function g with the stronger hypothesis

$$x^{-1} \sum_{n \leq x} |g(n)\overline{g(n+1)} - 1| < \text{a small constant ,}$$

was given by Hildebrand [10]. Not having Theorem 5 he iterated the hypothesis that $g(n+1) - g(n)$ be small. This limited the generality, and would not allow the mean-value of $g(n)\overline{g(n+1)}$ to essentially assume complex values. It was, however, an important step, since it showed the feasibility of a multiplicative analogue of Chapters 6–10 of my book on Arithmetic Functions and Integer Products. Perhaps an analogue of the results in Chapters 1–3 of that same work might now remove the auxiliary condition involving the early primes.

An example will show that Theorem 6 is non-trivial.

Let f be a real valued additive function. Let $\beta(x) > 0$, $\rightarrow \infty$ as $x \rightarrow \infty$, in such a way that $\beta(x^y)/\beta(x) \rightarrow 1$ for each fixed $y > 0$. Thus $\beta(x)$ is a slowly-oscillating function of $\log x$. Let $\nu_x(n; h_n \leq z)$ denote the frequency of those integers n , not exceeding x , for which $h_n \leq z$.

THEOREM 7. *In order that for a suitable $\alpha(x)$*

$$\nu_x(n; f_1(an+b) + f_2(An+B) - \alpha(x) \leq z\beta(x)) \Rightarrow F(z),$$

as $x \rightarrow \infty$, it is necessary and sufficient that there exist constants λ_j , $j = 1, 2$, such that

$$(9) \quad P \left(\sum_{3 \leq p \leq x} Y_p - \alpha_1(z) \leq z\beta(x) \right) \Rightarrow F(z),$$

where the independent random variables Y_p are distributed according to

$$(10) \quad Y_p = \begin{cases} f_1(p) - \lambda_1 \log p & \text{with probability } \frac{1}{p}, \\ f_2(p) - \lambda_2 \log p & \text{with probability } \frac{1}{p}, \\ 0 & \text{with probability } 1 - \frac{2}{p}, \end{cases}$$

with $\alpha_1(x) = \alpha(x) - (\lambda_1 + \lambda_2) \log x$.

For a function f_1 with $a = 1$, $b = 0$, and with f_2 identically zero, Levin and Timofeev proved in 1972 that (the analogue of) (10) implies (9). I proved the converse implication in 1976. The present theorem shows that the results of Chapter 16 of my book *Probabilistic Number Theory* (Springer, 1979/80), can largely be transferred to the sum of two (possibly distinct) functions on differing arithmetic progressions. Well-known theorems in the theory of probability proper enable us to read from (10) necessary and sufficient conditions for the weak convergence of the frequencies (9). Here there is no condition upon the second moments of the f_j , as I needed in my book on Arithmetic Functions and Integer Products. The characteristic function of the frequency (9) is

$$[x]^{-1} \sum_{n \leq x} g_1(an+b)g_2(An+B)\exp(-ita(x)\beta(x)^{-1}),$$

where $g_j(n) = \exp(it\beta(x)^{-1}f_j(n))$, and the relevance of Theorem 6 is clear. The dependence of the functions g_j upon x , due to the presence of the factor $\beta(x)^{-1}$, is offset by the existence of the real parameter t , whose values may be chosen favourably.

The same method applies to the consideration of frequencies

$$\nu_N(n; f_1(N-n) + f_2(n) - \alpha(N) \leq z\beta(N))$$

with N an integer, $f_1(0) = 0$, and so on. One may also establish an analogue of Theorem 7 when $\beta(x)$ is everywhere replaced by 1. The details —I have worked them out — are elaborate.

Manuscrit reçu le 30 mai 1988

BIBLIOGRAPHY

- [1] H. Delange.— *Sur les fonctions arithmétiques multiplicatives de module ≤ 1* , Acta Arithmetica XLII (1983), 121–151.
- [2] P.D.T.A. Elliott.— *On connections between the Turán-Kubilius inequality and the Large Sieve : Some applications*, Amer. Math. Soc. Proceedings of Symposia in Pure Math., Vol. 24, Providence, 1973, 77–82.
- [3] P.D.T.A. Elliott.— *Probabilistic Number Theory, I : Mean-Value Theorems, II : Central Limit Theorems*, Grund. der Math. Wiss. 239–240, Springer–Verlag, New York, Heidelberg, Berlin, 1979, 1980.
- [4] P.D.T.A. Elliott.— *A new inequality in the theory of additive arithmetic functions*, Journées Arithmétiques (S.M.F.) Colloque Hubert Delange, 7 et 8 juin 1982, Publications Mathématiques d'Orsay, Univ. de Paris–Sud.
- [5] P.D.T.A. Elliott.— *Arithmetic Functions and Integer Product*, Grund der Math. Wiss 272, Springer–Verlag, New York, Berlin, Heidelberg, Tokyo (1984/85).
- [6] P.D.T.A. Elliott.— *Multiplicative functions on arithmetic progressions*, Mathematika 34 (1987), 199–206.
- [7] P.D.T.A. Elliott.— *Multiplicative functions on arithmetic progressions, II*, Mathematika 35 (1988), 38–50.
- [8] G. Halász.— *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hung. 19 (1968), 365–403.
- [9] A. Hildebrand.— *Multiplicative functions in short intervals*, Canadian J. Math. 39 (1987), 646–672.

- [10] A. Hildebrand.— *An Erdős-Wintner theorem for differences of additive functions*, Preprint, August 26, 1987.
- [11] E. Wirsing.— *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, II, Acta Math. Acad. Sci. Hung. 18 (1967), 411–467.

P.D.T.A. ELLIOTT
Department of Mathematics
Box 426
University of Colorado
Boulder, Colorado 80309
U.S.A.

Séminaire de Théorie des Nombres

Paris 1987-88

ARITHMETIC OF 3 AND 4 BRANCH POINT COVERS

A bridge provided by noncongruence subgroups of $SL_2(\mathbb{Z})$

M.D. FRIED*

Abstract : The method of choice nowadays for achieving a group G as a Galois group of a regular extension of $\mathbb{Q}(x)$ goes under the heading of *rigidity*. It works essentially, only, to produce Galois extensions of $\mathbb{Q}(x)$ ramified over 3 points. The three *rigidity* conditions ((0.1) below) imply that G is generated in a very special way by two elements. Generalization of *rigidity* that considers extensions with any number r of branch points has been around even longer than *rigidity* (§ 5.1). Of the three conditions, the generalization of the *transitivity condition*, 0.1 c), requires only the addition of an action of the Hurwitz monodromy group H_r (a quotient of the Artin braid group). But it also adds a 4th condition that in many situations amounts to asking for a \mathbb{Q} -point on the Hurwitz space associated the data for the generators of G . Theorem 1 below –our main theorem– is that in the case $r = 4$ this is equivalent to finding a \mathbb{Q} -point on a curve derived from a quotient of the upper half plane by a subgroup of $PSL_2(\mathbb{Z})$.

Although the description of this curve is quite explicit, there is one big problem : while it is sometimes a modular curve (§ 4), more often it is not. For this exposition we apply the theory to a simple example that illustrates the main points that arise in the arithmetic of 4 branch point covers (§ 5.2 and 5.3). The group is just A_5 in this case, but this allows us to compare the generalizations of *rigidity* with the historical progenitor of this, Hilbert's method for realizing alternating groups as Galois groups (§ 5.3).

Description of the main results.

The theory of the arithmetic of covers of the sphere arises in many diophantine investigations. The most well known, of course, is a version of the inverse problem of Galois theory : does every finite group G arise as the group of a Galois extension $L/\mathbb{Q}(x)$ with $\bar{\mathbb{Q}} \cap L = \mathbb{Q}$ (i.e. $L/\mathbb{Q}(x)$ is a regular extension) ?

For this lecture we use the dual theory of finite covers $\phi : X \rightarrow \mathbb{P}^1$ of projective nonsingular curves. We shall consistently assume in this notation that \mathbb{P}^1 is identified with $\mathbb{C} \cup \infty = \mathbb{P}^1_x$, a copy of the complex plane uniformized by x , together with a point at ∞ . Such a cover corresponding to the field extension $L/\mathbb{Q}(x)$ would have the property that it is defined over \mathbb{Q} (§ 1.1) and the induced map on the function field level recovers the field extension $L/\mathbb{Q}(x)$. It is valuable, as we shall see in the key example of the paper, to consider covers $\phi : X \rightarrow \mathbb{P}^1$ that may not be Galois.

Branch points and monodromy groups : Denote the degree of such an extension by n . The branch points of the cover are the values of x for which the cardinality of the fiber $\phi^{-1}(x)$ is inferior to n . We will consistently denote the branch points of the cover by x_1, \dots, x_r (almost always assuming that each is a genuine branch point). The key parameter in all investigations is r .

From Riemann's existence theorem, degree n extensions L of $\mathbb{C}(x)$ ramified over r places x_1, \dots, x_r are in one-one correspondence – up to a natural equivalence – with the degree n equivalence classes of connected covers of $\mathbb{P}^1_x \setminus \{x_1, \dots, x_r\}$. These are in turn in one-one correspondence with equivalence classes of transitive permutation representations $T : \pi_1 \rightarrow S_n$ on the set $\{1, 2, \dots, n\}$ where π_1 denotes the fundamental group of $\mathbb{P}^1_x \setminus \{x_1, \dots, x_r\}$. The Galois group of the normal closure of the extension $L/\mathbb{C}(x)$ is identified with the *monodromy group of the cover*, the group $G = T(\pi_1)$.

Rigidity when $r = 3$: Excluding solvable groups, most of the success in achieving groups as Galois groups has come through the arithmetic theory of covers in the case $r = 3$. The apparatus that reduces this to a computation related to a description of the cover through Riemann's existence theorem has been named *rigidity* following Thompson's usage in [T] (the name has the unfortunate aspect of potential confusion with the concept of *rigidifying data*, a tool that does appear in the proofs of results that generalize rigidity. We do only an exposition on *rigidity* so no problems are likely to occur). The *rigidity test* starts with an r -tuple $C = (C_1, \dots, C_r)$ of conjugacy classes of G (§ 1.2). Our version (§ 5.1) includes the faithful permutation representation $T : G \rightarrow S_n$ of the monodromy group of the cover as part of the data of the statement. For the

moment we use a stronger set of conditions on (C, T) than is necessary – it is still more general than used by most practitioners – in order to simplify our exposition on the distinction between $r = 3$ and $r > 3$. A little more notation will help to keep the key statements relatively memorable.

Denote the normalizer of G in S_n by $N_{S_n}(G)$. We denote the subgroup of this that maps $\{C_1, \dots, C_r\}$ into itself (by conjugation) by $N_{S_n}(C)$. The group generated by the entries of $\sigma_1, \dots, \sigma_r$ is $G(\sigma)$. Recall that a conjugacy class of a group is said to be rational if it is closed under putting elements to powers relatively prime to the orders of elements in the class.

If the following hold, then G is the Galois group of a regular extension of $\mathbb{Q}(x)$ ramified at any r points $x_1, \dots, x_r \in \mathbb{Q}$:

- (0.1) a) $G = N_{S_n}(G)$;
 - b) each of the classes C_1, \dots, C_r is rational; and
 - c) G acts transitively by conjugation on the following set of r -tuples
- $$\{(\tau_1, \dots, \tau_r) \mid G(\tau) = G, \tau_i \in C_i \text{ and } \tau_1 \dots \tau_r = 1\}.$$

Condition (0.1 a) is not necessary, but weakening it is no triviality. Dealing with some version of (0.1 a) (as [Fr, 2] illustrates using the theory of complex multiplication) is a necessity. There have been successful attempts to finesse around consideration of (0.1 a) for special cases in Hilbert's original paper [Hi] and in Shih's use of modular curves to realize $PSL_2(\mathbb{Z}/p)$ as a Galois group when one of 2, 3 or 7 is a quadratic nonresidue modulo p [Sh]. Our example in § 5.3 offers a direct approach to weakening (0.1. a).

If the points of x_1, \dots, x_r are to be in \mathbb{Q} , then (0.1. b) is necessary. Our more general statement in § 5.1 (Prop. 5.2 and Prop. 5.4) relaxes the condition on the branch points being in \mathbb{Q} , but the replacement condition will now be an absolute necessity. Finally, no one yet has shed any serious light on relaxation of (0.1 c).

What is surprising is how very often the conditions are satisfied in *the case that* $r = 3$ (e.g., Belyi [Be], Feit [F] among others, many papers of Malle and

Matzat some of which are included in [Ma,1], and Thompson [T]). They are almost never satisfied when r exceeds 3 (e.g. no example has been found when G is a noncyclic simple group).

Suppose that even every finite *simple* group is generated by three elements τ_1, τ_2, τ_3 that give conjugacy classes that satisfy the necessary condition analogous to (0.1 b) and the mysterious condition (0.1 c). If all that were of concern were the inverse Galois theory problem, then it *might* make sense to concentrate all research efforts on relaxation of condition (0.1 a). The hypotheses, however, of these statements don't hold : generators of groups with such handy properties don't always exist; and few of the other applications allow the investigator to be so picky about the choice of generators (as in [DFr] and [FR,2 and 3], we are referring to applications to Hilbert's irreducibility theorem and Siegel's theorem, ranks of elliptic curves and values of rational functions over finite fields).

Generalizations of rigidity for $r > 3$: Fortunately there are generalizations of *rigidity* that hold quite frequently for $r \geq 4$ ([Fr,1 : Theorem 5.1] and [Fr,3 : Theorem 1.5]). Matzat has used versions of these [Ma,1] to realize several simple groups as Galois groups (among them the Matthew group of degree 24 [Ma,2]). Increasing r improves the possibility of satisfying all three of the conditions (0.1), as explained in [Fr,2; Remark 2.2]. But there are two serious points. First : the generalization of (0.1 c) (condition 5.5 c)) works by asking for transitivity of a group that contains the *Hurwitz monodromy group* H_r of degree r (a quotient of the Artin braid group; (§ 3.1). The calculations for this applied to one of the classical sequences of simple groups can be quite formidable (e.g., Ex. 2.3 of [Fr,3] to realize all of the A_n 's as Galois groups of 4 branch point covers of \mathbb{P}^1). For any one group, Matzat, for example, has put together a computer program to test this transitivity, but experience with the calculations is still more of an art than a science.

A later paper will consider the series of groups

$$PSL_2(\mathbb{Z}/p), \quad p \equiv \pm 1 \pmod{24}, \text{ and } 7 \text{ a quadratic nonresidue modulo } p.$$

For the other primes this is Shih's result [Sh]. While the calculations aren't quite complete, it doesn't seem that it is possible to achieve the groups of this series with covers of fewer than 4 branch points. And for each of these primes there does exist (C, T) with $r = 4$ satisfying the analog of the 3 conditions of (0.1)

(conditions 5.5. a–c). Why this doesn't quite finish the job of realizing these groups as Galois groups comes from our second point. The analog of (0.1) includes a condition d) which we now explain.

Parametrization of the covers associated to (C, T) : The collection of equivalence classes of covers associated to (C, T) is naturally parametrized by the associated *Hurwitz space* $\mathcal{H}(C)$ (with T understood from the context). This arises as a cover of $\mathbb{P}^r \setminus D_r$, coming from a representation of the Hurwitz monodromy group (§ 3.2). Here D_r is the classical discriminant locus in the respective spaces. We note this existence of the Noether cover $(\mathbb{P}^1)^r \rightarrow \mathbb{P}^r$, Galois with group S_r . When the analogs of the conditions 0.1) hold, $\mathcal{H}(C)$ (with its maps to \mathbb{P}^r) is defined over \mathbb{Q} . The extra condition d) for $r > 3$ demands that there be a \mathbb{Q} -point on a connected component of the pullback of $\mathcal{H}(C)$ to $(\mathbb{P}^1)^r$. Below we refer to this space as $\mathcal{H}(C)'$. If all of the conditions (0.1) hold (with the Hurwitz monodromy action added to (0.1 c)), then condition d) is necessary (and sufficient) when the conjugacy classes in C are distinct.

The problem with this is clear : the space $\mathcal{H}(C)$ is a production of such great abstraction that the diophantine reduction seems impossible to effect. The main result of this paper is an alternative description of (5.5 d) in the case that $r = 4$.

THEOREM 1 (special case of Conclusion 4.2). *There is a curve cover $\psi_C' : Y_C' \rightarrow \mathbb{P}^1$ ramified over just $0, 1, \infty$, such that $\mathcal{H}(C)'$ has a \mathbb{Q} -point if and only if*

$$Y_C'(\mathbb{Q}) - \psi_C'^{-1}(0, 1, \infty)$$

is nonempty. Furthermore, Y_C' is identified with the projective normalization of a quotient of the upper half plane by a subgroup H_C of $PSL_2(\mathbb{Z})$ (of finite index), in such a way that it identifies the covered copy of \mathbb{P}^1 with the classical λ -line \mathbb{P}_λ^1 . Finally, there is an explicit description of the branch cycles of the cover ψ_C' given by an action of the Hurwitz monodromy group H_4 .

There is an analogous curve cover $\psi_C \rightarrow \mathbb{P}^1$ in which \mathbb{P}^1 is identified with the classical j -line. Conclusion 4.2 is more general than Theorem 1 in that the former uses this cover as a replacement for that with Y_C . This gives a necessary statement replacing condition (5.5 d) even when the 4 conjugacy classes of C are not distinct (when they are distinct, $Y_C = Y_{\bar{C}}$).

Congruence and noncongruence subgroups : A part of the proof of Conclusion 4.2 consists of showing that special values of C , Y_C can be identified with the classical curve $Y_0(n)$ that arises from the quotient of the upper half plane by the subgroup called $\Gamma_0(n)$. Thus modular curves arise. But in general the curves Y_C belong to noncongruence subgroups of $PSL_2(\mathbb{Z})$. Indeed, recently Diaz, Donagi and Harbater [DDH] have actually shown that *every* curve defined over the algebraic closure of \mathbb{Q} occurs as Y_C for some choice of C . Their choice, however, of C has nothing to do with the classical modular curve arithmetic.

An example where $G = A_5$ appears in [FrT] to show how one might investigate (for the inverse Galois theory problem) the infinitely many totally nonsplit extensions of any given finite simple group. Here we use it for three straight forward reasons : to show in practice the distinction between the curves Y_C and $Y_{\bar{C}}$; to consider by example weakenings of condition (0.1 a); and to compare our results with the beginnings of this subject in [Hi].

1.– Basic data for covers.

One way to give an (irreducible) algebraic curve is to give a polynomial (irreducible) in two variables $f(x,y) \in \mathbb{C}[x,y]$ where \mathbb{C} denotes the complex numbers. Then the curve is

$$\{x,y) | f(x,y) = 0\} \stackrel{\text{def}}{=} X.$$

This curve, however, may have singular points : points $(x_0, y_0) \in X$ for which $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ evaluated at (x_0, y_0) are both 0. Furthermore, we are missing the points at infinity obtained by taking the closure of X in the natural copy of projective 2-space \mathbb{P}^2 that contains the affine space \mathbb{A}^2 with variables x and y (and these points, too, might be singular).

The x -coordinate projection : After this we assume that our algebraic curves X don't have these defects; they will be projective nonsingular curves, so we may not be able to regard them as given by a single polynomial in 2-space. But the essential ingredient of this presentation, represented by the x -coordinate, will still be there.

That is, we have a covering map

$$\{x,y) | f(x,y) = 0\} \rightarrow \mathbb{P}_x^1 \stackrel{\text{def}}{=} \mathbb{C} \cup \infty \text{ or } X \rightarrow \mathbb{P}_x^1$$

given by projection of the point (x,y) onto its first coordinate. When the context is clear we will identify \mathbb{P}_x^1 with \mathbb{P}^1 . We use this extra decoration by coordinate when it clarifies the context. The *monodromy group* of this cover is defined to be the Galois group G of the Galois closure of the field extension $\mathbb{C}(X)/\mathbb{C}(x)$ where $\mathbb{C}(X)$ denotes the quotient field of the ring $\mathbb{C}[x,y]/(f(x,y))$. In the sequel we will denote this Galois closure by $\widehat{\mathbb{C}(X)}$ or by the geometric version \hat{X} , the smallest Galois cover of \mathbb{P}_x^1 that factors through $X \rightarrow \mathbb{P}_x^1$.

Note that in this situation G automatically comes equipped with a transitive permutation representation $T: G \rightarrow S_n$. Denote the stabilizer in G of an integer (say, 1) by $G(T)$. Also, T is *primitive* (i.e., there are no proper groups between G and $G(T)$) if and only if there are no proper fields between $\mathbb{C}(X)$ and $\mathbb{C}(x)$ (equivalently, no proper covers fitting between $X \rightarrow \mathbb{P}_x^1$).

1.1.— Branch points and the classical $PSL_2(\mathbb{C})$ action : The first parameter for dealing with covers is the number r of branch points of a given cover : the number of distinct points x of \mathbb{P}^1 for which the fiber of X above x has fewer actual points than the degree of the map. We deal not with one polynomial at a time, but rather with a parametrized family of them. But clearly it is natural to assume that all members of the family have the same number of branch points. The Hurwitz monodromy groups H_r are the key for putting these covers into families. In § 2 for $r = 3$ and in § 3 for $r = 4$ we introduce these groups and their basic properties. Although § 2.1 uses nothing more than the transitive action of $PSL_2(\mathbb{C})$ on distinct triples of points of \mathbb{P}_x^1 , the notation used here is the main tool for the rest of the paper.

In classical algebraic geometry it has become a habit and a tradition to regard the parameter variety \mathcal{H} for a family of covers with r branch points as

the source for a quotient $\mathcal{H}/PSL_2(\mathbb{C})$. Consider covers $\phi_i : X_i \rightarrow \mathbb{P}_x^1$, $i = 1, 2$, associated to two points $m_1, m_2 \in H$. The action is the one that equivalences m_1 and m_2 if and only if there exists $\alpha \in PSL_2(\mathbb{C})$ such that $\alpha \circ \phi_1 = \phi_2$. In § 2.3–2.4 we display the arithmetic and geometric subtleties that would make it a disaster to do this even in the case of families of 3 branch point covers. Here are some of the negatives for forming the quotient frivolously :

- (1.1) a) there are technical difficulties in giving $\mathcal{H}/PSL_2(\mathbb{C})$ the structure of an algebraic variety and in visualizing its properties;
- b) taking the quotient often destroys subtle finite group actions that are valuable for using the parameter space as a moduli space;
- c) there are few quotable sources on the enriched family of covers structure; and
- d) forming the quotient often wipes out the possibility of dealing with problems of considerable consequence.

Our first 3 branch point example in § 2.3 should go a long way to make our case for (1.1 d). It is the other points, of course, that cause the lengthy preambles to this subject with so many down to earth applications.

1.2.— Riemann's existence theorem and Nielsen classes : The classical discussion of maps of degree n from curves of genus g to projective 1-space gives us data for a natural collection of covers. We call the data a *Nielsen class* (below), and it is this that we shall regard as being fixed in the consideration of any family of covers.

Suppose that we are given a finite set $\mathbf{x} = \{x_1, \dots, x_r\}$ of distinct points of \mathbb{P}_x^1 . For any element $\sigma \in S_n^r$ denote the group generated by its coordinate entries by $G(\sigma)$. Consider $\phi : X \rightarrow \mathbb{P}_x^1$, ramified only over \mathbf{x} up to the relation that regards $\phi : X \rightarrow \mathbb{P}_x^1$ and $\phi' : X' \rightarrow \mathbb{P}_x^1$ as equivalent if there exists a homeomorphism $\lambda : X \rightarrow X'$ such that $\phi' \circ \lambda = \phi$. These equivalence classes are in one-one correspondence with

$$(1.2) \{ \sigma = (\sigma_1, \dots, \sigma_r) \in S_n^r \mid \sigma_1 \dots \sigma_r = 1, G(\sigma) \text{ is a transitive subgroup of } S_n \}$$

modulo the relation that regards σ and σ' as equivalent if there is $\gamma \in S_n$ with $\gamma\sigma\gamma^{-1} = \sigma'$. This correspondence goes under the heading of Riemann's existence theorem [Gro]. The collection of ramified points x will be called the branch points of the cover $\phi : X \rightarrow \mathbb{P}_x^1$. (In most practical situations we shall mean that there truly is ramification over each of the points x_i , $i = 1, \dots, r$).

Riemann's existence theorem for families : Riemann's existence theorem generalizes through a combinatorial group situation to consider the covers above, not one at a time, but as topologized collections of families. That is, the branch points x run over the set $(\mathbb{P}^1)^r \setminus \Delta_r$ with Δ_r the r -tuples with two or more coordinates equal. In § 2 and § 3, respectively, we will introduce the coordinates for these families in the cases $r = 3$ and 4.

Suppose that $T : G \rightarrow S_n$ is any faithful transitive permutation representation of a group G . Let $C = (C_1, \dots, C_r)$ be an r -tuple of conjugacy classes from G . It is understood in our next definition that we have fixed the group G before introducing conjugacy classes from it.

DEFINITION 1.1. *The Nielsen class of C is $Ni(C) \stackrel{\text{def}}{=}$*

$$\{r \in G^T \mid G(r) = G \text{ and there is } C \in S_r \text{ with } \tau_{(i)}\beta \in C_i, i = 1, \dots, r\}.$$

Relative to canonical generators $\bar{\sigma}_1, \dots, \bar{\sigma}_r$ of the fundamental group $\pi_1(\mathbb{P}_x^1 - x, x_0)$, we say that a cover ramified only over x is in $Ni(C)$ if the classical representation of the fundamental group sends the respective canonical generators to an r -tuple $\sigma \in Ni(C)$.

2.— Families for $r = 3$ and the Hurwitz monodromy group H_3 .

2.1.— Complete families for $r = 3$ from transport of structure : It is clear that the fundamental group of $\mathbb{P}^3 \setminus D_3$ is of order 12 once it is shown that the fundamental group of $(\mathbb{P}^1)^3 \setminus \Delta_3$ is of order 2. But for any point $(x_1, x_2, x_3) = x$ there is a unique element $\beta = \beta_x \in PSL_2(\mathbb{C})$ that maps $(0, 1, \infty)$ to x :

$$\beta(0) = x_1, \beta(1) = x_2, \text{ and } \beta(\infty) = x_3.$$

Thus $\mathbb{P}^3 \setminus \Delta_3$ is a principal homogeneous space for $PSL_2(\mathbb{C})$. They therefore have the same fundamental groups. As is well known, $SL_2(\mathbb{C})$ has trivial fundamental group. Thus the cover $SL_2(\mathbb{C}) \rightarrow PSL_2(\mathbb{C})$ displays the representative permutation representation.

Below we will use this in the manner of [Fr 1, p. 42]. Let $\phi : X \rightarrow \mathbb{P}_x^1$ be any cover with three distinct branch points and order these as $(x_1^0, x_2^0, x_3^0) = \mathbf{x}^0$. Denote $(\mathbb{P}^1)^3 \setminus \Delta_3$ (resp., $\mathbb{P}^3 \setminus D_3$) by \mathcal{U}^3 (resp., \mathcal{U}_3). Also, denote the natural map $PSL_2(\mathbb{C}) \rightarrow \text{Aut}(\mathbb{P}_x^1)$ by \mathcal{A} . Form an irreducible family of covers from this data by transport of structure :

$$(2.1) \quad \begin{array}{ccccc} \mathcal{I} & \xrightarrow{\Phi} & \mathcal{U}^3 \times \mathbb{P}_x^1 & \xrightarrow{pr_1} & \mathcal{U}^3 \\ \downarrow & & \downarrow & & \downarrow \\ PSL_2(\mathbb{C}) \times X & \xrightarrow{(Id, \mathcal{A}) \circ Id \times \phi} & PSL_2(\mathbb{C}) \times \mathbb{P}_x^1 & \xrightarrow{pr_1} & PSL_2(\mathbb{C}), \end{array}$$

where the down map on the far right takes \mathbf{x} to $\beta_{\mathbf{x}} \circ \beta_{\mathbf{x}^0}^{-1}$. The down maps indicate that the usual *family* notation (i.e. \mathcal{I} denotes a *total* space) for the items in the bottom row is given in the top row. That is, with the identification of $\mathcal{U}^3 \times \mathbb{P}_x^1$ and $PSL_2(\mathbb{C}) \times \mathbb{P}_x^1$ based on \mathbf{x}^0 , \mathcal{I} is the fiber product in the leftmost square of diagram (2.1). For each $\mathbf{x} \in \mathcal{U}^3$ the points of \mathcal{I} over $\mathbf{x} \times \mathbb{P}_x^1$ give a cover of \mathbb{P}_x^1 equivalent to the cover $\beta_{\mathbf{x}} \circ \beta_{\mathbf{x}^0}^{-1} \circ \phi : X \rightarrow \mathbb{P}_x^1$.

Let $Ni(C)$ be the Nielsen class and G the monodromy group of $\phi : X \rightarrow \mathbb{P}_x^1$. Then \mathcal{U}^3 is the space $\mathcal{H}(C)_T$ (cf. § 3.2) much of the time. Indeed, consider the straight absolute Nielsen classes of C :

$$SNi(C) = \{\sigma \in Ni(C) \mid \sigma_i \in C_i, i = 1, 2, 3\}.$$

The normalizer of G in S_n , $N_T(G)$ acts by conjugation on the r -tuples of elements in G . The subset that stabilizes $Ni(C)$ is denoted by $N_T(C)$. Form the quotient of $SNi(C)$ by the subgroup of $N_T(C)$ that leaves this set stable to

get the absolute straight Nielsen classes, $SNi(C)_T^{ab}$. Note that the quotient of H_3 by the subgroup stabilizing each element of $SNi(C)_T^{ab}$ is itself a quotient of S_3 (and therefore is of order 1, 2, 3 or 6).

PROPOSITION 2.1. *In the notation of section 2.1 assume that*

$$(2.2) \quad |SNi(C)_T^{ab}| = 1.$$

Thus H_3 acts on $Ni(C)_T^{ab}$ through a transitive permutation representation of S_3 . Then, as covers of \mathcal{U}_3 , $\mathcal{H}(C)$ is isomorphic to \mathcal{U}^3 (resp., \mathcal{U}_3) if and only if this is the regular representation (resp., the trivial representation).

2.2.— Most 3 branch point families derive from transport of structure : A version of Proposition 2.1 appears in [BFr,1; § 4]. This analyzes when there exists a total representing family like that of (2.1) in the case when either (2.2) doesn't hold or when the action of H_3 isn't through the regular representation of S_3 . Below we will use a converse. That is, suppose that

$$\mathcal{I} \xrightarrow{\Phi} \mathcal{H} \times \mathbb{P}_x^1 \xrightarrow{pr_1} \mathcal{H}$$

is any family of 3 branch point covers with \mathcal{I} and \mathcal{H} irreducible nonsingular complex manifolds. We assume that all morphisms are smooth. Also, for each $m \in \mathcal{H}$, restriction of $pr_1 \circ \Phi$ to the fiber \mathcal{I}_m gives a 3 branch point cover $\mathcal{I}_m \rightarrow \mathbb{P}_x^1$.

As above consider the following natural maps : $\mathcal{U}^3 \rightarrow \mathcal{U}_3$; and $\Psi_{\mathcal{H}} : \mathcal{H} \rightarrow \mathcal{U}_3$ by $m \in \mathcal{H}$ goes to the unordered collection of branch points of the corresponding cover. Any connected component \mathcal{H}' of the fiber product $\mathcal{H} \times \mathcal{U}^3$ has over it a connected component \mathcal{I}' that gives a family of 3 branch point covers. Suppose that $m' \in \mathcal{H}'$, that x' is the image of projection of m' on \mathcal{U}^3 , and that $\mathcal{I}'_{m'} = X \rightarrow \mathbb{P}_x^1$ is the corresponding cover. Apply the

transport of structure construction to canonically form a family of three branch

point covers over \mathcal{U}^3 having the fiber $X \rightarrow \mathbb{P}_x^1$ over x' . Then take a connected component of its pullback to \mathcal{H}' .

PROPOSITION 2.2. *Consider an irreducible family \mathcal{F}' of 3 branch point covers over \mathcal{H}' which has $\mathcal{I}_{m'} = X \rightarrow \mathbb{P}_x^1$ as a fiber. Then all covers $X' \rightarrow \mathbb{P}_x^1$ that appear in such a family have X' analytically isomorphic to X . Furthermore all such families are in one-one correspondence with the elements of the set*

$$\text{Hom}(\pi_1(\mathcal{H}', m'), \text{Aut}(X/\mathbb{P}_x^1)).$$

In particular :

$$(2.3) \quad \text{if } \mathcal{H}' = \mathcal{U}^3 \text{ and } (|\text{Aut}(X/\mathbb{P}_{x'}^1)|, 2) = 1,$$

then \mathcal{F}' is uniquely determined by a single member of the family.

In this case the total space \mathcal{I}' of the family is analytically isomorphic to an open subset of $X \times (\mathbb{P}^1)^3$.

Proof : Form a locally constant sheaf of groups $\mathcal{A}\mathcal{U}\mathcal{I}(X/\mathbb{P}_x^1)$ on \mathcal{H}' as follows. For $m \in \mathcal{H}'$ there is a unique element $\beta \in \text{PSL}_2(\mathbb{C})$ that acts on \mathbb{P}_x^1 to map the (ordered) branch points of $\phi : \mathcal{I}_{m'} = X \rightarrow \mathbb{P}_x^1$ to those of $\mathcal{I}_{m'} \rightarrow \mathbb{P}_x^1$. From the transport of structure argument this last cover is equivalent to the cover $\beta \circ \phi : X \rightarrow \mathbb{P}_x^1$. Thus identify $\text{Aut}(X/\mathbb{P}_x^1)$ to $\text{Aut}(\mathcal{I}_{m'}/\mathbb{P}_x^1)$ by the identity map : an element $\gamma \in \text{Aut}(X/\mathbb{P}_x^1)$ has the property that $\phi \circ \gamma = \phi$, and this automatically implies that $\beta \circ \phi \circ \gamma = \beta \circ \phi$.

A well-known theory identifies bundles over \mathcal{H}' with constant fiber X and transition functions in $\mathcal{A}\mathcal{U}\mathcal{I}(X/\mathbb{P}_x^1)$ with the elements of $\text{Hom}(\pi_1(\mathcal{H}', m'), \text{Aut}(X/\mathbb{P}_x^1))$ (e.g., [Gu; p. 184–189]). If the groups $\pi_1(\mathcal{H}', m')$ and $\text{Aut}(X/\mathbb{P}_x^1)$ have relatively prime order this set consists of just one element. This happens if (2.3) holds. The family in this case must be the very one that we formed by transport of structure. \square

2.3.— Arithmetic constraints in placing branch points : we do an example. Here is the data for the Nielsen class : $r = 3$; $G = \mathbb{Z}/5 \times^S (\mathbb{Z}/5)^*$; $T: G \rightarrow S_5$ is the standard degree 5 affine action on the affine line over $\mathbb{Z}/5$; and C_1 is the class of (0,2), C_2 is the class of (0,3) and C_3 is the class of (1,1). Representatives $\sigma \in Ni(C)_T^{ab}$ of the Nielsen class are easy to write out. First consider those where $\sigma_i \in C_i$, $i = 1, 2, 3$. Up to conjugation by elements of G there's only one : $((0,2),(2,3),(1,1))$. Thus there are 6 total elements of $Ni(C)_T^{ab}$. Suppose that $X \rightarrow \mathbb{P}_x^1$ is a cover in this Nielsen class where the branch points are x_1, x_2, x_3 , corresponding in order to the three conjugacy classes as we have given them. The proof of next lemma is called the *branch cycle argument* in [Fr,1; § 5].

LEMMA 2.3. *If x_1, x_2, x_3 are in a field F disjoint from $\mathbb{Q}(i)$, then every field of definition of (X, ϕ) that contains x_1, x_2, x_3 also contains $\mathbb{Q}(i)$. In particular, (X, ϕ) can't be defined over \mathbb{Q} if the branch points are $0, 1, \infty$.*

Proof : For simplicity assume F to be inside $\bar{\mathbb{Q}}$, an algebraic closure of the rationals. Let $\hat{\phi}: \hat{X} \rightarrow \mathbb{P}_x^1$ be the Galois closure of the cover, and suppose that \hat{F} is a field of definition of $(\hat{X}, \hat{\phi})$ (note the momentary switch below in notation from subscript i to subscript j). Then giving data about inertial groups of points $\hat{m}_i \in \hat{X}$ lying over x_i , $i = 1, 2, 3$, is tantamount to giving an embedding

$$\psi_j: \hat{F}(\hat{X}) \rightarrow \hat{F}(i)((x-x_j)^{\frac{1}{4}}), \quad j = 1, 2, \quad \text{and} \quad \psi_j: \hat{F}(\hat{X}) \rightarrow \hat{F}(e^{\frac{2\pi i}{5}})((x-x_j)^{\frac{1}{5}}), \quad j = 3$$

(ordinarily we could only say that the embedding was into the power series fields over $\bar{\mathbb{Q}}$, but the simplicity of this situation allows considerable precision).

Also, the inertia groups are given by the restriction of the automorphisms $\bar{\sigma}_j$

that respectively take $(x-x_j)^{\frac{1}{k}}$ to $e^{\frac{2\pi i}{k}}(x-x_j)^{\frac{1}{k}}$, with k the inertia index corresponding to j .

If we assume that F does not contain $\mathbb{Q}(i)$, then there exists an element $\tau \in G(\bar{\mathbb{Q}}/F)$ with the property that $\tau(i) = -i$. Act on the Puiseux expansions about x_1 by acting trivially on $(x-x_1)^{\frac{1}{4}}$ and extend the action by applying τ to the coefficients. With no loss we may assume that the restriction of τ to the

embedding of $F(X)$ is trivial. But an application of $\tau^{-1} \circ \bar{\sigma}_1 \circ \tau \circ \psi_1$ to the conjugate of an element α of $F(X)$ whose initial Puiseux expansion term (around x_1) is $i^t(x-x_1)^{\frac{1}{4}}$ gives an element whose initial expansion is $i^{t-1}(x-x_1)^{\frac{1}{4}}$. Since the effect of this on $F(\hat{X})$ must be conjugate to the effect of $\bar{\sigma}_1 \circ \psi_1$, conclude that σ_1^{-1} is conjugate within the group G to σ_1 . This is a contradiction. \square

2.4.— Resolution of the subtleties when $r = 3$. One must not assume that the little solvable group of Lemma 2.3 is difficult to achieve as a Galois group of a regular extension of $\mathbb{Q}(x)$. The problem is only that we took the branch points to be in \mathbb{Q} . We explain this further.

Let $X \rightarrow \mathbb{P}_x^1$ be the cover of Lemma 2.3. Consider an element $\lambda \in (\bar{\mathbb{Q}}/\mathbb{Q})$ whose restriction to $\mathbb{Q}(i)$ is the generator of $G(\mathbb{Q}(i)/\mathbb{Q})$. Denote the effect of applying λ to the coefficients of the equations for (X, ϕ) by a subscript λ . The argument of Lemma 2.3 shows that $\phi^\lambda : X^\lambda \rightarrow \mathbb{P}_x^1$ isn't equivalent to $X \rightarrow \mathbb{P}_x^1$. But it also shows that the former cover is the only one in the Nielsen class that has the branch point 0 (resp., 1) associated to the conjugacy class C_2 (resp., C_1). Thus for some $\phi : X \rightarrow X'$ we have a commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & X^\lambda \\ \downarrow \phi & & \downarrow \phi^\lambda \\ \mathbb{P}_x^1 & \longrightarrow & \mathbb{P}_x^1 \end{array}$$

where ψ^0 is the linear fractional transformation that takes 1 to 0, 0 to 1, and leaves ∞ fixed.

Suppose that we take x_1 and x_2 to be i and $-i$ (or more generally conjugates in the field extension $\mathbb{Q}(i)$). Then we see that $\phi^\lambda : X^\lambda \rightarrow \mathbb{P}_x^1$ is equivalent to $X \rightarrow \mathbb{P}_x^1$. It is easy now, with the *Weil cocycle condition* (see [Fr, 1; p. 34–35], [Sh; Part 1] or [We]), to conclude that both covers are equivalent to a cover defined over \mathbb{Q} . Indeed, at the level of function fields there is a canonical exact sequence of Galois groups :

$$(2.4) \quad 1 \rightarrow G(\mathbb{C}(\hat{X})/\mathbb{C}(x)) \rightarrow \widehat{G(\mathbb{Q}(X)/\mathbb{Q}(x))} \rightarrow G(\hat{\mathbb{Q}}/\mathbb{Q}) \rightarrow 1,$$

where $\widehat{\mathbb{Q}(X)}$ is the Galois closure of the extension $\mathbb{Q}(X)/\mathbb{Q}$ and $\widehat{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} in $\widehat{\mathbb{Q}(X)}$. The first group — which is G — is identified with the same group obtained by replacing \mathbb{C} by $\widehat{\mathbb{Q}}$ and the map from the middle to the end is restriction of elements to the subfield $\widehat{\mathbb{Q}}$. Thus, the middle group is a subgroup of the normalizer of G in S_n . Since this normalizer is just G itself in this example, conclude that $\widehat{\mathbb{Q}} = \mathbb{Q}$ and the group G has been realized as a Galois group over \mathbb{Q} . This less than astounding example is here to aid with the example of § 5.3.

3.— Families for $r = 4$ and the Hurwitz monodromy group H_4

3.1.— The Hurwitz monodromy group H_r . Generators Q_1, \dots, Q_{r-1} of H_r satisfy the following relations :

- (3.1 a) $Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}, \quad i = 1, \dots, r-2;$
- b) $Q_i Q_j = Q_j Q_i, \quad 1 \leq i < j-1 \leq r-1;$ and
- c) $Q_1 Q_2 \dots Q_{r-1} Q_{r-1} \dots Q_1 = 1.$

Relations (3.1 a) and b) alone give the Artin braid group $B(r)$. It is relation (3.1 c) that indicates involvement with projective algebraic geometry. The Artin braid group is the fundamental group of $\mathbb{A}^r - D_r$, while the Hurwitz monodromy group is the fundamental group of $\mathbb{P}^r - D_r$. Here D_r is the classical discriminant locus in the respective spaces. Embed \mathbb{A}^r in \mathbb{P}^r by regarding \mathbb{A}^r as the space of monic polynomials of degree r and \mathbb{P}^r as the space of all nonzero polynomials of degree at most r up to the equivalence by multiplication by a nonzero constant. This embedding gives the natural surjective homomorphism from the braid group to the monodromy group.

This all fits together in a commutative diagram of fundamental groups induced from a geometric diagram :

$$(3.2) \quad \begin{array}{ccc} \mathbb{A}^r \setminus \Delta_r & \longrightarrow & (\mathbb{P}^1)^r \setminus \Delta_r \\ \Psi_r \downarrow & & \downarrow \Psi_r \\ \mathbb{A}^r \setminus \Delta_r & \longrightarrow & \mathbb{P}^r \setminus D_r \end{array}$$

where the map Ψ_r can be regarded as the quotient action of S_r acting as permutations on the coordinates of $(\mathbb{P}^1)^r$. The respective fundamental groups in the upper row of (3.2) will be called here the *straight* Artin braid and Hurwitz monodromy groups :

$$(3.3) \quad SH_r = \pi_1((\mathbb{P}^1)^r \setminus \Delta_r, \mathbf{x}^0) \quad \text{is the kernel of the homomorphism} \\ \Psi_r^*: H_r \rightarrow S_r \quad \text{that maps } Q_i \text{ to } (i \ i+1), \quad i = 1, \dots, r.$$

3.2.— Hurwitz action gives a moduli space. From the relations we compute that H_r acts on the absolute Nielsen classes by extension of the following formula :

$$(3.4) \quad (\tau_1, \dots, \tau_r)Q_i = (\tau_1, \dots, \tau_{i-1}, \tau_i \tau_{i+1} \tau_i^{-1}, \tau_i, \tau_{i+2}, \dots, \tau_r).$$

In the notation of Definition 1.1 we say that $\phi_T: X_T \rightarrow \mathbb{P}_x^1$ is in the absolute Nielsen class $Ni(C)_T^{ab}$.

Any permutation representation of a fundamental group defines a cover of the space. In this case we denote the cover corresponding to the Nielsen class by

$$\Psi(C): \mathcal{H}(C)_T \rightarrow \mathbb{P}^r \setminus D_r.$$

That is, an absolute Nielsen class $Ni(C)_T^{ab}$ defines a moduli space $\mathcal{H}(C)_T$ of covers $\phi_T: X_T \rightarrow \mathbb{P}_x^1$ of degree equal to $\deg(T)$ in that Nielsen class. In this situation this means that each point $m \in \mathcal{H}(C)_T$ corresponds to exactly one equivalence class of covers of $Ni(C)_T^{ab}$ [Fr,1; § 4]. A representative cover $\phi_m: X_m \rightarrow \mathbb{P}_x^1$ has coordinates $x \in (\mathbb{P}^1)^r$ as an ordering of its branch points where $\Psi_r(x) = \Psi(C)(m)$.

PROPOSITION 3.1. *The algebraic set $\mathcal{H}(C)_T$ is irreducible if and only if it is connected and this holds if and only if H_r is transitive on $Ni(C)_T^{ab}$.*

Proof : Since $\Psi(C)$ is unramified and $\mathbb{P}^r \setminus D_r$ is nonsingular, so is $\mathcal{H}(C)_T$.

Thus it is irreducible as an algebraic set (i.e., an open subset of some projective variety which is defined by a prime ideal in the ring of polynomials in the ambient projective space) if and only if it is connected. From the theory of fundamental groups this last property is equivalent to the transitivity of the permutation representation. \square

3.3.— H_4 as a $PSL_2(\mathbb{Z})$ extension. For applications we really want to know many explicit things about $\mathcal{H}(C)_T$, and about the function fields of its irreducible components. Unfortunately, not only is H_r a seemingly complicated group, but it isn't clear how knowing about H_r tells that much about $\mathcal{H}(C)_T$. Indeed, that is a complicated story that has much left in the telling. One can imagine, however, that if it were possible to compare $\mathcal{H}(C)_T$ with a classical heavily studied variety, then the very act of comparison would shed new light on both $\mathcal{H}(C)_T$ and the classical variety with which it is compared. This subsection and § 4 do just that, using a comparison with modular curves, when $r = 4$. As a preliminary we explain the *easy* case $r = 3$: a discussion that is totally compatible with our construction of the 3 branch point families related to diagram (2.1).

For simplicity in this beginning discussion assume that $\mathcal{H}(C)_T$ is connected. Also, here we take the field of definition to be \mathbb{C} . Denote the field of meromorphic functions on $\mathcal{H}(C)_T$ by $F_C = \mathbb{C}(\mathcal{H}(C)_T)$ and denote the subfield of $\mathbb{C}(x_1, \dots, x_r) = \mathbb{C}(\mathbf{x})$ invariant under the natural action of S_r by $\mathbb{C}(\mathbf{x})^{S_r} \stackrel{\text{def}}{=} \mathbb{C}(\mathbf{x}^*)$. That is, \mathbf{x}^* is the r -tuple of symmetric functions in \mathbf{x} . We may regard F_C as a field of definition of a generic cover $\phi : X \rightarrow \mathbb{P}_x^1$ of the family. In particular, F_C includes the coefficients of the curve X and of the graph of the covering map ϕ .

Also, $F_C/\mathbb{C}(\mathbf{x}^*)$ is naturally a field extension of degree equal to $|Ni(C)_T^{ab}|$. When $r = 3$, in considerations over \mathbb{C} , F_C is actually contained in $\mathbb{C}(\mathbf{x})$. This doesn't make arithmetic questions about 3 branch point covers trivial – not at all. But it makes them immensely easier than similar questions

when $r \geq 4$. Of course this all gets down to the sharp transitivity of $PSL_2(\mathbb{C})$ on distinct ordered triples from \mathbb{P}^1_x .

DEFINITION 3.2. *The dicyclic group of order $4n$ is characterized by having generators τ_1, τ_2 with $\text{ord}(\tau_1) = 2n$, $\text{ord}(\tau_2) = 4$, $\tau_2^{-1}\tau_1\tau_2 = \tau_1^{-1}$ and $\tau_2^2 \in \langle \tau_1 \rangle$.*

Here are the facts about H_3 in terms of the generators Q_1 and Q_2 :
 $Q_1 Q_2 = \tau_1$ and $Q_1 Q_2 Q_1 = \tau_2$ are generators of H_3 . From relation (3.1 a),
 $\tau_2^2 = \tau_1^3$. Thus :

- (3.5 a) $\text{ord}(\tau_1) = 6$ and $\text{ord}(\tau_2) = 4$; and
 b) H_3 is the dicyclic group of order 12.

In the case $r = 4$ we rarely expect to have $F_C \subset \mathbb{C}(x)$. It appears, however, to be far from hopeless to make things explicit in this case.

Let $\mathcal{Q} = \langle (Q_1 Q_2 Q_3)^2, Q_1 Q_3^{-1} \rangle$.

THEOREM 3.3. *In the case that $r = 4$ the following hold :*

- (3.6 a) H_4 contains precisely one involution;
 b) $\mathcal{Q} \triangleleft H_4$ and \mathcal{Q} is the quaternion group of order 8;
 c) $H_4/\mathcal{Q} \cong PSL_2(\mathbb{Z})$; and
 d) H_4 has precisely two conjugacy classes of subgroups isomorphic to $SL_2(\mathbb{Z})$.

This is due to John Thompson who has continued to investigate interpretations of the quaternion group kernel of H_4 [FrT].

4.– Modular curves and H_4

4.1.– Geometric interpretation of H_4 using $r = 3$. Suppose that $r = 4$ and that H' is a subgroup of H_4 of finite index. This gives an unramified cover

$$\Psi_{H'} : \mathcal{H}_{H'} \rightarrow \mathbb{P}^4 \setminus D_4$$

associated to H' as in § 3.2. Consider the pullback \mathcal{H}' of the fiber product $\mathcal{H} \times_{\mathcal{U}_3} \mathcal{U}^3$ that occurred at the outset of § 2.2. We perform the analogous operation here to consider a connected component \mathcal{H}' of the pullback of $\mathcal{H}_{H'}$ to $(\mathbb{P}^1)^4 \setminus \Delta_4$. If we identify the four copies of \mathbb{P}^1 , respectively, with \mathbb{P}^1_x (i.e., $x = x_1$) and $\mathbb{P}^1_{x_i}$, $i = 2, 3, 4$, then the fiber $\mathcal{H}'_{x_2, x_3, x_4}$ of points of \mathcal{H}' lying over points of the form (x, x_2, x_3, x_4) is a Zariski open subset of a projective algebraic curve that is a 3 branch point cover of \mathbb{P}^1_x (ramified over x_2, x_3, x_4). Proposition 2.2 says that for each value of (x_2, x_3, x_4) this curve is analytically isomorphic to a fixed curve $C(H')$ (i.e., independent of (x_2, x_3, x_4)). Furthermore, from the construction, the natural projection of $C(H')$ to \mathbb{P}^1_x is of degree equal to the index of $H' \cap SH_4$ in SH_4 . Finally, if this cover has no automorphism of order 2, then these identifications force $\mathcal{H}_{H'}$ to be a Zariski open subset of $C(H') \times \mathbb{P}^1_{x_2} \times \mathbb{P}^1_{x_3} \times \mathbb{P}^1_{x_4}$.

In the case when H' is the stabilizing subgroup of an absolute class through the permutation representation given by (3.4) there is an explicit description of the branch cycles of the cover $C(H') \rightarrow \mathbb{P}^1_x$ in terms of the Q 's and their action on $SNi(C)_T^{ab}$ [BFr; Lemma 1.6]. It is traditional (as in [BFr]) to use (a_{12}, a_{13}, a_{13}) instead of $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ for these branch cycles (as well as for the elements of H_4 that induce them) :

$$(4.1) \quad a_{12} = Q_1^{-2}, \quad a_{13} = Q_1 Q_2^{-2} Q_1^{-1}, \quad a_{14} = Q_1 Q_2 Q_3^{-2} Q_2^{-1} Q_1^{-1}.$$

As with the σ notation, denote the permutation group (acting on $SNi(C)_T^{ab}$) generated by the a 's of (4.1) by $G(a)$, and the subgroup that stabilizes a specific element of $SNi(C)_T^{ab}$ by $G(a,1)$. Recall also, that there is an effective procedure to decide if $(|\text{Aut}(C(H')/\mathbb{P}_x^1)|, 2) = 1$ since $\text{Aut}(C(H')/\mathbb{P}_x^1)$ may be identified with the quotient group $N_{G(a)}(G(a,1))/G(a,1)$ of the normalizer of $G(a,1)$ in $G(a)$. Furthermore (in the case that H' does come from a permutation representation given by (3.4)), we may count the number of connected components of the fiber product

$$\mathcal{H}_{H'} \times_{\mathbb{P}^4 \setminus D_4} ((\mathbb{P}^1)^4 \setminus \Delta_4)$$

as the number of orbits of SH_4 on $SNi(C)_T^{ab}$.

The next discussion starts to turn this around by trying to realize certain subgroups H' of H_4 as the stabilizing subgroup of some absolute Nielsen class through the permutation representation given by (3.4). The examples of § 5 will be helpful to the reader, but we start by seeing that examples of such H' are related to modular curves.

4.2.— Elliptic curves and the $PSL_2(\mathbb{Z})$ quotient of H_4 . The presentation of H_4 given in Theorem 3.3 shows an intimate relation between the appearance of the $PSL_2(\mathbb{Z})$ quotient and the theory of modular curves. It comes from the following diagram.

Suppose that E' and E are elliptic curves in Weierstrass normal form. Consider an integer $n \geq 1$. Fix a group A_0 that is isomorphic to a subgroup of $\mathbb{Z}/n \oplus \mathbb{Z}/n$. This latter group is isomorphic to the group of points of E of order dividing n . Now suppose that $\phi : E' \rightarrow E$ is an isogeny whose kernel is isomorphic to A_0 . On each of E' and E we may equivalence points p and $-p$ to form the quotients $E'/\langle \pm 1 \rangle$ and $E/\langle \pm 1 \rangle$. These may be respectively identified with $\mathbb{P}_{x'}^1$ and \mathbb{P}_x^1 where x' and x represent the corresponding x -coordinates of the Weierstrass normal form. This gives a commutative diagram of algebraic curves :

$$(4.2) \quad \begin{array}{ccc} E' & \xrightarrow{\phi} & E \\ pr(E') \downarrow & & \downarrow pr(E) \\ \mathbb{P}_{x'}^1 & \xrightarrow{\psi(f)} & \mathbb{P}_x^1 \end{array}$$

where $\psi(f)$ denotes the rational function that takes x' to x .

Let $G_{A_0} = G$ be the semidirect product $A_0 \times^s \langle -1 \rangle$ with $\langle -1 \rangle$ the group generated by multiplication by -1 on E' restricted to A_0 . Also denote the conjugacy class of $(v; -1) \in A_0 \times^s \langle -1 \rangle$ in this group by C_v . Then the Nielsen class of the cover in the bottom row is given by the argument of [Fr,2; p. 155] :

$$\{\tau \in G^4 \mid G(\tau) = G \text{ and } \tau_i \in C_{v_i}, v_i \in A_0, i = 1, 2, 3, 4 \text{ and } v_4 = v_1 - v_2 + v_3\}.$$

Note that if A_0 is cyclic and n is odd, then all of the C_v 's are conjugate to $(0; -1)$. Also, if we denote $\mathbb{Z} \oplus \mathbb{Z}$ by \mathbb{Z}^2 , then G is a quotient of $G_{\mathbb{Z}^2} = \mathbb{Z}^2 \times^s \langle -1 \rangle$. This latter group in turn may be identified with the quotient of the free group F_4 on 4 generators $\bar{\sigma}_i$, $i = 1, 2, 3, 4$, by the normal subgroup N generated by $\bar{\sigma}_1 \dots \bar{\sigma}_4$ and $\bar{\sigma}_i^2$, $i = 1, 2, 3, 4$. Indeed, consider :

$$(4.3) \quad \theta : F_4/N \rightarrow G_{\mathbb{Z}^2} \text{ by } \bar{\sigma}_i, i = 1, 2, 3, 4, \text{ go in order to}$$

$$((1,1); -1), ((0,1); -1), ((1,0); -1), ((2,0); -1).$$

Thus the images of $\bar{\sigma}_1 \bar{\sigma}_2$ and $\bar{\sigma}_1 \bar{\sigma}_3$ can be identified with the generators $(1,0)$ and $(0,1)$ of \mathbb{Z}^2 which is the normal subgroup of $G_{\mathbb{Z}^2}$ of index 2.

Replace the τ 's by $\bar{\sigma}$'s in (3.4) to get an action of the braid group $B(4)$ (as below (3.3)) on F_4/N ; and thereby on $G_{\mathbb{Z}^2}$. The action of $Q_1 Q_2 Q_3^2 Q_2 Q_1$ is given by conjugation by $\bar{\sigma}_1$, which induces multiplication by -1 on \mathbb{Z}^2 .

CONCLUSION 4.1. *The natural map above of $B(4)$ into $\text{Aut}(\mathbb{Z}^2)$ gives a natural homomorphism of H_4 into $\text{SL}_2(\mathbb{Z})/\langle \pm 1 \rangle \stackrel{\text{def}}{=} PSL_2(\mathbb{Z})$ (below we show it is onto).*

Relation with $C_0(n)$: We will see that the map of Conclusion 4.1 is onto. Consider the special case with A_0 cyclic of order n . Geometrically this ties the somewhat mysterious space $\mathcal{H}(C)_T$ to the well known modular curve $C_0(n)$. Recall that the latter is a projective nonsingular model for the upper half plane \mathcal{U} modulo the action of the $SL_2(\mathbb{Z})$ subgroup consisting of the matrices

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{n} \right\}.$$

Indeed, the covers $X \rightarrow \mathbb{P}_x^1$ in the Nielsen class $Ni(C)_T^{ab}$ can be completed to a diagram that looks like (4.2) with X replacing $\mathbb{P}_{x'}^1$, ψ replacing ϕ , \hat{X} replacing E' , etc., in that the genus of the pairs of corresponding curves are the same :

$$(4.4) \quad \begin{array}{ccc} \hat{X} & \longrightarrow & \hat{X}/A_0 \\ pr(\hat{X}, X) \downarrow & & \downarrow pr(\hat{X}/A_0, \mathbb{P}_x^1) \\ X & \longrightarrow & \mathbb{P}_x^1 \end{array}$$

Here \hat{X} is the Galois closure of the cover appearing in the bottom row, and \hat{X}/A_0 is the quotient of \hat{X} by the cyclic normal subgroup of order n of the dihedral group D_{2n} that along with -1 generates this group. The unramified cover in the upper row of (4.4), and thus it corresponds to a unique point of $C_0(n)$. This gives us the sought for commutative diagram :

$$(4.5) \quad \begin{array}{ccc} \mathcal{H}(C)_T & \xrightarrow{\Lambda_0(n)} & C_0(n) \\ \Psi(C) \downarrow & & \downarrow \psi(n) \\ \mathbb{P}^4 - D_4 & \xrightarrow{\Lambda_0(1)} & C_0(1) \end{array}$$

where the upper row maps $m \in \mathcal{H}(C)_T$ to the point of $C_0(n)$ that corresponds to diagram (4.4) with $\phi_m : X_m \rightarrow \mathbb{P}^1$ in the bottom row. The notation is that prior to Proposition 3.1.

Some classical clarifications : it is natural to identify $C_0(1)$ with the j -line \mathbb{P}_j^1 ; the map $\Lambda_0(1)$ takes an unordered collection of four distinct points $\{x_1, x_2, x_3, x_4\}$ in \mathbb{P}_x^1 to the isomorphism class of the elliptic curve represented by the Weierstrass equation

$$y^2 = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$$

with the convention that if one of the x_i 's is ∞ , then we remove the factor $(x-x_i)$; and $\Psi(C)$ is the natural map that takes the equivalence class of a cover $X \rightarrow \mathbb{P}_x^1$ to the unordered collection of its branch points.

The 3 branch point cover from Proposition 2.2 : The Legendre form of an elliptic curve has the algebraic curve $y^2 = x(x-1)(x-\lambda)$ corresponding to a value of the parameter λ . This gives a natural map from the λ -line, $\mathbb{P}_\lambda^1 \rightarrow \mathbb{P}_j^1$. Denote the fiber product $C_0(n) \times_{\mathbb{P}_j^1} \mathbb{P}_\lambda^1$ (i.e., pullback over \mathbb{P}_λ^1) by $C_0(n)_\lambda$. Similarly, as in (3.2) consider the natural map Ψ_4 from the ordered distinct points $(\mathbb{P}^1)^4 \setminus \Delta_4$ of \mathbb{P}_x^1 to the unordered set of such points $\mathbb{P}^4 \setminus D_4$.

From Proposition 2.2, for any possible choice of C , each connected component of the pullback of $\mathcal{H}(C)_T$ has attached to it a nonsingular algebraic curve $C(C)$ presented as a cover of \mathbb{P}_x^1 ramified over just the three points $0, 1$ and ∞ . Indeed, the computation in the middle of [Fr,2; p. 156] shows that, at least when n is odd, that not just H_4 , but even $G(a)$ (as in 4.1)) is transitive on this absolute Nielsen class. This curve is actually isomorphic to $C_0(n) \times_{\mathbb{P}_j^1} \mathbb{P}_\lambda^1$. In the next subsection we display a natural process by which one recovers $C_0(n)$ from $C(C)$. This is applied in the main examples of § 5.

4.3.— Automorphisms from branch point twists : Assume here that $r=4$ and that $Ni(C)_T^{ab}$. From [BFr] (in the case $r=4$ only) this is equivalent to the transitivity of the group $G(a)$ generated by the a 's of (4.1), so that $\mathcal{H}(C)$ has

but one irreducible component (Proposition 3.1). Consider the curve cover $\beta : C(C) \rightarrow \mathbb{P}_x^1$, ramified over x_2, x_3, x_4 given by Proposition 2.2. For this discussion alone, identify the permutations of the points x_2, x_3, x_4 with S_3 regarded as a subgroup of $PSL_2(\mathbb{C})$. That is, for $\pi \in S_3$, the automorphism ϕ_π associated to π is that which permutes x_2, x_3, x_4 according to π .

Consider the subset of those $\pi \in S_3$ for which the covers $\beta : C(C) \rightarrow \mathbb{P}_x^1$ and $\phi_\pi \circ \beta : C(C) \rightarrow \mathbb{P}_x^1$ are equivalent : there exists an analytic isomorphism $\mu_\pi : C(C) \rightarrow C(C)$ such that $\beta \circ \mu_\pi = \phi_\pi \circ \beta$. This is clearly a subgroup of S_3 , and we denote it by $T(C)$ (for *twisting* of C). The μ_π 's act on $C(C)$, and the ϕ_π 's act on \mathbb{P}_x^1 . Despite our concern that the notation could easily be misunderstood out of context, we denote the respective quotients by $C(C)/T(C)$ and $\mathbb{P}_x^1/T(C)$.

CONCLUSION 4.2 : *The cover $\beta : C(C) \rightarrow \mathbb{P}_x^1$ has a description of branch cycles given by the a's of (4.1) [BFR; Lemma 1.6]. For the special case where $Ni(C)_T^{ab}$ is the Nielsen class of covers in the bottom row of diagram (4.4), $T(C) = S_3$ and the map $\lambda_0(n)$ of (4.5) extended to the respective pullbacks identifies $C(C)/T(C)$ with $C_0(n)$, \mathbb{P}_x^1 with \mathbb{P}_λ^1 and $\mathbb{P}_x^1/T(C)$ with \mathbb{P}_j^1 . For the case of general C , both $C(C)$ and $C(C)/T(C)$ (respectively covering \mathbb{P}_λ^1 and \mathbb{P}_j^1) are identified with the projective normalization of the upper half plane modulo a subgroup (of finite index) of $PSL_2(\mathbb{Z})$. But only in rare circumstances would we expect this to be a congruence subgroup.*

In § 5.3 we give another example of a situation where $T(C)$ is not trivial so that the reader can see that the twisting automorphisms have serious application.

4.4.— Nielsen classes with markings and $C(n)$. More explicit identification of the curve $C(C)$ in conclusion 4.2 would be a marvelous thing, but it seems difficult. In some sense [DDH] describes all of the three branch point covers of \mathbb{P}_x^1 that

arise as $C(C)$ for some Nielsen class $Ni(C) \frac{ab}{T}$; all that are possible by Belyi's Theorem [Be], those defined over $\bar{\mathbb{Q}}$. But their result is not so explicit as the example above in its relation to the structure of the Hurwitz monodromy group, precisely because Belyi's result is not very explicit.

There is another point, too, related to [DDH]. While that paper does imply that there exists a C that gives the modular curve $C(n)$ this way, the natural extension of the above construction does not do so. Recall that $C(n)$ is the projective nonsingular model for the upper half plane \mathcal{U} modulo the action of the $SL_2(\mathbb{Z})$ subgroup consisting of the matrices

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cong \mathbb{I} \pmod{n} \right\}.$$

The natural way to get $C(n)$ is to consider Nielsen classes with markings – pointed Nielsen classes – the technical topic that was applied in [DFr] (after its introduction in [BFr]). Essentially the markings on a Nielsen class trace what happens to a disjoint cycle of an element representing a conjugacy class of C_i under the action of H . This therefore gives a permutation representation of H_r that extends that of the action on $Ni(C) \frac{ab}{T}$. From this example, these markings of Nielsen classes are a generalization of the level n structures that play a traditional role in the theory of modular curves and of moduli spaces of higher dimensional abelian varieties. From the quite different construction of [DDH; Theorem p. 4] :

THEOREM 4.3. *Let H be the subgroup of $SL_2(\mathbb{Z})$ that corresponds to \mathbb{P}_λ^1 . The 3 branch point curve covering $C(C) \rightarrow \mathbb{P}_x^1$ as C runs over pointed Nielsen classes are in one-one correspondence with the (congruence and noncongruence) curve covering of the λ -line \mathbb{P}_λ^1 that arise from subgroups of H of finite index.*

The twisting process of Conclusion 4.2 should give us a similar statement comparing the covers $C(C)/T(C) \rightarrow \mathbb{P}_x^1/T(C)$ with the covers, both congruence and noncongruence, of \mathbb{P}_j^1 in the cases where $T(C) = S_3$. But the Nielsen classes that appear in [DDH] aren't really set up to make this comparison.

5.— Generalizations of rigidity and examples

5.1.— Generalization of rigidity and (0.1) : The topic is how to check if there are covers in a given Nielsen class that are actually defined over \mathbb{Q} . Although the results that we state here are essentially in [Fr,1], it is the attention drawn to the special case of $r = 3$ by [T] that brought their significance to the mathematical public. There is a technically valuable game that compares the Galois and nonGalois situations. Even if one is ultimately interested in Galois extensions, many times it is better to start with a nonGalois cover and go to the Galois closure. The strong *rigidity* conditions may be harder to satisfy in the nonGalois situation than in the corresponding Galois situation. But if they do hold, that implies the vanishing of an obstruction for the field of definition that isn't easily checked from the Galois situation.

Galois action on branch points : Let $K \subset \mathbb{C}$ be a field of definition of the cover $\phi : X \rightarrow \mathbb{P}_x^1$. The cover is said to be g -regular over K if the Galois closure

$\widehat{K(X)}$ of the function field extension $K(X)/K(x)$ is a regular extension of $K(\mathbb{P}_x^1) = K(x)$ (i.e., if $K(X) \cap \bar{K} = K$). Informally we say that there is no extension of constants. More generally, however, we must deal with the group $\hat{G} = G(\widehat{K(X)}/K(x))$. This is also a subgroup of S_n . It contains G identified as

$G(\widehat{K(X)}/\hat{K}(x))$, with \hat{K} the algebraic closure of K in $\widehat{K(X)}$ (as in § 2.4). We also need a group theoretic definition extending the definition of rational conjugacy class of a group.

DEFINITION. Let G be a group and let C_i be the conjugacy class of σ_i , $i = 1, \dots, r$. Denote the order of σ_i by e_i , $i = 1, \dots, r$. Denote the least common multiple of the e_i 's by N . The set $\{C_1, \dots, C_r\}$ is said to be a rational set of conjugacy classes of G if

$$(5.1) \quad \text{the set } \bigcup_{i=1}^r C_i \text{ contains all powers } \sigma_i^k, \quad i = 1, \dots, r \text{ and } k \text{ relatively prime to } N.$$

Note that unions of rational sets of conjugacy classes are also rational. An alternative statement to (5.1) is the following :

(5.2) for $k \in (\mathbb{Z}/N)^*$, there exists $\beta \in S_r$ such that $\sigma_i^k \in C_{(i)\beta}$, $i = 1, \dots, r$.

Consider the orbits of the action of $G(\bar{K}/K)$ on the branch points x_1, \dots, x_r of the cover. We denote the orbit of x_i by $O(i)$, where the notation implies that we use the integer subscripts in place of the points themselves. Below we need to consider the union $\bigcup_{j \in O(i)} C_j$ of the conjugacy classes attached to this orbit of the branch points. Denote by $O(C_i)$ this orbit of C_i under $G(\bar{K}/K)$.

In many applications it is natural to make a basic assumption about the conjugacy classes C in the transitive subgroup G of S_n defined by a description σ of the branch cycles of a cover. With N as above for each $k \in (\mathbb{Z}/N)^*$ we define a unique conjugacy class C_i^k of G by putting each element of C_i to the power k . Put each coordinate of C to the power k to consider a new r -tuple C^k of conjugacy classes of G . Also, let $\sigma \in S_r$ act on C by permuting the coordinates. Denote the result by ${}^\sigma C$. Also, $C \bmod N_{S_n}(G)$ denotes the ordered collections of r -tuples of conjugacy classes $\gamma C \gamma^{-1}$, $\gamma \in N_{S_n}(C)$. Two special conditions are used below in Proposition 5.4 (the a) part implies b)) :

- (5.3) a) for each $k \in (\mathbb{Z}/N)^*$, $C^k \equiv C \bmod N_{S_n}(G)$; and
 b) for each $k \in (\mathbb{Z}/N)^*$, there exists $\sigma \in S_r$ such that
 $C^k \equiv {}^\sigma C \bmod N_{S_n}(G)$.

Suppose that the cover $X \rightarrow \mathbb{P}^1$ is in the Nielsen class $Ni(C)_T^{ab}$ (§ 1.2). Retain the association of x_i with the conjugacy class C_i , $i = 1, \dots, r$. Regard $G(K(\zeta_N)/K)$ as a subgroup of the units of the ring \mathbb{Z}/N . Here ζ_N is a primitive N th root of 1. If (5.3 b) holds regard $G(K(\zeta_N)/K)$ (acting through integers) as permutations on the coordinates of C modulo $N_{S_n}(G)$. If a number field K is

a field of definition of the cover, as earlier, denote the Galois closure of the field extension $K(X)/K(x)$ by $\widehat{K(X)}$. Its Galois group, \hat{G} is a subgroup of $N_{S_n}(G)$.

DEFINITION 5.1. *For each $\tau \in G(\bar{\mathbb{Q}}/K)$ denote the image of τ in $G(K(\zeta_N)/K)$ by $k = k_\tau$. The branch points x and conjugacy classes C are said to be Galois compatible (over K) if for each $\tau \in G(\bar{\mathbb{Q}}/K)$, if τ permutes the x_i 's as $\bar{\tau} \in S_r$, then*

$$(5.4) \quad C_i^k = \gamma C_{(i)\bar{\tau}\gamma^{-1}} \text{ for some } \gamma \in \hat{G} \text{ (independant of } i\text{), } i = 1, \dots, r.$$

The next result is a special case of the branch cycle argument [Fr,1; p. 61].

PROPOSITION 5.2. *Suppose that the cover $X \rightarrow \mathbb{P}^1$ is in $Ni(C)_T^{ab}$. If the cover is defined over \mathbb{Q} , then x and C are Galois compatible over \mathbb{Q} . In particular, (5.3) b) holds. If the cover is g-regular over \mathbb{Q} , then $O(C_i)$ is rational, $i = 1, \dots, r$.*

\mathbb{Q} -points on Hurwitz spaces : The point of the Hurwitz monodromy action is this (see [Fr,1], [Fr,3], [DFr] for details). Suppose that $SH(r)$ acts transitively on the straight Nielsen classes (§ 3.2), that $Cen_{S_n}(G)$ is trivial, and that each of the

conjugacy classes of C is rational. Then the Hurwitz space cover $\Psi(C) : \mathcal{H}(C)_T \rightarrow \mathcal{U}_r$ prior to Proposition 3.1 (including the total space of representing covers for the points of $\mathcal{H}(C)_T$) is defined over \mathbb{Q} . For $r > 3$ we improve upon condition (0.1) with the following statement (note that a) and b) are the same as in (0.1) :

- (5.5) a) $G = N_{S_n}(G)$;
- b) each of the classes C_1, \dots, C_r is rational;
- c) SH_r is transitive on the absolute straight Nielsen classe $SNi(C)_T^{ab}$ defined by C (expression (3.4)); and
- d) there exists a \mathbb{Q} -point on the Hurwitz space $\mathcal{H}(C)_T$.

Our next result is an analogue of *rigidity* as it is based directly on conditions (5.5). It is an immediate corollary of the following Proposition 5.4 whose hypotheses are much weaker because it uses just condition 5.3 b).

PROPOSITION 5.3. *Assume that $Ni(C)_T^{ab}$ is a Nielsen class for which one of the following holds. Either G is in its regular representation and G has no center; or*

$$(5.6) \quad \text{the centralizer, } \text{Cen}_{S_n}(G) \text{ of } G \text{ of } S_n \text{ is trivial.}$$

If the conditions (5.5) hold, then G is the Galois group of a regular extension of $\mathbb{Q}(x)$.

To state the next general proposition precisely we need to consider another variety which fits in a sequence of covers

$$(5.7) \quad \mathcal{H}(C)_T \rightarrow \mathcal{H}_q \rightarrow \mathcal{U}_r$$

where the map $\mathcal{H}(C)_T \rightarrow \mathcal{H}_q$ is Galois (e.g., it is of degree 1 under the hypotheses of Proposition 5.3). We explain the construction of \mathcal{H}_q in the comments after the statement of the result. The field K_M is the fixed field in $\mathbb{Q}(\zeta_N)$ of the integers k for which the expression (5.3 a) holds

$$C^k \equiv C \pmod{N_{S_n}(G)}.$$

PROPOSITION 5.4. *Let $Ni(C)_T^{ab}$ be a Nielsen class for which (5.3 b) and (5.5 c) hold. Assume also that either G is in its regular representation and G has no center or (5.6) holds. Then the cover $\mathcal{H}(C)_T \rightarrow \mathcal{H}_q$ is defined over K_M , and the cover $\mathcal{H}_q \rightarrow \mathcal{U}_r$ is defined over \mathbb{Q} . Suppose that the cover $\phi : X \rightarrow \mathbb{P}_x^1$ corresponds to the point $m \in \mathcal{H}(C)_T$ (as in Proposition 3.1) and let x (resp., m_q) be the image of m in \mathbb{P}^r (resp., \mathcal{H}_q). Then the cover is defined over \mathbb{Q} if and only if*

- (5.8 a) m_q is a \mathbb{Q} -point; and
 b) x and C are Galois compatible over \mathbb{Q} .

If in addition (5.5 a) holds then $\widehat{G(\mathbb{Q}(X)/\mathbb{Q}(x))}$ is isomorphic to G , and G has been realized as the Galois group of a regular extension of $\mathbb{Q}(x)$.

Comments on the proof : This is a special case of Proposition 1.5 of [Fr,3] (and most of it is from [Fr1, Thm. 5.1]). Without assuming that 5.5 a) holds we may only assert that, for $\bar{G} = \{\gamma \in N_{S_n}(G) \mid \text{there exists } k \in (\mathbb{Z}/N)^*, \sigma \in S_r \text{ with}$

(5.4) holding :

$$G \subset \widehat{G(\mathbb{Q}(X)/\mathbb{Q}(x))} \subset \bar{G}.$$

This will figure in the examples that follow. In § 5.2 we will also see a method that sometimes allows us to check for condition 5.5 d).

Here is the construction of \mathcal{H}_q starting from the result of Proposition 1.5 of [Fr,3] that says that $\mathcal{H}(C)_T \rightarrow \mathcal{U}_r$ is defined over K_M . As in § 2.2 consider a connected component \mathcal{H}' of the fiber product $\mathcal{H}^\times \mathcal{U}_r^r$. We form \mathcal{H}_q

using the same ideas that appear in the discussion of *branch point twists* in § 4.3. From (5.3 b) it is easy to show that to each $\tau \in G(K_M/\mathbb{Q})$ there exists $\bar{\tau} \in S_r$ (acting on \mathcal{U}^r by permutation of coordinates) and $\Psi_{\bar{\tau}} : (\mathcal{H}')^\tau \rightarrow \mathcal{H}'$ that makes the following diagram commutative :

$$\begin{array}{ccc} (\mathcal{H}')^\tau & \xrightarrow{\Psi_\tau} & \mathcal{H}' \\ (\Psi_C)^\tau \downarrow & & \downarrow \Psi_C \\ \mathcal{U}^r & \xrightarrow{\bar{\Psi}} & \mathcal{U}^r \end{array}$$

As usual the superscript τ is application of τ to the coefficients of the polynomials describing the varieties. Then \mathcal{H}_q is the variety that results from applying Weil's cocycle condition to this (cf. the proof of Prop. 1.5 of [Fr,3] for details). \square

5.2.– Unirational Hurwitz spaces and the group A_5 : As an application of the theory of § 5.1 we start by considering the geometry and arithmetic of degree 5 covers $X \rightarrow \mathbb{P}_x^1$ (and their Galois closures $\hat{X} \rightarrow \mathbb{P}_x^1$) whose monodromy group is A_5 and for which the representation T is the standard representation of degree 5.

Hilbert's trick: Hilbert [Hi] considered the groups A_n , $n = 5, 6, \dots$ in his famous paper applying the Hilbert irreducibility theorem to realize groups as Galois groups over \mathbb{Q} . The *trick* is to realize S_n as a 3 branch point Galois cover $\hat{X} \rightarrow \mathbb{P}_x^1$ (given by Nielsen class $Ni(C)$) defined over \mathbb{Q} , and then to consider the quotient $\hat{X}/A_n = Y$. The Nielsen class for Hilbert was that with C given by C_1 the class of 2-cycle, C_2 the class of an $n-1$ -cycle and C_3 the class of an n -cycle.

By necessity two of the conjugacy classes in C (say C_1 and C_2) must be represented by elements of $S_n \backslash A_n$. This implies that the degree two cover $Y \rightarrow \mathbb{P}_x^1$ is ramified only over the branch points x_1 and x_2 corresponding to these two classes. If in addition the two conjugacy classes are distinct, the respective points y_1 and y_2 on Y over the branch points are easily shown to be \mathbb{Q} -rational. A genus 0 curve with a rational point (actually any odd degree rational divisor) is isomorphic to \mathbb{P}_y^1 for some element y of the function field. This last observation, fittingly, is due to Hilbert and Hurwitz.

There are other situations where one may use Hilbert's idea, and difficulties around condition (0.1 a) offer motivation to do so. When it is possible to realize the automorphism group $\text{Aut}(G)$ of a sporadic simple group G as the Galois group of a 3 branch point cover over \mathbb{Q} , this may work if $\text{Aut}(G)/G$ is small. Matzat [Ma,1] has used this to realize a number of the sporadic groups as Galois groups. In addition, sometimes this trick can work even when the big group is realized by a Nielsen class consisting of 4 branch point covers. We used this in [Fr,3; Ex. 2.3] to introduce 5 independent transcendental parameters into realizations of A_n as a Galois group over \mathbb{Q} . We reviewed Hilbert's idea (as did Shih [Sh]) in [Fr,1; p. 70] in order to point out the difficulties in obtaining the information provided by it in a more direct manner. Although our example is

mainly designed to show the practical use of the twisting automorphisms of Conclusion 4.2, it can also be viewed as continuing the discussion of [Fr,1].

Nielsen classes given by 3-cycles : We consider the absolute Nielsen class of A_5 where $r = 4$, $T : A_5 \rightarrow S_5$ is the natural injection and $C = C_{3^4}$ has $C_1 = C_2 = C_3 = C_4$, each the conjugacy class of a 3-cycle. Let $X \rightarrow \mathbb{P}_x^1$ be a cover in the Nielsen class $Ni(C_{3^4})_T^{ab}$. In order to apply the result of § 5.1 we first show that H_4 is transitive on the elements of this Nielsen class.

Clearly $Ni(C_{3^4}) = S_5$. Thus with no loss we may assume that any representative σ of an element of $Ni(C_{3^4})_T^{ab}$ has $\sigma_1 = (123)$ and that σ_2 has either 1, 2 or 3 integers in its 3-cycle in common with $\{1,2,3\}$. If the third holds then $\sigma_2 = \sigma_1^{-1}$ and $\sigma_3 = (145)$; if the second holds, then we may assume $\sigma_2 = (214)$; and if the first, $\sigma_2 = (145)$. With this data we have uniquely determined a given Nielsen class.

List 5.5 :

$$\begin{aligned} X_1 : \sigma_2 &= (132), \sigma_3 = (145), \sigma_4 = (154); \quad X_2 : \sigma_2 = (145), \sigma_3 = (154), \sigma_4 = (132); \\ X_3 : \sigma_2 &= (145), \sigma_3 = (215), \sigma_4 = (243); \quad X_4 : \sigma_2 = (145), \sigma_3 = (321), \sigma_4 = (354); \\ X_5 : \sigma_2 &= (145), \sigma_3 = (432), \sigma_4 = (415); \quad X_6 : \sigma_2 = (145), \sigma_3 = (543), \sigma_4 = (521); \\ X_7 : \sigma_2 &= (214), \sigma_3 = (245), \sigma_4 = (532); \quad X_8 : \sigma_2 = (214), \sigma_3 = (325), \sigma_4 = (543); \\ X_9 : \sigma_2 &= (214), \sigma_3 = (435), \sigma_4 = (245). \end{aligned}$$

Replace X_i by the integer i , $i = 1, \dots, 9$, to give a degree 9 representation of H_4 . Here is the effect of the generators Q_i , $i = 1, 2, 3$, on $Ni(C_{3^4})_T^{ab}$:

$$(5.9) \quad Q_1 = (25364)(798), \quad Q_2 = (14985)(367) \text{ and } Q_3 = (25364)(798).$$

The action of H_4 is clearly transitive.

The cover $\beta : \mathcal{C}(C_{3^4}) \rightarrow \mathbb{P}_x^1$: Our next computation shows that the 3 branch point cover associated to $Ni(C_{3^4})$ is not of genus 0. In particular, the pullback

\mathcal{H}' of $\mathcal{H}(C_{3^4})$ over \mathcal{U}^4 is not a unirational variety. But, because we are repeating the same conjugacy class many times, we see in Theorem 5.6 that $\mathcal{H}(C_{3^4})$ itself is a \mathbb{Q} -unirational variety. In particular it has lots of rational points to satisfy condition (5.5 d).

Apply Conclusion 4.2 to the action of the Q_i 's on List 5.5 to get

$$\begin{aligned} a_{12} &= Q_1^{-2} = (26543)(798) \\ a_{13} &= Q_1 Q_2^{-2} Q_1^{-1} = (19627)(385) \\ a_{14} &= (a_{12} a_{13})^{-1} = (84591)(376). \end{aligned}$$

In particular, a_{12} and a_{13} generate a group that is transitive on the straight absolute Nielsen classes $SNi(C_{3^4})_T^{ab}$. From the comment at the end of § 4.1, the transitivity of the a_{1j} 's on the Nielsen classes (which are the straight Nielsen classes in this case) implies that the fiber product

$$\mathcal{H}', \stackrel{\text{def}}{=} \mathcal{H}(C_{3^4}) \times_{\mathbb{P}^4 \setminus D_4} (\mathbb{P}^1)^4 \setminus \Delta_4$$

is irreducible. Since the degree of the cover of Δ_4 is 9, Proposition 2.2 implies that \mathcal{H}' is isomorphic to an open subset of $C(C_{3^4}) \times (\mathbb{P}^1)^3$. From the Riemann–Hurwitz formula, compute the genus g of $C(C_{3^4})$ from the formula

$$2(9 + g - 1) = \sum_{i=2}^4 \text{ind}(a_{1i}) = 18, \text{ or } g = 1.$$

Unirationality of $\mathcal{H}(C_{3^4})$: We leave to the reader the final lemma of preparation.

Ramification Lemma : Assume that we have covers $X_i \rightarrow \mathbb{P}_x^1$, with $p_i \in X_i$ ramified of order e_i over $x_0 \in \mathbb{P}_x^1$, $i = 1, 2$. Then in the normalization Y of the fiber product $X_1 \times_{\mathbb{P}_x^1} X_2$ there are $\gcd(e_1, e_2)$ points above the point (p_1, p_2)

and each of them has ramification order over x_0 equal to $\text{lcm}(e_1, e_2)$. Furthermore, each of these points in Y has ramification order $\text{lcm}(e_1, e_2)/e_1$ over p_1 .

Our next result shows that all of the conditions of (5.5), except (5.5.a), are satisfied.

THEOREM 5.6. *With C_i the conjugacy class of a 3-cycle in A_5 , $i = 1, 2, 3, 4$, the parameter space $\mathcal{H}(C_{3^4})$ is a unirational variety over \mathbb{Q} . In particular, its \mathbb{Q} points are Zariski dense.*

Proof : Refer back to the discussion prior to Conclusion 4.2 with $C = C_{3^4}$. In this case the group $T(C)$ is S_3 . Here is why. Let $\phi : X \rightarrow \mathbb{P}_x^1$ be any cover in the Nielsen class corresponding to a point of $C(C)$ lying above x . Now let $\alpha : \mathbb{P}_x^1 \rightarrow \mathbb{P}_x^1$ be any linear fractional transformation that permutes 0, 1 and ∞ . Then $\alpha \circ \phi : X \rightarrow \mathbb{P}_x^1$ is in the same Nielsen class, and it has 3 of its branch points equal to 0, 1 and ∞ . In the case of C_{3^4} we already have noted that this cover is therefore represented by a point of $C(C)$ which has a representing cover of \mathbb{P}_x^1 whose 4th branch point is $\alpha(x)$.

Also $\mathcal{H}(C_{3^4})$ is in this case identified with the quotient of an action of S_4 on \mathcal{H}' , with $T(C_{3^4})$ identified with a copy of S_3 inside this S_4 . Thus we are done if we show that $C(C_{3^4})/T(C_{3^4}) \times (\mathbb{P}^1)^3$ is unirational. This is equivalent to show that $C(C_{3^4})/T(C_{3^4})$ is rational over \mathbb{Q} .

But $C(C)/T(C) \rightarrow \mathbb{P}_x^1/T(C)$ is a cover of degree 9. If we show that $C(C)/T(C)$ is of genus 0, as it has a rational class of odd (9) degree (see Hilbert's trick above) it is a \mathbb{Q} -rational curve. It is enough to show that the cover $C(C) \rightarrow C(C)/T(C)$ is ramified, in which case $C(C)/T(C)$ is of genus less than 1 (i.e., 0). It suffices also, to replace $T(C)$ by the subgroup generated by (13), which is regarded as leaving 1 fixed and permuting 0 and ∞ . Then $\mathbb{P}_x^1/\langle(13)\rangle$ is identified with \mathbb{P}_y^1 , $y = x + 1/x$. Note that $C(C)$ is identified with the normalization of the fiber product

$$(5.10) \quad C(C)/\langle(13)\rangle \times_{\mathbb{P}_x^1/\langle(13)\rangle} \mathbb{P}_y^1.$$

In the fiber product (5.10) the only possible branch points of $C(C)/\langle(13)\rangle \rightarrow \mathbb{P}_y^1$ can be identified with the images of $0, 1, \infty$, or -1 in the cover $\mathbb{P}_x^1 \rightarrow \mathbb{P}_y^1$. The images of 1 and -1 are respectively 2 and -2 , and both 0 and ∞ go to ∞ . The consideration of -1 comes from its being the other ramified point of $\mathbb{P}_x^1 \rightarrow \mathbb{P}_y^1$. It is clear that the disjoint cycle structure of the branch cycle over ∞ is the same as that for $C(C) \rightarrow \mathbb{P}_x^1$ over ∞ (or 0). For the other 2 points, however, the disjoint cycle structure of the branch cycle is potentially a bit more complicated. Here we have only to consider ramification over $-2 \in \mathbb{P}_x^1$ in order to draw our conclusion. But in Theorem 5.9 we will need analysis of the more complicated ramification over the other point too.

Consider the point $-1 \in \mathbb{P}_x^1$. Since there is no ramification in the cover $C(C) \rightarrow \mathbb{P}_x^1$ the Ramification Lemma (above) tells us that the points of $C(C)/\langle(13)\rangle$ over -2 , are ramified of order either 1 or 2 . The maximum that this contributes to the index is 4 . And then there are 4 points of order 2 ramified over -2 and one point, p_0 , unramified. By the Ramification Lemma, the point of $C(C)$ corresponding to $(p_0, -1)$ is ramified over p_0 . Thus $C(C) \rightarrow C(C)/\langle(13)\rangle$ is ramified. This proves the result. \square

5.3.—Further inspection of condition (5.5 a): From Theorem 5.6 we conclude the following about the Nielsen class $Ni(C_{3^4})_T$. There exist (a great many) covers $\phi : X \rightarrow \mathbb{P}_x^1$ defined over \mathbb{Q} in this Nielsen class. Furthermore, from the comments following Proposition 5.4, we have

$$(5.11) \quad A_5 \subset \widehat{G(\mathbb{Q}(X)/\mathbb{Q}(x))} \subset S_5.$$

That is, in this case $N_{S_n}(G) = S_5 = \bar{G}$ (defined after (5.8)).

For the possibility of analyzing the necessity of condition (5.5 a), and for considering how to incorporate Hilbert's *trick* in the general theory, it behooves us to be able to answer a natural question in this simple case.

Question 5.7. As $\phi : X \rightarrow \mathbb{P}_x^1$ runs over all covers in the Nielsen class $Ni(C_{3^4})_T$ does the middle term of (5.11) achieve both of the groups A_5 and S_5 ?

If the answer to the question is affirmative, we will say that $Ni(C_{3^4})_T$ achieves A_5 and S_5 . This is the conclusion of Theorem 5.9. The idea for treating this is already in [BFr; p. 95]. Instead of considering the action of H_4 on absolute Nielsen classes, we consider the action on just the Nielsen classes $Ni(C_{3^4})_T$ themselves. A complete list of these can be obtained by adding to List 5.5 the effect of conjugation the elements of List 5.5 by (45):

List 5.8.

- $X_{10} : \sigma_2 = (132), \sigma_3 = (154), \sigma_4 = (145); X_{11} : \sigma_2 = (154), \sigma_3 = (145), \sigma_4 = (132);$
- $X_{12} : \sigma_2 = (154), \sigma_3 = (214), \sigma_4 = (253); X_{13} : \sigma_2 = (154), \sigma_3 = (321), \sigma_4 = (345);$
- $X_{14} : \sigma_2 = (154), \sigma_3 = (532), \sigma_4 = (514); X_{15} : \sigma_2 = (154), \sigma_3 = (453), \sigma_4 = (421);$
- $X_{16} : \sigma_2 = (215), \sigma_3 = (254), \sigma_4 = (432); X_{17} : \sigma_2 = (215), \sigma_3 = (324), \sigma_4 = (453);$
- $X_{18} : \sigma_2 = (215), \sigma_3 = (534), \sigma_4 = (254).$

Just as in the previous computation we check the Hurwitz monodromy action on the union of List 5.5 and List 5.8. If the resulting $a_{1,j}$'s of Conclusion 4.2 generate a transitive group, we obtain a cover $C(C_{3^4})' \rightarrow \mathbb{P}_\lambda^1$ ramified over $0, 1, \infty$. We note from (5.12) below that this holds. Of course, $C(C_{3^4})'$ is a degree 2 cover of $C(C_{3^4})$ (defined over \mathbb{Q}). From this point we assume that $C = C_{3^4}$. Then as before we form the quotient $C(C)' / T(C)$. By the previous ideas if we put the last 3 branch points at arbitrary rational numbers x_2, x_3, x_4 , we consider the cover $C(C)' / T(C) \rightarrow C(C) / T(C)$. For each rational point $p \in C(C) / T(C)$, we showed in § 5.2 that we get a cover $X \rightarrow \mathbb{P}_x^1$ in this Nielsen class defined over \mathbb{Q} .

Extending this we determine that the algebraic closure of \mathbb{Q} in $\widehat{\mathbb{Q}(X)}$ is $\mathbb{Q}(p')$ where p' is a point of $C(C)'$ lying above p . From Hilbert's irreducibility theorem this will give a degree 2 extension of \mathbb{Q} for most values of p in \mathbb{Q} . Thus this Nielsen class achieves S_5 . To see that it achieves A_5 we

have only to see if $C(C)'/T(C)$ has a \mathbb{Q} -point. Here are the computation for the Q 's :

$$Q_1 = (1\ 10)(2\ 5\ 3\ 6\ 4)(7\ 9\ 8)(11\ 14\ 12\ 15\ 13)(16\ 18\ 17)$$

$$Q_2 = (2\ 11)(14\ 18\ 8\ 5)(10\ 13\ 9\ 17\ 14)(3\ 15\ 16)(12\ 6\ 7)$$

$$Q_3 = (1\ 10)(2\ 5\ 3\ 6\ 4)(7\ 9\ 8)(11\ 14\ 12\ 15\ 13)(16\ 18\ 17).$$

From this we get the a 's as previously :

$$(5.12) \quad \begin{aligned} a_{12} &= Q_1^{-2} = (2\ 6\ 5\ 4\ 3)(7\ 9\ 8)(11\ 15\ 14\ 13\ 12)(16\ 18\ 17) \\ a_{13} &= Q_1 Q_2^{-2} Q_1^{-1} = (1\ 18\ 15\ 11\ 7)(10\ 9\ 6\ 2\ 16)(3\ 8\ 14)(12\ 17\ 5) \\ a_{14} &= (a_{12} a_{13})^{-1} = (7\ 12\ 6)(18\ 1\ 8\ 4\ 5)(16\ 15\ 3)(9\ 10\ 17\ 13\ 14). \end{aligned}$$

Transitivity of the a 's on the elements of $Ni(C_{3^4})_T$ is now clear. Also the Riemann–Hurwitz formula gives the genus of $C(C)'$ as g' with

$$2(18 + g' - 1) = \sum_{i=2}^4 \text{ind}(a_{1i}) = 36, \text{ or } g' = 1.$$

THEOREM 5.9. *There is a group of automorphisms of $T(C)'$ acting on $C(C)'$ as S_3 extending the action of $T(C)$ on $C(C)$. The quotient $C(C)'/T(C)'$ is a genus zero curve. In addition this curve has a \mathbb{Q} -rational point. In the notation above $Ni(C_{3^4})_T$ achieves both A_5 and S_5 .*

Proof : Consider the formation of $C(C)'$. A representing cover is from an equivalence class of covers of $X \rightarrow \mathbb{P}_x^1$ with the following property with respect to a base point $x_0 \in \mathbb{P}_x^1 \setminus \{x_1, \dots, x_r\}$, a set of canonical homotopy classes of paths $\mathcal{P}_1, \dots, \mathcal{P}_r$ for the fundamental group of $\mathbb{P}_x^1 \setminus \{x_1, \dots, x_r\}$; and a labeling $\{p_1, \dots, p_n\}$ ($n = 5$ in this case) of the points of the cover over x_0 :

(5.13) the description (τ_1, \dots, τ_r) of the branch cycles of the cover produced by this data generates $G = A_5$ and the cover is in the Nielsen class C .

The G orbit of this data is given by conjugation by G on the resulting branch cycles descriptions. It is an easy observation that these G -orbits are independent of the choice of $\mathcal{P}_1, \dots, \mathcal{P}_r$. Furthermore, since parallel transport of the points above x_0 around a closed path in $\mathbb{P}_x^1 \setminus \{x_1, \dots, x_r\}$ permutes these points by an element of G , we may equivalence the labelings of the points over suitable base points. We shall call two such compatible labelings transportaties equivalent. Furthermore, over the curve $C(C)'$ we may form a local system of compatible transport equivalent labelings. Thus the G equivalence classes of covers are well defined. The construction of [Fr1; § 4] produces the corresponding Hurwitz space representing these G -orbits and $C(C)'$ is the result of the Hurwitz monodromy action on $Ni(C_{3,4})_T^G$. Each of the two points of $C(C)'$ lying above a given point $m \in C(C)$ corresponds to one of the two possible G equivalence classes of covers that produce the equivalence class of covers of m .

Following the argument of Theorem 5.6, let $\phi : X \rightarrow \mathbb{P}_x^1$ be any cover in the Nielsen class corresponding to a point of $C(C)'$ lying above x . If $\alpha : \mathbb{P}_x^1 \rightarrow \mathbb{P}_x^1$ is any linear fractional transformation that permutes 0, 1 and ∞ , then the G equivalence class of $\alpha \circ \phi : X \rightarrow \mathbb{P}_x^1$ corresponds to a point of $C(C)'$ lying over $\alpha(x)$.

Follow exactly the computation of the proof of Theorem 5.6, at the point of the discussion that considers "the point $-1 \in \mathbb{P}_x^1$ ". Here conclude (as in the notation there) that there must be k points of $C(C)' / \langle (13) \rangle$ ramified of order 2 over the image of $-2 \in \mathbb{P}_y^1$ of -1 , and $18 - 2k$ points unramified over -2 .

In a like manner we use the Ramification Lemma prior to Theorem 5.6 to analyze the disjoint cycle structure lengths $(s_1)(s_2)\dots(s_t)$ (with the s 's in nonincreasing order) of the branch cycle τ for the cover $C(C)' / \langle (13) \rangle \rightarrow \mathbb{P}_y^1$ over $2 \in \mathbb{P}_y^1$. The s 's give a possible disjoint cycle structure of $(3)(3)(5)(5)$ for $a_{1,3}$ when τ has the following form :

$$(5.14) \quad (3)(3)(5)(5), (6)(5)(5), (3)(3)(10) \text{ or } (6)(10).$$

Apply the Riemann–Hurwitz formula as previously to conclude that the genus of $C(C)' / \langle (13) \rangle$ is at most $\frac{26+k}{2} - 17$ and this maximum occurs under

three circumstances : when $k = 8$ and τ has type (6)(10); when $k = 9$ and τ has type (3)(3)(10) ; or when $k = 9$ and τ has type (6)(5)(5). In any of these cases $C(C)'/T(C)$ is of genus 0. But it is a degree 18 cover of $\mathbb{P}_x^1/T(C)$.

Nevertheless we can look in the divisors that have support over the branch locus of the cover $C(C)'/T(C) \rightarrow \mathbb{P}_x^1/T(C)$ to find a \mathbb{Q} divisor of odd degree. Indeed, since it is only the last three cases of (5.14) that can possibly occur, we note that any of the nonrepeated lengths of the disjoint cycles for τ in the last 3 cases of (5.14) correspond to a point over $2 \in \mathbb{P}_y^1$ that must be \mathbb{Q} -rational. \square

Manuscrit reçu le 13 septembre 1988.

Corrigé le 31 janvier 1989

(*) p. 77 : Stay in France supported by NSF grant DMS-8702150 and Institut Henri Poincaré.

BIBLIOGRAPHY

- [Be] G.V. Belyi.— *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR, Ser. Mat. 43 (1979), 267–276.
- [BFr] R. Biggers and M. Fried.— *Moduli spaces of covers and the Hurwitz monodromy group*, J. für die reine und Angew. Math. 335 (1982), 87–121.
- [DDH] S. Diaz, R. Donagi and D. Harbater.— *Every curve is a Hurwitz space*, preprint.
- [DFr] P. Debes and M. Fried.— *Arithmetic variation of fibers in families of curves Part I : Hurwitz monodromy criteria for rational points on all members of the family*; preprint.
- [F] W. Feit.— \hat{A}_5 and \hat{A}_7 as Galois groups over number fields, J. of Alg. 104 (1986), 231–260.
- [Fr,1] M. Fried.— *Fields of definition of function fields and Hurwitz families...*, Comm. in Alg. 5(1) (1977), 17–82.
- [Fr,2] M. Fried.— *Galois group and complex multiplication*, TAMS 235 (1978), 141–163.
- [Fr,3] M. Fried.— *Rigidity and applications of the classification of simple groups to monodromy Part I-Super rational connectivity with examples; Part II-Applications of connectivity; Davenport and Hilbert–Siegel problems*.
- [FrT] M. Fried and J.G. Thompson.— *The Hurwitz monodromy group H_4 and modular curves*, preprint.
- [Gro] A. Grothendieck.— *Géométrie formelle et géométrie algébrique*, Séminaire Bourbaki t. 11, 182 (1958/59).

- [Gu] R.C. Gunning.— *Lectures on Riemann Surfaces*, Princeton Math. Notes (1966).
- [Hi] D. Hilbert.— *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. 110 (1892), (Ges. Abh. II, 264–286).
- [Ma,1] H. Matzat.— *Konstruktive Galoistheorie*, Lecture Notes in Math—Springer Verlag 1284 (1986).
- [Ma,2] H. Matzat.— *Rationality Criteria for Galois Extensions*, preprint.
- [Sh] K. Shih.— *On the construction of Galois extensions of function fields and number fields*, Matematische Annalen 207 (1974), 99–120.
- [T] J.G. Thompson.— *Some finite groups which appear as $\text{Gal } L/K$ where $K \subseteq \mathbb{Q}(\mu_n)$* , J. of Alg. 98 (1984), 437–499.
- [W] A. Weil.— *The field of definition of a variety*, Amer. J. Math. 78 (1956), 509–524.

Mike Fried
 Department of Mathematics
 201 Walker Hall
 University of Florida
 Gainesville, Fl 32611
 and
 Department of Mathematics
 UC Irvine
 Irvine, California 92717

*Séminaire de Théorie des Nombres
1987-88*

**MINORATION DE HAUTEURS ET ANALYSE DIOPHANTIENNE
SUR LES COURBES ELLIPTIQUES**

M. HINDRY

Nous décrivons les résultats obtenus en collaboration avec Joseph Silverman [Hi–Si] et les plaçons dans leur contexte, essentiellement la recherche d'effectivité dans les problèmes diophantiens, et agrémentons le texte de quelques remarques sur le théorème de Mordell–Weil.

1.– Introduction.

K désigne un corps de nombres, \mathcal{O}_K son anneau d'entiers, S_K l'ensemble de ses places (prolongeant les places de \mathbb{Q}).

Soit C une courbe algébrique définie sur K , soit g son genre, l'arithmétique sur K est dominée par les trois résultats suivants, où $C(K)$ désigne l'ensemble des points de C rationnels sur K et $J = J_C$ désigne la jacobienne de C .

(A)–(Siegel) : L'ensemble des points de $C(K)$ entiers sur un modèle affine de C est fini, sauf peut-être si $g = 0$ et le modèle affine possède au plus deux points à l'infini.

(B)–(Mordell–Weil) : Le groupe des points de J rationnels sur K est de type fini ; en particulier, si $g = 1$, ou bien $C(K)$ est vide, ou bien c'est un groupe de type fini.

(C)–(Faltings) : Si $g \geq 2$, alors $C(K)$ est fini.

On peut consulter par exemple [La1] et [C–S] pour une preuve détaillée. Un caractère commun (dans l'état actuel de nos connaissances) est l'ineffectivité de ces résultats (sauf pour le théorème (A) lorsque la *méthode de Baker* s'applique, voir par exemple [B–Ma]). La *mesure* la plus communément utilisée

est la hauteur de Weil d'un point P de $\mathbb{P}^n(K)$ de coordonnées projectives $(x_0; \dots; x_n)$ définie par :

$$h(P) := [K:\mathbb{Q}]^{-1} \sum_{v \in S_K} n_v \log \max |x_i|_v$$

où $[K:\mathbb{Q}]$ est le degré de K sur \mathbb{Q} et n_v le degré local du complété K_v sur \mathbb{Q}_v . On vérifie que cette définition ne dépend ni des coordonnées ni du corps de rationalité et vérifie les énoncés de finitude attendus ; en particulier les ensembles $\{P \in \mathbb{P}^n(K) / h(P) \leq X\}$ sont finis et effectivement calculables.

Si V est une sous-variété de \mathbb{P}^n , on a donc une hauteur $h : V(\bar{\mathbb{Q}}) \rightarrow \mathbb{R}$.

Si V est une variété abélienne (disons plongée symétriquement pour simplifier) on a une variante plus jolie, la hauteur de Néron–Tate :

$$\hat{h}(P) := \lim_n n^{-2} h(nP).$$

Notons qu'elle dépend du plongement ; pour une courbe elliptique, on choisit toujours un plongement de Weierstrass et on normalise par un facteur $1/3$. On sait que \hat{h} est quadratique définie positive sur $V(K)$ modulo la torsion et que $\hat{h} - h$ est bornée sur $V(\bar{K})$ de façon effective (voir [Zi] pour les courbes elliptiques et [Ma–Za] pour le cas général). Une version effective des théorèmes (A), (B) et (C) donnerait une borne pour la hauteur des points des points entiers de C , d'un système de générateurs de $J(K)$ et des points de $C(K)$. Nous discutons ici du minimum de \hat{h} sur les points d'ordre infini de $J(K)$; remarquons que le sous-groupe de torsion de $J(K)$ est effectivement calculable. Ces résultats vont dans la direction d'une conjecture de Serge Lang reliant les théorèmes (A) et (B) de la façon suivante :

CONJECTURE 1 (Lang). *Le nombre de points entiers sur un modèle minimal sur K d'une courbe elliptique E définie sur K est borné par $C_1^{1+\text{Rang}_{\mathbb{Z}} E(K)}$, où C_1 est une constante ne dépendant que du corps K .*

Minimal ici peut être défini comme un modèle à coefficients entiers dont le discriminant est minimal en norme ; une hypothèse de ce type est clairement nécessaire.

On peut généraliser cela en devinant :

CONJECTURE 1bis. *Le nombre de points entiers sur un modèle minimal sur K d'une courbe C définie sur K de genre $g \geq 1$ est borné par $C_2^{1+\text{Rang}_{\mathbb{Z}} J(K)}$, où C_2 est une constante ne dépendant que de g et du corps K .*

Si $g \geq 2$ on peut même être plus audacieux et poser la question avec les points rationnels (ce qui évite de définir le mot minimal...) et même demander s'il est possible que pour tout sous-groupe Γ de rang fini de $J(\mathbb{C})$ le cardinal de $C \cap \Gamma$ soit borné par $C_3^{1+\text{Rang}_{\mathbb{Z}} \Gamma}$. Remarquons que cette question englobe une version uniforme inconnue de la *conjecture* de Manin–Mumford (conjecture prouvée par Raynaud [Ra] et étudiée par plusieurs auteurs, voir [Co], [Hi]). Nous redescendons sur terre au paragraphe suivant.

2.— Minoration de hauteurs.

Dans [Si1] Silverman prouve que la conjecture 1bis peut essentiellement se déduire de deux ingrédients : une borne uniforme pour la torsion et une bonne (*optimale*) minoration de la hauteur de Néron–Tate d'un point d'ordre infini. Il en déduit en particulier la conjecture 1bis pour la famille des courbes elliptiques à invariant entier et pour la famille des courbes de Catalan de genre donné (courbes du type $y^m = x^n + a$).

Pour énoncer le résultat de [Hi–Si] introduisons quelques notations ; pour toutes les notions arithmétiques sur les courbes elliptiques on consultera [Si3]. Si E est une courbe elliptique sur K , on note j_E son invariant modulaire, $\mathcal{D}_{E/K}$ son idéal discriminant minimal et $\mathcal{I}_{E/K}$ son idéal conducteur ; on définit son quotient de Szpiro $\sigma_E = \sigma_{E/K}$ et sa hauteur $h(E) = h(E/K)$ par :

$$h(E) := \frac{1}{12} \max (h(j_E), \log N_{\mathbb{Q}}^K(\mathcal{D}_{E/K}))$$

$$\sigma_E := \log N_{\mathbb{Q}}^K(\mathcal{D}_{E/K}) / \log N_{\mathbb{Q}}^K(\mathcal{I}_{E/K}) .$$

Si E possède bonne réduction partout on pose $\sigma_E = 1$; la hauteur $h(E)$ est comparable à la hauteur définie par Faltings mais a l'avantage d'être toujours positive.

THEOREME. *Toute courbe elliptique E sur K vérifie :*

(i) *L'ordre du groupe de torsion de $E(K)$ est majoré par $(20\sigma_E)^{8[K:\mathbb{Q}]_{10}} E^{4\sigma}$.*

(ii) *Si P est un point d'ordre infini de $E(K)$ alors :*

$$\hat{h}(P) \geq (20\sigma_E)^{-8[K:\mathbb{Q}]_{10}} E^{-4\sigma} h(E).$$

(iii) *Le nombre de points entiers sur un modèle minimal de E sur K est borné par $C^{(1+\text{Rang}_{\mathbb{Z}} E(K))\sigma_E}$, où C est une constante ne dépendant que de K .*

Commentaires :

La motivation initiale est la célèbre conjecture :

CONJECTURE 2 (Szpiro). *Soit $\epsilon > 0$ alors il n'y a qu'un nombre fini de courbes elliptiques sur K telles que $\sigma_{E/K} \geq 6 + \epsilon$; en particulier $\sigma_{E/K}$ est borné.*

Szpiro a initialement énoncé cette conjecture pour des courbes semi-stables (par analogie avec les corps de fonctions où il pouvait la prouver [Sz]) mais il n'y a pas de raison de s'y restreindre, en fait le cas semi-stable semble être le plus difficile. La conjecture de Szpiro y étant connue, on obtient du même coup des analogues précis du théorème sur les corps de fonctions.

Les constantes du théorème peuvent facilement être *un peu* améliorées mais aller plus loin semble requérir des techniques nouvelles, signalons que Silverman a obtenu une minoration $\hat{h}(P) \geq C(g)^{-1} h(E)$ avec C polynomiale pour une courbe définie sur un corps de fonctions de genre g (ce qui améliore le théorème 0.2 de [Hi–Si]).

Si on savait que σ_E était borné on aurait donc une borne uniforme pour la torsion des courbes elliptiques (conjecture attribuée au folklore par Cassels), une minoration $\hat{h}(P) \gg h(E) \gg \log N_{\mathbb{Q}}^K(\mathcal{D}_{E/K})$ pour les points d'ordre infini (conjecture formulée par Lang [La2] et déjà étudiée par le second auteur [Si2]) et bien sûr la conjecture 1.

La borne pour la torsion est connue si $K = \mathbb{Q}$ (et beaucoup plus !) grâce à Mazur ; on peut obtenir de bonnes majorations en fonction de $[K:\mathbb{Q}]$ sous diverses hypothèses sur la réduction de E aux places de K mais il semble que le théorème donne la seule borne inconditionnelle dans le cas semi-stable ; Frey a proposée dans [Fr] une excellente borne en fonction du maximum de σ_E , lorsque E' varie dans la classe des courbes K -isogènes à E .

Schéma de preuve du théorème (on écrira σ au lieu de σ_E) :

L'affirmation (iii) résulte de (i) et (ii) grâce aux résultats de [Si1] déjà mentionnés au début de ce paragraphe. On montre que si $mP \neq 0$ pour $1 \leq m \leq (20\sigma)^4 [K:\mathbb{Q}]^{10} 2^\sigma$ alors la hauteur de P est strictement positive et vérifie l'inégalité (ii), ce qui prouve également (i). Pour cela on utilise la décomposition de la hauteur de Néron–Tate en somme de hauteurs locales. Pour chaque place v il existe une (unique) fonction $\lambda_v : E(K_v) - \{0\} \rightarrow \mathbb{R}$; on sait que $\hat{h}(P) = [K:\mathbb{Q}]^{-1} \sum_v n_v \lambda_v(P)$ pour P non nul ; on connaît des formules exactes (voir [La2] par exemple, pour une caractérisation et des formules explicites) pour ces hauteurs locales, nous nous contenterons ici d'énoncer les propriétés que nous utiliserons.

LEMME 1 (cas archimédien). *Soit $\epsilon > 0$ (et ≤ 1), soit E isomorphe sur \mathbb{C} à $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ avec τ dans le domaine fondamental usuel, soit $z = a + b\tau$ avec $\max(|a|, |b|) \leq \epsilon/22$ alors :*

$$\lambda(z) \geq \frac{1-\epsilon}{12} \log \max(|j(\tau)|, 1).$$

Voir [Hi–Si] pour la preuve ; c'est une version effective du fait que $\lambda(z)$ tend vers l'infini quand z tend vers 0 et doit donc être positive au voisinage de zéro. Remarquons qu'en appliquant le principe des tiroirs il y a toujours un multiple d'un point donné qui vérifie les hypothèses du lemme 1.

Pour traiter le cas non–archimédien nous introduisons $E_0(K_v)$ le groupe des points qui se prolonge dans la composante neutre de la fibre spéciale du modèle de Néron (ceux qui restent non singuliers modulo v) et rappelons :

LEMME 2. *L'indice $(E(K_v) : E_0(K_v))$ est fini et vaut au plus 4 si la réduction est de type additif. Si la réduction est de type multiplicatif alors $E(K_v)/E_0(K_v)$ est isomorphe à $\mathbb{Z}/N_v\mathbb{Z}$; où l'on a noté $N_v = \text{ord}_v \mathcal{D}_{E/K} = -\text{ord}_v j_E$.*

Notons α_v cet isomorphisme (qui est canonique au signe près) et $v(a) = -\log |a|_v$, on peut alors énoncer :

LEMME 3 (Tate). *Si $P \in E_0(K_v)$ alors $\lambda_v(P) \geq \frac{1}{12} v(\mathcal{D}_{E/K})$.*

Si la réduction est multiplicative alors $\lambda_v(P) \geq \frac{1}{2} B(\alpha_v(P)/N_v) v(\mathcal{D}_{E/K})$ où B est la fonction définie par $B(t) = t^2 - t + \frac{1}{6}$ sur $[0,1]$ et prolongée par périodicité.

Quitte à considérer $12P$ au lieu de P les places non multiplicatives contribuent donc $v(\mathcal{D}_{E/K})$; malheureusement $-\frac{1}{12} \geq B(t) \geq \frac{1}{6}$ et donc si le point P se réduit en un point singulier pour beaucoup de places multiplicatives on peut obtenir une grosse contribution négative. Pour compenser ceci on introduit une moyenne pondérée. Soit $M \geq 1$ un entier, pour $1 \geq m \geq M$ on pose $a_m = 2(M-m+1)/M(M+1)$; notons que $\sum_{m=1}^M a_m = 1$ et

$$\sum_{m=1}^M m^2 a_m = (M+1)(M+2)/6.$$

LEMME 4. *Pour tout $t \in \mathbb{R}$ on a :*

$$\sum_{m=1}^M a_m B(mt) \geq -1/6M.$$

Voir [Hi–Si]; l'idée de la preuve est de développer B en série de Fourier, l'utilisation de ce type d'analyse harmonique est due à Blanksby et Montgomery.

On applique maintenant ces estimations pour minorer la hauteur d'un point P_0 ayant beaucoup de multiples non nuls :

On choisit un entier M (on prendra $[3\sigma_E]$), on note $q_M = \text{ppcm}\{1, \dots, M\}$ et on pose $P_1 = q_M P_0$; on choisit par le principe des tiroirs un multiple $P = nP_1$ tel que les points P, \dots, MP vérifient les hypothèses du lemme 1 en chaque place archimédienne (on peut réaliser cela avec $n \leq [22M/\epsilon]^{2[K:\mathbb{Q}]}$). Soit S_∞ l'ensemble des places archimédien-nes de K , S_1 l'ensemble des places finies avec $(E(K_v) : E_0(K_v)) \leq M$ (il contient les places additives) et S_2 les autres places; notons \mathcal{D}_1 (resp. \mathcal{D}_2) la partie de $\mathcal{D}_{E/K}$ première avec S_2 (resp. avec S_1), alors :

D'après le lemme 1 :

$$\sum_{m=1}^M a_m \sum_{v \in S_\infty} n_v \lambda_v(mP) \geq \frac{1-\epsilon}{12} \sum_{v \in S_\infty} n_v \log \max(|\mathcal{J}_v|, 1).$$

D'après les lemmes 2 et 3 :

$$\sum_{m=1}^M a_m \sum_{v \in S_1} n_v \lambda_v(mP) \geq \frac{1}{12} \log N_{\mathbb{Q}}^K(\mathcal{D}_1).$$

D'après les lemmes 3 et 4 on a :

$$\sum_{m=1}^M a_m \sum_{v \in S_2} n_v \lambda_v(mP) \geq \frac{1}{2} \sum_{m=1}^M a_m \sum_{v \in S_2} B(a_v(mP)/N_v v(\mathcal{D}_2)) \geq -\log N_{\mathbb{Q}}^K(\mathcal{D}_2)/12M.$$

Regroupant ces inégalités et utilisant la quadraticité de \hat{h} on obtient :

$$12 \sum_{m=1}^M a_m \hat{h}(mP) \geq (1-\epsilon) \sum_{v \in S_\infty} n_v \log \max(|\mathcal{J}_v|, 1) + \log N_{\mathbb{Q}}^K(\mathcal{D}_1) - (\log N_{\mathbb{Q}}^K(\mathcal{D}_2))/M,$$

le terme de gauche valant $2n^2 q_M^2 (M+1)(M+2) \hat{h}(P_0)$.

Mais il est aisément de voir que la norme de \mathcal{D}_2 est bornée par une puissance (dépendant de σ_E bien sûr) de la norme de \mathcal{D}_1 et on obtient alors une inégalité du type cherché en prenant $\epsilon = 1/M$.

3.– Remarque sur le théorème de Mordell–Weil.

Rappelons le lemme de Hermite (voir [La1]) :

LEMME 5. *Soit Γ un réseau de \mathbb{R}^r , muni d'une forme quadratique q et soit $R(\Gamma)$ le régulateur associé et μ le minimum de la forme sur $\Gamma - \{0\}$, alors il existe une \mathbb{Z} -base P_1, \dots, P_r de Γ telle que :*

$$i) \quad \mu = q(P_1) \leq (4/3)^{(r-1)/2} R(\Gamma)^{1/r}.$$

$$ii) \quad q(P_1) \dots q(P_r) \leq (4/3)^{r(r-1)/2} R(\Gamma).$$

En particulier on peut trouver une \mathbb{Z} -base telle que :

$$q(P_i) \leq (4/3)^{i(r-1)/2(r-i+1)} (R(\Gamma)/\mu^{i-1})^{1/r-i+1}.$$

Ainsi une borne explicite de la hauteur d'un système de générateurs du groupe de Mordell–Weil peut être obtenue à partir d'une minoration explicite de μ donnée par le théorème précédent et d'un majorant pour le régulateur, malheureusement inaccessible à l'heure actuelle. Manin a toutefois observé (voir aussi [La3]) qu'une telle borne peut provenir d'un résultat du type conjecture de Birch et Swinnerton–Dyer.

Par souci de simplicité bornons-nous aux courbes E définies sur \mathbb{Q} ; notons r le rang de $E(\mathbb{Q})$, Ω la période réelle de E et $a(E)$ le premier coefficient non nul du développement de Taylor de la fonction $L(E,s)$ en $s = 1$ (ceci a un sens si l'on a prolongé analytiquement $L(E,s)$ jusqu'au voisinage de 1).

La conjecture de Birch et Swinnerton–Dyer nous dit (en particulier) que $L(E,s) \sim a(E)(s-1)^r$ et que $R(E(\mathbb{Q})) \leq |E(\mathbb{Q})_{\text{tor}}|^2 a(E)/\Omega$.

Il n'est pas difficile d'approcher numériquement Ω ou de démontrer une inégalité de la forme $\Omega^{-1} \ll \exp h(E)$; pour obtenir une version effective de Mordell–Weil (modulo la conjecture de Birch et Swinnerton–Dyer) ajoutons le :

LEMME 6. *Soit E/\mathbb{Q} une courbe elliptique dont la fonction L se prolonge analytiquement avec équation fonctionnelle (par exemple si E est modulaire) soit N son conducteur alors : $|a(E)| \leq 2^r N^{1/4} (\log N)^2$.*

On peut obtenir bien sûr de meilleures bornes modulo diverses hypothèses sur les zéros de L .

Preuve : Posons $\Lambda(s) = N^{s/2}(2\pi)^{-s}T(s)L(E,s)$, alors $\Lambda(2-s) = \pm \Lambda(s)$. On voit aisément que si $\sigma = Re(s) > 3/2$ alors $|L(E,s)| \leq \zeta(\sigma-1/2)^2$ et donc si $e > 0$ on a :

$$|\Lambda(3/2+e+it)| = |\Lambda(1/2-e+it)| \leq \Gamma(3/2+e)(2\pi)^{-3/2-e}N^{3/4+e/2}\zeta(1+e)^2.$$

Par le principe de Phragmen–Lindelöf la même estimation vaut dans la bande $1/2 - e \leq Re(s) \leq 3/2 + e$. Utilisant $\zeta(1+e) \leq 1 + 1/e$ et les formules de Cauchy (appliquées au cercle de centre 1 et rayon $1/2 + e$), notant que $\Lambda^{(r)}(1) = (\sqrt{N}/2\pi)L^{(r)}(E,1)$ on obtient un peu mieux que le lemme en prenant $e = 2/\log N$ (en tout cas lorsque $N \geq 43$).

Manuscrit reçu le 24 septembre 1988

BIBLIOGRAPHIE

- [B–Ma] A. Baker, D. Masser.— *Transcendance theory : advances and applications*, Academic Press. Orlando Florida 1977.
- [Co] R. Coleman.— *Ramified torsion points on curves*, Duke Math. J. 1987 54, 615–640.
- [C–S] G. Cornell, J.H. Silverman.— *Arithmetic geometry*, Springer 1986.
- [Fr] G. Frey.— *Letter to Serge Lang*, 1986.
- [Hi] M. Hindry.— *Points de torsions sur les sous-variétés de variétés abéliennes*, C.R.A.S. 1987 N° 12 Série 304, 311–314..
- [Hi–Si] M. Hindry, J.H. Silverman.— *The canonical height and integral points on elliptic curves*, Inv. Math. 93, 419–450 (1988).
- [La1] S. Lang.— *Fundamentals of diophantine geometry*, Springer–Verlag 1983.
- [La2] S. Lang.— *Elliptic curves : diophantine analysis*, Springer 1978.
- [La3] S. Lang.— *Conjectured diophantine estimates* 155–171 (1983) in Arithmetic and Geometry, Birkhäuser (Ed. Artin, Tate).
- [Ma–Za] Y. Manin, J. Zarhin.— *Heights on families of abelian varieties*, Math. Sbornik 89 (1972), 171–181.
- [Ra] M. Raynaud.— *Courbe sur une variété abélienne et points de torsion*, Invent. Math. (1983) 71, 207–233.
- [Si1] J.H. Silverman.— *A quantitative version of Siegel's theorem*, J. Reine Angew. Math. 378, (1987) 60–100.
- [Si2] J.H. Silverman.— *Lower bound for the canonical height on elliptic curves*, Duke math. J. 48, (1981) 633–648.

- [Si3] J.H. Silverman.— *The arithmetic of elliptic curves*, Springer 1986.
- [Sz] L. Szpiro.— *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque 86 (1981).
- [Zi] H. Zimmer.— *On the difference between the Weil and Néron-Tate height*, Math. Z. 147, (1976) 35–51.

Marc HINDRY
Département de Mathématiques
Tour 45–55, 5ème étage
Université de Paris 7
2, place Jussieu
75221 PARIS CEDEX 05

*Séminaire de Théorie des Nombres
Paris 1987-88*

RANG p -ADIQUE D'UNITÉS : UN POINT DE VUE TORIQUE

M. LAURENT

1.— Introduction.

Après avoir rappelé l'énoncé de la conjecture de Leopoldt dans le cas galoisien, nous présentons brièvement le résultat essentiel de [5], dont les corollaires furent l'objet de l'exposé oral, et nous en proposons ici une démonstration dans un style différent, utilisant le langage des tores linéaires. Un tel point de vue a le mérite de justifier géométriquement les constructions et les choix effectués dans [5]. Il met aussi en évidence l'origine géométrique de certains calculs de répartition (voir le § 6). En outre, le théorème de transcendance de M. Waldschmidt sur lequel nous nous appuyons, est énoncé en termes de groupes algébriques. Nous espérons que cette approche plus conceptuelle du sujet engendrera automatiquement de nouveaux résultats, dès lors que l'outil de transcendance aura progressé. On notera d'ailleurs que M. Emsalem a reformulé récemment ses résultats sur les \mathbb{Z}_p -extensions en termes de tores, cf. [2], [3].

2.— Enoncé des résultats.

Soit K un corps de nombres et soit p un nombre premier. Pour chaque place v de K divisant p , on désignera par U_v^1 le groupe multiplicatif des **unités principales** (i.e. congrues à 1 modulo v) du complété K_v de K , et on notera

$$U = \prod_{v|p} U_v^1.$$

Il est clair que U est muni d'une structure naturelle de \mathbb{Z}_p -module. Désignons par E le groupe multiplicatif formé des unités globales de K appartenant à U_v^1

pour chaque place $v \mid p$, vu comme un sous-groupe de U par le plongement diagonal. Soit

$$\bar{E} = E^{\mathbb{Z}_p}$$

l'adhérence p -adique de E dans U . La conjecture de Leopoldt affirme alors que le rang sur \mathbb{Z}_p de \bar{E} est égal au rang sur \mathbb{Z} de E , ou ce qui revient au même que l'inclusion $E \subseteq U$ se prolonge \mathbb{Z}_p -linéairement en une injection

$$E \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow U.$$

Supposons maintenant que le corps K soit une extension galoisienne de \mathbb{Q} . Soit $G = \text{Gal}(K/\mathbb{Q})$ et soit $c \in G$ une conjugaison complexe du corps K . Alors U se trouve muni d'une structure de $\mathbb{Z}_p[G]$ -module qui prolonge l'action naturelle de G sur $K^\times \cap U$. Comme E est stable sous l'action de G , il s'ensuit que \bar{E} est un sous- $\mathbb{Z}_p[G]$ -module de U . En fait, d'après la conjecture de Leopoldt, les $\mathbb{Z}_p[G]$ -modules $E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ et \bar{E} devraient être isomorphes. Nous nous proposons de comparer les $\bar{\mathbb{Q}}_p[G]$ -modules

$$E \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}_p \quad \text{et} \quad \bar{E} \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p,$$

déduits des précédents par extension des scalaires de \mathbb{Z}_p à $\bar{\mathbb{Q}}_p$.

Désignons par Φ l'ensemble des caractères absolument irréductibles de G , à valeurs dans $\bar{\mathbb{Q}}_p$. Pour chaque $\varphi \in \Phi$, notons

$$d_\varphi = \varphi(1) = \text{degré de } \varphi,$$

$$r_\varphi = (\varphi(1) + \varphi(c))/2.$$

Lorsque $\varphi \neq 1_G$, le nombre r_φ est la multiplicité de φ dans le module $E \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}_p$: ce résultat, connu depuis J. Herbrand, se déduit par exemple aisément

de la proposition 1 ci-dessous. Désignons par ρ_φ la multiplicité de φ dans $\bar{E} \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$. On a alors le :

THEOREME. *Pour tout $\varphi \in \Phi$, $\varphi \neq 1_G$, on a la minoration*

$$\rho_\varphi \geq \frac{r_\varphi d_\varphi}{r_\varphi + d_\varphi}.$$

On trouvera dans [5] un certain nombre d'exemples concrets, où cet énoncé permet d'établir la conjecture de Leopoldt dans de nouveaux cas particuliers. Signalons simplement que cette recherche d'exemples pose des problèmes intéressants de théorie des groupes : existe-t-il un tel exemple avec un groupe G non résoluble, ou bien peut-on décrire les groupes résolubles G qui donnent lieu à ces exemples ?

3.- Généralités sur les tores linéaires.

Nous rassemblons dans ce paragraphe les résultats standards sur les tores linéaires, qui nous seront utiles. On en trouvera par exemple des démonstrations dans [1] et [7].

Un \mathbb{Q} -tore linéaire T est un groupe algébrique défini sur \mathbb{Q} , qui, après extension des scalaires de \mathbb{Q} à $\bar{\mathbb{Q}}$, devient isomorphe au groupe multiplicatif \mathbb{G}_m^d :

$$T/\bar{\mathbb{Q}} \simeq \mathbb{G}_m^d/\bar{\mathbb{Q}}.$$

On dit que le tore T est déployé par le corps de nombres $K \subseteq \bar{\mathbb{Q}}$, si l'isomorphisme ci-dessus est défini sur K . Soit

$$X(T) = \text{Hom}(T/\bar{\mathbb{Q}}, \mathbb{G}_m/\bar{\mathbb{Q}})$$

le groupe des caractères de T . Le groupe de Galois absolu $\mathcal{G} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ agit naturellement sur $X(T)$ et cette action se factorise par $G = \text{Gal}(K/\mathbb{Q})$ si T est déployé par l'extension galoisienne K/\mathbb{Q} .

Le foncteur $T \mapsto X(T)$ établit alors une antiéquivalence de catégories entre

- i) la catégorie des \mathbb{Q} -tôres linéaires déployés par l'extension galoisienne K/\mathbb{Q} , avec pour flèches le groupe $\text{Hom}(T, T')$ des morphismes $T \rightarrow T'$ de \mathbb{Q} -groupes algébriques,
- ii) la catégorie des $\mathbb{Z}[G]$ -modules, libres sur \mathbb{Z} et de type fini, où $G = \text{Gal}(K/\mathbb{Q})$.

De même, le foncteur

$$T \longmapsto Y(T) = X(T) \otimes_{\mathbb{Z}} \mathbb{Q},$$

établit une correspondance analogue avec en i) la catégorie formée des mêmes objets, avec pour flèches

$$\text{Hom}_0(T, T') = \text{Hom}(T, T') \otimes_{\mathbb{Z}} \mathbb{Q}$$

(catégorie des \mathbb{Q} -tôres à \mathbb{Q} -isogénie près) et en ii) la catégorie des $\mathbb{Q}[G]$ -modules de type fini.

Par évaluation des caractères en un point, le groupe $T(\mathbb{Q})$ des points \mathbb{Q} -rationnels d'un \mathbb{Q} -tore T s'identifie à

$$\text{Hom}_{\mathcal{G}}(X(T), \mathbb{Q}^\times).$$

On notera $T(\mathbb{Z})$ le sous-groupe de $T(\mathbb{Q})$ égal à

$$\text{Hom}_{\mathcal{G}}(X(T), \mathcal{O}^\times),$$

où \mathcal{O}^\times désigne le groupe multiplicatif des unités de l'anneau \mathcal{O} des entiers de \mathbb{Q} . Le groupe $T(\mathbb{Z})$ est de type fini et tout sous-groupe arithmétique de $T(\mathbb{Q})$ est contenu dans $T(\mathbb{Z})$ avec un indice fini. Il s'agit là simplement d'une notation suggestive car il n'existe pas en général de modèle affine de T dans un groupe de matrices GL_n tel que $T(\mathbb{Z}) = T(\mathbb{Q}) \cap GL_n(\mathbb{Z})$.

Un \mathbb{Q} -tore T est dit **anisotrope** si le groupe

$$X(T)_{\mathbb{Q}} = \text{Hom}(T, \mathbb{G}_{m/\mathbb{Q}}) \subseteq X(T)$$

des caractères \mathbb{Q} -rationnels de T est réduit à $\{1\}$. Il revient au même de dire que T ne contient aucun \mathbb{Q} -sous-tore isomorphe à \mathbb{G}_m . On a alors la

PROPOSITION 1. *Soit T un \mathbb{Q} -tore anisotrope, et soit χ le caractère de l'action de \mathcal{G} sur $X(T)$. Le rang du groupe $T(\mathbb{Z})$ est alors égal à*

$$r_\chi = (\chi(1) + \chi(c))/2,$$

où c désigne une conjugaison complexe de $\bar{\mathbb{Q}}$.

Pour une démonstration, voir par exemple le théorème 4 de [6]. On notera que cet énoncé contient le théorème des unités de Dirichlet.

Fixons dorénavant un nombre premier p et un plongement $\bar{\mathbb{Q}} \subseteq \bar{\mathbb{Q}}_p$ induisant une inclusion

$$\mathcal{G}_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \subseteq \mathcal{G}.$$

Le groupe $T(\mathbb{Q}_p)$ des points \mathbb{Q}_p -rationnels du \mathbb{Q} -tore T s'identifie alors à

$$\text{Hom}_{\mathcal{G}_p}(X(T), \bar{\mathbb{Q}}_p^\times),$$

et l'inclusion naturelle $T(\mathbb{Q}) \subseteq T(\mathbb{Q}_p)$ se traduit par la restriction de \mathcal{G} à \mathcal{G}_p :

$$\text{Hom}_{\mathcal{G}}(X(T), \bar{\mathbb{Q}}^\times) \rightarrow \text{Hom}_{\mathcal{G}_p}(X(T), \bar{\mathbb{Q}}_p^\times).$$

Soit t l'espace tangent à l'origine du tore T . Grâce au logarithme p -adique, on a de même les identifications :

$$t(\mathbb{Q}_p) = \text{Hom}_{\mathcal{G}_p}(X(T), \bar{\mathbb{Q}}_p) \subseteq t(\bar{\mathbb{Q}}_p) = \text{Hom}(X(T), \bar{\mathbb{Q}}_p).$$

D'autre part, le groupe topologique $T(\mathbb{Q}_p)$ contient un sous-groupe compact maximal, noté $T(\mathbb{Z}_p)$, égal à

$$\mathrm{Hom}_{\mathcal{G}_p}(X(T), \mathcal{O}_p^\times),$$

où \mathcal{O}_p^\times désigne le groupe multiplicatif des unités p -adiques de $\bar{\mathbb{Q}}_p$. Par définition même, il est clair que

$$T(\mathbb{Z}) \subseteq T(\mathbb{Z}_p).$$

Pour démontrer notre théorème, nous étudierons l'adhérence p -adique $\overline{T(\mathbb{Z})}$ de $T(\mathbb{Z})$ dans $T(\mathbb{Z}_p)$, pour le tore T particulier considéré dans le paragraphe suivant. Pour cela, il est utile de dévisser le tore T en ses facteurs isotypiques, ce qui permet par ailleurs de décrire l'adhérence de Zariski de $T(\mathbb{Z})$ dans T .

Soit T un \mathbb{Q} -tore linéaire déployé par l'extension galoisienne K/\mathbb{Q} , de groupe de Galois G . Désignons par Λ l'ensemble des classes d'isomorphisme des représentations \mathbb{Q} -linéaires irréductibles du groupe G . Si $\lambda \in \Lambda$, on notera par la même lettre λ le caractère de la représentation correspondante. Le $\mathbb{Q}[G]$ -module $Y(T)$ se décompose en somme directe

$$Y(T) = \bigoplus_{\lambda \in \Lambda} Y(T)_\lambda$$

de ses composantes isotypiques. Soit T_λ le \mathbb{Q} -tore linéaire dont le groupe des caractères est

$$X(T_\lambda) = X(T) \cap Y(T)_\lambda \subseteq X(T), \quad \lambda \in \Lambda.$$

Les inclusions ci-dessus définissent par dualité une isogénie

$$T \rightarrow \prod_{\lambda \in \Lambda} T_\lambda,$$

qui induit un **quasi-isomorphisme** (i.e. noyau et conoyau finis)

$$T(\mathbb{Z}) \xrightarrow{\sim} \prod_{\lambda \in \Lambda} T_\lambda(\mathbb{Z}).$$

On notera que le groupe $T_\lambda(\mathbb{Z})$ est Zariski-dense dans T_λ , dès que ce groupe est infini, c'est-à-dire lorsque $\lambda \neq 1_G$ et $r_\lambda > 0$. Voir l'appendice du chapitre 2 de [8] pour une preuve de ce fait.

Désignons enfin par t et t_λ , $\lambda \in \Lambda$, les espaces tangents à l'origine des tores respectifs T et T_λ . L'isogénie ci-dessus permet alors d'identifier t_λ à un sous-espace de t :

$$t = \bigoplus_{\lambda \in \Lambda} t_\lambda.$$

4.- Le tore $T = \text{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$.

Le \mathbb{Q} -tore T dont il s'agit est obtenu par restriction des scalaires de K à \mathbb{Q} du K -groupe algébrique \mathbb{G}_m , cf. [11]. On trouvera par exemple dans l'appendice de [4] une description concrète du tore T par des équations. Ce tore possède la vertu essentielle de représenter géométriquement le groupe multiplicatif du produit tensoriel par K : pour toute \mathbb{Q} -algèbre L , on peut identifier $T(L)$ à $(K \otimes_{\mathbb{Q}} L)^\times$ de manière fonctorielle en L . Il s'ensuit en particulier que

$$T(\mathbb{Q}) = K^\times, \quad T(\mathbb{Q}_p) = \prod_{v|p} K_v^\times,$$

l'inclusion $T(\mathbb{Q}) \subseteq T(\mathbb{Q}_p)$ correspondant alors au plongement diagonal de K^\times dans $\prod_{v|p} K_v^\times$. De même, $T(\mathbb{Z})$ s'identifie au groupe des unités de K , tandis que

$$T(\mathbb{Z}_p) = \prod_{v|p} U_v,$$

où U_v désigne le groupe des unités v -adiques de K_v . L'adhérence p -adique \bar{E} de E dans $U = \prod_{v|p} U_v^1 \subseteq T(\mathbb{Z}_p)$ peut être ainsi vue comme un sous-groupe analytique de $T(\mathbb{Z}_p)$.

Supposons à partir de maintenant que K soit une extension galoisienne de \mathbb{Q} , de groupe de Galois G . Le tore T est alors déployé par K et $X(T)$ s'identifie à l'algèbre de groupe $\mathbb{Z}[G]$, vue comme un G -module à gauche, de la manière suivante : pour tout $\sigma \in G$, le caractère

$$\sigma : T(\bar{\mathbb{Q}}) = (K \otimes \bar{\mathbb{Q}})^\times \rightarrow \bar{\mathbb{Q}}^\times$$

désigne la restriction aux unités du morphisme $K \otimes \bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}$ de $\bar{\mathbb{Q}}$ -algèbres déterminé par $\sigma(a \otimes 1) = \sigma(a)$, $a \in K$.

Considérons l'isogénie

$$T \rightarrow \prod_{\lambda \in \Lambda} T_\lambda,$$

introduite ci-dessus. Nous allons déterminer l'algèbre des endomorphismes des \mathbb{Q} -tores T et T_λ . Dans ce cas particulier, les G -modules

$$X(T) = \mathbb{Z}[G], \quad X(T_\lambda) = \mathbb{Z}[G] \cap \mathbb{Q}[G]_\lambda$$

sont des sous-algèbres de $\mathbb{Z}[G]$. Il s'ensuit que la multiplication à droite par un élément β de $\mathbb{Z}[G]$ définit des endomorphismes de G -modules (à gauche)

$$X(T) \xrightarrow{\times \beta} X(T), \quad X(T_\lambda) \xrightarrow{\times \beta} X(T_\lambda),$$

et induit par dualité un endomorphisme \mathbb{Q} -rationnel de chacun des tores T et T_λ . On obtient ainsi tous les \mathbb{Q} -endomorphismes de T et de T_λ :

$$\text{End}(T) \simeq \mathbb{Z}[G], \quad \text{End}(T_\lambda) \simeq \mathbb{Z}[G] \cap \mathbb{Q}[G]_\lambda.$$

L'action algébrique de G ainsi définie sur les tores T et T_λ est compatible à l'isogénie ci-dessus, et prolonge l'action naturelle de G sur $T(\bar{\mathbb{Q}}) = K^\times$. Grâce à cette action, nous pouvons donner maintenant une interprétation géométrique des composantes isotypiques de $\bar{E} \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$.

Rappelons tout d'abord le lien entre l'ensemble Λ des caractères de représentations \mathbb{Q} -irréductibles du groupe G et l'ensemble Φ de ses représentations absolument irréductibles : le groupe de Galois absolu \mathcal{G} opère sur Φ (le conjugué d'un caractère absolument irréductible est encore un caractère absolument irréductible) et il y a correspondance biunivoque entre Λ et l'ensemble des orbites déterminées dans Φ par l'action de \mathcal{G} . Autrement dit, on a une partition de Φ , de la forme :

$$\Phi = \coprod_{\lambda \in \Lambda} \Phi_\lambda ,$$

où Φ_λ est formé de caractères conjugués qui ont en particulier même degré.

Le groupe G agit donc sur les espaces tangents respectifs t et t_λ de chacun des tores T et T_λ . Pour tout caractère $\varphi \in \Phi$, notons t_φ la φ -composante isotypique du G -module $t(\bar{\mathbb{Q}}_p)$. On a alors

$$t_\varphi \simeq \text{Hom}(\bar{\mathbb{Q}}_p[G]_\varphi, \bar{\mathbb{Q}}_p) ,$$

d'où il s'ensuit que

$$\dim(t_\varphi) = d_\varphi^2 .$$

D'autre part, comme $\text{End}_0(T_\lambda) \simeq \mathbb{Q}[G]_\lambda$, on a

$$t_\lambda(\bar{\mathbb{Q}}_p) = \bigoplus_{\varphi \in \Phi_\lambda} t_\varphi , \quad \lambda \in \Lambda .$$

Désignons alors par

$$\mathcal{E} \subseteq t(\bar{\mathbb{Q}}_p)$$

le \mathbb{Q}_p -espace tangent à l'origine du groupe analytique \bar{E} . Ce sous-espace \mathcal{E} est stable sous l'action de G . Soit \mathcal{E}_φ , $\varphi \in \Phi$, la φ -composante isotypique du G -module

$$\bar{\mathbb{Q}}_p \mathcal{E} \subseteq t(\bar{\mathbb{Q}}_p) .$$

L'exponentielle p -adique, qui est localement inversible, permet alors d'identifier les $\bar{\mathbb{Q}}_p$ -espaces vectoriels \mathcal{E}_φ et $(\bar{E} \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p)_\varphi$. Ces espaces ont donc même dimension.

$$\dim (\mathcal{E}_\varphi) = \rho_\varphi d_\varphi, \varphi \in \Phi .$$

5.— Un énoncé de transcendance.

Nous présentons maintenant en termes de groupes algébriques un résultat de transcendance, dû à M. Waldschmidt, qui constitue l'argument essentiel de la preuve du théorème. Il s'agit d'un cas particulier du théorème 4.1 de [10]. Dans ce paragraphe, les questions de rationalité sont sans importance : le corps de base des groupes algébriques considérés est $\bar{\mathbb{Q}}$.

Soient T un tore linéaire, Γ un sous-groupe de type fini de $T(\bar{\mathbb{Q}}_p)$, et W un sous-espace vectoriel de $t(\bar{\mathbb{Q}}_p)$ (t désigne comme précédemment l'espace tangent à l'origine du tore T). Supposons que W soit distinct de $t(\bar{\mathbb{Q}}_p)$. On définit alors un coefficient de répartition $\mu^\#(\Gamma, T, W)$ comme la valeur minimale des quotients

$$\frac{\dim(T/T') + rg(\Gamma / \Gamma \cap T')}{\dim(T/T') - \dim(W/W \cap t'(\bar{\mathbb{Q}}_p))},$$

où T' décrit l'ensemble des sous-tores de T tels que

$$t'(\bar{\mathbb{Q}}_p) + W \neq t(\bar{\mathbb{Q}}_p),$$

et où $t' \subseteq t$ désigne l'espace tangent à l'origine du sous-tore T' . Supposons que Γ' soit contenu dans un voisinage de l'origine de $T(\bar{\mathbb{Q}}_p)$, où le logarithme du groupe de Lie p -adique $T(\bar{\mathbb{Q}}_p)$ est inversible. Soit V un sous-espace vectoriel de $t(\bar{\mathbb{Q}}_p)$ tel que :

$$W \subseteq V, \log \Gamma \subseteq V.$$

Le résultat en question est l'énoncé suivant :

PROPOSITION 2. *Supposons que V soit distinct de $t(\bar{\mathbb{Q}}_p)$, que W soit rationnel sur $\bar{\mathbb{Q}}$, et que $\Gamma \subseteq T(\bar{\mathbb{Q}})$. Alors*

$$\mu^\#(\Gamma, T, W) \leq \frac{\dim T}{\dim T - \dim V}.$$

Nous dirons qu'un sous-groupe Γ de T est bien réparti relativement à un sous-espace W de t si

$$\mu^\#(\Gamma, T, W) = \frac{\dim T + rg \Gamma}{\dim T - \dim W},$$

autrement dit, si le minimum des quotients ci-dessus est atteint pour $T' = \{1\}$. Lorsque W ne contient aucun espace tangent de sous-tore non trivial de T , les inégalités

$$\frac{\dim T' + rg(T \cap T')}{\dim T' - \dim(W \cap t'(\bar{\mathbb{Q}}_p))} \leq \frac{\dim T + rg \Gamma}{\dim T - \dim W},$$

pour tout sous-tore non trivial $T' \subseteq T$, suffisent à assurer la bonne répartition de Γ relativement à W .

Remarque : Nous avons conservé la terminologie de *bonne répartition* introduite par M. Waldschmidt dans [9] dans le cas particulier du groupe additif. En général, cette notion ne coïncide pas nécessairement avec l'intuition; ainsi le groupe nul est bien réparti dans le tore T_λ relativement aux sous-espaces W envisagés dans le paragraphe qui suit.

6.– Questions de répartition dans les tores T_λ .

On examine ici le cas particulier du tore $T = \text{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$. Reprenons les notations du paragraphe 4 et fixons un caractère $\varphi \in \Phi$. Désignons par λ l'élément de Λ tel que $\varphi \in \Phi_\lambda$, et considérons le sous-espace

$$W = \bigoplus_{\psi \in \Phi_\lambda \setminus \{\varphi\}} t_\psi$$

de $t_\lambda(\bar{\mathbb{Q}}_p)$. On a alors la

PROPOSITION 3. *Le groupe $\Gamma = T_\lambda(\mathbb{Z})$ est bien réparti dans le tore T_λ relativement au sous-espace W .*

Preuve : Soit T' un sous-tore non trivial de T_λ , et soit t' son espace tangent à l'origine, vu comme un sous-espace de t_λ . Notons

$$d' = \dim T', \quad \ell' = rg(\Gamma \cap T'), \quad \tau' = \dim(W \cap t'(\bar{\mathbb{Q}}_p)), \quad f = \text{card } \Phi_\lambda.$$

On a :

$$\dim T_\lambda = fd_\varphi^2, \quad rg\Gamma = fd_\varphi r_\varphi, \quad \dim W = (f-1)d_\varphi^2,$$

de telle sorte que nous devons vérifier $\tau' \neq d'$ et l'inégalité :

$$\frac{\ell' + d'}{d' - \tau'} \leq \frac{f(d_\varphi + r_\varphi)}{d_\varphi}.$$

Pour tout caractère $\psi \in \Phi_\lambda$, désignons par t'_ψ la projection du sous-espace $t'(\bar{\mathbb{Q}}_p)$ sur la composante t_ψ dans la décomposition isotypique

$$t_\lambda(\bar{\mathbb{Q}}_p) = \bigoplus_{\psi \in \Phi_\lambda} t_\psi.$$

Puisque

$$t'_\varphi \simeq (t'(\bar{\mathbb{Q}}_p) + W)/W,$$

le dénominateur $d' - \tau'$ s'interprète comme la dimension du $\bar{\mathbb{Q}}_p$ -espace vectoriel t'_φ . D'autre part, le sous-espace $t'(\bar{\mathbb{Q}}_p)$ s'identifie à $\text{Hom}(X(T_\lambda)/H, \bar{\mathbb{Q}}_p)$, où H désigne l'orthogonal de T' dans $X(T_\lambda)$. Comme H est rationnel sur \mathbb{Q} , et que les sous-espaces t_ψ , $\psi \in \Phi_\lambda$, admettent des bases rationnelles sur $\bar{\mathbb{Q}}$ deux à deux conjuguées sur \mathbb{Q} , les t'_ψ , $\psi \in \Phi_\lambda$ admettent aussi de telles bases. En particulier, ceux-ci ont même dimension. De

l'inclusion

$$t'(\bar{\mathbb{Q}}_p) \subseteq \bigoplus_{\psi \in \Phi_\lambda} t'_\psi,$$

on déduit l'inégalité

$$d' = \dim T' \leq \sum_{\psi \in \Phi_\lambda} \dim(t'_\psi) = f \dim(t'_\varphi) = f(d' - r') ,$$

qui fournit une minoration du dénominateur $d' - r'$, et qui montre incidemment que W ne contient aucun espace tangent de sous-tore non trivial de T_λ .

Désignons maintenant par G'' l'adhérence de Zariski dans T_λ du groupe $\Gamma \cap T'$, et par T'' la composante connexe de l'origine du groupe algébrique (de type multiplicatif) G'' . Puisque Γ est formé de points \mathbb{Q} -rationnels, les groupes algébriques G'' et T'' sont définis sur \mathbb{Q} . D'autre part, il est clair que

$$\Gamma \cap T' = \Gamma \cap G''$$

et que

$$\Gamma \cap T'' = T_\lambda(\mathbb{Z}) \cap T'' = T''(\mathbb{Z}) .$$

Par ailleurs, on peut supposer sans restriction que $\lambda \neq 1_G$, de telle sorte que le tore T_λ soit anisotrope. D'après la proposition 1, on a alors

$$\ell' = rg(T''(\mathbb{Z})) = r_\chi ,$$

où χ désigne le caractère de l'action de G sur $X(T'')$. Comme $T'' \subseteq T'$, on obtient finalement la majoration

$$\frac{\ell' + d'}{d' - r'} \leq f(1 + \frac{\ell'}{d'}) \leq f(1 + \frac{\ell'}{\dim T''}) = f(1 + \frac{r_\chi}{d_\chi}) .$$

Il suffit alors de remarquer que $r_\chi/d_\chi = r_\varphi/d_\varphi$, puisque χ est un multiple entier du caractère $\sum_{\psi \in \Phi_\lambda} \psi$.

7.- Preuve du théorème.

Soit φ le caractère absolument irréductible considéré dans le théorème et soit λ l'élément de Λ tel que $\varphi \in \Phi_\lambda$.

Fixons un sous-groupe Γ_λ d'indice fini de $T_\lambda(\mathbb{Z})$, qui soit contenu dans un voisinage de l'origine de $T_\lambda(\mathbb{Z}_p)$ où le logarithme p -adique est inversible. Conservons les notations des paragraphes 4 et 6 et considérons le sous-espace

$$V = \mathcal{E}_\varphi \oplus W$$

de $t_\lambda(\bar{\mathbb{Q}}_p)$. Il est clair que W est un sous-espace $\bar{\mathbb{Q}}$ -rationnel de V et que

$$\log \Gamma_\lambda \subseteq V.$$

Puisque Γ_λ est d'indice fini dans $T_\lambda(\mathbb{Z})$, la proposition 3 nous permet de calculer le coefficient $\mu^\#(\Gamma_\lambda, T_\lambda, W)$:

$$\mu^\#(\Gamma_\lambda, T_\lambda, W) = \mu^\#(\Gamma_\lambda(\mathbb{Z}), T_\lambda, W) = \frac{f(r_\varphi + d_\varphi)}{d_\varphi}.$$

Il est alors loisible d'appliquer la proposition 2 aux données $(\Gamma_\lambda, T_\lambda, V, W)$. Dans ce cas,

$$\dim V = \rho_\varphi d_\varphi + (f-1)d_\varphi^2, \quad \dim T_\lambda = f d_\lambda^2.$$

La minoration attendue de ρ_φ s'ensuit immédiatement.

Manuscrit reçu le 28 septembre 1988

BIBLIOGRAPHIE

- [1] A. Borel.— *Linear algebraic groups*, Benjamin, Reading Mass., 1969.
- [2] M. Emsalem.— *Places totalement décomposées dans des \mathbb{Z}_p -extensions d'un corps de nombres*, Colloque de théorie des nombres de Laval, 1987, à paraître.
- [3] M. Emsalem.— *Transcendance et \mathbb{Z}_p -extensions*, Séminaire de Théorie des Nombres de Bordeaux, 1987/88.
- [4] S. Lang.— *Représentations localement algébriques dans les corps cyclotomiques*, dans le Séminaire de Théorie des Nombres, Paris 1981/82, Birkhäuser, P.M. 38.
- [5] M. Laurent.— *Rang p -adique d'unités et action de groupes*, à paraître au J. reine angew. Math. .
- [6] T. Ono.— *Some arithmetic properties of linear algebraic groups*, Annals of Math., 70, 1959, 266–290.
- [7] T. Ono.— *Arithmetic of algebraic tori*, Annals of Math., 74, 1961, 101–139.
- [8] J.-P. Serre.— *Abelian ℓ -adic representations and elliptic curves*, W.A. Benjamin, 1979.
- [9] M. Waldschmidt.— *Nombres transcendants et groupes algébriques*, Astérisque 69–70, 1979.

- [10] M. Waldschmidt.— *On the transcendence methods of Gel'fond and Schneider*, New Advances in Transcendence Theory, éd. par A. Baker, Cambridge University Press., 1988.
- [11] A. Weil.— *Adeles and algebraic groups*, Birkhäuser, P.M. 23.

Michel LAURENT
Institut Henri Poincaré
11, rue P. et M. Curie
75231 PARIS CEDEX 05

Séminaire de Théorie des Nombres

Paris 1987-88

LE GROUPE DES CLASSES AMBIGES (AU SENS STRICT)

S. LOUBOUTIN

Nous complétons et concluons ici l'étude de l'arithmétique des corps quadratiques réels, à l'aide de la technique des cycles d'idéaux réduits introduite par A. Chatelet (2) et réinterprétée en termes de fractions continues dans (4), en déterminant l'ordre du groupe des classes ambiges au sens strict. Ce résultat s'obtient habituellement, comme corollaire de la théorie des genres, en utilisant les symboles de Hilbert et le résultat analytique de Dirichlet sur l'infinité des nombres premiers dans les progressions arithmétiques (voir (1) ou (6)), mais peut aussi s'obtenir par des méthodes purement algébriques (voir (3)). Il nous paraît néanmoins intéressant d'en donner une preuve indépendante de la théorie des genres nous permettant de l'énoncer plus précisément : nous donnons explicitement la relation de principialité (stricte) entre les idéaux premiers ramifiés sous une forme différente de celle habituellement donnée qui, elle, fait intervenir l'unité fondamentale et oblige donc, pour être explicitée, à manipuler de grands nombres, dès lors que cette unité est grande (voir (7)). Si nous n'utilisons que la notion *moderne* d'idéal, les résultats que nous obtenons sont néanmoins déjà plus ou moins contenus dans des travaux plus anciens utilisant la technique des formes quadratiques binaires (nous pensons aux travaux princeps de Gauss).

1.— Notations et rappels.

Nous reprenons les notations de (4) : $d \geq 2$ désigne un entier libre de carrés, D le discriminant du corps quadratique réel $\mathbb{Q}(\sqrt{d})$, t le nombre de facteurs premiers distincts de D , \mathcal{H} et \mathcal{H}_+ les groupes des classes au sens large et restreint, \mathcal{A} et \mathcal{A}_+ les sous-groupes des classes ambiges au sens large et restreint (les classes d'ordre 2, ou encore, les classes invariantes) et ω_0 le générateur habituel de l'anneau \mathbb{R} des entiers du corps ($\omega_0 = \sqrt{d}$ si 4 divise D

et $\omega_0 = (1 + \sqrt{d})/2$ sinon). Nous supposons l'unité fondamentale de norme +1, sinon la notation de classe restreinte coïncide avec celle de classe stricte et nous avons alors déjà vu dans (4) que \mathcal{A} était alors d'ordre 2^{t-1} et engendré par les idéaux premiers ramifiés.

Un idéal entier \mathbb{I} est dit primitif s'il n'est divisible par aucun idéal de la forme (n) , n entier et $n \geq 2$. Les idéaux primitifs s'écrivent, en tant que \mathbb{Z} -modules, sous la forme $\mathbb{I} = \mathbb{Z}Q + \mathbb{Z}(P+\sqrt{D})/2 := (Q, (P+\sqrt{D})/2)_{\mathbb{Z}}$ avec $4Q$ divisant $D - P^2$, où Q est la norme de cet idéal \mathbb{I} . Un idéal primitif est dit réduit si on peut choisir P (de façon alors unique) modulo $2Q$ pour que son réel quadratique associé, défini par $x_0(\mathbb{I}) = (P+\sqrt{D})/2Q$, soit réduit (i.e. vérifie $x_0(\mathbb{I}) > 1$ et $-1/x_0(\mathbb{I})' > 1$, où " $'$ " désigne le conjugué dans le corps).

L'application qui à un idéal associe son réel quadratique définit une bijection de l'ensemble des idéaux réduits du corps sur l'ensemble fini des réels quadratiques réduits de discriminant D . Chaque classe large d'idéaux contenant au moins un idéal réduit, le nombre $h(d)$ des classes d'idéaux au sens large est fini. Deux idéaux réduits sont équivalents au sens large (respectivement, au sens restreint) dans le groupe des classes d'idéaux si et seulement si leurs réels quadratiques associés sont équivalents sous l'action de $GL_2(\mathbb{Z})$ (respectivement, sous l'action de $SL_2(\mathbb{Z})$).

Soit $\mathbb{I} = \mathbb{I}_0$ un idéal réduit. $x_0(\mathbb{I})$ admet un développement en fractions continues purement périodique : $x_0(\mathbb{I}) = [n_0, n_1, \dots, n_{L(\mathbb{I})-1}]$. Les $L(\mathbb{I})$ réels quadratiques réduits définis par $x_i(\mathbb{I}) = [n_i, \dots, n_{L(\mathbb{I})-1}, n_0, \dots, n_{i-1}]$, $0 \leq i \leq L(\mathbb{I}) - 1$, sont les seuls réels quadratiques réduits équivalents sous l'action de $GL_2(\mathbb{Z})$ à $x_0(\mathbb{I})$ ($x_i(\mathbb{I})$ est appelé le i -ième quotient complet de $x_0(\mathbb{I})$). Ils s'écrivent de manière unique sous la forme $x_i(\mathbb{I}) = (P_i(\mathbb{I}) + \sqrt{D})/2Q_i(\mathbb{I})$ avec $P_i(\mathbb{I})$ et $Q_i(\mathbb{I})$ entiers, et $Q_i(\mathbb{I})$ divisant $(D - P_i(\mathbb{I})^2)/4$. Les \mathbb{Z} -modules $\mathbb{I}_i = (Q_i(\mathbb{I}), (P_i(\mathbb{I}) + \sqrt{D})/2)_{\mathbb{Z}}$ sont des idéaux réduits de réels quadratiques associés $x_0(\mathbb{I}_i)$ égaux à $x_i(\mathbb{I})$. L'ensemble $\mathcal{C}(\mathbb{I}) = \{\mathbb{I}_i ; 0 \leq i \leq L(\mathbb{I}) - 1\}$ est appelé le cycle large des idéaux réduits de l'idéal réduit \mathbb{I} ; en tant qu'ensemble, c'est l'ensemble des idéaux réduits équivalents au sens large à \mathbb{I} (pour ces rappels, voir (4)).

L'unité fondamentale étant supposée de norme +1, les cycles larges d'idéaux réduits sont de longueur paire. Les $L(\mathbb{I})/2$ réels quadratiques réduits $\mathbb{I}_i(\mathbb{I})$, $0 \leq i \leq L(\mathbb{I})-1$ et i pair, sont alors les seuls quadratiques réduits équivalents sous l'action de $SL_2(\mathbb{Z})$ à $x_0(\mathbb{I})$. L'ensemble $\mathcal{C}_s(\mathbb{I}) = \{\mathbb{I}_i ; 0 \leq i \leq L(\mathbb{I})-1, i \text{ pair}\}$ est appelé le cycle strict des idéaux réduits de l'idéal réduit \mathbb{I} ; en tant qu'ensemble, c'est l'ensemble des idéaux réduits équivalents au sens strict à \mathbb{I} . Nous partitionnons donc les idéaux réduits du corps en $h(d)$ cycles larges disjoints d'idéaux réduits, et en $2h(d)$ cycles stricts disjoints d'idéaux réduits. Chaque cycle large $\mathcal{C}_\ell(\mathbb{I})$ se décompose en deux cycles stricts : $\mathcal{C}_{s,0}(\mathbb{I}) = \{\mathbb{I}_i ; 0 \leq i \leq L(\mathbb{I})-1 \text{ et } i \text{ pair}\} = \mathcal{C}_s(\mathbb{I}_0)$ et $\mathcal{C}_{s,1}(\mathbb{I}) = \{\mathbb{I}_i ; 0 \leq i \leq L(\mathbb{I})-1 \text{ et } i \text{ impair}\} = \mathcal{C}_s(\mathbb{I}_1)$. Rappelons que si \mathbb{I} est réduit, son idéal conjugué \mathbb{I}' l'est également et nous extrayons de (4) le résultat suivant :

PROPOSITION. Si $N(\epsilon_0) = +1$ on est dans un des deux cas exclusifs suivants :

- α) Le cycle large d'idéaux réduits ambiges contient exactement 2 idéaux invariants. Il y a exactement 2^{t-2} cycles larges d'idéaux réduits ambiges de ce type.
- β) Le cycle large d'idéaux réduits ambiges ne contient pas d'idéal invariant. Il n'existe de cycles de ce type que si D est somme de deux carrés, et il en existe alors exactement 2^{t-2} .
- γ) On est dans le cas α) si et seulement si $\mathbb{I}' = \mathbb{I}_i$ avec i pair pour tout idéal \mathbb{I} du cycle et les deux idéaux invariants du cycle sont alors $\mathbb{I}_{i/2}$ et $\mathbb{I}_{(i+L(\mathbb{I}))/2}$; on est dans le cas β) si et seulement si $\mathbb{I}' = \mathbb{I}_i$ avec i impair pour tout idéal \mathbb{I} du cycle.

2.- 2-rang du groupe des classes (au sens strict).

Soit \mathbb{I} un idéal réduit ambigu au sens strict. Son idéal conjugué \mathbb{I}' est réduit et lui est équivalent au sens strict; il est donc dans le cycle strict $\mathcal{C}_s(\mathbb{I})$. Nous avons donc $\mathbb{I}' = \mathbb{I}_i$ pour un i pair. D'après le théorème ci-dessus, le cycle large $\mathcal{C}_\ell(\mathbb{I})$ contient deux idéaux réduits invariants. Réciproquement si le cycle

large $\mathcal{C}_\ell(\mathbb{I})$ contient deux idéaux réduits invariants, $\mathbb{J}' = \mathbb{J}_j$ avec j pair pour tout idéal \mathbb{J} du cycle strict $\mathcal{C}_s(\mathbb{I})$ qui est donc stable par conjugaison, et \mathbb{I} est ambigu au sens strict. Puisqu'il existe précisément 2^{t-2} cycles larges d'idéaux réduits contenant deux idéaux invariants et que ces cycles larges se décomposent chacun en deux cycles stricts, il y a précisément 2^{t-1} cycles stricts d'idéaux ambigus au sens strict et \mathcal{A}_+ est d'ordre 2^{t-1} .

Soit \mathbb{I} un idéal réduit ambigu au sens strict avec $\mathbb{I}' = \mathbb{I}_i$, les deux idéaux invariants du cycle large $\mathcal{C}_\ell(\mathbb{I})$ sont d'indices $i/2$ et $(i+L(\mathbb{I}))/2$. Si 4 divise $L(\mathbb{I})$, ils sont donc tous deux dans le même cycle strict : si 4 ne divise pas $L(\mathbb{I})$, chaque cycle strict $\mathcal{C}_{s,0}(\mathbb{I})$ et $\mathcal{C}_{s,1}(\mathbb{I})$ contient un de ces deux idéaux invariants. Pour δ libre de carrés divisant D , nous notons \mathbb{I}_δ l'unique idéal primitif invariant de norme δ et notons $\tilde{\mathbb{I}}_\delta$, appelé l'idéal dual de \mathbb{I}_δ , l'idéal primitif invariant $\mathbb{I}_{\delta'}$ de norme δ' où δ' est libre de carrés et défini par : $d\delta = \delta'n^2$. Puisque $(\sqrt{d})\mathbb{I}_\delta = (n)\tilde{\mathbb{I}}_\delta$, un idéal invariant et son idéal dual sont dans la même classe large d'idéaux, mais dans deux classes strictes distinctes. Nous en déduisons que toute classe stricte ambigu contient au moins, puis exactement deux idéaux invariants primitifs : si un des cycles strict contient deux idéaux réduits invariants, alors l'autre classe stricte contient les idéaux duals de ceux-ci; si chacun des cycles stricts contient un idéal réduit invariant, alors chaque classe stricte contient un idéal invariant réduit et l'idéal primitif invariant dual de l'idéal invariant réduit de l'autre cycle strict. \mathcal{A}_+ est donc engendré par les 2^t idéaux premiers ramifiés et nous connaissons la relation de principauté stricte entre ces idéaux. En effet, prenons pour idéal réduit l'anneau \mathbb{R} des entiers et notons δ_0 la norme de l'idéal $\mathbb{R}_{L(\mathbb{R})}/2$, c'est un entier libre de carrés et divisant D comme norme d'un idéal primitif invariant (voir également (5)). La relation de principauté stricte entre les idéaux premiers ramifiés est alors : $\mathbb{I}_{\delta_0} = (\alpha)$ si $L(\mathbb{R})$ est congru à 0 modulo 4, et $\tilde{\mathbb{I}}_{\delta_0} = (\beta)$ si $L(\mathbb{R})$ est congru à 2 modulo 4. Soit :

THEOREME 1. Si $N(\epsilon_0) = +1$, \mathcal{A}_+ est d'ordre 2^{t-1} et engendré par les idéaux premiers ramifiés. La relation de principauté stricte entre les 2^t idéaux premiers ramifiés est entièrement déterminée par le $L/2$ ième quotient complet du développement en fractions continues de w_0 (où L est la longueur de la période primitive de ce développement).

3.- 4-rang du groupe des classes (au sens strict) et application.

Supposons maintenant D somme de deux carrés et soit $\mathcal{C}_\ell(\mathbb{I})$ un cycle large d'idéaux réduits ne contenant pas d'idéal invariant (il y a 2^{t-2} tels cycles d'idéaux par la proposition précédente) et $\mathcal{C}_{s,0}(\mathbb{I})$ et $\mathcal{C}_{s,1}(\mathbb{I})$ sa décomposition en deux cycles stricts disjoints. Si \mathbb{J} est dans $\mathcal{C}_\ell(\mathbb{I})$, nous avons d'après la proposition précédente : $\mathbb{J}' = \mathbb{J}_j$ avec j impair. Conséquemment $\mathcal{C}_{s,0}(\mathbb{I})$ et $\mathcal{C}_{s,1}(\mathbb{I})$ sont échangées par conjugaison. Les classes strictes qu'ils définissent sont donc d'ordre exactement quatre dans le groupe des classes strictes. En effet, elles sont d'ordre deux dans le groupe des classes larges, donc d'ordre divisant quatre dans le groupe des classes strictes, et ne sont pas d'ordre deux au sens strict puisqu'échangées par conjugaison et distinctes. En particulier, nous avons :

THEOREME 2. Si d est somme de deux carrés et si l'unité fondamentale est de norme $+1$, le 4-rang du groupe \mathcal{H}_+ n'est pas nul.

Nous en déduisons le résultat suivant bien connu (voir (1) ou (6)) :

COROLLAIRE. Si $d = pq$, p et q premiers congrus à 1 modulo 4 de symbole de Legendre (p/q) valant -1 , l'unité fondamentale est de norme -1 .

Preuve : Supposons-la égale à $+1$. d étant somme de deux carrés il existe un idéal \mathbb{I} d'ordre quatre dans \mathcal{H}_+ . \mathbb{I}^2 est alors d'ordre deux dans \mathcal{A}_+ qui est, d'après le théorème 1, de cardinal deux et engendré par l'idéal premier \mathcal{P} au dessus de (p) , ou par l'idéal premier \mathcal{Q} au-dessus de (q) . C'est deux idéaux étant d'ordre 2 dans \mathcal{A}_+ , on peut supposer \mathbb{I} non divisible par \mathcal{P} et \mathcal{Q} . Nous avons, en supposant par exemple que \mathcal{P} engendre \mathcal{A}_+ , $\mathbb{I}^2 = (\alpha)\mathcal{P}$ avec

α de norme positive. Ecrivons $\alpha = x/y$ avec x et y entiers algébriques. La valuation \mathcal{L} -adique de α étant nulle, x et y ont même valuation, disons n . L'idéal fractionnaire $\mathcal{P}\mathcal{L}^{-1} = (\sqrt{d}/q)$ étant principal, les idéaux $\mathcal{P}^n\mathcal{L}^{-n}(x)$ et $\mathcal{P}^n\mathcal{L}^{-n}(y)$ sont premiers à \mathcal{L} et principaux. Dans l'écriture $\alpha = x/y$, on peut donc supposer x et y premiers à \mathcal{L} . Nous avons : $N(y)N(\mathbb{I})^2 = pN(x)$ et q ne divise pas $N(x)$. En passant modulo q et remarquant que q divisant d les normes des entiers du corps sont des carrés modulo q , nous obtenons alors : $(p/q) = +1$.

Manuscrit reçu le 30 juillet 1988

BIBLIOGRAPHIE

- [1] Z.I. Borevitch et I.R. Chafarevitch.— *Théorie des Nombres*, Gauthiers-Villars Paris, 1967, Chapitre III, § 8.
- [2] A. Chatelet.— *L'arithmétique des corps quadratiques*, l'Enseignement mathématique, N° 9; Genève 1962.
- [3] Nguyen Quang Do.— *Unités de norme -1 d'un corps quadratique réel*, Séminaire Delange—Pisot—Poitou; 1975/76, N° 66.
- [4] S. Louboutin.— *Groupes des classes d'idéaux triviaux*, à paraître, Acta Arithmetica, Vol. 54, N° 1.
- [5] S. Louboutin.— *Continued fractions and real quadratic fields*, J. of Nb. Th., Vol. 30, Nb. 2, October 1988, 167–176.
- [6] P. Morton.— *On Redei's theory of the Pell equation*, J. Reine, 307/308 (1979), 373–398.
- [7] D.B. Zagier.— *Zetafunktionen und quadratische Körper*, Hochschultext, Springer—Verlag (1981).

Stéphane LOUBOUTIN
 Université de Paris VII
 U.E.R. de Mathématiques et Informatique
 Unité Associée au C.N.R.S. N° 212
 Tour 45–55, 5ème étage
 2, place Jussieu
 75251 PARIS CEDEX 05

*Séminaire de Théorie des Nombres
Paris 1987-88*

SUR L'ARITHMÉTIQUE DES CORPS DE NOMBRES p -RATIONNELS
A. MOVAHHEDI et T.NGUYEN QUANG DO

0.— Introduction et heuristique.

Soient K un corps de nombres, de degré fini sur \mathbb{Q} , et p un nombre premier fixé. Soient S_p l'ensemble des p -places (i.e. des places au-dessus de p) de K et S un ensemble fini de places de K contenant S_p . Soient K_S la pro- p -extension S -ramifiée (i.e. non ramifiée en dehors de S) maximale de K , et $G_S = G_S(K) = \text{Gal}(K_S/K)$. L'objet essentiel de la théorie de la S -ramification, ou **ramification restreinte**, est l'étude du groupe de Galois G_S , dont la structure reflète les propriétés arithmétiques du corps K par rapport au nombre premier p . On sait que la théorie habituelle du corps de classes décrit (mais de façon non totalement explicite) la structure de l'abélianisé $G_S^{ab} = G_S/[G_S, G_S]$, où $[G_S, G_S]$ désigne le sous-groupe fermé engendré par les commutateurs. En procédant par *approximations successives*, on peut se proposer de développer le corps de classes dans un certain nombre de directions, chaque étape correspondant à l'étude d'un objet naturellement associé à G_S . Ainsi :

a) Le **corps de classes explicite** serait la description explicite de G_S^{ab} (voir par exemple [M-W]). D'après la théorie classique, on a un isomorphisme de \mathbb{Z}_p -modules : $G_S^{ab}(K) \cong \mathbb{Z}_p^\rho \times T_S(K)$, où ρ est le \mathbb{Z}_p -rang, lié à la conjecture de Leopoldt, et $T_S(K)$ est la \mathbb{Z}_p -torsion, liée aux fonctions L p -adiques (quand elles sont définies pour K) ainsi qu'à divers noyaux de la K -théorie (voir par exemple [NG2]). Le corps K sera dit **p -rationnel** (2-1) si K vérifie la conjecture de Leopoldt en p et si $T_{S_p}(K) = 0$. Sous ces hypothèses simplificatrices, la structure de $G_S^{ab}(K)$ est bien sûr entièrement connue, le problème se reportant sur la description de $G_S^{ab}(L)$, où L est une extension de K contenue dans K_S (3-7).

b) Le *corps de classes nilpotent* serait la description des quotients $G_S/G_S^{(i)}$, où les $G_S^{(i)}$ sont les termes de la suite centrale descendante de G_S . Une étude du *corps de classes nilpotent de classe deux* (i.e. la description de $G_S/G_S^{(2)}$) a été amorcée par Fröhlich pour $K = \mathbb{Q}$ ([F], § 4) et par Ullom et Watt pour $K = \mathbb{Q}(\mu_p)$, p régulier ([UW]). Ces auteurs utilisent de façon essentielle la non-divisibilité par p du nombre de classes de K , mais l'on verra en fait (§ 4) que la bonne hypothèse simplificatrice est la p -rationalité de K .

C) Le *corps de classes résoluble* serait la description des quotients $G_S/G_S^{(i)}$, où les $G_S^{(i)}$ sont les termes de la suite dérivée de G_S . Par exemple, le *corps de classes résoluble de classe deux* pourrait être abordé via l'étude du module $G_S^{(1)}/G_S^{(2)}$ sur l'algèbre complète $\Lambda_S = \mathbb{Z}_p[[G_S^{ab}]]$, c'est-à-dire via une généralisation naturelle de la théorie d'Iwasawa. Pour K totalement réel, l'algèbre Λ_S est par exemple étudiée dans [G3] du point de vue des mesures p -adiques; si K est totalement réel et p -rationnel (par exemple, si $K = \mathbb{Q}$), l'algèbre Λ_{S_p} se réduit à l'algèbre d'Iwasawa habituelle $\mathbb{Z}_p[[T]]$.

d) Enfin, le *corps de classes non abélien* (en p) serait la description de G_S en entier. Suivant le point de vue local-global habituel, on introduit, pour toute place $v \in S$, le groupe de Galois G_v de la pro- p -extension maximale $K_v(p)$ du complété K_v de K en v . L'abélianisé G_v^{ab} est isomorphe, par le corps de classes local, au complété p -adique $\mathcal{K}_v = \varprojlim K_v^\times / K_v^\times p^m$. Quant au pro- p -groupe G_v lui-même, sa description par générateurs et relations est bien connue depuis Šafarevič et Demuškin (voir [SE]). On peut se proposer, comme le fait H. Koch [KO], de décrire G_S par générateurs et relations, par des méthodes locales-globales. En adoptant un point de vue légèrement différent, on peut aussi étudier le morphisme $\psi_S: \prod_{v \in S} G_v \rightarrow G_S$, qui est un relèvement non abélien du morphisme de reciprocité du corps de classes $\psi_S^{ab}: \prod_{v \in S} \mathcal{K}_v \rightarrow G_S^{ab}$. Ici, $\prod_{v \in S}$ désigne le pro- p -produit libre (i.e. le produit libre dans la catégorie des pro- p -groupes) et le morphisme ψ_S est fabriqué de la façon suivante :

Pour $v \in S$, on choisit un prolongement de v à K_S , et l'on note G_S^v le groupe de décomposition correspondant : G_S^v est un quotient de G_v , d'où un homomorphisme $\psi_v : G_v \rightarrow G_S^v \hookrightarrow G_S$, qui dépend du choix du prolongement de v à K_S (i.e. du choix d'un plongement de K_S dans $K_v(p)$). Par définition, $\psi_S = \bigcup_{v \in S} \psi_v : \psi_S$ dépend aussi du choix des prolongements des places $v \in S$, mais son abélianisé ψ_S^{ab} n'en dépend pas. Par analogie avec le cas géométrique (voir ci-dessous), on étudie séparément les morphismes $\psi_{S_p} : \bigcup_{v \in S_p} G_v \rightarrow G_S$ et $\psi_T : \bigcup_{w \in T} G_w \rightarrow G_S$, où $T = S \setminus S_p$. Dans certains cas favorables, et au niveau infini (i.e. en remplaçant K par une extension infinie, par exemple par K_{S_p} ou par la \mathbb{Z}_p -extension cyclotomique de K), ψ_T est un isomorphisme ([KZ2], [NM], [WB2],...). Au niveau fini, la situation est naturellement plus compliquée. H. Koch ([Ko], § 11–5) et K. Wingberg ([WB1], § 3) ont donné des caractérisations de couples (K, S) tels que ψ_T soit un isomorphisme. On montrera en 3.3 que ψ_T est un isomorphisme si et seulement si K est p -rationnel et S vérifie une certaine condition de *primitivité*. Les corps de nombres p -rationnels apparaissent ainsi comme de bons analogues des corps de fonctions de genre zéro, et l'isomorphisme ψ_T comme une généralisation non abélienne de la **formule du produit**. Plus précisément :

Soit X une courbe projective, lisse, irréductible sur un corps algébriquement clos k , de caractéristique nulle. Soient F le corps de fonctions de X sur k , et $S = \{P_1, \dots, P_s, \infty\}$ un ensemble fini de points de X . Le groupe de Galois de l'extension algébrique S -ramifiée maximale de F s'identifie, d'après la théorie des revêtements, au groupe fondamental algébrique $\pi_1(X \setminus S)$, i.e. au groupe de Galois du revêtement universel étale de $X \setminus S$. Pour déterminer $\pi_1(X \setminus S)$, on se ramène, par un raisonnement standard, au cas où $k = \mathbb{C}$. Le théorème d'existence de Riemann entraîne alors que $\pi_1(X \setminus S)$ est le complété profini du groupe fondamental topologique $\pi_1^{top}(X \setminus S)$, qui se décrit par la topologie algébrique. En particulier, si X est de genre zéro, on obtient un

isomorphisme : $\pi_1(X \setminus \{P_1, \dots, P_s, \infty\}) \cong \prod_{1 \leq i \leq s}^* G_{P_i}$, où G_{P_i} est le groupe d'inertie (pro-cyclique) en P_i . En termes de générateurs et relations, $\pi_1(X \setminus S)$ peut être décrit par $(s+1)$ générateurs $u_1, u_2, \dots, u_s, u_\infty$ et une seule relation $u_1 \cdot u_2 \cdots u_s \cdot u_\infty = 1$ (formule non abélienne du produit).

Voici maintenant un plan de ce travail. Dans une première partie nous rappelons certains résultats plus ou moins connus sur la structure de G_S^{ab} , tournant principalement autour de la conjecture de Leopoldt (§ 1). Nous donnons ensuite les définitions équivalentes et les premières propriétés des corps p -rationnels, ainsi qu'une première description de G_S par générateurs et relations (§ 2). Les relations en question font intervenir des relèvements $\sigma_{\mathcal{L}}$ à G_S des Frobenius en les places finies \mathcal{L} de $S \setminus S_p$. En cherchant à mettre les $\sigma_{\mathcal{L}}$ dans un système minimal de générateurs de G_S , on tombe sur la notion d'ensemble S primitif, qui permet de décrire complètement G_S en termes de pro- p -produit libre de groupes de décomposition (§ 3). Si l'on ne suppose plus que S est primitif, on peut chercher à exprimer les Frobenius $\sigma_{\mathcal{L}}^{ab}$ de G_S^{ab} ($\mathcal{L} \in S \setminus S_p$) dans une base donnée de G_S^{ab} , ce qui permet de décrire $G_S/G_S^{(2)}$ par générateurs et relations (§ 4). Comme application de cette description, nous donnons une nouvelle preuve de la loi de réciprocité pour les symboles de Hilbert. Enfin nous montrons l'existence d'une loi de réciprocité que nous appelons primitive (§ 5), et qui peut être considérée comme une généralisation sensible d'un lemme bien connu de Kummer sur les puissances p ^{ièmes} dans les corps cyclotomiques $\mathbb{Q}(\mu_p)$, p régulier.

1.— Rappels sur la structure de G_S^{ab} .

Fixons d'abord quelques notations :

K = une extension finie de \mathbb{Q} .

p = un nombre premier fixé.

$S_p = S_p(K)$ = l'ensemble des p -places de K .

$S_\infty = S_\infty(K)$ = l'ensemble des places archimédiennes de K .

$S = S(K)$ = un ensemble fini de places de K , contenant $S_p(K)$.

$$\Sigma = \Sigma(K) = S(K) \cup S_\infty(K).$$

$S_f = S_f(K)$ = l'ensemble des places finies de $S(K)$.

S_c (resp. S_r) = l'ensemble des places complexes (resp. réelles) de $S(K)$.

Ω_S = l'extension algébrique S -ramifiée maximale de K .

$$\mathcal{G}_S = \mathcal{G}_S(K) = \text{Gal}(\Omega_S/K).$$

K_S = la pro- p -extension maximale de K contenue dans Ω_S .

$G_S = G_S(K) = \text{Gal}(K_S/K)$ (c'est donc le quotient maximal de \mathcal{G}_S qui soit un pro- p -groupe).

Remarquons que les places suivantes ne peuvent pas se ramifier dans une p -extension de K :

- les places $\mathfrak{L} \in S_f \setminus S_p$ t.q. $N\mathfrak{L} \not\equiv 1 \pmod{p}$, où $N\mathfrak{L}$ désigne la norme absolue de l'idéal premier \mathfrak{L} .
- les places archimédienennes complexes.
- si $p \neq 2$ ou K est totalement imaginaire, les places réelles.

On imposera donc à S les conditions suivantes :

- toute place $\mathfrak{L} \in S_f \setminus S_p$ vérifie la congruence $N\mathfrak{L} \equiv 1 \pmod{p}$.
- S ne contient pas de places complexes.
- si $p = 2$ et K est réel, et si S contient une place réelle, S contient toutes les places réelles.

Pour $v \in S$, posons :

K_v = le complété de K en la place v .

\bar{K}_v = une clôture algébrique de K_v .

$$\mathcal{G}_v = \text{Gal}(\bar{K}_v/K).$$

$K_v(p)$ = la pro- p -extension maximale de K_v .

$$G_v = \text{Gal}(K_v(p)/K_v).$$

Pour toute place $v \in S$, le groupe de décomposition G_S^v (correspondant à un prolongement fixé de v à K_S) est un quotient de G_v . Si v est une non- p -place, i.e. $v \in S \setminus S_p$, il n'est pas difficile de voir que $G_S^v = G_v$. Mais si v est une p -place, en général $G_S^v \neq G_v$ (voir § 5 ci-dessous).

Pour décrire l'abélianisé G_S^{ab} , nous ferons les conventions suivantes (légèrement différentes des conventions habituelles) sur les unités :

$E = E(K)$ = le groupe des unités de K .

$$U_v = \begin{cases} \text{l e g r o u p e d e s u n i t é s d e } K_v^\times \text{ si } v \text{ e s t n o n - a r c h i m é d i e n n e} \\ K_v^\times \text{ si } v \text{ e s t a r c h i m é d i e n n e c o m p l e x e} \\ K_v^{\times 2} \text{ si } v \text{ e s t a r c h i m é d i e n n e r é e l l e} \end{cases}$$

\mathcal{K}_v = le complété p -adique de $K_v^\times = \varprojlim_m K_v^\times / K_v^{\times p^m}$.

\mathcal{U}_v = le complété p -adique de $U_v = \varprojlim_m U_v / U_v^{p^m}$.

(donc $\mathcal{U}_v = 0$ si v est archimédienne).

Avec ces conventions, la suite exacte (relative à l'inertie) du corps de classes s'écrit :

$$E \otimes \mathbb{Z}_p \xrightarrow{s} \prod_{v \in S} \mathcal{U}_v \longrightarrow G_S^{ab} \longrightarrow Cl \longrightarrow 0,$$

où $Cl = Cl(K)$ désigne le p -groupe des classes d'idéaux (resp. des classes de diviseurs) de K si $S = S_f$ (resp. $S \neq S_f$). Les deux cas ne sont à distinguer que si $p = 2$ et K n'est pas totalement imaginaire^(*).

Le noyau Δ_S de l'homomorphisme de semi-localisation s est le S -noyau de Leopoldt pour K . C'est le dual de Pontryagin du groupe de cohomologie $H^2(\mathcal{G}_S, \mathbb{Q}_p/\mathbb{Z}_p) = H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p)$ (voir [KZ1] ou [HB], 4–4). Son \mathbb{Z}_p -rang δ_K est indépendant de $S \supset S_p$: c'est le défaut de Leopoldt pour K et p , conjecturalement nul. La suite exacte du corps de classes donne l'égalité : $\text{rang}_{\mathbb{Z}_p} G_S^{ab} = 1 + r_2 + \delta_K$, où $r_2 = r_2(K)$ est le nombre de places complexes de K .

Deux autres invariants cohomologiques de G_S sont ([SE], chap. I) :

- le nombre minimal de générateurs $d(G_S) = \dim H^1(G_S, \mathbb{Z}/p\mathbb{Z})$
- le nombre minimal de relations $r(G_S) = \dim H^2(G_S, \mathbb{Z}/p\mathbb{Z})$.

Posons :

μ_{p^m} = le groupe des racines p^m -ièmes de l'unité

$\mu_{p^\infty} = \bigcup_{m \geq 1} \mu_{p^m}$

$\mu_{p^m}(L)$ = le groupe des racines p^m -ièmes de l'unité contenues dans un corps L .

$\mu(L) = \bigcup_{m \geq 1} \mu_{p^m}(L)$.

$\epsilon(L) = 1$ (resp. 0) si $\mu_p(L) \neq 1$ (resp. $\mu_p(L) = 1$).

$V = V(K) = \{x \in K^\times / x \in K^\times \forall v \in S, x \in UK^\times \forall v \notin S\}/K^\times$.

$\mathcal{C}\ell_S = \mathcal{C}\ell_S(K)$ = le p -groupe des S -classes de diviseurs de K .

Avec les conventions précédentes sur les unités locales, il est bien connu que $V_S \cong \text{Hom}_\Delta(\mathcal{C}\ell_S, \mu_p)$, où $\Delta = \text{Gal}(K(\mu_p)/K)$ (voir par exemple [NK1], 7–3).

Si S contient $S_p \cup S_\infty$ (i.e. $S = \Sigma$), la suite exacte longue de Poitou–Tate s'écrit :

$$0 \longrightarrow V_S^* \longrightarrow H^2(G_S, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \prod_{v \in S} H^2(G_v, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mu_p(K)^* \longrightarrow 0$$

où $()^*$ désigne le dual de Pontryagin.

Dans le cas général ($S \supset S_p$), on a les formules :

$$(2) \quad d(G_S) = 1 + r_2 + \sum_{v \in S} \epsilon(K_v) - \epsilon(K) + \dim V_S$$

$$(3) \quad r(G_S) \leq \sum_{v \in S} \epsilon(K_v) - \epsilon(K) + \dim V_S,$$

avec égalité si $S \supset S_p \cup S_\infty$ (voir [KO], § 11 et 13).

2.- Corps p -rationnels et première description de G_S .

D'après les rappels du paragraphe 1, on a un isomorphisme de \mathbb{Z}_p -modules $G_S^{ab}(K) \simeq \mathbb{Z}_p^{1+r_2+\delta_K} \times T_S(K)$, où δ_K est le défaut de la conjecture de Leopoldt et $T_S(K)$ est le sous-groupe de torsion de G_S^{ab} , laissant fixe le compositum \tilde{K} des \mathbb{Z}_p -extensions de K .

THEOREME et DEFINITION 2.1. *Les conditions suivantes sont équivalentes :*

- i) K vérifie la conjecture de Leopoldt et $T_{S_p}(K) = 0$
- ii) $G_{S_p}^{ab}(K) \simeq \mathbb{Z}_p^{1+r_2}$.
- iii) $G_{S_p}(K)$ est un pro- p -groupe libre sur $(1+r_2)$ générateurs
- iv) $\epsilon(K) = \sum_{v \in S_p} \epsilon(K_v)$ et $V_{S_p}(K) = 0$.

Si K contient μ_p , la condition iv) équivaut alors à

- v) $\# S_p = 1$ et $\mathcal{O}_{S_p}(K) = 0$.

Si K vérifie l'une de ces conditions, on dira que K est p -rationnel.

Remarque 2.2.

Soit R_2K la partie p -primaire du noyau régulier du groupe K_2K (si $p \neq 2$ ou K est totalement imaginaire, le noyau régulier coïncide avec le noyau modéré habituel ; si $p = 2$ et K est réel, il faut modifier la définition du noyau modéré en décrétant que les symboles de Hilbert aux places réelles sont des symboles modérés ; voir [G2], § I). Dans [GJ], le corps K est appelé p -régulier si $R_2K = 0$. Compte-tenu des relations entre la K -théorie et la cohomologie galoisienne (voir [T]), on voit sans difficulté que la p -régularité équivaut à la nullité de $H^2(G_{S_p}, \mathbb{Z}/p\mathbb{Z}(2))$, où $M(2)$ désigne le module M tordu deux fois par le caractère cyclotomique. Comme la p -rationalité équivaut à la nullité de $H^2(G_{S_p}, \mathbb{Z}/p\mathbb{Z})$ (condition iii) de 1.1), on obtient immédiatement la propriété :

Si K contient $\mathbb{Q}(\mu_p)^+$, le sous-corps totalement réel maximal de $\mathbb{Q}(\mu_p)$, alors K est p -régulier si et seulement si K est p -rationnel.

Preuve de 2.1.

D'après les rappels du paragraphe 1, l'équivalence des conditions i) et ii) est évidente, ainsi que celle des conditions iv) et v). Montrons les autres implications :

ii) \Rightarrow iv) : si $G_{S_p}^{ab} \simeq \mathbb{Z}_p^{1+r_2}$, on a en particulier $d(G_{S_p}) = 1 + r_2$ et la formule (2) du paragraphe 1 entraîne les relations de iv).

iv) \Rightarrow iii) : d'après les formules (2) et (3) du paragraphe 1, les relations de iv) entraînent que $d(G_{S_p}) = 1 + r_2$ et $r(G_{S_p}) = 0$, i.e. le pro- p -groupe G_{S_p} est libre sur $(1+r_2)$ générateurs.

iii) \Rightarrow ii) : c'est clair. QED

Exemples :

- a) Le corps \mathbb{Q} est p -rationnel pour tout nombre premier p .
- b) Si $p \geq 5$ et si K est un corps quadratique imaginaire, K est p -rationnel dès que p ne divise pas le nombre de classes de K .
- c) Le corps cyclotomique $\mathbb{Q}(\mu_p^n)$ est p -rationnel si et seulement si le nombre premier p est régulier, i.e. ne divise pas le nombre de classes de $\mathbb{Q}(\mu_p)$ (pour des détails, voir [MV], Chap. II).

D'une certaine façon, les propriétés arithmétiques des corps p -rationnels (ou p -réguliers) généralisent celles des corps cyclotomiques $\mathbb{Q}(\mu_p^n)$, p régulier (voir § 4). Comme première illustration, donnons une généralisation immédiate d'un critère de Kummer sur les puissances p -ièmes ([WA], 5.36). Notons que ce critère bien connu peut être considéré comme une version précoce de la conjecture de Leopoldt (voir [SA], 1.8) :

COROLLAIRE 2.3. *Soient p impair, K un corps p -rationnel et u une unité de K . Si $u \equiv 1 \pmod{p^2}$, alors c'est une puissance p -ième d'une unité de K .*

Preuve :

Pour toute p -place v de K , d'indice de ramification absolu e_v , on a par hypothèse : $v(u-1) \geq 2e_v > \frac{p}{p-1} e_v$, donc $u \in K_v^{\times p}$ pour toute place $v \in S_p$. Comme u est une unité, u appartient en fait à V_{S_p} , qui est nul puisque K est p -rationnel. QED

Ce critère sera sensiblement amélioré au paragraphe 5.

Donnons maintenant une première description du pro- p -groupe $G_S(K)$ (quand K est p -rationnel) par générateurs et relations. Nous aurons besoin de deux lemmes, l'un algébrique, l'autre arithmétique.

Le lemme algébrique est le pro- p -analogue d'un résultat bien connu de la théorie des groupes :

LEMME 2.4. *Soient G et H deux pro- p -groupes et $\varphi : H \rightarrow G$ un homomorphisme surjectif. Pour que φ soit un isomorphisme, il suffit que les conditions suivantes soient remplies :*

i) *L'application $H^{ab} \rightarrow G^{ab}$ induite par φ est un isomorphisme.*

ii) $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Preuve :

Notons N le noyau de φ :

$$1 \rightarrow N \rightarrow H \rightarrow G \rightarrow 1.$$

Ecrivons la suite exacte d'inflation-restriction à coefficients dans $\mathbb{Q}_p/\mathbb{Z}_p$,

$$0 \rightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(H, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(N, \mathbb{Q}_p/\mathbb{Z}_p)^G \rightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p).$$

Les conditions i) et ii) montrent alors que $H^1(N, \mathbb{Q}_p/\mathbb{Z}_p)^G = 0$. Comme $H^1(N, \mathbb{Q}_p/\mathbb{Z}_p)$ est p - primaire et G est un pro- p -groupe, on obtient $H^1(N, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Comme N aussi est un pro- p -groupe on en tire que $N = (1)$.

QED

Le lemme arithmétique donne la structure du module de \mathbb{Z}_p -torsion $T_S(K)$.

LEMME 2.5. *Soient K un corps p -rationnel et S un ensemble fini de places contenant S_p . Les homomorphismes de réciprocité locaux induisent un isomorphisme : $\prod_{w \in S \setminus S_p} \mu(K_w) \xrightarrow{\sim} T_S(K)$, où chaque facteur $\mu(K_w)$ s'identifie au sous-groupe d'inertie de $G_S^{ab}(K)$ en w .*

Preuve :

Pour simplifier, supposons d'abord que $S = S_f$.

D'après les rappels du paragraphe 1, on a un diagramme commutatif aux lignes exactes (l'exactitude à gauche provient de la conjecture de Leopoldt)

$$\begin{array}{ccccccc} 0 & \longrightarrow & E \otimes \mathbb{Z}_p & \longrightarrow & \prod_{v \in S} \mathcal{U}_v & \longrightarrow & G_S^{ab} \longrightarrow \mathcal{Cl} \longrightarrow 0 \\ & & \downarrow \parallel & & \downarrow \text{proj.} & & \downarrow \parallel \\ 0 & \longrightarrow & E \otimes \mathbb{Z}_p & \longrightarrow & \prod_{v \in S_p} \mathcal{U}_v & \longrightarrow & G_{S_p}^{ab} \longrightarrow \mathcal{Cl} \longrightarrow 0 \end{array}$$

Une simple chasse dans le diagramme fournit la suite exacte :

$$0 \longrightarrow \prod_{W \in S \setminus S_p} \mathcal{U}_w \longrightarrow G_S^{ab} \longrightarrow G_{S_p}^{ab} \longrightarrow 0.$$

Or G_S^{ab} et $G_{S_p}^{ab}$ ont le même quotient sans torsion, qui est le groupe de Galois du compositum \tilde{K} de toutes les \mathbb{Z}_p -extensions de K .

De plus, pour $w \in S \setminus S_p$, on a $\mathcal{U}_w = \mu(K_w)$, d'où finalement la suite exacte :

$$0 \longrightarrow \prod_{W \in S \setminus S_p} \mu(L_w) \longrightarrow T_S \longrightarrow T_{S_p} \longrightarrow 0.$$

Comme K est p -rationnel, $T_{S_p} = 0$, d'où le résultat cherché.

Le cas général se traite de façon analogue.

QED

Remarque 2.6 :

La suite exacte $0 \longrightarrow \prod_{W \in S \setminus S_p} \mu(K_w) \longrightarrow G_S^{ab} \longrightarrow G_{S_p}^{ab} \longrightarrow 0$

(modulo la conjecture de Leopoldt) fournie par le corps de classes peut être considérée comme l'abélianisée de la suite exacte de Neumann $1 \rightarrow N \rightarrow G_S \rightarrow G_{S_p} \rightarrow 1$, où N est un produit pro- p -libre de certains groupes d'inertie (pour un énoncé précis, voir [NM], thm. 2). Cependant (et c'est

une question fondamentale pour le problème c) de l'introduction), l'action de G_{S_p} sur N n'est pas explicitement connue.

Faisons maintenant le choix d'un système minimal de générateurs du pro- p -groupe $G_S(K)$, où K est p -rationnel :

- soit $\{\sigma_i; 1 \leq i \leq 1 + r_2\}$ un relèvement arbitraire à G_S d'une base $\{\sigma_i^{ab}; 1 \leq i \leq 1 + r_2\}$ du \mathbb{Z}_p -module libre $G_S^{ab} = \text{Gal}(\tilde{K}/K)$.

- pour $\mathfrak{L} \in S_f \setminus S_p$, soit $T_{\mathfrak{L}}$ le groupe d'inertie dans $\text{Gal}(K_S/K_{S_p})$ d'un prolongement fixé de \mathfrak{L} à K_S . Comme la place \mathfrak{L} est modérément ramifiée, $T_{\mathfrak{L}}$ est isomorphe à \mathbb{Z}_p . On notera $\tau_{\mathfrak{L}}$ un générateur topologique arbitraire de $T_{\mathfrak{L}}$ ($\mathfrak{L} \in S_f \setminus S_p$, $N\mathfrak{L} \equiv 1 \pmod{p}$)).

- si $p = 2$ et K est réel, pour toute place réelle $v_j \in S$, $1 \leq j \leq r_1$, où $r_1 = r_1(K)$ est le nombre de places réelles de K , choisissons pareillement un générateur τ_j d'un groupe d'inertie T_{v_j} ($\simeq \mathbb{Z}/2\mathbb{Z}$).

D'après 2.5 et le théorème de Burnside pour les pro- p -groupes, le système $\{\sigma_i, \tau_{\mathfrak{L}}, \tau_j; 1 \leq i \leq 1 + r_2, v_j \in S_r, \mathfrak{L} \in S_f \setminus S_p\}$ forme un système minimal de générateurs de $G_S(K)$.

Pour $\mathfrak{L} \in S_f \setminus S_p$, le Frobenius $\sigma_{\mathfrak{L}}^{ab}$ de G_S^{ab} est bien défini. Soit $\sigma_{\mathfrak{L}}$ un relèvement arbitraire de $\sigma_{\mathfrak{L}}^{ab}$ à G_S . On a la relation :

$$\tau_{\mathfrak{L}}^{N\mathfrak{L}-1} [\tau_{\mathfrak{L}}, \sigma_{\mathfrak{L}}] = 1.$$

En effet, le pro- p -groupe $G_{\mathfrak{L}}$ est engendré par les générateurs $\tau_{\mathfrak{L}}$ et $\sigma_{\mathfrak{L}}$ et la relation précédente ([KO], § 10.2), et $G_{\mathfrak{L}}$ s'identifie au sous-groupe de décomposition $G_S^{\mathfrak{L}}$.

THEOREME 2.7. *Supposons K p -rationnel. Alors :*

- i) *si $p \neq 2$, ou K est totalement imaginaire, ou S ne contient pas de place réelle, $G_S(K)$ est engendré minimalement par les générateurs $\{\sigma_i, \tau_{\mathcal{L}}; 1 \leq i \leq 1 + r_2, \mathcal{L} \in S_f \setminus S_p\}$ et les relations $\tau_{\mathcal{L}}^{N\mathcal{L}-1}[\tau_{\mathcal{L}}, \sigma_{\mathcal{L}}] = 1$ pour $\mathcal{L} \in S_f \setminus S_p$.*
- ii) *sinon, il faut ajouter les générateurs $\{\tau_j; 1 \leq j \leq r_1\}$ et les relations $\tau_j^2 = 1$.*

Preuve :

Faisons la démonstration dans le cas ii), qui est le plus compliqué.

Soient F le pro- p -groupe libre sur les générateurs $\sigma_i, \tau_{\mathcal{L}}, \tau_j$ et H le pro- p -groupe décrit dans l'énoncé. Comme G_S est engendré par les $\sigma_i, \tau_{\mathcal{L}}, \tau_j$, on a un homomorphisme surjectif $F \rightarrow G_S$. Comme les relations de l'énoncé sont vérifiées dans G_S , cet homomorphisme se factorise à travers H , i.e. donne naissance à un homomorphisme surjectif $\varphi : H \rightarrow G$. D'après 2.5, $\varphi^{ab} : H^{ab} \rightarrow G^{ab}$ est un isomorphisme. Comme $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ (conjecture de Leopoldt), le lemme 2.4 montre que φ est un isomorphisme. QED

COROLLAIRE 2.8. *Plaçons-nous dans le cas ii). Alors $G_S \simeq G_{S_f}^* (\mathbb{Z}/2\mathbb{Z})^{*r_1}$.*

Ici, $*$ désigne le pro- p -produit libre (i.e. le produit libre dans la catégorie des pro- p -groupes) et G^{*n} est le pro- p -produit libre de n copies de G .

Preuve :

G_{S_f} est décrit par les générateurs et relations de i). Pour décrire G_S il faut ajouter les générateurs τ_j ($1 \leq j \leq r_1$) et les relations $\tau_j^2 = 1$. Comme ces derniers générateurs et relations ne figurent pas dans i), cela signifie que $G_S \simeq G_{S_f}^* \underset{1 \leq j \leq r_1}{\underset{*}{\times}} \langle \tau_j \rangle$. Or chaque $\langle \tau_j \rangle$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. QED

Si $p = 2$, si $S = S_2 \cup S_{\infty}$, et si K est totalement réel, alors $G_{S_f} \simeq \mathbb{Z}_2$ et l'on retrouve un résultat de Wingberg ([WB1], 1.4).

Le théorème 2.7 ne décrit complètement la structure de G_S que si l'on sait exprimer les Frobenius $\sigma_{\mathcal{L}}$ en fonction des générateurs $\sigma_i, \tau_{\mathcal{L}}$. Ce problème fera l'objet des paragraphes 3 et 4 ci-dessous. En particulier, l'on étudiera systématiquement au paragraphe 3 les conditions pour lesquelles la situation de l'exemple suivant ([KO], p. 125) se produit :

Exemple : Le corps $K = \mathbb{Q}(\sqrt{-23})$ est 3–rationnel, et son nombre de classes est 3. Soit $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathcal{L}, q\}$, où $\mathfrak{p}_1, \mathfrak{p}_2$ sont les deux diviseurs de 3, q un nombre premier inerte avec $q \equiv 1 \pmod{3}$, $q \not\equiv 1 \pmod{9}$, et \mathfrak{p} un autre idéal premier, tel que $G_S(K)$ soit engendré par les éléments $\sigma_q, \tau_q, \sigma_{\mathcal{L}}, \tau_{\mathcal{L}}$. Alors les relations sont : $\tau_q^{q-1}[\tau_q, \sigma_q] = 1$ et $\tau_{\mathcal{L}}^{N\mathcal{L}-1}[\tau_{\mathcal{L}}, \sigma_{\mathcal{L}}] = 1$. Autrement dit, $G_S \cong \mathcal{L}^* G_q$.

3.– Ensembles primitifs et seconde description de G_S .

Fixons quelques notations supplémentaires :

\tilde{K} = le compositum de toutes les \mathbb{Z}_p –extensions de K .

Si K est p –rationnel, $\text{Gal}(\tilde{K}/K)$ n'est autre que G_S^{ab} .

$\tilde{K}(1)$ = la sous–extension élémentaire maximale de \tilde{K} , i.e. le compositum des premiers étages des \mathbb{Z}_p –extensions de K .

Rappelons que S_f désigne l'ensemble des places finies de S . Posons $T = S_f \setminus S_p$, $t = \# T$ et $\tilde{K}(1, T)$ = le sous–corps de $\tilde{K}(1)$ décomposant totalement toutes les places de T .

PROPOSITION et DEFINITION 3.1. *Les conditions suivantes sont équivalentes :*

i) *Les Frobenius $\sigma_{\mathcal{L}}$ de $\text{Gal}(\tilde{K}/K)$ (i.e. les symboles d'Artin $(\mathcal{L}, \tilde{K}/K)$), pour $\mathcal{L} \in T$, engendrent un \mathbb{Z}_p -facteur direct libre de $\text{Gal}(\tilde{K}/K)$, de rang égal à t .*

ii) *Les Frobenius $\sigma_{\mathcal{L}}^1$ de $\text{Gal}(\tilde{K}(1)/K)$ (i.e. les symboles d'Artin $(\mathcal{L}, \tilde{K}(1)/K)$), pour $\mathcal{L} \in T$, engendrent un sous- \mathbb{F}_p –espace vectoriel de $\text{Gal}(\tilde{K}(1)/K)$, de dimension égale à t .*

iii) $\dim \text{Gal}(\tilde{K}(1)/\tilde{K}(1, T)) = t$.

Si l'une de ces conditions est vérifiée, on dit que l'ensemble S est primitif (pour K et p).

Preuve :

- i) \Leftrightarrow ii) d'après le théorème de Burnside pour les pro- p -groupes et les propriétés fonctorielles des Frobenius.
- ii) \Leftrightarrow iii) : immédiat

Remarque 3.2.

- a) L'ensemble S_p est, par définition, primitif pour tout couple (K, p) .
- b) La condition iii) est utilisée par H. Miki dans [MK]. La condition i) permet de fabriquer des ensembles primitifs en utilisant le logarithme de Gras ([G1], § 2). La condition ii) permet de faire de même en utilisant les symboles locaux modérés ([MV], § 3).
- c) Le théorème de densité de Čebotarev garantit l'existence d'une infinité d'ensembles primitifs ne rencontrant pas un ensemble fini donné de places.
- d) Si l'ensemble S est primitif, forcément $t \leq 1 + r_2 + \delta_K$. Sous la conjecture de Leopoldt, les **ensembles primitifs maximaux** (pour l'inclusion) sont exactement ceux pour lesquels $t = 1 + r_2$.

Exemples d'ensembles primitifs S .

- i) $K = \mathbb{Q}(\mu_3)$, $p = 3$, $S = \{\mathfrak{p}_3, \mathcal{L}_7, \mathcal{L}_{19}\}$, où \mathfrak{p}_3 est l'unique place au-dessus de 3, où \mathcal{L}_7 (resp. \mathcal{L}_{19}) est une place au-dessus de 7 (resp. 19).
- ii) $K = \mathbb{Q}(\mu_5)$, $p = 5$, $S = \{\mathfrak{p}_5, \mathcal{L}_{11}, \mathcal{L}'_{11}, \mathcal{L}''_{11}\}$, avec des notations analogues.
- iii) Si K est totalement réel vérifiant la conjecture de Leopoldt (pour p), les ensembles primitifs S sont exactement ceux de la forme $S = S_p$ ou $S = S_p \cup \{\mathcal{L}\}$, où \mathcal{L} est une non- p -place finie, totalement inerte dans la \mathbb{Z}_p -extension cyclotomique de K .

Si S est primitif et K est p -rationnel, le théorème 2.7 permet de décrire complètement la structure du pro- p -groupe $G_S(K)$. Pour toute non- p -place $w \in S$, choisissons un prolongement arbitraire de w à K_S , et soit ψ_w

l'homomorphisme composé $G_w \xrightarrow{\sim} G_S^w \hookrightarrow G_S$ (ψ_w dépend du choix du prolongement de w , mais son abélianisé ψ_w^{ab} n'en dépend pas).

THEOREME 3.3. *Supposons K p-rationnel et S primitif. Alors les homomorphismes ψ_w , $w \in S \setminus S_p$ induisent un isomorphisme :*

$$\psi_T: \prod_{\mathcal{L} \in T}^* G_{\mathcal{L}}^* (\mathbb{Z}/2\mathbb{Z})^{*u} * F \xrightarrow{\sim} G_S(K)$$

ù F est un pro-p-groupe libre à $(1+r_2-t)$ générateurs, et où

$$u = \begin{cases} r_1 & \text{si } p = 2, K \text{ n'est pas totalement imaginaire et } S^\circ \text{ contient les} \\ & \text{places réelles (cas i)} \\ 0 & \text{sinon (cas ii).} \end{cases}$$

Réiproquement, si $G_S(K)$ est de l'un des types précédents, K est p-rationnel et S est primitif.

(comparer à [WB 1], 3.1).

Preuve :

Supposons K p-rationnel, S primitif et montrons i). D'après la condition c) de 3.1, un système minimal de générateurs de G_S est $\{s_{\mathcal{L}}, t_{\mathcal{L}}, \sigma_i ; \mathcal{L} \in T, 1 \leq i \leq 1 + r_2 - t\}$, soumis aux relations $\tau_{\mathcal{L}}^{N\mathcal{L}-1}[\tau_{\mathcal{L}}, \sigma_{\mathcal{L}}] = 1$, $\mathcal{L} \in T$. Or l'on sait que le pro-p-groupe $G_{\mathcal{L}}$ est décrit par les générateurs $\sigma_{\mathcal{L}}, \tau_{\mathcal{L}}$ et la relation $\tau_{\mathcal{L}}^{N\mathcal{L}-1}[\tau_{\mathcal{L}}, \sigma_{\mathcal{L}}] = 1$ ([Ko], 5.10.2). Donc $G_S \simeq \prod_{\mathcal{L} \in T}^* G_{\mathcal{L}}^* F$, où F est libre sur les σ_i , $1 \leq i \leq 1 + r_2 - t$.

Le cas ii) se démontre de la même façon.

Réiproquement, supposons i). La cohomologie du pro-p-produit libre ([NK 2], 4.1) nous donne un isomorphisme $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \prod_{\mathcal{L} \in T} H^2(G_{\mathcal{L}}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, i.e. K vérifie la conjecture de

Leopoldt. De plus, par abélianisation, on voit immédiatement que $T_S(K) \simeq \prod_{\mathcal{L} \in T} \mu(\mathcal{L})$. La suite exacte du corps de classes (preuve de 2.5) montre alors que $T_{S_p}(K) = 0$. Donc K est p -rationnel d'après 2.1 i). Quant à la primitivité de S , elle est immédiate.

La démonstration se fait de façon analogue en partant de ii). QED

Remarque 3.4.

Dans la décomposition précédente de G_S , le pro- p -groupe libre F est engendré minimalement par les σ_i , $1 \leq i \leq 1 + r_2 - t$. On peut en faire un choix plus ou moins canonique de la façon suivante :

Elargissons l'ensemble primitif S en un ensemble primitif maximal S_m (c'est possible, d'après Čebotarev). Choisissons pour les σ_i , $1 \leq i \leq 1 + r_2 - t$, les Frobenius σ_w , $w \in S_m \setminus S_f$. Alors le pro- p -groupe libre F engendré par les σ_w est isomorphe à $\prod_{w \in S_m \setminus S_f}^{*} G_w / T_w$, où T_w est le sous-groupe d'inertie de G_w . Voir aussi [WB 3], Thm. Aii).

COROLLAIRE 3.5. *Les homomorphismes de réciprocité locaux ψ_w^{ab} , $w \in S \setminus S_p$, induisent un isomorphisme :*

$$G_S^{ab}(K) \simeq \mathbb{Z}_p^{1+r_2-t} \times \prod_{w \in S \setminus S_p} \mathcal{K}_w$$

si et seulement si K est p -rationnel et S est primitif.

Preuve : C'est immédiat, par abélianisation à partir de 3.3. Comme $\mathbb{Z}/2\mathbb{Z}$ est le complété 2-adique de \mathbb{R}^\times , il n'y a pas lieu de faire la distinction entre les cas i) et ii). QED

COROLLAIRE 3.6. (*lemme d'approximation simultanée par les S-unités*).

Supposons K p-rationnel et S primitif maximal. L'injection diagonale du groupe des S-unités $E_S(K)$ dans le produit $\prod_{v \in S_p} K_v^\times$ induit un isomorphisme des complétés p-adiques : $E_S(K) \otimes \mathbb{Z}_p \simeq \prod_{v \in S_p} \mathcal{K}_v$.

Preuve :

On a un diagramme commutatif :

$$\begin{array}{ccccccc} \Delta_S = 0 & \longrightarrow & E_S \otimes \mathbb{Z}_p & \longrightarrow & \prod_{v \in S} \mathcal{K}_v & \longrightarrow & G_S^{ab} \longrightarrow \mathcal{O}_S(K) = 0 \\ & & \uparrow \text{inj.} & & \parallel \uparrow & & \\ & & \prod_{v \in S \setminus S_p} \mathcal{K}_v & \longrightarrow & G_S^{ab} & & \end{array}$$

où la suite exacte du haut est la suite exacte du corps de classes relative à la décomposition, et l'isomorphisme du bas celui de 3.5. Une simple chasse dans le diagramme montre l'isomorphisme de 3.6.

Si K contient μ_p , des précisions supplémentaires peuvent être apportées à la structure des S-unités (voir § 5).

Le théorème de structure 3.3 permet de compléter un résultat de *montée* pour la conjecture de Leopoldt, dû à H. Miki (voir [MK]; mais la démonstration de Miki est assez peu éclairante).

DEFINITION 3.6. *Une p-extension L/K (i.e. une extension galoisienne finie dont le groupe de Galois est un p-groupe) est appelée **primitivement ramifiée** ([G2], III-1) si l'ensemble S des p-places de K et des places finies de K qui se ramifient dans L, est **primitif** (pour p et K).*

THEOREME 3.7. *Soit L/K une p-extension de corps de nombres. Les conditions suivantes sont équivalentes :*

- a) *L est un corps p-rationnel*
- b) *K est un corps p-rationnel et l'extension L/K est primitivement ramifiée.*

Preuve :

a) \Rightarrow b) : soit S la réunion de S_p et des places finies ramifiées de L/K .

D'après 3.3 (où l'on considère le cas i), pour simplifier), on a un isomorphisme :

$$G_S(K) = \underset{\mathcal{L} \in S \setminus S_p}{*} G_{\mathcal{L}}(K) * F_K,$$

où F_K est le pro- p -groupe libre à $1 + r_2(K) - t_K$ générateurs, et où t_K désigne le nombre de non- p -places finies de K que S contient. Le théorème sur les sous-groupes ouverts de produits pro- p -libres, (voir [BNW]), nous fournit un isomorphisme

$$G_S(L) \simeq \underset{\mathcal{L} \in S(L) \setminus S_p(L)}{*} G_{\mathcal{L}}(L) * E_L * F,$$

où E_L et F sont libres avec

$$\text{rang}(E_L * F) = \underset{\mathcal{L} \in S(L) \setminus S_p(L)}{\Sigma} ([\mathcal{L} : K_{\mathcal{L}}] - 1) + (1 + r_2(K) - t_K)([L : K] - [L : K] + 1).$$

En posant $F_L = E_L * F$, il vient

$$G_S(L) = \underset{\mathcal{L} \in S \setminus S_p}{*} G_{\mathcal{L}}(L) * F_L,$$

où F_L est le pro- p -groupe libre de rang $1 + r_2(L) - t_L$. A nouveau le théorème 3.3 nous montre que L est p -rationnel, et que l'ensemble S est primitif pour le couple (L, p) .

Pour montrer b) \Rightarrow a), on peut utiliser le même genre d'argument (voir [MV], § 3), ou bien faire intervenir la formule des points fixes de G. Gras ([G2], III1 ou App.) :

Si $G = \text{Gal}(L/K)$ et K vérifie la conjecture de Leopoldt, on a la formule :

$$(T_{S_p}(L) : T_{S_p}(K)) = \left(\prod_{\mathcal{L} \in S \setminus S_p} e_{\mathcal{L}} \right) / \left(<\alpha_{\mathcal{L}}(\tilde{K}/K)^{\frac{1}{e_{\mathcal{L}}}} ; \mathcal{L} \in S \setminus S_p > \cdot \tilde{X}_K : \tilde{X}_K \right),$$

où S est la réunion de S_p et des places finies ramifiées de L/K , $\tilde{X}_K = \text{Gal}(\tilde{K}/K)$, $\alpha_{\mathcal{L}}(\tilde{K}/K)$ est le Frobenius en \mathcal{L} de \tilde{X}_K et $e_{\mathcal{L}}$ est l'indice de ramification de \mathcal{L} dans L/K .

Si L est p -rationnel, $T_{S_p}(L) = 0$, d'où d'une part la nullité de $T_{S_p}(K)$, i.e. la p -rationalité de K , d'autre part l'égalité

$$\prod_{\mathcal{L} \in S \setminus S_p} e_{\mathcal{L}} = \left(<\alpha_{\mathcal{L}}(\tilde{K}/K)^{\frac{1}{e_{\mathcal{L}}}} ; \mathcal{L} \in S \setminus S_p > \cdot \tilde{X}_K : \tilde{X}_K \right),$$

i.e. la primitivité de S . QED.

Remarque 3.8. Une démonstration indépendante de ce théorème a été obtenue par G. Gras et J.-F. Jaulent (voir [G-J]).

COROLLAIRE 3.9. ([MK], thm 3). *Si K est p -rationnel, toute p -extension primitivement ramifiée de K vérifie la conjecture de Leopoldt (en p).*

Cela permet de construire une double infinité (en faisant varier K et S) de corps de nombres (non abéliens) vérifiant la conjecture de Leopoldt.

4.– Description de $G_S/G_S^{(2)}$ et lois de réciprocité.

Dans cette section, nous allons généraliser des résultats de Fröhlich [F] et Ullom et Watt [U–W] sur la structure de $G_S(K)/G_S(K)^{(2)}$, quand le corps de base K est p -rationnel. Pour simplifier, et bien que ce ne soit pas nécessaire, nous supposerons que $p \neq 2$ et K contient μ_p . Dans ces conditions nous pouvons exclure de S les places archimédiennes. Posons :

$E_S = E_S(K)$ = le groupe des S -unités de K .

$\mathcal{C}\ell_S = \mathcal{C}\ell_S(K)$ = le p -groupe des S -classes d'idéaux de K .

Il s'agit ici encore d'appliquer le théorème 2.7. Comme S n'est plus supposé primitif, on va se contenter de calculer les Frobenius $\sigma_{\mathcal{L}}^{ab}$ de $\text{Gal}(\tilde{K}/K)$ dans une base bien choisie de $\text{Gal}(\tilde{K}/K)$. On obtiendra ainsi $\sigma_{\mathcal{L}} \bmod G_S^{(1)}$ en fonction des générateurs de G_S , d'où, par application de 2.7, une description de $G_S/G_S^{(2)}$. Les calculs étant quand même assez compliqués, on va les organiser en plusieurs sous-paragraphe distincts.

Rappels de cohomologie galoisienne.

Pour une place finie \mathcal{Y} de K , notons $F_{\mathcal{Y}}^m$ la p -extension abélienne d'exposant p^m maximale de \mathcal{Y} . L'homomorphisme de réciprocité local $\theta: K_{\mathcal{Y}}^* \rightarrow G_{\mathcal{Y}}^{ab}$ induit alors un isomorphisme

$$K_{\mathcal{Y}}^*/K_{\mathcal{Y}}^{*p^m} \xrightarrow{\sim} G(F_{\mathcal{Y}}^m/K_{\mathcal{Y}}),$$

que nous convenons de noter $\bar{\theta}_{\mathcal{Y}}$.

Soit K un corps de nombres quelconque. Pour chaque place \mathcal{Y} de K , le cup-produit

$$H^1(G_{\mathcal{Y}}, \mathbb{Z}/p^n\mathbb{Z}) \times H^1(G_{\mathcal{Y}}, \mu_{p^n}) \rightarrow (1/p^n\mathbb{Z})/\mathbb{Z}$$

met en dualité $H^1(G_{\mathcal{Y}}, \mathbb{Z}/p^n\mathbb{Z})$ et $H^1(G_{\mathcal{Y}}, \mu_{p^n})$. Cette dualité est celle qui est donnée par la théorie du corps de classes local, entre $\text{Hom}(G_{\mathcal{Y}}, \mathbb{Z}/p^n\mathbb{Z})$ et $K_{\mathcal{Y}}^*/K_{\mathcal{Y}}^{*p^n}$:

$$\begin{aligned} \text{Hom}(G_{\mathcal{Y}}, \mathbb{Z}/p^n\mathbb{Z}) \times K_{\mathcal{Y}}^*/K_{\mathcal{Y}}^{*p^n} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ (\chi, \bar{a}) &\longrightarrow \chi(\theta_{\mathcal{Y}}(a)). \end{aligned}$$

Si de plus K contient les racines p^n -ièmes de l'unité, la dualité précédente donne lieu au **symbole de Hilbert**:

$$\frac{K^*}{\mathcal{Y}} / \frac{K^*}{\mathcal{Y}}^{p^n} \times \frac{K^*}{\mathcal{Y}} / \frac{K^*}{\mathcal{Y}}^{p^n} \rightarrow \mu_{p^n},$$

qui est une forme bilinéaire antisymétrique non dégénérée. Pour les propriétés du symbole de Hilbert, voir [SE], Chap. XIV.

Posons maintenant $R_S = \prod_{\mathcal{Y} \in S} H^1(G_{\mathcal{Y}}, \mu_{p^n})$ et $R'_S = \prod_{\mathcal{Y} \in S} H^1(G_{\mathcal{Y}}, \mathbb{Z}/p^n\mathbb{Z})$.

Par multiplication, nous obtenons une dualité

$$R_S^\times : R'_S \rightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

A nouveau, si K contient μ_{p^n} , alors le $\mathbb{Z}/p^n\mathbb{Z}$ -module $R_S = \prod_{\mathcal{Y} \in S} \frac{K^*}{\mathcal{Y}} / \frac{K^*}{\mathcal{Y}}^{p^n}$ est muni d'une forme bilinéaire antisymétrique non dégénérée.

PROPOSITION 4.1. *Supposons que le corps de nombres K contienne les racines p^n -ièmes de l'unité, et que l'ensemble S soit suffisamment gros pour que $\mathcal{O}_S(K)$ soit trivial. Nous avons alors une suite exacte canonique*

$$0 \longrightarrow E_S / E_S^{p^n} \longrightarrow R_S \longrightarrow X_S / X_S^{p^n} \longrightarrow 0.$$

où $X_S = G_S^{ab}(K)$.

Preuve :

Puisque S est suffisamment gros nous savons d'après le paragraphe 1, que $H^1(G_S, \mu_{p^n})$ s'injecte dans R_S . Le théorème de Poitou–Tate nous fournit donc

la suite courte exacte

$$0 \longrightarrow H^1(G_S, \mu_{p^n}) \longrightarrow R_S \longrightarrow H^1(G_S, \mathbb{Z}/p^n\mathbb{Z})^* \longrightarrow 0.$$

Evaluons maintenant, sous nos hypothèses, le groupe $H^1(G_S, \mu_{p^n})$. Ecrivons

pour cela la suite exacte

$$1 \longrightarrow \mu_{p^n} \longrightarrow E_S(\Omega_S) \xrightarrow{p^n} E_S(\Omega_S) \longrightarrow 1,$$

où $E_S(\Omega_S)$ est la limite inductive des groupes des S -unités $E_S(L)$ pour les extensions S -ramifiées L de K , et passons à la cohomologie pour l'action de \mathcal{G}_S :

$$\begin{aligned} 1 &\longrightarrow \mu_{p^n} \cap K^* \longrightarrow E_S(K) \xrightarrow{p^n} E_S(K) \\ &\longrightarrow H^1(\mathcal{G}_S, \mu_{p^n}) \longrightarrow H^1(\mathcal{G}_S, E_S(\Omega_S)) \xrightarrow{p^n} H^1(\mathcal{G}_S, E_S(\Omega_S)). \end{aligned}$$

Or, la cohomologie de $E_S(\Omega_S)$ est bien connue (voir [HB], prop. 6): $H^1(\mathcal{G}_S, E_S(\Omega_S))$ est isomorphe au groupe des S -classes d'idéaux de K . En utilisant à nouveau la trivialité du p -groupe $\mathcal{C}\ell_S(K)$, nous obtenons

$$H^1(G_S, \mu_{p^n}) \simeq E_S(K)/E_S(K)^{p^n}.$$

La suite exacte de Poitou–Tate s'écrit donc

$$0 \rightarrow E_S/E_S^{p^n} \rightarrow R_S \rightarrow X_S/X_S^{p^n} \rightarrow 0. \quad \text{QED}$$

COROLLAIRE 4.2. *Soit K un corps p -rationnel contenant les racines p^n -ièmes de l'unité, alors le $\mathbb{Z}/p^n\mathbb{Z}$ -module symplectique R_{S_p} admet une décomposition (non canonique) :*

$$R_{S_p} \simeq E_{S_p}/E_{S_p}^{p^n} \oplus X_{S_p}/X_{S_p}^{p^n},$$

en deux sous $\mathbb{Z}/p^n\mathbb{Z}$ -modules totalement isotropes maximaux, duals l'un de l'autre.

Preuve : K étant p -rationnel et contenant μ_p , le groupe $\mathcal{C}\ell_S(K)$ est trivial et nous avons la suite exacte

$$0 \rightarrow E_{S_p}/E_{S_p}^{p^n} \rightarrow R_{S_p} \rightarrow X_{S_p}/X_{S_p}^{p^n} \rightarrow 0.$$

D'autre part, la formule du produit sur les symboles de Hilbert montre que l'image de $E_{S_p}/E_{S_p}^{p^n}$ est un sous-module totalement isotrope de R_{S_p} qui est, vu son ordre, maximal. En outre $X_{S_p}/X_{S_p}^{p^n}$ étant, par hypothèse, un $\mathbb{Z}/p^n\mathbb{Z}$ -module libre, la suite est scindée et nous avons bien la décomposition annoncée. QED

Bases symplectiques.

Soient maintenant K un corps p -rationnel et $m \geq 1$ la plus grande puissance de p telle que $\mu_p^m \subset K$. Notons que si \mathfrak{p} désigne l'unique p -place de K , alors m est également la plus grande puissance de p telle que $\mu_p^m \subset K_{\mathfrak{p}}$. Cela résulte du fait que \mathfrak{p} ne se décompose pas dans la \mathbb{Z}_p -extension cyclotomique $K(\mu_{\infty})/K$.

Grâce à la section précédente, nous allons construire une base symplectique du $\mathbb{Z}/p^m\mathbb{Z}$ -module R_S . Nous avons

$$R_S = \bigoplus_{\gamma \in S} \frac{K^*}{\gamma} / \frac{K^*}{\gamma}^{p^m} \quad (\text{somme orthogonale}).$$

Une base symplectique de R_S s'obtient donc comme réunion de bases symplectiques des $\frac{K^*}{\gamma} / \frac{K^*}{\gamma}^{p^m}$, $\gamma \in S$.

Base de $K_{\mathcal{L}}^*/K_{\mathcal{L}}^{*p^m}$ pour $\mathcal{L} \in S \setminus S_p$:

Chaque facteur $K_{\mathcal{L}}^*/K_{\mathcal{L}}^{*p^m}$ est de rang 2. Notons en effet $\bar{\pi}_{\mathcal{L}}$ une uniformisante de $K_{\mathcal{L}}$, alors $K_{\mathcal{L}}^* \simeq \mu_{N\mathcal{L}-1} \times \mathbb{U}_{\mathcal{L}}^{(1)} \times \pi_{\mathcal{L}}^{\mathbb{Z}}$, où $\mathbb{U}_{\mathcal{L}}^{(1)}$ est un \mathbb{Z}_ℓ -module ($\ell \neq p$). $K_{\mathcal{L}}^*/K_{\mathcal{L}}^{*p^m}$ admet la base symplectique $\{\bar{\pi}_{\mathcal{L}}, \bar{\omega}_{\mathcal{L}}\}$ où $\bar{\omega}_{\mathcal{L}}$ est un générateur de $\mu_{N\mathcal{L}-1}$, et où la barre au-dessus de chaque élément de $K_{\mathcal{L}}^*$ désigne la classe de cet élément modulo $K_{\mathcal{L}}^{*p^m}$.

L'isomorphisme de réciprocité local $\bar{\theta}_{\mathcal{L}} : K_{\mathcal{L}}^*/K_{\mathcal{L}}^{*p^m} \rightarrow G(E_{\mathcal{L}}^m/K_{\mathcal{L}})$ fait correspondre à $\bar{\omega}_{\mathcal{L}}$ un générateur $\tau_{\mathcal{L}}(F_{\mathcal{L}}/K_{\mathcal{L}})$ du groupe d'inertie et à $\bar{\pi}_{\mathcal{L}}$ un relèvement $\alpha_{\mathcal{L}}(E_{\mathcal{L}}^m/K_{\mathcal{L}})$ du Frobenius en \mathcal{L} , à $E_{\mathcal{L}}^m$.

Base de $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m}$, où \mathfrak{p} est l'unique p -place de K :

Le $\mathbb{Z}/p^m\mathbb{Z}$ -module symplectique $R_{S_p} = K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m}$ se décompose, d'après le corollaire 4.2, en somme directe de deux sous-modules isotropes maximaux : $E_{S_p}/E_{S_p}^{p^m}$ et son dual, qui est (non canoniquement) isomorphe à $X_{S_p}/X_{S_p}^{p^m}$:

$$K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m} \simeq E_{S_p}/E_{S_p}^{p^m} \oplus X_{S_p}/X_{S_p}^{p^m}.$$

Nous allons choisir une base de $E_{S_p}/E_{S_p}^{p^m}$, puis une base duale, la réunion des deux fournissant une base symplectique de R_{S_p} . Une base de $E_{S_p}/E_{S_p}^{p^m}$ peut être choisie de la forme $\{\bar{e}_1 = \zeta_{p^m}, \bar{e}_2, \dots, \bar{e}_{1+r_2}\}$, où e_2 est une p -unité de K et où $\{e_3, \dots, e_{1+r_2}\}$ est une \mathbb{Z} -base des unités de K .

D'après la théorie de Kummer nous pouvons choisir une base $\{\bar{e}_1, \bar{e}'_1, \dots, \bar{e}_{1+r_2}, \bar{e}'_{1+r_2}\}$ de $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m}$ telle que

$$K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m} \simeq \bigoplus_{i=1}^{1+r_2} \text{plans hyperboliques } \langle e_i, e'_i \rangle,$$

où le système $\{\bar{e}_1, \dots, \bar{e}'_{1+r_2}\}$ correspond, par l'homomorphisme composé

$$K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m} \rightarrow J_K/J_K^{p^m} \rightarrow X_{S_p}/X_{S_p}^{p^m} \quad (\text{où } J_K \text{ est le groupe des idèles}),$$

à une base $\{\sigma_1(K_{S_p}(m)/K), \dots, \sigma_{1+r_2}(K_{S_p}(m)/K)\}$ du $\mathbb{Z}/p^m\mathbb{Z}$ -module $X_{S_p}/X_{S_p}^{p^m}$:

$$\sigma_i(K_{S_p}(m)/K) = \text{l'image de } \bar{\theta}_{\mathfrak{p}}(\bar{e}_i) \text{ dans } X_{S_p}/X_{S_p}^{p^m}.$$

Il existe des relèvements $\widetilde{\theta_{\mathfrak{p}}(e_i)}$; $\widetilde{\theta_{\mathfrak{p}}(e'_i)}$; $i = 1, \dots, 1 + r_2$; des $\bar{\theta}_{\mathfrak{p}}(\bar{e}_i)$ et $\bar{\theta}_{\mathfrak{p}}(\bar{e}'_i)$ à $\mathcal{K}_{\mathfrak{p}}$ satisfaisant à la congruence suivante (voir [F], thm. 4.6) :

$$(I) \quad \widetilde{\theta_{\mathfrak{p}}(e_1)}^{p^m} \equiv [\widetilde{\theta_{\mathfrak{p}}(e_1)}, \widetilde{\theta_{\mathfrak{p}}(e'_1)}] \dots [\widetilde{\theta_{\mathfrak{p}}(e_{1+r_2})}, \widetilde{\theta_{\mathfrak{p}}(e'_{1+r_2})}] \pmod{G_{\mathfrak{p}}^{(2)}}.$$

Description de $G_S/G_S^{(2)}$.

Puisque K est p -rationnel et contient μ_p , pour chaque place $\mathcal{L} \in S \setminus S_p$, il existe un entier naturel $h_{\mathcal{L}}$ premier à p , un entier $a_{\mathcal{L}}$ et un élément $u_{\mathcal{L}}$ de K tels que $\zeta_{p^m}^{h_{\mathcal{L}}} = (u_{\mathcal{L}})$. $u_{\mathcal{L}}$ est en fait une S -unité de K . $h_{\mathcal{L}}$, $a_{\mathcal{L}}$ et $u_{\mathcal{L}}$ seront désormais fixés.

Soit $w_{\mathcal{L}}$ comme auparavant un générateur du groupe multiplicatif $\mu_{N\mathcal{L}-1}$ des racines de l'unité contenues dans $K_{\mathcal{L}}$. Puisque toute unité de $K_{\mathcal{L}}$ est, modulo \mathcal{L} , congrue à une puissance de $w_{\mathcal{L}}$, nous définissons les entiers p -adiques $\alpha_{\mathcal{L}, \mathcal{L}'}$, en posant

$$(II) \quad u_{\mathcal{L}} \equiv w_{\mathcal{L}}^{\alpha_{\mathcal{L}, \mathcal{L}'}} \pmod{\mathcal{L}'},$$

pour tout couple $(\mathcal{L}, \mathcal{L}')$ de non- p -places finies de S .

De même, nous définissons les entiers p -adiques $\alpha_{i,\mathcal{L}}$; $\mathcal{L} \in S \setminus S_p$ et $i = 1, \dots, 1+r_2$; par les congruences

$$(III) \quad e_i \equiv \omega_{\mathcal{L}}^{\alpha_{i,\mathcal{L}}} \pmod{\mathcal{L}}.$$

Enfin pour $i \in \{1, \dots, 1+r_2\}$ et $\mathcal{L} \in S \setminus S_p$ soient $\alpha_{\mathcal{L},i}$ et $\alpha'_{\mathcal{L},i}$ des entiers p -adiques définis par

$$(IV) \quad \underline{\gamma} = \xi \prod_{i=1}^{1+r_2} e_i^{\alpha_{\mathcal{L},i}} \prod_{i=1}^{1+r_2} e'_i^{\alpha'_{\mathcal{L},i}},$$

l'égalité étant considérée dans le corps local K_p , et $\xi \in \mu_{Np-1}$ étant une racine de l'unité d'ordre premier à p .

Notons que tous les entiers $\alpha_{\mathcal{L},\mathcal{L}}, \alpha_{i,\mathcal{L}}, \alpha_{\mathcal{L},i}$ et $\alpha'_{\mathcal{L},i}$ que l'on vient d'introduire s'obtiennent par des calculs abéliens et finis.

Pour chaque $\mathcal{Y} \in S$ nous avons, d'après la théorie du corps de classes, un diagramme commutatif

$$(V) \quad \begin{array}{ccccc} K_{\mathcal{Y}}^* & \xrightarrow{\hspace{2cm}} & J_K & \xrightarrow{\hspace{2cm}} & J_K/J_K^{p^m} \\ \theta_{\mathcal{Y}} \downarrow & \searrow & \theta \downarrow & \searrow & \bar{\theta} \downarrow \\ K_{\mathcal{Y}}^* / K_{\mathcal{Y}}^{* p^m} & \xrightarrow{\hspace{2cm}} & G_S^{ab} & \xrightarrow{\hspace{2cm}} & X_S/X_S^{p^m} \\ G_{\mathcal{Y}}^{ab} \xrightarrow{\hspace{2cm}} & \xrightarrow{\hspace{2cm}} & G_S^{ab} & \xrightarrow{\hspace{2cm}} & \\ \theta_{\mathcal{Y}} \downarrow & \searrow & \theta \downarrow & \searrow & \bar{\theta} \downarrow \\ G(F_{\mathcal{Y}}^m / K_{\mathcal{Y}}) & \xrightarrow{\hspace{2cm}} & & & \end{array}$$

où les flèches verticales représentent les morphismes de réciprocité et où les autres flèches sont naturelles.

Pour chaque non- p -place finie \mathcal{L} de S , l'entier $\underline{\gamma}_{\mathcal{L}}$ est inversible dans \mathbb{Z}_p , et $\theta_{\mathcal{L}}(\underline{\gamma}_{\mathcal{L}})^{\underline{\gamma}_{\mathcal{L}}^{-1}}$ est un relèvement du Frobenius en \mathcal{L} à $K_{\mathcal{L}}^{ab}$:

$$(VI) \quad \theta_{\mathcal{L}}(\underline{\gamma}_{\mathcal{L}})^{\underline{\gamma}_{\mathcal{L}}^{-1}} = \sigma_{\mathcal{L}}(K_{\mathcal{L}}^{ab}/K_{\mathcal{L}}).$$

Nous allons exprimer $\theta_{\mathcal{L}}(\psi)$ (en fait son image dans G_S^{ab}) en fonction des éléments $\sigma_1(K_S^{ab}/K), \dots, \sigma_{1+r_2}(K_S^{ab}/K)$ et $\tau_{\mathcal{L}}(K_S^{ab}/K)$, $\mathcal{L} \in S \setminus S_p$, qui engendrent de façon minimale le groupe de Galois G_S^{ab} .

Notons i_S le composé de l'injection canonique $\prod_{\mathcal{L} \in S} K_{\mathcal{L}}^* \rightarrow J_K$ avec l'injection diagonale $K^* \rightarrow \prod_{\mathcal{L} \in S} K_{\mathcal{L}}^*$:

$$i_S : K^* \rightarrow J_K.$$

Comme ψ est une S -unité, l'image de l'idèle $i_S(\psi)$ par l'homomorphisme de réciprocité θ est triviale :

$$\theta(i_S(\psi)) = \theta_{\mathcal{L}}(\psi) \cdot \theta_{\mathfrak{p}}(\psi) \cdot \prod_{\mathcal{L}' \neq \mathcal{L}} \theta_{\mathcal{L}'}(\psi) = 1.$$

D'où, en utilisant (II) et (IV)

$$\theta_{\mathcal{L}}(\psi) \prod_{i=1}^{1+r_2} \theta_{\mathfrak{p}}(e_i)^{\alpha_{\mathcal{L}}, i} \prod_{i=1}^{1+r_2} \theta_{\mathfrak{p}}(e_i)^{\alpha_{\mathcal{L}'}, i} \prod_{\mathcal{L}' \neq \mathcal{L}} \tau_{\mathcal{L}'}(K_S^{ab}/K)^{\alpha_{\mathcal{L}'}, \mathcal{L}'} = 1.$$

Soit encore

$$(VII) \quad \theta_{\mathcal{L}}(\psi) = \prod_{i=1}^{1+r_2} \theta_{\mathfrak{p}}(e_i)^{-\alpha_{\mathcal{L}}, i} \prod_{i=1}^{1+r_2} \sigma_i(K_S^{ab}/K)^{-\alpha_{\mathcal{L}}, i} \prod_{\mathcal{L}' \neq \mathcal{L}} \tau_{\mathcal{L}'}(K_S^{ab}/K)^{-\alpha_{\mathcal{L}'}, \mathcal{L}'}.$$

Il nous reste à exprimer $\theta_{\mathfrak{p}}(e_i)$ (en fait son image dans G_S^{ab}) en fonction des éléments du système minimal de générateurs $\{\sigma_i(K_S^{ab}/K), \tau_{\mathcal{L}}(K_S^{ab}/K)/i = 1, \dots, 1+r_2; \mathcal{L} \in S \setminus S_p\}$ de G_S^{ab} . Pour cela nous reprenons le précédent procédé en remplaçant ψ par e_i :

$$\theta(i_S(e_i)) = \theta_{\mathfrak{p}}(e_i) \prod_{\mathcal{L}} \theta_{\mathcal{L}}(e_i) = 1,$$

et en utilisant (III) il vient

$$(VIII) \quad \theta_{\mathfrak{p}}(e_i) = \prod_{\mathcal{L}'} \tau_{\mathcal{L}'} (K_S^{ab}/K)^{-\alpha_{i,\mathcal{L}'}}.$$

En substituant dans (VII), nous obtenons finalement l'expression de $\theta_{\mathcal{L}}(\psi)$ en termes des éléments du système minimal de générateurs de G_S^{ab} choisi :

$$\begin{aligned} \theta_{\mathcal{L}}(\psi) &= \prod_{i=1}^{1+r_2} \sigma_i (K_S^{ab}/K)^{-\alpha_{\mathcal{L}},i} \cdot \tau_{\mathcal{L}} (K_S^{ab}/K)^{\sum_{i=1}^{1+r_2} \alpha_{i,\mathcal{L}} \cdot \alpha_{\mathcal{L},i}} \\ &\quad \prod_{\mathcal{L}' \neq \mathcal{L}} \tau_{\mathcal{L}'} (K_S^{ab}/K)^{-\alpha_{\mathcal{L}},\mathcal{L}'} + \sum_{i=1}^{1+r_2} \alpha_{\mathcal{L},i} \cdot \alpha_{i,\mathcal{L}}. \end{aligned}$$

Comme les commutateurs sont bilinéaires dans un groupe de classe 2, cette dernière égalité, jointe à (VI), nous fournit, en vertu du théorème 2.7, la congruence :

$$\begin{aligned} \frac{(N\mathcal{L}-1)h_{\mathcal{L}}}{\mathcal{L}} &\equiv \prod_{\substack{\mathcal{L}' \in S \setminus S_p \\ \mathcal{L}' \neq \mathcal{L}}} [\tau_{\mathcal{L}}, \tau_{\mathcal{L}'}]^{\alpha_{\mathcal{L}}, \mathcal{L}' - \sum_{i=1}^{1+r_2} \alpha_{i,\mathcal{L}} \cdot \alpha_{i,\mathcal{L}'}} \\ &\quad \prod_{i=1}^{1+r_2} [\tau_{\mathcal{L}}, \sigma_i]^{\alpha_{\mathcal{L}}, i} \pmod{G_S^{(2)}}. \end{aligned}$$

En résumé nous avons le résultat suivant, qui décrit les relations du pro- p -groupe G_S modulo $G_S^{(2)}$:

THEOREME 4.3. Soient K un corps p -rationnel contenant μ_p , et S un ensemble fini de places finies de K contenant S_p (si $\mathcal{L} \in S \setminus S_p$, alors p divise $N\mathcal{L}-1$). Il existe une présentation minimale $1 \rightarrow R_S \rightarrow F_S \rightarrow G_S \rightarrow 1$ de G_S , où le pro- p -groupe libre F_S est engendré par le système

$$\{s_i, t_{\mathcal{L}} / i = 1, \dots, 1 + r_2; \mathcal{L} \in S \setminus S_p\},$$

et R_S est le sous-groupe fermé distingué de F_S , engendré par le système

$$\begin{aligned} \{t_{\mathcal{L}}^{(N\mathcal{L}-1)h_{\mathcal{L}}} \prod_{\substack{\mathcal{L}' \in S \setminus S_p \\ \mathcal{L}' \neq \mathcal{L}}} \left[t_{\mathcal{L}}, t_{\mathcal{L}'} \right]^{-\alpha_{\mathcal{L}}, \mathcal{L}'} \prod_{i=1}^{1+r_2} \left[t_{\mathcal{L}}, s_i \right]^{\alpha_{\mathcal{L}}, i} \}_{\mathcal{L} \in S \setminus S_p} ; \\ \times \prod_{i=1}^{1+r_2} \left[t_{\mathcal{L}}, s_i \right]^{\alpha_{\mathcal{L}}, i} \}_{\mathcal{L} \in S \setminus S_p} ; \end{aligned}$$

où pour chaque non- p -place finie \mathcal{L} de S , l'élément $t_{\mathcal{L}}$ se trouve dans $F_S^{(2)}$, et où les exposants $\alpha_{\mathcal{L}, \mathcal{L}'}$, $\alpha_{\mathcal{L}, i}$, $\alpha_{i, \mathcal{L}'}$ et $\alpha_{\mathcal{L}, i}$ sont définis par les égalités (II), (III) et (IV).

Gardons les hypothèses et les notations du théorème précédent. Puisque le corps de nombres K satisfait à la conjecture de Leopoldt en p , le multiplicateur de Schur $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p)^*$ est nul. Le corollaire de la proposition 4.3 de [F] montre alors qu'en tant que pro- p -groupe de classe deux, un système minimal de relations de $G_S/G_S^{(2)}$ est donné par

$$\begin{aligned} \bar{t}_{\mathcal{L}}^{(N\mathcal{L}-1)h_{\mathcal{L}}} = \prod_{\substack{\mathcal{L}' \in S \setminus S_p \\ \mathcal{L}' \neq \mathcal{L}}} \left[\bar{t}_{\mathcal{L}}, \bar{t}_{\mathcal{L}'} \right]^{\alpha_{\mathcal{L}}, \mathcal{L}'} \prod_{i=1}^{1+r_2} \left[\bar{t}_{\mathcal{L}}, \bar{s}_i \right]^{\alpha_{\mathcal{L}}, i} , \quad \mathcal{L} \in S \setminus S_p , \end{aligned}$$

où la barre au-dessus de chaque élément de F_S désigne la classe de cet élément, modulo $F_S^{(2)}$.

Ce dernier résultat généralise le théorème 4.6 de [UW].

Comme application, on va donner, par une méthode calquée sur celle de Fröhlich et Ullom—Watt, une nouvelle démonstration de la loi de réciprocité pour les symboles de puissance.

Rappels :

Soit n un entier naturel, et K un corps de nombre contenant les racines n -ièmes de l'unité μ_n . Pour un élément non nul $a \in K^*$, et un idéal \mathcal{Y} étranger aux idéaux principaux (a) et (n) de K , le symbole de résidu de puissance n -ième $(\frac{a}{\mathcal{Y}})$ est défini par l'égalité suivante :

$$\sigma_{\mathcal{Y}}(\sqrt[n]{a}) = (\frac{a}{\mathcal{Y}}) \cdot \sqrt[n]{a};$$

où $\sigma_{\mathcal{Y}}$ est comme auparavant le Frobenius de l'idéal \mathcal{Y} . Comme par hypothèse les racines n -ièmes de l'unité se trouvent dans K , le symbole ainsi défini est une racine n -ième de l'unité et sa définition ne dépend pas du choix de la racine n -ième de a . Le symbole $(\frac{a}{\mathcal{Y}})$ est l'unique racine n -ième de l'unité satisfaisant à la congruence suivante :

$$(\frac{a}{\mathcal{Y}}) \equiv a^{\frac{Np-1}{n}} \pmod{\mathcal{Y}}.$$

On généralise cette définition en posant, pour un idéal b de K ,

$$(\frac{a}{b}) = \prod_{\mathcal{Y}} (\frac{a}{\mathcal{Y}})^{\nu_{\mathcal{Y}}(b)},$$

où \mathcal{Y} parcourt les idéaux premiers de K étrangers aux idéaux principaux (n) et (a) , et où $\nu_{\mathcal{Y}}$ désigne la valuation associée à la place \mathcal{Y} .

Si l'idéal $b = (b)$ est un idéal principal, on écrit $(\frac{a}{b})$ au lieu de $(\frac{a}{\mathcal{Y}})$.

Les propriétés de ce symbole sont bien connues, (voir par exemple [HA]). Voici les propriétés principales, valables dès que les symboles intervenant ont bien un sens :

- i) $(\frac{a}{yy'}) = (\frac{a}{y})(\frac{a}{y'})$.
- i bis) $(\frac{a}{bb'}) = (\frac{a}{b})(\frac{a}{b'})$.
- ii) $(\frac{aa'}{y}) = (\frac{a}{y})(\frac{a'}{y})$.
- ii bis) $(\frac{aa'}{b}) = (\frac{a}{b})(\frac{a'}{b})$, dès que les idéaux premiers ne divisant pas n , intervenant dans la décomposition de l'idéal principal (b) , différents de ceux intervenant dans la décomposition de (a) ou de (a') .
- iii) Si a est un entier et si $a' \equiv a \pmod{b}$, alors $(\frac{a'}{b}) = (\frac{a}{b})$.
- iv) Si ζ est une racine n -ième de l'unité, alors $(\frac{\zeta}{b}) = \zeta^{\frac{Nb-1}{n}}$.

Le théorème suivant donne une nouvelle preuve de la loi de réciprocité de résidu de puissance p^n -ième lorsque K est un corps p -rationnel, contenant les racines p^n -ièmes de l'unité.

THEOREME 4.4. Soit K un corps de nombre p -rationnel contenant μ_{p^n} . Soient \mathcal{L} et \mathcal{L}' deux idéaux premiers de K étrangers à p avec, comme auparavant,

$$\mathcal{L}^{h_{\mathcal{L}}} \mathfrak{p}^{\alpha_{\mathcal{L}}} = (\underline{u}_{\mathcal{L}}), \quad \mathcal{L}'^{h_{\mathcal{L}'}} \mathfrak{p}^{\alpha_{\mathcal{L}'}} = (\underline{u}_{\mathcal{L}'}) .$$

Alors

$$(\frac{\underline{u}_{\mathcal{L}}}{\underline{u}_{\mathcal{L}'}})(\frac{\underline{u}_{\mathcal{L}'}}{\underline{u}_{\mathcal{L}}})^{-1} = \zeta^{\frac{t_{\mathcal{L}}}{p^n}, \mathcal{L}'},$$

où $(\frac{\underline{u}_{\mathcal{L}}}{\underline{u}_{\mathcal{L}'}})$ est le symbole de résidu de puissance p^n -ième, où

$$t_{\mathcal{L}, \mathcal{L}'} = \sum_{i=1}^{1+r_2} \alpha_{\mathcal{L}, i} \alpha_{\mathcal{L}'}^{'}, i - \sum_{i=1}^{1+r_2} \alpha_{\mathcal{L}', i} \alpha_{\mathcal{L}, i}^{'},$$

et où les entiers $\alpha_{\mathcal{L}, i}$, $\alpha_{\mathcal{L}', i}$, $\alpha_{\mathcal{L}, i}^{'}$ et $\alpha_{\mathcal{L}', i}^{'}$ sont définis par la relation (IV).

Preuve : Avec les notations précédemment introduites, nous avons les égalités suivantes :

$$\begin{aligned} \left(\frac{\underline{\omega}}{\underline{\omega}'}\right) &= \left(\frac{\underline{\omega}}{\underline{\omega}'}\right)^{\underline{h}_{\underline{\omega}'}} = \left(\frac{\underline{\omega}'}{\underline{\omega}'}\right)^{\underline{\alpha}_{\underline{\omega}}, \underline{\omega}', \underline{h}_{\underline{\omega}'}} \\ &= \left(\underline{\omega}', p^n\right)^{\frac{N\underline{\omega}'-1}{p^n}} \underline{\alpha}_{\underline{\omega}}, \underline{\omega}', \underline{h}_{\underline{\omega}'} = \zeta_{p^n}^{\underline{\alpha}_{\underline{\omega}}, \underline{\omega}', \underline{h}_{\underline{\omega}'}}. \end{aligned}$$

Pareillement

$$\left(\frac{\underline{\omega}'}{\underline{\omega}}\right) = \zeta_{p^n}^{\underline{\alpha}_{\underline{\omega}'}, \underline{\omega}, \underline{h}_{\underline{\omega}}},$$

d'où

$$\left(\frac{\underline{\omega}}{\underline{\omega}'}\right)\left(\frac{\underline{\omega}'}{\underline{\omega}}\right)^{-1} = \zeta_{p^n}^{\underline{\alpha}_{\underline{\omega}}, \underline{\omega}, \underline{h}_{\underline{\omega}}, -\underline{\alpha}_{\underline{\omega}'}, \underline{\omega}, \underline{h}_{\underline{\omega}}}.$$

Soit $m \geq n$ le plus grand entier tel que $\mu_m \subset K$. Nous allons maintenant calculer l'expression $\underline{\alpha}_{\underline{\omega}}, \underline{\omega}, \underline{h}_{\underline{\omega}}, -\underline{\alpha}_{\underline{\omega}'}, \underline{\omega}, \underline{h}_{\underline{\omega}}$ modulo p^m , en supprimant $\underline{h}_{\underline{\omega}}$ et $\underline{h}_{\underline{\omega}'}$.

En posant $S = \{\mathfrak{p}, \underline{\omega}, \underline{\omega}'\}$, et en reprenant les notations de la section précédente, il vient

$$\theta(i_S(\zeta_{p^m})) = \theta_{\mathfrak{p}}(\zeta_{p^m}) \cdot \theta_{\underline{\omega}}(\zeta_{p^m}) \cdot \theta_{\underline{\omega}'}(\zeta_{p^m}) = 1,$$

d'où

$$\theta_{\mathfrak{p}}(\zeta_{p^m}) \cdot \tau_{\underline{\omega}}^{\frac{N\underline{\omega}-1}{p^m}} \cdot \tau_{\underline{\omega}'}^{\frac{N\underline{\omega}'-1}{p^m}} \in [G_S, G_S],$$

et

$$(IX) \quad \theta_{\mathfrak{p}}(\zeta_{p^m})^{p^m} \cdot \tau_{\underline{\omega}}^{N\underline{\omega}-1} \cdot \tau_{\underline{\omega}'}^{N\underline{\omega}'-1} \in [G_S, G_S]^{p^m}.$$

Nous avons également, en utilisant la congruence (I) donnant la relation locale en \mathfrak{p} , et la congruence (VIII) :

$$(X) \quad \theta_{\mathfrak{p}} (\zeta_p m)^{p^m} \equiv \prod_{i=1}^{1+r_2} [\tau_{\mathcal{L}, \sigma_i}]^{-\alpha_{i, \mathcal{L}}} \prod_{i=1}^{1+r_2} [\tau_{\mathcal{L}', \sigma_i}]^{-\alpha_{i, \mathcal{L}'}} \pmod{G_S^{(2)}}.$$

D'autre part, en faisant intervenir les relations de $G_S/G_S^{(2)}$ établies dans le théorème 1, nous avons les congruences suivantes :

$$(XI) \quad \begin{aligned} & \tau_{\mathcal{L}}^{(N\mathcal{L}-1)h_{\mathcal{L}}, h_{\mathcal{L}}}, \\ & \equiv [\tau_{\mathcal{L}}, \tau_{\mathcal{L}'}]^{(\alpha_{\mathcal{L}}, \mathcal{L}' - \sum_{i=0}^{r_2} \alpha_{\mathcal{L}, i} \alpha_{i, \mathcal{L}}), 1+r_2} \prod_{i=1}^{1+r_2} [\tau_{\mathcal{L}, \sigma_i}]^{\alpha_{\mathcal{L}, i} h_{\mathcal{L}'}} \pmod{G_S^{(2)}}, \end{aligned}$$

et

$$(XII) \quad \begin{aligned} & \tau_{\mathcal{L}'}^{(N\mathcal{L}'-1)h_{\mathcal{L}'}, h_{\mathcal{L}'}} \\ & \equiv [\tau_{\mathcal{L}'}, \tau_{\mathcal{L}}]^{\alpha_{\mathcal{L}'}, \mathcal{L}' - \sum_{i=0}^{r_2} \alpha_{\mathcal{L}'}, i \alpha_{i, \mathcal{L}'}) h_{\mathcal{L}'} 1+r_2} \prod_{i=1}^{1+r_2} [\tau_{\mathcal{L}', \sigma_i}]^{\alpha_{\mathcal{L}', i} h_{\mathcal{L}'}} \pmod{G_S^{(2)}} \\ & , \end{aligned}$$

En regroupant les congruences (IX), (X), (XI) et (XII), nous obtenons

$$(XIII) \quad \begin{aligned} & \prod_i [\tau_{\mathcal{L}, \sigma_i}]^{-\alpha_{i, \mathcal{L}} h_{\mathcal{L}}, h_{\mathcal{L}}} + \alpha_{\mathcal{L}, i} h_{\mathcal{L}}, \\ & \times \prod_i [\tau_{\mathcal{L}', \sigma_i}]^{-\alpha_{i, \mathcal{L}'}, h_{\mathcal{L}'}, h_{\mathcal{L}}} + \alpha_{\mathcal{L}', i} h_{\mathcal{L}'} \\ & \times [\tau_{\mathcal{L}}, \tau_{\mathcal{L}'}]^{(\alpha_{\mathcal{L}}, \mathcal{L}' - \sum_i \alpha_{\mathcal{L}, i} \alpha_{i, \mathcal{L}}), h_{\mathcal{L}}}, - (\alpha_{\mathcal{L}'}, \mathcal{L}' - \sum_i \alpha_{\mathcal{L}'}, i \alpha_{i, \mathcal{L}}) h_{\mathcal{L}'} \\ & \in [G_S, G_S]^{p^m} G_S^{(2)}. \end{aligned}$$

Cela étant, montrons le lemme suivant :

LEMME 4.5. Soit G un pro- p -groupe avec $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Alors le quotient $G^{(1)}/G^{(2)}$ est canoniquement isomorphe au multiplicateur de Schur $M(G^{ab})$ de G^{ab} .

Preuve : La suite courte exacte

$$0 \rightarrow G^{(1)} \rightarrow G \rightarrow G^{ab} \rightarrow 0$$

donne, par inflation-restriction,

$$\begin{aligned} 0 &\rightarrow H^1(G^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(G^{(1)}, \mathbb{Q}_p/\mathbb{Z}_p)^{G^{ab}} \\ &\rightarrow H^2(G^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p). \end{aligned}$$

D'où, en nous servant de l'hypothèse de l'énoncé, nous obtenons un isomorphisme

$$H^1(G^{(1)}, \mathbb{Q}_p/\mathbb{Z}_p)^{G^{ab}} \xrightarrow{\sim} H^2(G^{ab}, \mathbb{Q}_p/\mathbb{Z}_p).$$

En prenant le dual, il vient

$$\begin{aligned} M(G^{ab}) &\simeq (H^1(G^{(1)}, \mathbb{Q}_p/\mathbb{Z}_p)^{G^{ab}})^* \\ &\simeq (G^{(1)})^{ab}/I_{G^{ab}} \cdot (G^{(1)})^{ab} \\ &\simeq G^{(1)}/[G, G^{(1)}], \end{aligned}$$

$$\text{soit } M(G^{ab}) \simeq G^{(1)}/G^{(2)}. \quad \text{QED}$$

Suite de la démonstration du théorème 4.4. Puisque K est p -rationnel, nous avons $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, et le lemme précédent nous montre que le pro- p -groupe abélien $G_S^{(1)}/G_S^{(2)}$ admet pour système minimal de générateurs

$$\{[\tau_{\mathcal{L}}, \tau_{\mathcal{L}}], [\tau_{\mathcal{L}}, \sigma_i], [\tau_{\mathcal{L}}, \sigma_j], [\sigma_j \sigma_i] / i = 1, \dots, 1 + c, j = 1, \dots, 1 + c; j \neq i\}.$$

Nous disposons ainsi, en tenant compte de (XIII), des congruences suivantes :

$$\begin{aligned} \alpha_{i,\mathcal{L}} h_{\mathcal{L}} h_{\mathcal{L}} &\equiv \alpha'_{i,\mathcal{L}} h_{\mathcal{L}} \quad (\text{mod. } p^m) \\ \alpha_{i,\mathcal{L}}, h_{\mathcal{L}} h_{\mathcal{L}} &\equiv \alpha'_{i,\mathcal{L}} h_{\mathcal{L}} \quad (\text{mod. } p^m) \\ (\alpha_{\mathcal{L},\mathcal{L}} - \sum_i \alpha_{i,\mathcal{L}} \alpha_{i,\mathcal{L}}) h_{\mathcal{L}} &\equiv (\alpha'_{\mathcal{L},\mathcal{L}} - \sum_i \alpha'_{i,\mathcal{L}} \alpha_{i,\mathcal{L}}) h_{\mathcal{L}} \quad (\text{mod. } p^m). \end{aligned}$$

D'où, visiblement,

$$\begin{aligned} \alpha_{\mathcal{L},\mathcal{L}}, h_{\mathcal{L}}, -\alpha_{\mathcal{L},\mathcal{L}} h_{\mathcal{L}} &\equiv \sum_i \alpha_{i,\mathcal{L}} \alpha_{i,\mathcal{L}}, h_{\mathcal{L}}, - \sum_i \alpha'_{i,\mathcal{L}} \alpha_{i,\mathcal{L}} h_{\mathcal{L}} \quad (\text{mod. } p^m) \\ &\equiv \sum_i \alpha_{i,\mathcal{L}} \alpha'_{i,\mathcal{L}}, i - \sum_i \alpha'_{i,\mathcal{L}} \alpha'_{i,\mathcal{L}}, i \quad (\text{mod. } p^m), \end{aligned}$$

ce qui achève la démonstration du théorème.

QED

Notons que la somme alternée $\sum_i \alpha_{i,\mathcal{L}} \alpha'_{i,\mathcal{L}}, i - \sum_i \alpha'_{i,\mathcal{L}} \alpha'_{i,\mathcal{L}}, i$ n'est autre que l'expression du symbole de Hilbert en \mathfrak{p} , dans la base symplectique $\{e_i, e'_i / i = 1, \dots, 1+c\}$ de $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p^m}$.

5.— Ensembles primitifs maximaux et lois de réciprocité primitives.

Dans toute cette section, on supposera que K contient μ_p . Si K est p -rationnel, il n'existe qu'une seule place \mathfrak{p} au-dessus de p , et la loi de réciprocité pour les symboles de Hilbert s'écrit :

$$\forall a,b \in K^\times, (a,b)_{\mathfrak{p}}^{-1} = \prod_{\mathcal{L} \neq \mathfrak{p}} (a,b)_{\mathcal{L}}^{p^{\frac{m_{\mathcal{L}}}{2}} - 1},$$

où $p^m = \#\mu(K) = \#\mu(K_{\mathfrak{p}})$

$$p^{\frac{m_{\mathcal{L}}}{2}} = \#\mu(K_{\mathcal{L}}).$$

On se propose ici de déterminer une loi de réciprocité, appelée primitive, pour le symbole sauvage $(\cdot, \cdot)_{\mathfrak{p}}$, ne mettant en jeu qu'un nombre fini de symboles modérés $(\cdot, \cdot)_{\mathcal{L}}$. On regarde d'abord la structure des S -unités.

PROPOSITION 5.1. *Supposons \$K\$ \$p\$-rationnel, contenant \$\mu_p\$, et \$S\$ primitif maximal. L'injection diagonale \$E_S(K) \rightarrow \prod_{w \in S \setminus S_p} K_w^\times\$ induit un homomorphisme surjectif \$E_S(K) \otimes \mathbb{Z}_p \rightarrow \prod_{w \in S \setminus S_p} \mathcal{K}_w\$,*

(ici, \$E_S(K)\$ désigne le groupe des \$S_f\$-unités de \$K\$).

Preuve :

Comme \$S\$ est primitif maximal, le théorème de structure 3.5 montre que \$G_S^{ab} \simeq \prod_{w \in S \setminus S_p} \mathcal{K}_w\$, d'où \$\mathrm{Hom}(G_S^{ab}, \mu_p) \simeq \prod_{w \in S \setminus S_p} \mathrm{Hom}(\mathcal{K}_w, \mu_p)\$. D'après la théorie de Kummer, \$\mathrm{Hom}(\mathcal{K}_w, \mu_p) \simeq K_w^\times / K_w^{\times p}\$ et, puisque \$\mathcal{O}_S = 0\$, \$\mathrm{Hom}(G_S^{ab}, \mu_p) \simeq E_S / E_S^p\$. Le théorème de Burnside pour les pro-\$p\$-groupes montre alors que l'homomorphisme \$E_S \otimes \mathbb{Z}_p \rightarrow \prod_{w \in S \setminus S_p} \mathcal{K}_w\$ est surjectif. QED

Remarque 5.2.

L'épimorphisme de 5.1 n'est évidemment pas un isomorphisme (regarder les \$\mathbb{Z}_p\$-rangs). Si \$K\$ contient \$\mu_{2p}\$, en utilisant des résultats de Kuz'min sur les normes universelles des \$S\$-unités ([KZ2], 3.2), on obtient une suite exacte de modules galoisiens

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathbb{Z}_p(1)^{1+r_2} \longrightarrow E_S \otimes \mathbb{Z}_p \longrightarrow \prod_{w \in S \setminus S_p} \mathcal{K}_w \longrightarrow 0$$

où \$\mathbb{Z}_p(1) := \varprojlim_p \mu_n\$ est le module de Tate.

COROLLAIRE 5.3 (*"lemme d'approximation simultanée par les S-unités"*). *Sous les hypothèses de 5.1, et si K contient μ_{p^n} , les injections diagonales $E_S \rightarrow K_p^\times$ (où p est l'unique place de K au-dessus de p) et $E_S \rightarrow \prod_{w \in S \setminus S_p} K_w^\times$ induisent des isomorphismes :*

$$K_p^\times / K_p^{\times p^n} \xleftarrow{\alpha} E_S / E_S^{\times p^n} \xrightarrow{\beta} \prod_{w \in S \setminus S_p} K_w^\times / K_w^{\times p^n}.$$

Preuve : Cela résulte immédiatement de 3.5 et 5.1.

QED

THEOREME 5.4 (*"loi de réciprocité primitive"*). *Supposons K p-rationnel, contenant μ_{p^n} , et S primitif maximal. Alors les modules $K_p^\times / K_p^{\times p^n}$ et $\prod_{w \in S \setminus S_p} K_w^\times / K_w^{\times p^n}$ sont naturellement anti-isométrique pour la structure (symplectique si $p \neq 2$) induite par les symboles de Hilbert.*

Preuve :

Le lemme d'approximation simultanée par les S-unités nous fournit un isomorphisme canonique $\theta_S : K_p^\times / K_p^{\times p^n} \xrightarrow{\sim} \prod_{w \in S \setminus S_p} K_w^\times / K_w^{\times p^n}$, qui vérifie

$$(a, b)_p^{-1} = \prod_{w \in S \setminus S_p} (\beta \alpha^{-1}(a), \beta \alpha^{-1}(b))_w,$$

compte tenu de la formule usuelle du

produit et de la factorisation de θ_S à travers les S-unités.

QED

Remarques 5.5 :

- i) La loi de réciprocité primitive précédente fournit une loi de réciprocité explicite (les symboles modérés étant explicitement calculables; voir [HA]) si l'on sait trouver une base de $E_S / E_S^{\times p^n}$ adaptée à la structure héritée des symboles de Hilbert (une base symplectique si $p \neq 2$). C'est le type de calculs qu'on a fait au paragraphe 4.

ii) Si K est p -rationnel et contient μ_p , et S est primitif maximal, les théorèmes 2.1, 3.3 et 3.7 montrent qu'il existe une seule place \mathfrak{p} de K_S au-dessus de p et que le groupe de décomposition $G_S^{\mathfrak{p}}$ en cette place vérifie l'isomorphisme : $G_S^{\mathfrak{p}} \underset{w \in S \setminus S_p}{\sim} \ast$ (en convenant, comme dans [J], que $\mathbb{Z}/2\mathbb{Z}$ est un groupe de décomposition en une place réelle). Cet isomorphisme peut être considéré comme une généralisation non abélienne de la formule du produit.

APPENDICE

Soit L/K une p -extension de corps de nombres de groupe de Galois G . La fonction Logarithme de Gras permet d'exprimer, moyennant la conjecture de Leopoldt pour L en p , l'ordre de $T_{S_p}(L)^G$ – les éléments de $T_{S_p}(L)$ invariants par G – en fonction de l'ordre de $T_{S_p}(K)$ et la ramification dans L/K (voir par exemple [G2], III.1).

Le but de cet appendice est de donner une démonstration de ce résultat, par voie cohomologique, qui présente un intérêt en elle-même (voir la suite exacte du théorème ci-dessous).

LEMME 1. *Soit F/E une extension galoisienne de corps locaux, de groupe de Galois G . Soit \check{F} (resp. \check{E}) le quotient sans \mathbb{Z}_p -torsion du complété p -adique \check{F} de F (resp. E). Alors \check{E} s'injecte dans \check{F}^G , et le quotient \check{F}^G/\check{E} est canoniquement isomorphe au groupe de cohomologie $H^1(G, \mu(F))$.*

Preuve :

Partons de la suite courte exacte de $\mathbb{Z}_p[G]$ -modules $1 \rightarrow \mu(F) \rightarrow \check{F} \rightarrow \check{F} \rightarrow 1$ définissant le \mathbb{Z}_p -module libre \check{F} . En passant à la cohomologie pour l'action naturelle de G , il vient

$$1 \rightarrow \mu(E) \rightarrow \check{F}^G \rightarrow \check{F}^G \rightarrow H^1(G, \mu(F)) \rightarrow H^1(G, \check{F}).$$

Or, $\check{F}^G = \check{E}$ et $H^1(G, \check{F}) = 0$ (c'est un résultat de formations de classes ; voir par exemple [NG1], § 1). D'où la suite exacte

$$1 \rightarrow \check{E} \rightarrow \check{F}^G \rightarrow H^1(G, \mu(F)) \rightarrow 0 . \quad \text{Q.E.D.}$$

Replaçons-nous dans la situation du lemme précédent, et supposons que l'extension locale F/E est modérément ramifiée, et notons e l'indice de ramification de cette extension. F contient alors μ_e , et il existe une uniformisante π_E de E telle que $\pi_F := \pi_E^{1/e}$ soit une uniformisante de F . Le choix de l'uniformisante π_F nous détermine un isomorphisme

$$\check{F} \simeq \mu(F) \times \pi_F^p ,$$

et la surjection $\check{F} \rightarrow \check{F}$ n'est rien d'autre que la projection

$$\mu(F) \times \pi_F^p \rightarrow \pi_F^p .$$

Soit σ un élément du groupe de Galois $G = G(F/E)$, alors

$$\frac{\sigma(\pi_F)}{\pi_F} = \frac{\sigma(\pi_E^{1/e})}{\pi_E^{1/e}} \in \mu_e \subset \mu(F) ,$$

de sorte que $\tilde{\pi}_F$, la classe de π_F dans \check{F} , est invariante par G . Ainsi $\check{F}^G = \check{F}$, et le quotient \check{F}/\check{E} est cyclique d'ordre e , engendré par $\tilde{\pi}_F$. L'isomorphisme $\check{F}/\check{E} \xrightarrow{\sim} H^1(G, \mu(F))$ du lemme précédent fait correspondre à la classe de $\tilde{\pi}_F$, la classe du 1-cocycle

$$\sigma \mapsto \frac{\sigma \tilde{\pi}_F}{\tilde{\pi}_F} .$$

Le lemme 1, étant un résultat de formations de classes, possède un analogue global :

LEMME 2. Soit L/K une p -extension de corps de nombres, de groupe de Galois G . Soit S l'ensemble des places divisant p ou ramifiées dans L/K . Notons \tilde{X}_L (resp. \tilde{X}_K) le quotient sans \mathbb{Z}_p -torsion de $X_S(L) = G_S^{ab}(L)$ (resp. $X_S(K)$). Si L satisfait à la conjecture de Leopoldt en p , alors \tilde{X}_K s'injecte, via l'homomorphisme de transfert, dans \tilde{X}_L^G , et le quotient $\tilde{X}_L^G/\tilde{X}_K$ est canoniquement isomorphe au groupe de cohomologie $H^1(G, T_S(L))$.

Preuve : Partons de la suite courte exacte de $\mathbb{Z}_p[G]$ -modules

$$1 \rightarrow T_S(L) \rightarrow X_S(L) \rightarrow \tilde{X}_L \rightarrow 1$$

définissant le \mathbb{Z}_p -module libre \tilde{X}_L .

La suite de cohomologie associée s'écrit :

$$0 \rightarrow T_S(L)^G \rightarrow X_S(L)^G \rightarrow X_L^G \rightarrow H^1(G, T_S(L)) \rightarrow H^1(G, X_S(L)) .$$

Or $T_S(L)^G = T_S(K)$, $X_S(L)^G = X_S(K)$, et $H^1(G, X_S(L)) = 0$ (c'est un résultat de formations de classes ; voir par exemple [NG1], § 1). D'où la suite exacte

$$0 \rightarrow X_K \rightarrow X_L^G \rightarrow H^1(G, T_S(L)) \rightarrow 0 .$$

Comme L est supposé satisfaire à la conjecture de Leopoldt en p , la théorie du corps de classes nous fournit la suite courte exacte suivante (voir 2.5) :

$$1 \rightarrow \prod_{\mathcal{L}' \in S \setminus S_p} \mu(I_{\mathcal{L}'}) \rightarrow T_S(L) \rightarrow T_{S_p}(L) \rightarrow 1 .$$

Pour chaque place \mathcal{L} de K , fixons-nous une place de L au-dessus de \mathcal{L} qui sera encore notée \mathcal{L} , et désignons par $D_{\mathcal{L}}$ le groupe de décomposition de cette place, pour l'extension L/K . Nous disposons ainsi du diagramme commutatif, aux lignes exactes, suivant :

$$\begin{array}{ccccccc}
1 \rightarrow \prod_{\mathcal{L}}^{\text{II}} \mu(K_{\mathcal{L}}) \rightarrow T_{S_p}(K) & \rightarrow & T_{S_p}(K) & \rightarrow & 1 \\
\downarrow & \downarrow & \downarrow & & \\
1 \rightarrow \prod_{\mathcal{L}}^{\text{II}} \mu(K_{\mathcal{L}}) \rightarrow T_{S_p}(L) & \xrightarrow{G} & T_{S_p}(L) & \xrightarrow{G} & \prod_{\mathcal{L} \in S(K) \setminus S_p(K)}^{\text{II}} H^1(D_{\mathcal{L}}, \mu(L_{\mathcal{L}})) \rightarrow H^1(G, T_S(L)),
\end{array}$$

où les flèches verticales sont induites par l'homomorphisme de transfert. D'où la suite exacte

$$1 \longrightarrow T_{S_p}(L)^G / T_{S_p}(K) \longrightarrow \prod_{\mathcal{L} \in S(K) \setminus S_p(K)}^{\text{II}} H^1(D_{\mathcal{L}}, \mu(L_{\mathcal{L}})) \xrightarrow{\psi} H^1(G, T_S(L)).$$

De ce qui précéde, et des lemmes 1 et 2, nous déduisons le résultat suivant :

THEOREME. Soient L/K une p -extension de corps de nombres, de groupe de Galois G , et S l'ensemble des places de K divisant p ou ramifiées dans L . Pour chaque place $\mathcal{L} \in S \setminus S_p$, notons $e_{\mathcal{L}}$ l'indice de ramification de \mathcal{L} dans L/K . Pour chaque $\mathcal{L} \in S \setminus S_p$, fixons-nous une place de L au-dessus de \mathcal{L} et continuons à la noter \mathcal{L} . Si L satisfait à la conjecture de Leopoldt en p , alors nous avons une suite exacte canonique

$$1 \longrightarrow T_{S_p}(L)^G / T_{S_p}(K) \longrightarrow \prod_{\mathcal{L} \in S(K) \setminus S_p(K)}^{\text{II}} \tilde{L}_{\mathcal{L}} / \tilde{K}_{\mathcal{L}} \xrightarrow{\psi} \tilde{X}_L^G / \tilde{X}_K,$$

où l'homomorphisme ψ est induit par le produit des homomorphismes d'Artin locaux. Pour chaque $\mathcal{L} \in S \setminus S_p$, la classe du Frobenius $\alpha_{\mathcal{L}}(\tilde{K}/K)$ dans l'image de ψ est uniquement divisible par $e_{\mathcal{L}}$ (\tilde{X}_K s'identifie à un sous-module de \tilde{X}_L^G par le transfert). L'image de ψ est en fait le sous-module de $\tilde{X}_L^G / \tilde{X}_K$ engendré par les classes des éléments $\alpha_{\mathcal{L}}(\tilde{K}/K)^{1/e_{\mathcal{L}}}$:

$$\text{Im } \psi = \langle \alpha_{\mathcal{L}}(\tilde{K}/K)^{1/e_{\mathcal{L}}} / \mathcal{L} \in S \setminus S_p \rangle \cdot \tilde{X}_K / \tilde{X}_K.$$

Il en résulte, en particulier que

$$|T_{S_p}(L)^G/T_{S_p}(K)| = \frac{\prod_{\mathcal{L} \in S \setminus S_p} e_{\mathcal{L}}}{|\langle \sigma_{\mathcal{L}}(\tilde{K}/K) \rangle^{1/e_{\mathcal{L}}} / \langle \mathcal{L} \in S \setminus S_p \rangle \cdot \tilde{X}_K/\tilde{X}_K|}.$$

(*) p. 160 : Les résultats du corps de classes s'énoncent de façon plus commode dans le formalisme p -adique de [J], chap. I.

Manuscrit reçu le 30 septembre 1988

BIBLIOGRAPHIE

- [BNW] E. Binz, J. Neukirch et G.H. Wenzel.— *A subgroup theorem for profinite groups*, J. Algebra 19 (1971), 104–109.
- [F] A. Fröhlich.— *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Math. 24, AMS (1983).
- [G1] G. Gras.— *Logarithme p -adique et groupe de Galois*, J. für reine und angew. Math., 343 (1983), 64–80.
- [G2] G. Gras.— *Remarks on K_2 of number fields*, J. Number Theory, 23,3 (1986), 322–335.
- [G3] G. Gras.— *Théorie des genres analytique des fonctions L p -adiques des corps totalement réels*, Invent. Math. 86 (1986), 1–17.
- [G–J] G. Gras et J.–F. Jaulent.— *Sur les corps de nombres réguliers*, à paraître dans Math. Zeitschrift.
- [HA] H. Hasse.— *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, II, Physica, Würzburg–Wien (1965).
- [HR] K. Haberland.— *Galois Cohomology of algebraic number fields*, Deutsch. Verlag Wissen., Berlin (1978).
- [J] J.–F. Jaulent.— *L’arithmétique des ℓ -extensions*, Thèse d’Etat, Besançon (1986).
- [KO] H. Koch.— *Galoissche Theorie der p -Erweiterungen*, Deutsch–Verlag Wissen., Berlin (1970).
- [KZ1] L.V. Kuz'min.— *Homology of profinite groups, Schur multipliers and class field theory*, Math. USSR Izv., 3 (1969), 1149–1182.

- [KZ2] L.V. Kuz'min.— *Local extensions associated with ℓ -extensions with given ramification*, Math. USSR Izv., 9 (1975), 653–726.
- [MK] H. Miki.— *On the Leopoldt conjecture on the p -adic regulators*, J. Number Theory, 26 (1987), 117–128.
- [MV] A. Movahhedi.— *Sur les p -extensions des corps p -rationnels*, Thèse Paris VII (1988).
- [MW] B. Mazur and A. Wiles.— *Class-fields of abelian extensions of \mathbb{Q}* , Invent. Math., 76, 2 (1984), 179–330.
- [NG1] T. Nguyen Quang Do.— *Formations de classes et modules d'Iwasawa*, dans *Number Theory Noordwijkerhout 1983*, Springer LNM 168 (1984), 167–185.
- [NG2] T. Nguyen Quang Do.— *Sur la \mathbb{Z}_p -torsion de certains modules galoisiens*, Ann. Inst. Fourier, 36, 2 (1986), 27–46.
- [NK1] J. Neukirch.— *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math., 21 (1973), 59–116.
- [NK2] J. Neukirch.— *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie*, Arch. Math., 22 (1971), 337–357.
- [NM] O. Neumann.— *On p -closed number fields and an analogue of Riemann's existence theorem in algebraic number fields*, dans *Algebraic Number Fields*, Academic Press (1977), 625–647.
- [SA] J.-W. Sands.— *Kummer's and Iwasawa's version of Leopoldt's conjecture*, prépublication (1986).
- [SE] J.-P. Serre.— *Cohomologie Galoisienne*, Springer LNM5 (1965).
- [T] J. Tate.— *Relations between K_2 and Galois cohomology*, Invent. Math., 36 (1976), 257–274.

- [UW] S.V. Ullom et S.B. Watt.— *Generators and relations for certain class two Galois groups*, J. London Math. Soc. 2, 34 (1986), 235–244.
- [WA] L.C. Washington.— *Introduction to cyclotomic fields*, Springer GTM 83 (1982).
- [WB1] K. Wingberg.— *Freie Produktzerlegungen von Galoisgruppen und Iwasawa Invarianten für p -Erweiterungen von \mathbb{Q}* , J. reine und angew. Math., 343 (1983), 111–129.
- [WB2] K. Wingberg.— *On the product formula in Galois groups*, J. reine und angew. Math., 368 (1986), 172–183.
- [WB3] K. Wingberg.— *On Galois groups of p -closed algebraic number fields with restricted ramification*, prépublication (1988).

T. Nguyen Quang Do
 et A. Movahhedi
 Université Paris VII
 UER de Mathématique—Informatique
 UA 212 du C.N.R.S.
 2, place Jussieu
 75251 Paris Cedex

*Séminaire de Théorie des Nombres
Paris 1987-88*

ALGEBRAIC INDEPENDENCE OF CERTAIN POWER SERIES
K. NISHIOKA

According to a theorem of Liouville [6], in 1844, if θ is an algebraic number of degree $n > 1$, then any approximation by rationals, p/q has the property :

$$|\theta - p/q| \geq cq^{-n},$$

where c is a positive constant depending only on θ . By this property, he constructed transcendental numbers for the first time. For example $\sum_{k=1}^{\infty} 10^{-k!}$ is a transcendental number.

In 1946, Cohn [4] generalized Liouville's result and proved the following as a corollary : if α is an algebraic number with $0 < |\alpha| < 1$, then $\sum_{k=1}^{\infty} \alpha^{k!}$ is transcendental. Several authors studied the transcendency of the values of such gap series. Finally in 1973, Cijssouw and Tijdeman proved the following. Let $\{e_k\}_{k \geq 0}$ be an increasing sequence of non-negative integers, $\{a_k\}_{k \geq 0}$ be a sequence of non-zero algebraic numbers. Assume that the power series $\sum_{k=0}^{\infty} a_k z^{e_k}$ has radius of convergence $R > 0$. Put $S_k = [\mathbb{Q}(a_0, \dots, a_k) : \mathbb{Q}]$, $A_k = \max\{1, |\overline{a_0}|, \dots, |\overline{a_k}|\}$ and $M_k = \min\{d \in \mathbb{N} \mid da_0, \dots, da_k \text{ are algebraic integers}\}$.

THEOREM ([3]). Suppose

$$(1) \quad \lim_{k \rightarrow \infty} (e_k + \log M_k + \log A_k) S_k / e_{k+1} = 0.$$

Then $\sum_{k=0}^{\infty} a_k \alpha^{e_k}$ is transcendental for every algebraic α with $0 < |\alpha| < R$.

For the algebraic independence of such series, Bundschuh and Wylegala [1] proved :

THEOREM ([1]). Suppose that $f(z) = \sum_{k=0}^{\infty} a_k z^{e_k}$ satisfies the assumption (1). If $\alpha_1, \dots, \alpha_n$ are non-zero algebraic numbers of distinct absolute values less than R , then $f(\alpha_1), \dots, f(\alpha_n)$ are algebraically independent.

This theorem is proved using the fact that if $|\alpha_i| < |\alpha_j|$ then $f(\alpha_i)$ converges more rapidly than $f(\alpha_j)$. By this method, however, we cannot treat the equal absolute value case. In this direction, Masser conjectured the following :

CONJECTURE. Let $f(z) = \sum_{k=0}^{\infty} z^{k!}$, $\alpha_1, \dots, \alpha_n$ be algebraic numbers with $0 < |\alpha_i| < 1$ and no α_i/α_j ($i \neq j$) being a root of unity. Then $f(\alpha_1), \dots, f(\alpha_n)$ are algebraically independent.

In [7], the author proved the p -adic analogue of this conjecture by using Skolem's method. In the complex number field, the conjecture for the case of $n = 3$ was proved in [8], by Baker's theorem on linear forms in logarithms. Finally in [9], the author proved Masser's conjecture by using Evertse's theorem [5].

More precise surveys are found in Bundschuh [1] or Waldschmidt [12]. Here we shall give necessary and sufficient conditions for algebraic independence of the values of function $f(z) = \sum_{k=0}^{\infty} a_k z^{e_k}$ which satisfies the assumption (1) in both cases of archimedean norm and non-archimedean norm. Let p be ∞ or a prime number. By C_p we denote the complex number field or the completion of

the algebraic closure of the p -adic number field \mathbb{Q}_p according to whether p is ∞ or a prime number. We denote the absolute value of C_p by $| \cdot |_p$. For a power series $f(z)$ with algebraic coefficients and an algebraic number α , $f(\alpha)_p$ denotes the value of $f(z)$ at α in C_p if it converges. For an algebraic number α , we denote by $|\bar{\alpha}|$ the maximum of the absolute values of the conjugates of α and by $\text{den } \alpha$ the smallest positive rational integer d such that $d\alpha$ is an algebraic integer. Let $K \subset C_p$ be an algebraic number field. Let

$f(z) = \sum_{k=0}^{\infty} a_k z^{e_k}$ be a power series with coefficients in K , satisfying the equality

(1) and the convergence radius $R_p > 0$ in C_p .

THEOREM. Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers with $0 < |\alpha_i|_p < R_p$ ($1 \leq i \leq n$).

Then the following three properties are equivalent.

- i) $f(\alpha_1)_p, \dots, f(\alpha_n)_p$ are algebraically dependent over the rationals.
- ii) There exist non-empty subset $\{\alpha_{i_1}, \dots, \alpha_{i_s}\} \subset \{\alpha_1, \dots, \alpha_n\}$, an algebraic number γ , roots of unity ζ_1, \dots, ζ_s and algebraic numbers d_1, \dots, d_s which are not all zero and satisfy

$$\alpha_{i_q} = \zeta_q \gamma, \quad q = 1, \dots, s,$$

$$\sum_{q=1}^s d_q \zeta_q^{e_k} = 0$$

for any sufficiently large k .

- iii) $1, f(\alpha_1)_p, \dots, f(\alpha_n)_p$ are linearly dependent over the algebraic numbers.

In the archimedean case, we can replace the property i) by the following one :

i') $f^{(\ell)}(\alpha_i)_{\infty}$ ($1 \leq i \leq n, 0 \leq \ell$) are algebraically dependent over the rationals where $f^{(\ell)}(z)$ denotes the ℓ -th derivative of $f(z)$.

This is proved in Nishioka [10]. The theorem is proved by the following lemma. We denote the set of all primes on K by S_K and the set of all infinite primes on K by S_{∞} . For every prime v on K lying above a prime p on \mathbb{Q} , we choose a valuation $\|\cdot\|_v$ such that

$$\|\alpha\|_v = |\alpha|_p^{[K_v:\mathbb{Q}_p]} \text{ for all } \alpha \in \mathbb{Q}.$$

Then we have the product formula :

$$\prod_{v \in S_K} \|\alpha\|_v = 1 \text{ for all } \alpha \in K, \alpha \neq 0.$$

For $X = (x_0 : x_1 : \dots : x_n) \in P^n(K)$, put

$$H_K(X) = H(X) = \prod_{v \in S_K} \max(\|x_0\|_v, \|x_1\|_v, \dots, \|x_n\|_v).$$

By the product formula, this height is well-defined. Put

$$h_k(\alpha) = h(\alpha) = H(1 : \alpha) \text{ for } \alpha \in K.$$

LEMMA. Let Ω be an infinite subset of the positive integers \mathbb{N} and $\gamma_1, \dots, \gamma_n$ be non-zero elements of K with no γ_i/γ_1 ($\#1$) being a root of unity. Suppose that $A_1(m), \dots, A_n(m)$ are elements of K for each $m \in \Omega$ satisfying

- (i) $A_1(m) \neq 0$ for any $m \in \Omega$,
- (ii) $\lim_{\substack{m \rightarrow \infty \\ m \in \Omega}} \log h(A_i(m))/m = 0$, for $i = 1, \dots, n$.

Then for any fixed θ with $0 < \theta < 1$, we have

$$|A_1(m)\gamma_1^m + \dots + A_n(m)\gamma_n^m|_p > |\gamma_1|^m p^m$$

if $m \in \Omega$ is sufficiently large.

The lemma is proved by using Evertse's theorem on sums of S -units, which reposes on the results of simultaneous approximation of algebraic numbers of Schmidt and Schlickewei. The lemma for the archimedean case is prove in Nishioka [11], where the author studied the algebraic independence of the values of Mahler function $\sum_{k=1}^{\infty} [k\omega]z^k$ for a real irrational number ω with unbounded partial quotients in its continued fraction.

In this paper, we shall give the proof of Lemma and Theorem; the latter one is simpler than that in [10].

Proof of Lemma : There exist a prime $v_0 \in S_k$ and a positive constant c such that $|\cdot|_p^c = \|\cdot\|_{v_0}$ on K . Let S be a finite subset of S_K which includes S_∞ , v_0 and all divisors of γ_i ($1 \leq i \leq n$). For each $m \in \Omega$, there exists a positive integer D_m not greater than $h(A_1(m)) \dots h(A_n(m))$ such that $D_m A_1(m), \dots, D_m A_n(m)$ are algebraic integers. Therefore we may assume that $A_i(m)$ ($1 \leq i \leq n$) are algebraic integers without loss of generality. Then $A_i(m)\gamma_i^m$ ($1 \leq i \leq n$) are S -integers.

We prove Lemma by induction on m . If $m = 1$, then the lemma follows by the assumptions (i), (ii) and the fundamental inequality. We suppose $m \geq 2$ and

$$(2) \quad A_1(m)\gamma_1^m + \dots + A_n(m)\gamma_n^m = 0$$

for any element m of an infinite subset Ω_1 of Ω . By induction hypothesis, any proper subsum of the left hand side of the equality (2) is not zero, if $m \in \Omega_1$ is sufficiently large. In particular, $A_i(m) \neq 0$ ($1 \leq i \leq n$) for sufficiently large $m \in \Omega_1$. We put

$$H_m = H(A_1(m)\gamma_1^m + \dots + A_n(m)\gamma_n^m).$$

Since

$$(3) \quad \begin{aligned} H_m &\geq \left(\prod_{i=1}^n h(A_i(m)) \right)^{-1} H(\gamma_1 \cdots \gamma_n)^m \\ &\geq \left(\prod_{i=1}^n h(A_i(m)) \right)^{-1} H(\gamma_2 / \gamma_1)^m \end{aligned}$$

and $h(\gamma_2 / \gamma_1) > 1$, we have

$$\lim_{\substack{m \rightarrow \infty \\ m \in \Omega_1}} H_m = \infty.$$

Therefore by Theorem 1 in Evertse [5], $(A_1(m)\gamma_1^m \cdots A_n(m)\gamma_n^m)$ is not $(1, 1/2, S)$ -admissible and

$$(4) \quad \prod_{v \in S} \prod_{i=1}^n \|A_i(m)\gamma_i^m\|_v > H_m^{\frac{1}{2}}$$

for any sufficiently large $m \in \Omega_1$. On the other hand, by the product formula, the left hand side of the inequality (4) is not greater than $\prod_{i=1}^n h(A_i(m))$. This contradicts the assumption (ii). Hence we have

$$(5) \quad A_1(m)\gamma_1^m + \cdots + A_n(m)\gamma_n^m \neq 0$$

if $m \in \Omega$ is sufficiently large.

Assume

$$(6) \quad |A_1(m)\gamma_1^m + \cdots + A_n(m)\gamma_n^m|_p < |\gamma_1|^m \theta^m$$

for any element m of an infinite subset Ω_2 of Ω . We define δ_m as

$$(7) \quad A_1(m)\gamma_1^m + \cdots + A_n(m)\gamma_n^m + \delta_m = 0.$$

By induction hypothesis, the inequalities (5) and (6), any proper subsum of the left hand side of the equality (7) is not zero if $m \in \Omega_2$ is sufficiently large. Let ϵ be any positive number less than 1. Since

$$H(A_1(m)\gamma_1^m : \dots : A_n(m)\gamma_n^m : \delta_m) \geq H_m,$$

by Theorem 1 in Evertse [5], $(A_1(m)\gamma_1^m : \dots : A_n(m)\gamma_n^m : \delta_m)$ is not $(1, 1-\epsilon, S)$ -admissible and

$$(8) \quad \left(\prod_{v \in S} \prod_{i=1}^n \|A_i(m)\gamma_i^m\|_v \right) \left(\prod_{v \in S} \|\delta_m\|_v \right) > H_m^{1-\epsilon},$$

for any sufficiently large $m \in \Omega_2$. By the assumption and the inequality (6), for any $m \in \Omega_2$, the left hand side of the inequality (8) is less than

$$n^{[K:\mathbb{Q}]} \left(\prod_{i=1}^n h(A_i(m))^2 H(\gamma_1 : \dots : \gamma_n)^m \left(\max_{1 \leq i \leq n} |\gamma_i|_p \right)^{-cm} |\gamma_1|_p^{cm} \theta^{cm} \right).$$

Therefore by the inequalities (3) and (8), we have

$$n^{[K:\mathbb{Q}]} \left(\prod_{i=1}^n h(A_i(m)) \right)^3 \theta^{cm} > H(\gamma_1 : \dots : \gamma_n)^{-\epsilon m}$$

for any sufficiently large $m \in \Omega_2$. As m tends to infinity,

$$c \log \theta > -\epsilon \log H(\gamma_1 : \dots : \gamma_n).$$

Since ϵ is an arbitrary positive number < 1 , this implies $\log \theta \geq 0$. This contradicts the assumption $\theta < 1$ and completes the proof of Lemma.

Proof of Theorem : Obviously the property ii) implies the property iii) and the property iii) implies the property i). We prove that property i) implies the property ii). Suppose the property i) is satisfied. Changing the indices of the α 's, we may assume

$$|\alpha_1|_p = \dots = |\alpha_t|_p \geq |\alpha_{t+1}|_p \geq \dots \geq |\alpha_n|_p,$$

α_i/α_1 ($1 \leq i \leq t$) are roots of unity,

α_i/α_1 ($t+1 \leq i \leq n$) are not roots of unity.

Define U and $U_m \in \mathbb{C}^n$ by

$$U = (f(\alpha_i)_p)_{1 \leq i \leq n},$$

$$U_m = (\sum_{k=0}^{m-1} a_k \alpha_i^{e_k})_{1 \leq i \leq n}.$$

Then $\lim_{m \rightarrow \infty} U_m = U$ and there is a nonzero polynomial $F \in \bar{\mathbb{Q}}[y_1, \dots, y_n]$ such that $F(U) = 0$. We may assume F has the least total degree among such polynomials, algebraic integer coefficients and $\partial F / \partial y_1 \neq 0$. Then $\partial F / \partial y_1(U) \neq 0$. By Taylor expansion we have

$$-F(U_m) = F(U) - F(U_m) = \sum_{|J| \geq 1} J!^{-1} \partial^{|J|} F / \partial y^J (U - U_m)^J,$$

where $J = (j_1, \dots, j_n)$ with j_i being nonnegative integers and $|J|$, $J!$, $\partial^{|J|} / \partial y^J$ and $(U - U_m)^J$ are defined in the usual way. There is a positive number $\theta < 1$ such that $|a_m|_p |\alpha_1|_p^{e_m} = O(\theta^{e_m})$ (in what follows, the constants implicit in the symbol O depend only on $K, f(z), \alpha_1, \dots, \alpha_n$ and F). Then we have

$$\sum_{k=m}^{\infty} a_k \alpha_i^{e_k} = a_m \alpha_i^{e_m} + O(\theta^{e_{m+1}}).$$

By the fundamental inequality :

for any algebraic $\alpha \neq 0$, $\log |\alpha|_p \geq -[\mathbb{Q}(\alpha):\mathbb{Q}] \{ \log |\alpha| + \log(\text{den } \alpha) \}$,

we have $\log |a_m|_p \geq -[K:\mathbb{Q}] \{ \log M_m + \log A_m \}$. Therefore by (1),

$\theta^{e_{m+1}} = O(|a_m|_p |\alpha_1|_p^{e_m})$ and

$$(9) \quad -F(U_m) = \sum_{i=1}^n \partial F / \partial y_i(U_m) a_m^{e_m} \alpha_i^{e_m} + O(|a_m|_p |\alpha_1|_p^{e_m} \theta^{e_m}) = O(\theta^{e_m}).$$

Let g be the total degree of F and d be a positive integer with $\alpha_i d$ ($1 \leq i \leq n$) being algebraic integers. Then $|\overline{F(U_m)}| = O((A_{m-1} c_1^{e_{m-1}})^g)$ and $(M_{m-1} d^{e_{m-1}})^g F(U_m)$ is an algebraic integer. Hence by (1), (9) and the fundamental inequality, we have $F(U_m) = 0$ for sufficiently large m . By (2),

$$(10) \quad \sum_{i=1}^n \partial F / \partial y_i(U_m) \alpha_i^{e_m} = O(|\alpha_1|_p^{e_m} \theta^{e_m}).$$

For each i ($1 \leq i \leq t$), there exists a root of unity ζ_i such that $\alpha_i = \zeta_i \alpha_1$. Then we have

$$(11) \quad \left(\sum_{i=1}^t \partial F / \partial y_i(U_m) \zeta_i^{e_m} \right) \alpha_1^{e_m} + \sum_{i=t+1}^n \partial F / \partial y_i(U_m) \alpha_i^{e_m} = O(|\alpha_1|_p^{e_m} \theta^{e_m}).$$

Since $\lim_{m \rightarrow \infty} h(\partial F / \partial y_i(U_m)) / e_m = 0$, by Lemma

$$\sum_{i=1}^t \partial F / \partial y_i(U_m) \zeta_i^{e_m} = 0$$

for any sufficiently large m . Let N be a positive integer such that $\zeta_i^N = 1$ for all i , $1 \leq i \leq t$.

Suppose that there exist infinitely many e_m such that $e_m \equiv a \pmod{N}$ for an integer a ($0 \leq a < N$). As m tends to infinity, we have

$$\sum_{i=1}^t \partial F / \partial y_i(U) \zeta_i^a = 0.$$

Therefore

$$\sum_{i=1}^t \frac{\partial F}{\partial y_i}(U) \zeta_i^{e_m} = 0$$

if m is sufficiently large. Since $\frac{\partial F}{\partial y_1}(U) \neq 0$ and ζ_i are algebraic numbers, there exist algebraic numbers d_1, \dots, d_t , not all zero and satisfying

$$\sum_{i=1}^t d_i \zeta_i^{e_m} = 0$$

for any sufficiently large m . This completes the proof of the Theorem.

Manuscrit reçu le 28/08/88

BIBLIOGRAPHY

- [1] P. Bundschuh.— *A criterion for algebraic independence with some application*, to appear in Osaka J. Math. 25 (1988).
- [2] P. Bundschuh and F.T. Wylegala.— *Über algebraische Unabhängigkeit bei gewissen nichtfortsetzbaren Potenzreihen*, Arch. Math. 34 (1980), 32–36.
- [3] P.L. Cijssouw and R. Tijdeman.— *On the transcendence of certain power series of algebraic numbers*, Acta Arith. 23 (1973), 301–305.
- [4] H. Cohn.— *Note on almost algebraic numbers*, Bull. Amer. Math. Soc. 52 (1946), 1042–1045.
- [5] J.–H. Evertse.— *On sums of S-units and linear recurrences*, Comp. Math. 53 (1984), 225–244.
- [6] J. Liouville.— *Sur les classes très étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques*, Comptes Rendus Acad. Sci. Paris, 18 (1844) 883–885, 910–911; Journal Math. Pures et Appl. 16 (1851), 133–142.
- [7] K. Nishioka.— *Algebraic independence of certain power series of algebraic numbers*, J. Number Theory, 23 (1986), 354–364.
- [8] K. Nishioka.— *Algebraic independence of three Liouville series*, Arch. Math., 47 (1986), 117–120.
- [9] K. Nishioka.— *Proof of Masser's conjecture on the algebraic independence of values of Liouville series*, Proc. Japan Acad., Ser. A, 62 (1986), 219–222.
- [10] K. Nishioka.— *Conditions for algebraic independence of certain power series of algebraic numbers*, Comp. Math., 62 (1987), 53–61.

- [11] K. Nishioka.— *Evertse theorem in algebraic independence*, to appear in Arch. Math.
- [12] M. Waldschmidt.— *Indépendence algébrique de nombres de Liouville*, Actes des Journées à la Mémoire d'Alain Durand (Preprint).

K. Nishioka
Department of Mathematics
Nara Women's University
Kita-Uoya Nishimachi
Nara 630, JAPAN

Séminaire de Théorie des Nombres

Paris 1987-88

**REPRÉSENTATIONS p -ADIQUES, PÉRIODES ET
FONCTIONS L p -ADIQUES**
B. PERRIN-RIOU

Le point de départ de la rédaction de ce texte était l'espoir de mélanger un jour les fonctions L p -adiques associées à une représentation p -adique (presque) quelconque (fonctions dont l'existence est d'ailleurs tout à fait conjecturale) avec les anneaux B_{cris} , B_{st} et B_{dR} de Fontaine et de donner un complément à [2] en introduisant les périodes p -adiques en même temps que les périodes de Deligne. Il en est résulté un texte en deux parties. La première partie peut être vue comme une introduction au séminaire de Bures 1988 ([17], [4] à [10]). On a donc commencé par rappeler diverses définitions sur les représentations p -adiques d'un corps p -adique et les φ -modules filtrés et à expliquer la situation dans le cas des représentations ordinaires (d'après J.-M. Fontaine). C'est en effet dans le cadre des représentations ordinaires que Greenberg a généralisé la théorie d'Iwasawa.

La deuxième partie complète [2] dans la mesure où, après avoir repris la définition des périodes complexes de Deligne [3] (qui sont les facteurs de rationalité présumés des valeurs spéciales de fonctions L complexes), on la transcrit au cas p -adique en utilisant les isomorphismes de comparaison p -adique entre cohomologie de de Rham et de Betti (Fontaine-Messing). On expliquera ensuite dans le cas d'une représentation ordinaire l'hypothèse qu'il est nécessaire de faire sur le facteur local en p de la fonction L du motif.

On parlera ensuite plus précisément de fonctions L p -adiques. Suit un calcul facile de variation des périodes p -adiques par isogénie, ce qui permet de rêver à un lien avec les fonctions L p -adiques définies par Greenberg.

Je ne prétends dans ce texte à aucune originalité. Je remercie Jean-Marc Fontaine dont l'influence est tout à fait claire ainsi que John Coates.

Plan :

- 1.— Définitions et exercices sur les représentations p -adiques et les φ -modules filtrés.
 - 1.1.— φ -modules filtrés et (φ, N) -modules filtrés (définitions, admissibilité, nombres de Hodge et de Newton, φ -modules filtrés ordinaires).
 - 1.2.— Représentations p -adiques (de Hodge-Tate, de Rham, cristallines, semi-stables, (φ, N) -modules filtrés associés).
 - 1.3.— Représentations p -adiques ordinaires.
 - 1.4.— Construction d'un réseau adapté associé à un réseau d'une représentation p -adique dans le cas cristallin.
- 2.— Motifs.
 - 2.1.— Présentation (données, hypothèse de compatibilité en p , nombres de Hodge, de Hodge-Tate, de Newton, cas ordinaire).
 - 2.2.— Périodes complexes et p -adiques.
 - 2.3.— Fonctions L complexes et p -adiques.
 - 2.4.— Structure sur \mathbb{Z} . Variation de la période p -adique.

1.— Définitions et exercices sur les représentations p -adiques et les φ -modules filtrés.1.1.— φ -modules filtrés et (φ, N) -modules filtrés.

Nous allons donner dans ce paragraphe quelques définitions relatives aux φ -modules filtrés sur un corps p -adique non ramifié sur \mathbb{Q}_p . Elles ne sont pas les plus générales possibles. Leur but est seulement de donner un guide. Les références sont [4], [7], [8], [17].

Soient K une extension finie de \mathbb{Q}_p non ramifiée sur \mathbb{Q}_p , k son corps résiduel, $W(k)$ l'anneau des vecteurs de Witt de k . Soit σ le Frobenius absolu sur k et sur $W(k)$. Soit \bar{k} une clôture algébrique de k et \hat{K}^{nr} le corps des fractions de $W(\bar{k})$.

Un φ -iso-cristal sur K est un K -espace vectoriel de dimension finie muni d'un automorphisme σ -linéaire φ .

Un φ -module filtré sur K est un φ -iso-cristal D muni d'une filtration décroissante exhaustive et séparée $(D^i)_{i \in \mathbb{Z}}$ par des sous-espaces vectoriels.

Soit D un φ -module filtré sur K . Un réseau M de D est dit adapté à D si

- (1) $M^i = M \cap D^i$ est facteur direct dans M ,
- (2) $\Sigma_{i \in \mathbb{Z}} p^{-i} \varphi M^i = M$.

Un φ -module filtré est dit **faiblement admissible** s'il admet un réseau adapté.

Donnons maintenant différentes définitions de nombres de Hodge et de Newton que l'on peut trouver dans la littérature ([4], [11], [12]).

Si D est un φ -module filtré sur K , les **nombres de Hodge** de D sont définis par

$$h_H(D, i) = \dim_K D^i / D^{i+1} \text{ pour } i \in \mathbb{Z}.$$

Soit M un $W(k)$ -module tel que $M \otimes_{W(k)} K$ soit un φ -iso-cristal sur K . Soient p^{r_1}, \dots, p^{r_d} les invariants du réseau φM relativement à M avec $r_1 \leq \dots \leq r_d$. Les **nombres de Hodge** de M relativement à φ sont

$$h_H(M, i) = \#\{j \text{ t.q. } r_j = i\}.$$

LEMME 1.1. — *Soit D un φ -module filtré faiblement admissible et M un réseau adapté à D . Alors, on a*

$$h_H(D, i) = h_H(M, i).$$

Démonstration : Les conditions (1) et (2) sont équivalentes à

- (1)' $M^i = M \cap D^i$ est facteur direct dans M et $\varphi M^i \subset p^i M$
- (2)' si $M(i) = p^i M \cap \varphi M$, alors

$$\varphi M^i / p \varphi M^i \rightarrow M(i) / p M(i-1)$$

est un isomorphisme.

On remarque alors que

- (a) $\Sigma_{j \geq i} h_H(M, j) = \dim_k (M(j) / p M(j-1))$
- (b) $\Sigma_{j \geq i} h_H(D, j) = \dim_K D^j = \dim_k (M^j / p M^j)$.

On en déduit que

$$\Sigma_{j \geq i} h_H^{(M,i)} = \Sigma_{j \geq i} h_H^{(D,i)}$$

en utilisant (2)' et l'égalité

$$\dim_k (M^i/pM^i) = \dim_k (\varphi M^i/p\varphi M^i).$$

D'où le lemme.

Soit D un φ -iso-cristal. Alors $\bar{D} = D \otimes_K \hat{K}^{nr}$ est somme directe de ses composantes isotypiques $(D_r)_{r \in \mathbb{Q}}$ où si $r = m/n$ avec m et n premiers entre eux, D_r est le sous- \hat{K}^{nr} -espace vectoriel de \bar{D} engendré par les x tels que $\varphi^n x = p^m x$. On définit alors les **nombres de Newton** de D par

$$h_N(D,r) = \dim_{\hat{K}^{nr}} D_r.$$

On peut aussi les définir de la manière suivante. Soit p^a le cardinal de k . Soit

$$L(D,X) = \det(1 - \varphi^a X \mid D)$$

(φ^a est maintenant $W(k)$ -linéaire). Alors les nombres de Newton de D sont presque les nombres de Newton du polynôme $L(D,X)$ c'est-à-dire que si

$$L(D,X) = \prod (1 - \alpha X),$$

on a

$$h_N(D,r) = \#\{\alpha \text{ t.q. } \text{ord}_p(\alpha) = r/a\}$$

où ord_p est la valuation p -adique sur \mathbb{Q}_p normalisée par $\text{ord}_p(p) = 1$.

Passons maintenant aux φ -modules filtrés ordinaires.

Soit D un φ -iso-cristal et M un réseau de D . Alors M est dit **ordinaire** si les nombres de Hodge de M et les nombres de Newton de D sont égaux. Un φ -module filtré faiblement admissible D est ordinaire si ses nombres de Hodge et de Newton sont égaux. Il est donc ordinaire s'il admet un réseau adapté qui l'est (et ils le sont alors tous).

LEMME 1.2. ([11]).— Soit M un réseau d'un φ -iso-cristal. Soit $M_{[i]}$ le plus grand $W(k)$ -sous-module de M vérifiant

- (i) $\varphi M_{[i]} \subset p^i M_{[i]}$
- (ii) $p^{-i}\varphi$ est un automorphisme de $W(k)$ -modules de $M_{[i]}$.

Alors, M est ordinaire si et seulement si $M = \oplus M_{[i]}$.

Passons à une notion un peu plus générale, qui est celle de (φ, N) -module filtré.

Un (φ, N) -module filtré est un φ -module filtré muni de plus d'un endomorphisme N vérifiant $N\varphi = p\varphi N$. Cette dernière condition implique que N est nilpotent car son extension à $D \otimes_K \hat{K}^{nr}$ envoie D_α dans $D_{\alpha-1}$. Il y a de nouveau une définition de faible admissibilité qui ne peut ici se traduire en termes de réseau. Nous ne la donnons pas ([8]).

1.2.— Représentations p -adiques.

Soit W une représentation p -adique de $\text{Gal}(\bar{K}/K)$. Soit χ le caractère cyclotomique à valeurs dans \mathbb{Z}_p^\times . On pose

$$(W \otimes_{\mathbb{Q}_p} \mathbb{C}_p \{i\}) = \{X \in W \otimes_{\mathbb{Q}_p} \mathbb{C}_p \text{ t.q. } gx = \chi^i(g)x \text{ pour tout } g \in \text{Gal}(\bar{K}/K)\}.$$

D'après un théorème de Tate [16], on a une injection

$$\oplus (W \otimes_{\mathbb{Q}_p} \mathbb{C}_p \{i\}) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \subset W \otimes_{\mathbb{Q}_p} \mathbb{C}_p.$$

La représentation W est dite de Hodge–Tate si

$$\oplus (W \otimes_{\mathbb{Q}_p} \mathbb{C}_p \{i\}) \otimes_{\mathbb{Q}_p} \mathbb{C}_p = W \otimes_{\mathbb{Q}_p} \mathbb{C}_p.$$

Les nombres de Hodge–Tate de W sont

$$h_{HT}(W, i) = \dim_{\mathbb{Q}_p} W \otimes_{\mathbb{Q}_p} \mathbb{C}_p \{i\}.$$

Donc W est de Hodge–Tate si et seulement si

$$\sum_i h_{HT}(W,i) = \dim_{\mathbb{Q}_p} W.$$

Les poids de Hodge–Tate de W sont les nombres i tels que $h_{HT}(W,i)$ est non nul.

Une autre manière d'écrire cette définition est d'introduire la \mathbb{C}_p –algèbre graduée

$$B_{HT} = \bigoplus_{i \in \mathbb{Z}} \mathbb{Q}_p(i) \otimes_{\mathbb{Q}_p} \mathbb{C}_p.$$

Comme d'habitude, $\mathbb{Q}_p(1) = \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, $\mathbb{Z}_p(1)$ est le module de Tate des racines de l'unité d'ordre une puissance de p , $\mathbb{Q}_p(i) = \mathbb{Q}_p(1)^{\otimes i}$ pour $i > 0$, $\mathbb{Q}_p(i) = \text{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p(-i), \mathbb{Q}_p)$ pour $i < 0$.

On associe à W le K –espace vectoriel gradué

$$D_{HT}^*(W) = \text{Hom}_{\mathbb{Q}_p}(W, B_{HT})^{\text{Gal}(\bar{K}/K)}$$

Alors W est de Hodge–Tate si et seulement si

$$\dim_K D_{HT}^*(W) = \dim_{\mathbb{Q}_p} W.$$

Le signe $*$ qui intervient dans la notation D_{HT}^* ainsi que dans les notations D_{dR}^* , D_{cris}^* qui suivent est là pour rappeler que les foncteurs ainsi définis sont contravariants.

Soit B_{dR} le corps construit par Fontaine. Rappelons quelques unes de ses propriétés. C'est un corps complet pour une valuation discrète et vérifiant les propriétés suivantes. Son corps résiduel s'identifie à \mathbb{C}_p ; il contient canoniquement $\mathbb{Q}_p(1)$; tout générateur t du module de Tate $\mathbb{Z}_p(1)$ est une

uniformisante de B_{dR} : il est donc muni d'une filtration par les $\text{Fil}^i B_{dR} = t^i B_{dR}^+$ où B_{dR}^+ est l'anneau des entiers de B_{dR} pour sa valuation; il est muni d'une action de $\text{Gal}(\bar{K}/K)$. Soit $O_{\mathbb{C}_p}$ l'anneau des entiers de \mathbb{C}_p et notons ici O_K l'anneau des entiers de K . On considère les couples (E, θ) formés d'une O_K -algèbre E séparée complète pour la topologie p -adique et d'un homomorphisme surjectif θ de O_K -algèbres

$$\theta : E \rightarrow O_{\mathbb{C}_p}$$

vérifiant $(\text{Ker } \theta)^{m+1} = 0$. On montre qu'il existe un tel objet (D_m, θ_m) universel c'est-à-dire que pour tout (E, θ) comme ci-dessus, il existe un morphisme

$$\lambda : D_m \rightarrow E$$

rendant commutatif le diagramme

$$\begin{array}{ccc} D_m & \longrightarrow & O_{\mathbb{C}_p} \\ \lambda \downarrow & & \downarrow = \\ E & \longrightarrow & O_{\mathbb{C}_p} \end{array}$$

L'anneau B_{dR}^+ est alors par définition la limite projective des $D_m \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Les morphismes θ_m induisent un morphisme

$$\theta : B_{dR}^+ \rightarrow \mathbb{C}_p$$

dont on montre que le noyau est principal. Le corps B_{dR} est alors obtenu en inversant un générateur du noyau de θ . Indiquons comment on associe à un système compatible $(\zeta_n)_n$ de racines de l'unité ζ_n d'ordre p^n (c'est-à-dire vérifiant $\zeta_n^p = \zeta_{n-1}$) un élément t engendrant le noyau de θ et tel que

$$\sigma t = \chi(\sigma)t$$

si $\sigma \in \text{Gal}(\bar{K}/K)$ et si χ est le caractère cyclotomique. Soit $\hat{\zeta}_{n,m}$ un relèvement de ζ_n dans D_m . Alors $(\hat{\zeta}_{n,m})^{p^n} - 1$ appartient au noyau de θ_m . Comme ce noyau est nilpotent $((\text{Ker } \theta_m)^{m+1} = 0)$,

$$\log((\zeta_{n,m})^{p^n}) = \sum_k (-1)^k ((\hat{\zeta}_{n,m})^{p^n} - 1)^{k/k}$$

a un sens dans $D_m \otimes \mathbb{Q}_p$. On montre facilement que la suite (indexée par n) $\log((\hat{\zeta}_{n,m})^{p^n})$ a une limite lorsque $n \rightarrow \infty$ indépendante du choix des représentants et que les limites définissent un élément t de B_{dR} qui vérifie $\sigma t = \chi(\sigma)t$.

On pose

$$D_{dR}^*(W) = \text{Hom}_{\mathbb{Q}_p}(W, B_{dR})^{\text{Gal}(\bar{K}/K)}.$$

Le K -espace vectoriel $D_{dR}^*(W)$ est muni d'une filtration induite par celle de B_{dR} :

$$D_{dR}^*(W)^i = \text{Hom}_{\mathbb{Q}_p}(W, t^i B_{dR}^+)^{\text{Gal}(\bar{K}/K)}.$$

Le K -espace vectoriel gradué associé à cette filtration est canoniquement contenu dans $D_{HT}^*(W)$:

$$\bigoplus_{i \in \mathbb{Z}} D_{dR}^*(W)^i / D_{dR}^*(W)^{i+1} \subset D_{HT}^*(W).$$

La représentation p -adique W est dite **de de Rham** si et seulement si

$$\dim_K D_{dR}^*(W) = \dim_{\mathbb{Q}_p} W.$$

Posons

$$h_{dR}(W, i) = h_H(D_{dR}^*(W), i) = \dim_K D_{dR}^*(W)^i / D_{dR}^*(W)^{i+1}$$

Alors, W est une représentation de de Rham si et seulement si W est de Hodge-Tate et si

$$h_{dR}(W, i) = h_{HT}(W, i).$$

Soit B_{cris} le sous-anneau de B_{dR} défini par J.-M. Fontaine ; il est stable par l'action de $\text{Gal}(\bar{K}/K)$, contient t et t^{-1} et est muni d'un endomorphisme σ -linéaire φ . On peut encore le construire de la manière suivante. Soit W_n l'anneau des vecteurs de Witt de longueur n (on a en particulier $W_n = W(k)/p^n W(k)$). L'idéal pW_n est muni de puissances divisées. On considère les couples (F, ψ) formés d'une W_n -algèbre E et d'un homomorphisme surjectif ψ de O_K -algèbres

$$\psi : E \rightarrow O_{\mathbb{C}_p} / p^n O_{\mathbb{C}_p}$$

dont le noyau est muni de puissances divisées compatibles à celles de p (on rappelle rapidement qu'un idéal I à puissances divisées est muni d'une famille d'applications $\gamma_n : I \rightarrow I$ pour $n \geq 1$ vérifiant les propriétés formelles de $x^n/n!$). On montre que la limite projective de ces objets existe ; on la note (A_n, ψ_n) , on a donc une suite exacte

$$0 \rightarrow I_n \rightarrow A_n \rightarrow O_{\mathbb{C}_p} / p^n O_{\mathbb{C}_p} \rightarrow 0$$

et l'idéal I_n est muni de puissances de divisées. On note alors $A_{cris} = H_{cris}^0(O_{\bar{K}}/pO_{\bar{K}})$ la limite projective des A_n . Il est contenu dans B_{dR} . Il est facile de voir en reprenant la construction de t que t appartient à A_{cris} (il suffit de remarquer que le logarithme converge sur l'idéal à puissances

divisées I_n) . L'anneau B_{cris}^+ est alors obtenu en inversant $p : B_{cris}^+ = A_{cris}[p^{-1}]$ et B_{cris} en inversant $t : B_{cris} = B_{cris}^+[t^{-1}] = A_{cris}[t^{-1}]$. On a un endomorphisme σ -linéaire φ sur B_{cris} et t vérifie $\varphi t = pt$.

Pour toute représentation p -adique W , on pose

$$D_{cris}^*(W) = \text{Hom}_{\mathbb{Q}_p}(W, B_{cris})^{\text{Gal}(\bar{K}/K)}.$$

C'est un sous- K -espace vectoriel de $D_{dR}^*(W)$, muni de la structure de φ -module filtré induite par celle de B_{cris} .

La représentation W est dite cristalline si et seulement si

$$\dim_K D_{cris}^*(W) = \dim_{\mathbb{Q}_p} W.$$

Le φ -module filtré $D_{cris}^*(W)$ est alors dit admissible. On pose

$$h_{cris}(W, i) = h_H(D_{cris}^*(W), i).$$

La représentation W est cristalline si et seulement si elle est de Hodge-Tate et si

$$h_{cris}(W, i) = h_{HT}(W, i).$$

De plus, si W est cristalline, $D_{cris}^*(W)$ est un φ -module filtré faiblement admissible.

Soit enfin l'anneau B_{st} . Il est contenu dans B_{dR} , est stable par $\text{Gal}(\bar{K}/K)$, est isomorphe à une algèbre de polynômes à une variable sur B_{cris} , est muni d'un endomorphisme σ -linéaire φ prolongeant celui de B_{cris} et d'une B_{cris} -dérivation N dépendant du choix de u tel que $B_{st} = B_{cris}[u]$ (et du choix d'un logarithme sur K prolongeant le logarithme usuel) : on peut par exemple poser $\varphi u = pu$, $Nu = 1$.

Pour toute représentation p -adique W , on pose

$$D_{st}^*(W) = \text{Hom}_{\mathbb{Q}_p}(W, B_{st})^{\text{Gal}(\bar{K}/K)}.$$

C'est un sous- K -espace vectoriel de $D_{dR}^*(W)$, muni de la structure de (φ, N) -module filtré induite par celle de B_{st} .

La représentation W est dite semi-stable si et seulement si

$$\dim_K D_{st}^*(W) = \dim_{\mathbb{Q}_p} W.$$

Le (φ, N) -module filtré $D_{st}^*(W)$ est alors dit semi-stable.

Si D est un (φ, N) -module filtré, on pose

$$V_{st}^*(D) = \{u \in \text{Hom}_{W(k)}(D, B_{st}) \text{ t.q. } uN = Nu, u\varphi = \varphi u, u(D^i) \subset \text{Fil}^i B_{st}\}.$$

1.3.— Représentations p -adiques ordinaires.

Une représentation p -adique W de $\text{Gal}(\bar{K}/K)$ est dite **ordinaire** s'il existe une filtration $(\text{Fil}^i W)_{i \in \mathbb{Z}}$ de W décroissante exhaustive et séparée par des sous-espaces $\text{Fil}^i W$ stables par $\text{Gal}(\bar{K}/K)$ et telle que le groupe d'inertie I_p agit sur $\text{Fil}^i W / \text{Fil}^{i+1} W$ par la puissance du caractère cyclotomique χ^i .

PROPOSITION 1.3.— Une représentation ordinaire W est semi-stable et on a

$$h_{HT}(W, i) = \dim_{\mathbb{Q}_p} \text{Fil}^i W / \text{Fil}^{i+1} W.$$

Plus précisément, V_{st}^ et D_{st}^* fournissent une anti-équivalence de catégories entre la catégorie des représentations p -adiques ordinaires et la catégorie des (φ, N) -modules filtrés ordinaires.*

Nous ne donnons pas ici la démonstration. Remarquons cependant que la filtration de $W = V_{st}^*(D)$ est donnée par

$$Fil^i W = V_{st}^*(D/\oplus_{j < i} D[j]) ,$$

(on déduit du fait que D est ordinaire que $\oplus_{j < i} D[j]$ est un sous-objet de D dans la catégorie des (φ, N) -modules filtrés ordinaires, ce qui signifie que $D/\oplus_{j < i} D[j]$ a une structure naturelle de (φ, N) -module filtré).

Par contre, nous allons montrer le fait plus faible qu'une représentation p -adique ordinaire est de de Rham. Les méthodes utilisées (dues à Fontaine) sont différentes et utilisent le théorème de Tate sur la cohomologie de \mathbb{C}_p .

LEMME 1.4.— Soient W_1 et W_2 deux représentations de Hodge-Tate dont les poids sont distincts. Alors, si

$$0 \rightarrow W_1 \rightarrow W \rightarrow W_2 \rightarrow 0$$

est une suite exacte de représentations p -adiques, W est une représentation de Hodge-Tate.

Démonstration : Pour toute représentation p -adique W , on a

$$\Sigma_i h_{HT}(W, i) \leq \dim_{\mathbb{Q}_p} W$$

et W est de Hodge-Tate si et seulement s'il y a égalité. Il suffit donc de montrer que

$$h_{HT}(W, i) = h_{HT}(W_1, i) + h_{HT}(W_2, i) .$$

On se ramène d'abord au cas où $i = 0$ en tordant les trois représentations p -adiques par une puissance du caractère cyclotomique. Il s'agit donc de montrer que l'on a la suite exacte

$$0 \rightarrow (W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} \rightarrow (W \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} \rightarrow (W_2 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} \rightarrow 0 .$$

Si 0 n'est pas un poids de W_2 , on a par définition

$$(W_2 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} = 0.$$

Si 0 est un poids de W_2 , par hypothèse, 0 n'est pas un poids de W_1 . On a alors

$$0 \rightarrow (W \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} \rightarrow (W_2 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\text{Gal}(\bar{K}/K)} \rightarrow H^1(\text{Gal}(\bar{K}/K), W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p).$$

Mais

$$W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p = {}^{\oplus, \#} (W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\{j\}} \otimes_{\mathbb{Q}_p} \mathbb{C}_p.$$

D'après un théorème de Tate [16], cela implique que

$$H^1(\text{Gal}(\bar{K}/K), W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p) = 0$$

et donc le lemme.

Par récurrence sur la dimension de W , on en déduit que toute représentation ordinaire est de Hodge–Tate et que l'on a

$$h_{HT}(W, i) = \dim_{\mathbb{Q}_p} F_i i^* W / F_i i^{*+1} W.$$

LEMME 1.5.— Soient W_1 et W_2 deux représentations p -adiques de de Rham. On suppose que les poids de W_2 sont strictement inférieurs à ceux de W_1 et que l'une des deux a un seul poids. Alors toute extension W

$$0 \rightarrow W_1 \rightarrow W \rightarrow W_2 \rightarrow 0$$

de représentations p -adiques est une représentation de de Rham.

Démonstration : Supposons d'abord que le seul nombre de Hodge-Tate de W_1 est $h_{HT}(W_1, m)$ c'est-à-dire

$$W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p = (W_1 \otimes_{\mathbb{Q}_p} \mathbb{C}_p)^{\{m\}} \otimes_{\mathbb{Q}_p} \mathbb{C}_p$$

et que les poids de W_2 sont tous positifs (et strictement inférieurs à m d'après les hypothèses du lemme à montrer). Si l'on pose $B_m = B_{dR}^+ / t^m B_{dR}^+$, on a la suite exacte galoisienne de modules filtrés

$$0 \rightarrow \mathbb{C}_p^{\{m\}} \rightarrow B_m \rightarrow B_{m-1} \rightarrow 0.$$

Montrons que l'on a

$$D_{dR}^*(W) = \text{Hom}_{\mathbb{Q}_p}(W, B_m)^{\text{Gal}(\bar{K}/K)}$$

lorsque les poids de W sont compris entre 0 et m . Il suffit de montrer que pour $n \geq m$, $\text{Hom}_{\mathbb{Q}_p}(W, B_n)^{\text{Gal}(\bar{K}/K)}$ est stationnaire car

$$D_{dR}^*(W) = \varprojlim_n \text{Hom}_{\mathbb{Q}_p}(W, B_n)^{\text{Gal}(\bar{K}/K)}$$

Pour $n > m$, on a la suite exacte de modules filtrés

$$\begin{aligned} 0 \rightarrow \text{Hom}_{\mathbb{Q}_p}(W, \mathbb{C}_p^{\{n\}})^{\text{Gal}(\bar{K}/K)} &\rightarrow \text{Hom}_{\mathbb{Q}_p}(W, B_n)^{\text{Gal}(\bar{K}/K)} \\ &\rightarrow \text{Hom}_{\mathbb{Q}_p}(W, B_{n-1})^{\text{Gal}(\bar{K}/K)} \rightarrow H^1(\text{Gal}(\bar{K}/K), \text{Hom}_{\mathbb{Q}_p}(W, \mathbb{C}_p^{\{n\}})) \end{aligned}$$

Comme $h_{HT}(W, n)$ est nul, on a

$$\text{Hom}_{\mathbb{Q}_p}(W, \mathbb{C}_p^{\{n\}})^{\text{Gal}(\bar{K}/K)} = 0$$

et d'après [16],

$$H^1(\text{Gal}(\bar{K}/K), \text{Hom}_{\mathbb{Q}_p}(W, \mathbb{C}_p\{n\})) = 0,$$

ce qui démontre l'assertion voulue.

Pour montrer que W est une représentation de de Rham, il suffit de nouveau de montrer l'égalité

$$\begin{aligned} \dim_K \text{Hom}_{\mathbb{Q}_p}(W, B_m)^{\text{Gal}(\bar{K}/K)} &= \\ \dim_K \text{Hom}_{\mathbb{Q}_p}(W_1, B_m)^{\text{Gal}(\bar{K}/K)} + \dim_K \text{Hom}_{\mathbb{Q}_p}(W_2, B_m)^{\text{Gal}(\bar{K}/K)}. \end{aligned}$$

On a le diagramme commutatif et exact suivant, en posant $G = \text{Gal}(\bar{K}/K)$

$$\begin{array}{ccccccc} 0 \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_2, B_{m-1})^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W, B_{m-1})^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_1, B_{m-1})^G \\ \uparrow & \uparrow & \uparrow \\ 0 \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_2, B_m)^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W, B_m)^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_1, B_m)^G \\ \uparrow & \uparrow & \uparrow \\ 0 \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_2, \mathbb{C}_p\{m\})^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W, \mathbb{C}_p\{m\})^G & \rightarrow \text{Hom}_{\mathbb{Q}_p}(W_1, \mathbb{C}_p\{m\})^G \\ \uparrow & \uparrow & \uparrow \\ 0 & 0 & 0 \end{array}$$

On remarque alors que

$$\text{Hom}_{\mathbb{Q}_p}(W_1, B_{m-1})^{\text{Gal}(\bar{K}/K)} = 0$$

car $h_{HT}(W_1, i) = 0$ pour $i \leq m-1$ et que

$$\text{Hom}_{\mathbb{Q}_p}(W_2, \mathbb{C}_p\{m\})^{\text{Gal}(\bar{K}/K)} = 0$$

car $h_{HT}(W_2, m) = 0$. On en déduit que

$$\mathrm{Hom}_{\mathbb{Q}_p}(W_2, B_m)^{\mathrm{Gal}(\bar{K}/K)} \text{ et } \mathrm{Hom}_{\mathbb{Q}_p}(W_1, \mathbb{C}_p\{m\})^{\mathrm{Gal}(\bar{K}/K)}$$

sont d'intersection nulle dans $\mathrm{Hom}_{\mathbb{Q}_p}(W, B_m)^{\mathrm{Gal}(\bar{K}/K)}$ et donc que

$$\begin{aligned} \dim_K \mathrm{Hom}_{\mathbb{Q}_p}(W, B_m)^{\mathrm{Gal}(\bar{K}/K)} &\geq \\ \dim_K \mathrm{Hom}_{\mathbb{Q}_p}(W_1, B_m)^{\mathrm{Gal}(\bar{K}/K)} + \dim_K \mathrm{Hom}_{\mathbb{Q}_p}(W_2, B_m)^{\mathrm{Gal}(\bar{K}/K)} & \\ &\geq \dim_{\mathbb{Q}_p} W. \end{aligned}$$

D'où le lemme dans ce cas.

On peut enlever l'hypothèse que les poids de W_2 sont positifs en tordant par une puissance convenable du caractère cyclotomique. Si W_2 a un seul poids, on se ramène au cas précédent en prenant la suite exacte duale.

On en déduit de nouveau par récurrence sur la dimension de W qu'une représentation ordinaire est une représentation de de Rham et l'on a encore

$$h_{dR}(W, i) = h_{HT}(W, i) = \dim_{\mathbb{Q}_p} \mathrm{Fil}^i W / \mathrm{Fil}^{i+1} W.$$

1.4.— Construction d'un réseau adapté associé à un réseau d'une représentation p -adique.

Soit W une représentation p -adique cristalline et soit L un réseau de W stable par $\mathrm{Gal}(\bar{K}/K)$. Nous allons lui associer de manière naturelle un réseau adapté du φ -module filtré $D_{\mathrm{cris}}^*(W)$ en utilisant la *structure entière* que possède B_{cris} . Rappelons que B_{cris}^+ contient une \mathbb{Z}_p -algèbre A_{cris} dans laquelle p n'est pas inversible. On a alors

$$B_{\mathrm{cris}}^+ = A_{\mathrm{cris}}[p^{-1}].$$

On pose si les poids de Hodge-Tate de W sont tous supérieurs à $-h$ (avec $h \geq 0$)

$$D_{\text{cris}}^*(L) = \text{Hom}_{\mathbb{Z}_p}(L, t^{-h} A_{\text{cris}})^{\text{Gal}(\bar{K}/K)}.$$

C'est un réseau de $D_{\text{cris}}^*(W)$ qui peut aussi s'interpréter comme l'ensemble des éléments f de $D_{\text{cris}}^*(W)$ tels que $f(x) \in t^{-h} A_{\text{cris}}$ pour tout $x \in L$. On pose aussi si M est un réseau adapté de $D_{\text{cris}}^*(W)$

$$\begin{aligned} V_{\text{cris}}^*(M) = \\ \{u \in \text{Hom}_{W(k)}(M, t^{-h} A_{\text{cris}}) \text{ t.q. } \varphi u = u\varphi, u(Fil^i M) \subset Fil^i(t^{-h} A_{\text{cris}})\}. \end{aligned}$$

LEMME 1.6. — Soit W une représentation cristalline dont les poids de Hodge-Tate appartiennent à un intervalle de longueur strictement inférieure à $p-1$. Alors $D_{\text{cris}}^*(L)$ est un réseau adapté au φ -module filtré admissible $D_{\text{cris}}^*(W)$.

Démonstration : On se ramène d'abord au cas où les poids sont positifs par torsion à la Tate de W par $\mathbb{Q}_p(h)$ et de L par $\mathbb{Z}_p(h)$. Posons $M = D_{\text{cris}}^*(L)$, $D = D_{\text{cris}}^*(W)$ et comme d'habitude $M^i = D^i \cap M$. Le fait que $\varphi M^i \subset p^i M$ (qui se déduit de ce que $\varphi(Fil^i A_{\text{cris}}) \subset p^i A_{\text{cris}}$) implique que M est un réseau adapté (c'est un fait général dans un φ -module filtré faiblement admissible). En effet, montrons d'abord que M^i est facteur direct dans M . Il s'agit de montrer que

$$p^n M \cap M^i = p^n M^i$$

pour tout entier $n \geq 0$. Soit $x = p^n y \in M^i$. Comme on a par définition $M^i = M \cap D^i$, y appartient à D^i donc $y \in M \cap D^i = M^i$ et $x \in p^n M^i$. L'homomorphisme

$$\varphi M^i / p\varphi M^i \rightarrow M(i)/pM(i-1)$$

est injectif : en effet si $x \in \varphi M^i \cap p\varphi M$ c'est-à-dire $x = \varphi y = p\varphi z$ avec $y \in M^i$ et $z \in M$ on a $y \in pM \cap M^i = pM^i$ (M^i facteur direct dans M) et $x \in p\varphi M^i$. On en déduit que cette injection est un isomorphisme pour tout i en comparant des dimensions :

$$\begin{aligned} \Sigma \dim_{\mathbb{Z}/p\mathbb{Z}} M(i)/pM(i-1) &= \text{longueur } M/\varphi M = t_N(D) \\ \Sigma \dim_{\mathbb{Z}/p\mathbb{Z}^\varphi} M^i/p\varphi M^i &= \Sigma \dim_{W(k)} M^i = \Sigma \dim_K D^i = \Sigma i \dim_K D^i/D^{i+1} = t_H(D). \end{aligned}$$

Comme D est admissible, on a

$$t_H(D) = t_N(D),$$

d'où les égalités

$$\dim_{\mathbb{Z}/p\mathbb{Z}} M(i)/pM(i-1) = \dim_{\mathbb{Z}/p\mathbb{Z}^\varphi} M^i/p\varphi M^i.$$

On en déduit le lemme.

2.- Motifs

On considérera toujours $\bar{\mathbb{Q}}$ comme contenu dans \mathbb{C} . On fixe un nombre premier p et un plongement de $\bar{\mathbb{Q}}$ dans \mathbb{C}_p .

2.1.- Présentation.

Un **motif** V pur de poids m et de dimension $d(V)$ sur \mathbb{Q} fournit un certain nombre de réalisations et des isomorphismes de compatibilité vérifiant certaines propriétés éventuellement conjecturales que l'on rappelle ici. On considère donc

(H.1) un \mathbb{Q} -espace vectoriel $H_B^B(V)$ de dimension $d(V)$ muni d'une involution ρ_B .

(H.1) _{∞} On fait agir le groupe de Galois $G_{\mathbb{R}} = \text{Gal}(\mathbb{C}/\mathbb{R})$ à travers ρ_B . On pose

$$H_B(V)_{\mathbb{C}} = \text{Hom}_{\mathbb{Q}}(H_B^B(V), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$$

et soit σ l'involution de $H_B(V)_{\mathbb{C}}$ induite par ρ_B sur $H_B(V)$ et l'identité sur \mathbb{C} . Alors le \mathbb{C} -espace vectoriel $H_B(V)_{\mathbb{C}}$ admet une décomposition en somme

directe de \mathbb{C} -espaces vectoriels $(H_B(V)^{i,j})_{i,j \in \mathbb{Z}, i+j=m}$ tels que $\sigma H_B(V)^{i,j} = H_B(V)^{j,i}$.

(H.2) Un \mathbb{Q} -espace vectoriel $H_{dR}(V)$ de dimension $d(V)$ muni d'une filtration décroissante exhaustive et séparée $F^i H_{dR}(V)$ par des \mathbb{Q} -espaces vectoriels.

(H.1 \longleftrightarrow H.2) _{∞} Une forme bilinéaire *canonique* non dégénérée de \mathbb{Q} -espaces vectoriels

$$\theta_\infty : H_{dR}(V) \times H^B(V) \rightarrow \mathbb{C}$$

compatible à l'action de $G_{\mathbb{R}}$ (qui agit de manière naturelle sur \mathbb{C} à travers la conjugaison complexe ρ) ; on en déduit un isomorphisme T_∞

$$H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{C} \rightarrow H_B(V)_{\mathbb{C}}$$

à travers lequel on demande que les filtrations $F^i H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{C}$ et

$$F^i H_B(V)_{\mathbb{C}} = \oplus_{i' \geq i} H_B(V)^{i', m-i'}$$

se correspondent.

(H.1 \longleftrightarrow H.2) _{p} : une forme bilinéaire *canonique* non dégénérée de \mathbb{Q}_p -espaces vectoriels

$$\theta_p : H_{dR}(V) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \times H^B(V) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \rightarrow B_{dR}$$

compatible à l'action de $G_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ et compatible aux filtrations $(H^B(V) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p)$ étant muni de la structure de la filtration triviale).

(H.3) Un système de représentations ℓ -adiques strictement compatibles, c'est-à-dire

pour tout nombre ℓ premier, un \mathbb{Q}_ℓ -espace vectoriel $H^\ell(V)$ de dimension $d(V)$ muni d'une action continue de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$;

il existe un ensemble fini S de nombres premiers tel que pour tout ℓ et pour toute place r dont la restriction à \mathbb{Q} n'appartient pas à $S \cup \{\ell\}$, $H^\ell(V)$ est non ramifiée en r (i.e. le groupe d'inertie I_r de r agit trivialement sur $H^\ell(V)$) ;

pour tout r , on note $(H^\ell(V))_{I_r}$ le plus grand quotient de $H^\ell(V)$

sur lequel I_r agit trivialement ; alors, si Frob_r est le Frobenius arithmétique en r , le polynôme

$$\det(1 - \text{Frob}_r X \mid (H^\ell(V))_{I_r})$$

est à coefficients dans \mathbb{Q} , ne dépend pas de ℓ différent de r (on le note $L_r(V, X)$) et le conducteur de $H^\ell(V)$ en r différent de ℓ ne dépend pas de ℓ .

(H.3)_{oo} Les racines réciproques de $L_r(V, X)$ sont de valeurs absolues complexes égales à $r^{m/2}$.

(H.3 \longleftrightarrow H.1) un isomorphisme de \mathbb{Q}_ℓ -espaces vectoriels

$$H^B(V) \otimes \mathbb{Q}_\ell \xrightarrow{\sim} H^\ell(V).$$

Remarquons que la forme bilinéaire θ_p induit un isomorphisme de modules filtrés T_p entre $D_p(V) = H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ et $D_{dR}^*(H^p(V))$.

Donnons maintenant un ensemble de conditions (H.4) _{p, nr} (resp. (H.4) _{p, st}) assurant que le motif V a bonne réduction en p (resp. réduction semi-stable en p).

(H.4)_{*p,nr*} Le système de représentations $(H^\ell(V))_\ell$ a bonne réduction en p , c'est-à-dire que le groupe d'inertie en p agit trivialement sur $H^\ell(V)$ pour $\ell \neq p$. Le module filtré $D_p(V) = H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ est muni d'une structure de φ -module filtré ; de plus Θ_p est à valeurs dans B_{cris} , est compatible aux structures de φ -modules filtrés et on a

$$L_p(V, X) = \det(1 - \varphi X| D_p(V)).$$

Rappelons qu'une représentation ℓ -adique de $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ (pour $\ell \neq p$) est dite semi-stable si l'action du sous-groupe d'inertie I_p est unipotente. Soit t_ℓ l'homomorphisme de I_p dans $\mathbb{Z}_\ell(1)$ défini par

$$t_\ell(\sigma) = ((\pi^{1/\ell^n})^{\sigma-1})_n \in \lim_{\leftarrow n} \mu_{\ell^n} = \mathbb{Z}_\ell(1)$$

où π est une uniformisante de \mathbb{Q}_p . Une représentation ℓ -adique (ρ, V_ℓ) de $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ est alors semi-stable s'il existe un élément N_ℓ de

$$\text{Hom}_{\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)}(V_\ell \otimes \mathbb{Z}_\ell(1), V_\ell)$$

tel que

$$\rho_\ell(g) = \exp(N_\ell t_\ell(g))$$

pour tout élément g de I_p . D'après un théorème de Grothendieck, une représentation ℓ -adique ρ de $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ est toujours potentiellement semi-stable (c'est-à-dire semi-stable si on se restreint à un sous-groupe ouvert de I_p).

(H.4)_{*p,st*} Le système de représentations $(H^\ell(V))_\ell$ a réduction semi-stable en p pour $\ell \neq p$. Le module filtré $D_p(V) = H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ est muni d'une structure de (φ, N) -module filtré ; de plus Θ_p est à valeurs dans B_{st} , est

compatible aux structures de (φ, N) -modules filtrés et on a

$$L_p(V, X) = \det(1 - \varphi X| D_p(V))^{N=0}.$$

De nouveau, la forme bilinéaire Θ_p induit alors un isomorphisme entre les φ -modules filtrés (resp. les (φ, N) -modules filtrés) $D_p(V) = H_{dR}(V) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p$ et $D_{\text{cris}}^*(H^p(V))$ (resp. $D_{\text{cris}}^*(H^p(V))$). En particulier, $D_p(V)$ est un (φ, N) -module filtré faiblement admissible.

Si le motif V est semi-stable en p , le motif V est dit **ordinaire** en p si les conditions équivalentes suivantes sont vérifiées :

(i) la représentation p -adique $H^p(V)$ est ordinaire

ou

(ii) le (φ, N) -module filtré $D_p(V)$ est ordinaire.

Ces hypothèses ont les conséquences suivantes sur les nombres de Hodge-Tate et les nombres de Hodge. Les nombres de Hodge sont définis à partir des réalisations complexes de V par

$$h_H(i) = h_H(i, m-i) = \dim_{\mathbb{C}} H_B^{i, m-i}.$$

Les divers isomorphismes dont on a imposé l'existence entraînent l'égalité des nombres de Hodge (qui se lisent sur la filtration de $H_{dR}(V)$) et des nombres de Hodge-Tate de $D_p(V)$ qui sont aussi les nombres de Hodge du (φ, N) -module filtré dans le cas où V a réduction semi-stable en p

$$h_H(i) = h_{HT}(D_p(V), i).$$

L'hypothèse (H.4) _{p, nr} entraîne que dans le cas de bonne réduction, les nombres de Newton du facteur L du motif V en p sont égaux aux nombres de Newton du φ -isocristal $D_p(V)$, c'est-à-dire que $h_N(D_p(V), i)$ est égal au nombre de racines réciproques de $L_p(V, X)$ qui sont de valuation i (i est ici un

rationnel). En particulier, si la représentation $H^p(V)$ a bonne réduction ordinaire en p , $h_H(i)$ est donc égal au nombre de racines réciproques de $L_p(V, X)$ qui sont de valuation i (ici, i est maintenant nécessairement un entier).

2.2.— Périodes complexes et p -adiques.

Faisons maintenant l'hypothèse que V est spécial, c'est-à-dire que, si m est pair, σ agit sur $H_B(V)^{m/2, m/2}$ comme une homothétie $\lambda \in \{+1, -1\}$.

Cette condition est nécessaire et suffisante pour qu'il existe un entier critique pour le motif V . Pour $\epsilon \in \{+, -\}$, on pose

$$H^B(V)^\epsilon = \{x \in H^B(V) \text{ tel que } \rho_B(x) = \epsilon x\}$$

$$F^\epsilon H_{dR}(V) = \begin{cases} F^{[m/2]} H_{dR}(V) & \text{si } \epsilon = \lambda \\ F^{[m/2]+1} H_{dR}(V) & \text{si } \epsilon = -\lambda \end{cases}$$

$(F^\epsilon H_{dR}(V) \otimes \mathbb{C})$ est isomorphe à

$$\oplus_{i>j} H_B(V)^{i,j} \oplus \{x \in H_B(V)^{m/2, m/2} \text{ tel que } \sigma x = \epsilon x\}.$$

Posons

$$d(V, \epsilon) = \dim_{\mathbb{Q}} F^\epsilon H_{dR}(V)$$

$$= \begin{cases} \sum_{i>m/2} h_H(i) & \text{si } \epsilon \neq \lambda \\ \sum_{i \geq m/2} h_H(i) & \text{si } \epsilon = \lambda. \end{cases}$$

On vérifie alors facilement que

$$d(V, \epsilon) = \dim_{\mathbb{Q}} H^B(V)^\epsilon$$

$$d(V, +) + d(V, -) = d(V) = \dim_{\mathbb{Q}} H^B(V)$$

$$|d(V, +) - d(V, -)| = h_H(V, m/2).$$

On introduit d'autre part les nombres suivants : si j est un entier, on pose

$$t_H(V, j) = \sum_{i \geq j} i h_H(V, i)$$

et en particulier si j est un entier tel que $F^\epsilon H_{dR}(V) = F^j H_{dR}(V)$,

$$t_H(V, \epsilon) = t_H(V, j).$$

Lorsque j est assez petit, $t_H(V, j) = t_H(V)$ est simplement le nombre de Hodge de $\det(V)$ et est égal à $md(V)/2$.

Si E et F sont deux \mathbb{Q} -espaces vectoriels et si Θ est une forme bilinéaire sur $E \times F$, si L (resp. M) est un \mathbb{Z} -module de E (resp. de F de même rang que L), on notera

$$\text{discr } \Theta(L, M)$$

le discriminant de Θ restreinte à $L \times M$.

Choisissons un réseau L_B du \mathbb{Q} -espace vectoriel $H^B(V)$ et un réseau M_{dR} du \mathbb{Q} -espace vectoriel $F^\epsilon H_{dR}(V)$ et posons

$$\begin{aligned} L_B^\epsilon &= L_B \cap H^B(V)^\epsilon \\ M_{dR}^\epsilon &= F^\epsilon H_{dR}(V) \cap M_{dR}. \end{aligned}$$

Posons

$$\gamma_\infty(V) = (2\pi i)^{-md(V)/2} \text{discr } \Theta_\infty(L_B, M_{dR}).$$

Nous verrons plus tard que $\gamma_\infty(V)$ est lié à la constante de l'équation fonctionnelle. On pose

$$\Omega_\infty(V)^\epsilon = (2\pi i)^{-t_H(V, \epsilon)} \gamma_\infty(V) \text{discr } \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon).$$

C'est un nombre complexe non nul. La propriété de compatibilité de la forme bilinéaire Θ_∞ relativement au groupe de Galois de \mathbb{C}/\mathbb{R} implique que $\Omega_\infty(V)^+$ et $\Omega_\infty(V)^-$ sont réels ou imaginaires purs. Nous verrons plus loin que ces nombres sont essentiellement les périodes de Deligne. Ce sont les facteurs de

rationalité de valeurs spéciales de la fonction L complexe du motif V définie avec les facteurs à l'infini, ce qui explique les différences. Nous y reviendrons au paragraphe suivant.

Pour construire les périodes p -adiques, on a besoin de fixer ce qu'est $2i\pi$. Pour cela, on fait le choix hypocrite suivant. Rappelons que l'on a fixé des plongements de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$ et dans \mathbb{C} . Alors, $2i\pi$ détermine un système compatible de racines de l'unité d'ordre une puissance de p dans $\bar{\mathbb{Q}}$ plongé dans \mathbb{C} qui est simplement $\exp(2i\pi/p^n)$. Ce système de racines vu maintenant dans $\bar{\mathbb{Q}}_p$ détermine un élément de $\text{Fil}^t B_{dR}$ et même de $\text{Fil}^t B_{\text{cris}}$ de la manière décrite au paragraphe 1.2 ; c'est cet élément que l'on appellera désormais $t = 2i\pi$ dans B_{dR} .

On pose

$$\begin{aligned}\gamma_p(V) &= (2i\pi)^{-md(V)/2} \text{discr } \Theta_p(L_B, M_{dR}) \\ \Omega_p(V)^\epsilon &= (2i\pi)^{-t_H(V, \epsilon)} \gamma_p(V) \text{discr } \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon).\end{aligned}$$

C'est un élément de B_{dR} qui est en fait dans B_{cris} lorsque V a bonne réduction en p et dans B_{st} lorsque V a réduction semi-stable en p . Le couple

$$(\Omega_\infty(V)^\epsilon, \Omega_p(V)^\epsilon) \in (\mathbb{C} \times B_{dR})/\mathbb{Q}^\times$$

est indépendant du choix des réseaux L_B et M_{dR} . Le comportement de la forme bilinéaire Θ_p relativement aux modules filtrés implique que $\Omega_p(V)^\epsilon$ appartient naturellement à B_{dR}^+ . En effet, si α est un élément de L_B^ϵ et β un élément de $F^j M_{dR}$, on a

$$\Theta_p(\alpha, \beta) \in \text{Fil}^j B_{dR}.$$

On conjecture ici que les périodes $\Omega_p(V)^\epsilon$ et $\Omega_\infty(V)^\epsilon$ sont les mêmes.

Posons

$$\underline{\Omega}_\infty = \mathbb{Q}\Omega_\infty(V)^+ + \mathbb{Q}\Omega_\infty(V)^-$$

et

$$\underline{\Omega}_p = \mathbb{Q}\Omega_p(V)^+ + \mathbb{Q}\Omega_p(V)^-.$$

On identifiera les deux $\bar{\mathbb{Q}}$ -espaces vectoriels $\bar{\mathbb{Q}}\Omega_\infty$ et $\bar{\mathbb{Q}}\Omega_p$ en envoyant $\Omega_\infty(V)^\epsilon$ sur $\Omega_p(V)^\epsilon$. Ceci est un cas particulier d'une conjecture faite par Fontaine sur les $\bar{\mathbb{Q}}$ -espaces vectoriels engendrés par l'image des formes bilinéaires θ_∞ et θ_p .

Intermède. Il est intéressant de regarder l'exemple des courbes elliptiques et plus particulièrement le cas des courbes elliptiques ayant bonne réduction ordinaire. Dans les calculs qui suivent et qui ne sont que la traduction de la théorie générale, on écrit indifféremment t ou $2i\pi$ (t dans les calculs et $2i\pi$ dans les résultats).

Soit E une courbe elliptique ordinaire sur K ayant bonne réduction ordinaire. On considère la représentation p -adique associée, c'est-à-dire le module de Tate $T_p(E)$ de E . Soit \tilde{E} la réduction de E dans un modèle minimal sur l'anneau des entiers de K et \hat{E} le groupe formel associé à l'origine. On a la suite exacte

$$0 \rightarrow T_p(\hat{E}) \rightarrow T_p(E) \rightarrow T_p(\tilde{E}) \rightarrow 0.$$

On pose $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Soit κ^* le caractère non ramifié non trivial de $\text{Gal}(\bar{K}/K)$ donnant son action sur $T_p(\tilde{E})$. L'action de $\text{Gal}(\bar{K}/K)$ sur $T_p(\hat{E})$ est alors donnée par κ où $\kappa = \kappa^{*-1}\chi$ et où χ est le caractère cyclotomique. L'extension $T_p(E)$ est alors déterminée par un élément de

$$H^1(\bar{K}/K, \text{Hom}(T_p(\tilde{E}), T_p(\hat{E})))$$

c'est-à-dire par la théorie de Kummer par un élément de

$$\{x \in \hat{K}^{nr} \text{ tel que } gx = \chi^{\psi(g)}\}$$

où $\psi = \kappa^{*2}$. Notons q un élément représentant l'extension considérée.

Soit Ω un élément de $\hat{K}^{nr \times}$ tel que

$$g\Omega/\Omega = \kappa^*(g)^{-1}.$$

On a alors

$$\log_p(q) = \lambda \Omega^{-2}$$

avec $\lambda \in K$.

Choisissons une base v_0, v_1 de $T_p(E)$ tel que v_1 soit une base de $T_p(\hat{E})$. Une base $\{e_0, e_1\}$ du φ -module filtré $D = D_{cris}^*(V_p(E))$ est alors donnée par

$$\begin{cases} e_0(v_0) = \Omega^{-1} & e_1(v_0) = \Omega(\text{LOG}(q) + \log(q)) \\ e_0(v_1) = 0 & e_1(v_1) = \Omega t \end{cases}$$

où $\text{LOG}(q)$ est un élément de $\text{Fil}^1 B_{DR}$ dont nous donnerons une définition explicite. Avant de le faire, donnons les propriétés que l'on attend de lui. La représentation V est déterminée par un cocycle $a(g)$ vérifiant

$$gv_0 = \kappa^*(g)v_0 + a(g)v_1.$$

On demande donc que

$$g\text{LOG}(q) - k^*(g)^2\text{LOG}(q) = a(g)t.$$

Cela assure que e_1 appartient bien à D . De plus, $\text{LOG}(q) + \log(q)$ appartiendra à B_{cris} et vérifiera

$$\varphi(\text{LOG}(q) + \log(q)) = p(\text{LOG}(q) + \log(q)).$$

On a alors

$$\varphi e_0 = \kappa^*(\sigma)e_0, \quad \varphi e_1 = \kappa^*(\sigma)^{-1}pe_0$$

et D^1 est la droite engendrée par le vecteur $e_1 - \lambda e_0$

$$(e_1 - \lambda e_0)(v_0) = \Omega \text{LOG}(q)$$

$$(e_1 - \lambda e_0)(v_1) = \Omega t .$$

Donnons la construction de $\text{LOG}(q)$. Il ne sera en fait déterminé qu'à un multiple de $\Omega^{-2}t$ près. Le cocycle $a(g)$ peut être calculé de la manière suivante : soit $(q_n)_n$ une suite d'éléments de \bar{K} vérifiant

$$(q_{n+1})^p = q_n, \quad q_0 = q;$$

on a

$$g(q_n)/(q_n)^{\kappa^*(g)^2} = \zeta_n^{a(g)}$$

où (ζ_n) est le système compatible de racines de l'unité ayant permis de construire t . Pour tout $m \geq 1$, on choisit un relèvement $\hat{q}_{n,m}$ de q_n dans A_m (voir définition de B_{cris}). Comme $(\hat{q}_{n,m})^{p^n}/q_0$ appartient à A_m et a une image égale à 1 par ψ_m dans $O_{\mathbb{C}_p}/p^m O_{\mathbb{C}_p}$ et que le noyau de ψ_m est à puissances divisées, $\log((\hat{q}_{n,m})^{p^n}/q_0)$ existe dans A_m . La condition $q_n^p = q_{n-1}$ implique que $\hat{q}_{n,m}^p/\hat{q}_{n-1,m}$ appartient à $1 + \ker \Psi_m$. On en déduit que $\log((\hat{q}_{n,m})^p/\hat{q}_{n-1,m})$ appartient à A_m et que

$$\log((\hat{q}_{n,m})^{p^n}/(\hat{q}_{n-1,m})^{p^{n-1}}) \in p^{n-1} A_m.$$

Comme A_m est complète et séparée pour la topologie p -adique, la suite $\log((\hat{q}_{n,m})^{p^n}/q_0)$ a une limite λ_m dans A_m . On montre de même que cette limite ne dépend pas du choix des représentants $\hat{q}_{n,m}$ choisis. Les λ_m forment alors un système compatible et définissent un élément de A_{cris} que l'on note abusivement $\text{LOG}(q)$ bien qu'il dépende du choix des q_n . On remarque que comme $(\hat{q}_{n,m})^{p^n}/q$ appartient à $1 + \ker \psi_m$, son logarithme appartient au

noyau de ψ_m et donc $\text{LOG}(q)$ appartient à $Fil^t B_{dR} = tB_{dR}^+$. Montrons maintenant que $\text{LOG}(q)$ vérifie bien les propriétés attendues. Soit $\hat{\zeta}_{n,m}$ un relèvement de ζ_n dans A_m . Comme l'image par ψ_m de

$$g(\hat{q}_{n,m})/(\hat{q}_{n,m})^{\kappa^*(g)^2}(\hat{\zeta}_{n,m})^{a(g)}$$

est 1, on a

$$\begin{aligned} \log((\hat{q}_{n,m})/(\hat{q}_{n,m})^{\kappa^*(g)^2}(\hat{\zeta}_{n,m})^{a(g)})^{p^n} = \\ p^n \log g(\hat{q}_{n,m})/(\hat{q}_{n,m})^{\kappa^*(g)^2}(\hat{\zeta}_{n,m})^{a(g)} \rightarrow 0 \end{aligned}$$

lorsque $n \rightarrow \infty$. On en déduit que

$$g\text{LOG}(q) - \kappa^*(g)^2\text{LOG}(q) = a(g)t.$$

Par les théorèmes de comparaison, D est isomorphe à $H_{DR}^1(E)$ (nous avons supposé K non ramifié sur \mathbb{Q}_p). Il y a donc trois droites particulières dans D qui sont

$$\begin{aligned} L_0 &= Ke_0 \text{ vérifiant } \varphi(W(k)e_0) = W(k)e_0 \\ L_1 &= Ke_1 \text{ vérifiant } \varphi(W(k)e_1) = pW(k)e_1 \\ D^1 &\simeq H^0(E, \Omega_E^1) \quad (\text{espace des formes différentielles invariantes de } E). \end{aligned}$$

Dans le cas de multiplication complexe et dans ce cas uniquement, l'extension $V_p(E)$ est scindée c'est-à-dire que le cocycle $a(g)$ est un cobord. Donc $\text{LOG}(q)$ peut être choisi nul, q est une racine de l'unité et les deux droites L_1 et D^1 coïncident.

Ce qui précède est un calcul tout à fait local en p . Revenons à la situation où E est définie sur \mathbb{Q} . La définition des périodes $\Omega_p(V)^\epsilon$ utilise ce fait. Si u^+ et u^- sont des bases de $H^B(V)^+$ et $H^B(V)^-$, on peut les voir

comme des éléments de $V_p(E)$ par les isomorphismes de comparaison (qui dépendent des plongements de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$ et dans \mathbb{C}). Lorsque la courbe elliptique est à multiplication complexe par un corps quadratique imaginaire K contenu dans $\bar{\mathbb{Q}}$, choisissons v_0 de manière que $a(g)$ soit nul. Si $p = \text{III}^*$ avec II uniformisante de l'image de K dans $\bar{\mathbb{Q}}_p$, v_1 est alors une base de $T_{\text{II}}(E) = \varprojlim_n E_{\text{II}^n}$ et v_0 est une base de $T_{\text{II}^*}(E) = \varprojlim_n E_{\text{II}^{*n}}$. Soit alors

$$\Omega_\infty = \int_{E(\mathbb{R})} \omega$$

la période réelle de E où ω est une forme différentielle invariante de E minimale. On a alors

$$\Omega_\infty(V)^+ = \Omega_\infty / 2i\pi, \Omega_\infty(V)^- = \Omega_\infty \sqrt{D} / 2i\pi$$

si D est le discriminant du corps quadratique imaginaire,

$$\Omega_p(V)^+ = (\Omega_p 2i\pi) / 2i\pi = \Omega_p, \Omega_p(V)^- = \Omega_p \sqrt{D}.$$

En effet, $\omega = e_1(\epsilon D^1)$ engendre $F^*H_{dR}(V)$ et par l'isomorphisme de comparaison, $H^B(V)^+ \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \simeq H^p(V)^+ = V_p(E)^+$ est engendré sur \mathbb{Q}_p par un générateur u de $T_{\text{II}}(E)$ et $V_p(E)^-$ est engendré par $(\sqrt{D})u$. Plus exactement, le choix d'une \mathbb{Q} -base de $H^B(V)^+$ fixe une \mathbb{Q}_p -base u de $H^p(V)^+$. L'élément

$$\Omega_p(V)^+ = \Theta_p(u, \omega) (2i\pi)^{-1}$$

de B_{cris} (qui appartient en fait à $\hat{\mathbb{Q}}_p^{nr}$) vérifie alors la propriété

$$\text{Frob}_p(\Omega_p(V)^+)/\Omega_p(V)^+ = \kappa^*(\text{Frob}_p)^{-1}$$

où κ^* est le caractère donnant l'action de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur le module de Tate des points de II^{*n} -torsion.

Remarque : Supposons toujours E définie sur \mathbb{Q} . Soit ω une forme différentielle invariante sur E définie sur \mathbb{Q} . Soit E_1 la série d'Eisenstein de poids 1 attachée au réseau de Weierstrass construit à l'aide de la forme différentielle ω . Soit $v = (v_n)_n$ un élément du module de Tate $T_p(E)$ et ρ_n des représentants dans \mathbb{C} des points v_n (à travers la paramétrisation de Weierstrass). Alors

$$\delta_0(v) = \lim_{n \rightarrow \infty} (-p^n E_1(\rho_n))$$

définit un élément δ_0 de D proportionnel à e_0 ([13]).

Les calculs qui précèdent ont été faits car il nous semble qu'ils permettent de supprimer le flottement qui existe dans la littérature au sujet de la *bonne définition* des périodes p -adiques attachées à une courbe elliptique à multiplication complexe ordinaire en p . Il semble clair ainsi que le pendant p -adique de $\Omega_\infty/2\pi$ est $\Omega_p(2\pi)/2\pi = \Omega_p$ où Ω_p vérifie

$$\text{Frob}_p \Omega_p / \Omega_p = \kappa^*(\text{Frob}_p^{-1}) = \mathbb{I}^{*-1},$$

comme on l'affirme déjà dans [1]. La notation Ω_p malheureusement n'est pas très bien choisie, car Ω_p n'intervient pas comme coefficient de la matrice de l'accouplement Θ_p appelée matrice des périodes (période signifiant alors intégrale d'une forme différentielle contre un cycle)...

2.3.— Fonctions L complexes et p -adiques.

Introduisons enfin la fonction L complexe du motif V . Nous avons déjà introduit les facteurs $L_r(V, X)$ pour r nombre premier. Rappelons maintenant celle des facteurs à l'infini ([15]). La définition classique est la suivante. On pose lorsque m est pair

$$H_B(V)^{m/2, \epsilon} = \{x \in H_B(V)^{m/2, m/2} \mid t.q. \sigma x = \epsilon (-1)^{m/2} x\}$$

pour $\epsilon \in \{+,-\}$ et $h_H(m/2, \epsilon) = \dim_{\mathbb{C}} H_B(V)^{m/2, \epsilon}$,

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2), \Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1) = 2(2\pi)^{-s} \Gamma(s).$$

Le facteur L à l'infini associé à $H_B(V)_{\mathbb{C}}$ est alors donné par

$$L_{\infty}(V, s) = \prod_{i < j} \Gamma_{\mathbb{C}}(s-i) {}^{h_H(i,j)} \Gamma_{\mathbb{R}}(s-m/2) {}^{h_H(m/2,+)} \Gamma_{\mathbb{R}}(s+1-m/2) {}^{h_H(m/2,-)}$$

(remarquons qu'un seul au plus des facteurs $\Gamma_{\mathbb{R}}$ intervient, car $h_H(m/2,+)$ ou $h_H(m/2,-)$ est nul sous l'hypothèse que V est spécial). Pour des raisons esthétiques intervenant dans la formulation de la conjecture de Deligne, on introduit des facteurs à l'infini modifiés de la manière suivante (déjà introduits dans [2] sous une notation différente). Nous ne les utiliserons que pour des valeurs entières de s . On pose

$$\tilde{L}_{\infty}(V, s) = \prod_{i < j} \Gamma_{\mathbb{C}}(s-i) {}^{h_H(i,j)} \text{ si } \operatorname{Re}(s) < m/2+1$$

et

$$\begin{aligned} \tilde{L}_{\infty}(V, s) = \prod_{i < j} \Gamma_{\mathbb{C}}(s-i) {}^{h_H(i,j)} \Gamma_{\mathbb{R}}(s-m/2) {}^{h_H(m/2,+)} \Gamma_{\mathbb{R}}(s+1-m/2) {}^{h_H(m/2,-)} \\ \Gamma_{\mathbb{R}}(2-s+m/2) {}^{-h_H(m/2,-)} \Gamma_{\mathbb{R}}(1-s+m/2) {}^{-h_H(m/2,+)} \end{aligned}$$

si $\operatorname{Re}(s) \geq m/2+1$. La modification a simplement consisté à supprimer les facteurs réels lorsque $\operatorname{Re}(s) < m/2+1$ et à conserver l'équation fonctionnelle qui suit. Faisons encore une modification dictée par la philosophie que $2i\pi$ est plus naturel que 2π . Pour les entiers n que l'on considérera, il existe un entier h tel que $\tilde{L}_{\infty}(V, n)/(2\pi)^h$ appartienne à \mathbb{Q} . On pose alors

$$\tilde{L}_{\infty}(V, n) = i^{-h} L_{\infty}(V, n).$$

Soit

$$\begin{aligned} \Lambda(V, s) &= L_{\infty}(V, s) \prod_r L_r(V, r^{-s})^{-1} \\ \tilde{\Lambda}(V, s) &= \tilde{L}_{\infty}(V, s) \prod_r L_r(V, r^{-s})^{-1}. \end{aligned}$$

Conjecturellement, la fonction Λ admet un prolongement analytique à \mathbb{C} et vérifie une équation fonctionnelle la reliant à la fonction L du dual de Kummer V^* (dont les réalisations ℓ -adiques sont $H^\ell(V^*) = \text{Hom}_{\mathbb{Q}_\ell}(H^\ell(V), \mathbb{Q}_\ell(1))$)

$$\Lambda(V, s) = \epsilon(V) C(V)^{(m+1)/2-s} \Lambda(V^*, 2-s)$$

où $C(V)$ est le conducteur de V et $\epsilon(V)$ un nombre complexe de module 1. Dans [3], une autre normalisation $\epsilon^*(V)$ de $\epsilon(V)$ est utilisée. Les liens entre $\gamma_\infty(V)$, $\epsilon(V)$ et $\epsilon^*(V)$ sont

$$\begin{aligned} \epsilon^*(V) &= \epsilon(V) C(V)^{(m+1)/2} \\ \gamma_\infty(V) &\sim_{\mathbb{Q}} \epsilon^*(V)^{-1} i^{md(V)/2 + d(V, -)}. \end{aligned}$$

On définit $\tilde{\Lambda}(V, n)$ en modifiant $\Lambda(V, n)$ par une puissance de i , plus précisément $\tilde{\Lambda}(V, n)/\Lambda(V, n) = \tilde{L}_\infty(V, n)/L(V, n)$.

Donnons maintenant la définition d'un entier critique pour le motif V . Plutôt que de donner la définition usuelle en termes des pôles des facteurs L à l'infini de V , on prendra la définition suivante (qui lui est équivalente d'après une remarque de Bloch). On dit donc qu'un entier n est **critique** pour le motif V si et seulement si on a

$$F^n H_{dR}(V) = F^{(-1)^{n+1}} H_{dR}(V)$$

(ici, bien sûr, $(-1)^{n+1}$ doit être considéré comme un signe).

La conjecture de Deligne peut alors s'énoncer de la manière suivante (où $(-1)^{n+1}$ est considéré comme un signe $\in \{+, -\}$) .

CONJECTURE (Deligne). Si n est critique pour V , alors

$$\tilde{\Lambda}(V, n) \in \mathbb{Q} \Omega_\infty(V)^{(-1)^{n+1}}.$$

Vérifions rapidement que cet énoncé est bien le même que celui de Deligne. En utilisant les formules et les notations de [3], on a

$$L(V, n) \in c^*(V(n))\mathbb{Q}$$

avec

$$\begin{aligned} c^*(V(n)) &\sim_{\mathbb{Q}} (2i\pi)^{nd(V, (-1)^n)} \operatorname{discr} \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon) / \operatorname{discr} \Theta_\infty(L_B, M_{dR}) \\ &\sim_{\mathbb{Q}} (2i\pi)^{nd(V, (-1)^n) - md(V)/2} \gamma_\infty(V)^{-1} \operatorname{discr} \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon) . \end{aligned}$$

Nous allons montrer que si n est un entier critique

$$\tilde{L}_\infty(V, n)(2i\pi)^{nd(V, (-1)^n) - md(V)/2} \sim_{\mathbb{Q}} (2i\pi)^{-t_H(V, (-1)^n)}$$

La démonstration consiste à regarder tous les cas successivement, l'entier n étant supposé critique.

Rappelons que si r est un entier, l'on a

$$\begin{aligned} \Gamma_{\mathbb{C}}(r) &\sim_{\mathbb{Q}} (2\pi)^{-r} \\ \Gamma_{\mathbb{R}}(r) &\sim_{\mathbb{Q}} (2\pi)^{-(1-r)/2} \quad \text{si } r \text{ est impair} \\ \Gamma_{\mathbb{R}}(r) &\sim_{\mathbb{Q}} (2\pi)^{-r/2} \quad \text{si } r \text{ est pair et } > 0 . \end{aligned}$$

Posons

$$\tilde{L}_\infty(V, n)(2i\pi)^{nd(V, (-1)^n) - md(V)/2} \sim_{\mathbb{Q}} (2i\pi)^\alpha$$

et calculons α .

Pour simplifier les notations, on écrira ici F^j pour $F^j H_{dR}(V)$, $h(i)$ à la place de $h_H(i) = h_H(i, m-i)$ et d pour $d(V)$.

1) $m - 2(n-1) > 0$. On a les inclusions

$$F^{n-1} \supset F^n \supset F^{m/2} \supset F^{m/2+1} .$$

Lorsque $h(m/2)$ est non nul, $F^{m/2+1}$ est différent de F^n . Comme n est critique, on a donc nécessairement $F^n = F^{(-1)^{n+1}} = F^{m/2}$ et donc $\lambda = (-1)^{n+1}$, d'où $d(V, (-1)^n) = \sum_{i > m/2} h(i)$.

On a

$$\tilde{L}_\infty(V, n) \sim_{\mathbb{Q}} (2i\pi)^{\sum_{i < j} (i-n)h(i)}.$$

D'où

$$\begin{aligned} \alpha &= \sum_{j > i} (m-n-j)h(j) - md/2 + nd(V, (-1)^n) = -\sum_{j \geq m/2} jh(j) \\ &= -\sum_{j \geq n} jh(j) = -t_H(V, (-1)^{n+1}). \end{aligned}$$

2) $m - 2(n-1) \leq 0$. On a $F^{m/2} \supset F^{n-1} \supset F^n$ et $n > m/2$. Si $h(m/2)$ est non nul, $F^{m/2}$ est différent de F^n . Comme n est critique, c'est-à-dire $F^{(-1)^{n+1}} = F^n$, on a nécessairement $F^{(-1)^{n+1}} = F^{1+m/2}$, c'est-à-dire que $\lambda = (-1)^n$ et

$$d(V, (-1)^n) = \sum_{i \geq m/2} h(i).$$

On trouve donc alors

$$\begin{aligned} \alpha &= \sum_{j > i} (m-n-j)h(j) - md/2 + nd(V, (-1)^n) - (n-m/2)h(m/2) \\ &= -\sum_{j > m/2} jh(j) = -\sum_{j \geq n} jh(j) = -t_H(V, (-1)^{n+1}). \end{aligned}$$

On en déduit donc que

$$\begin{aligned} \tilde{L}_\infty(V, n) c^*(V(n)) &\sim_{\mathbb{Q}} (2i\pi)^{-t_H(V, (-1)^{n+1})} \gamma_\infty(V)^{-1} \operatorname{discr} \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon) \\ &= \Omega_\infty(V)^{(-1)^{n+1}}. \end{aligned}$$

Revenons à la conjecture de Deligne. Soit $\Omega_\infty(V)$ le \mathbb{Q} -espace vectoriel engendré par $\Omega_\infty(V)^+$ et $\Omega_\infty(V)^-$ dans \mathbb{C} . Alors, si n est critique, $\tilde{\Lambda}(V, n)$ appartient à $\Omega_\infty(V)$.

Remarque : En reprenant les mêmes calculs, on montre que lorsque n est critique, l'équation fonctionnelle prise en n devient

$$\tilde{\Lambda}(V, n) = i^{-md(V)/2 + nd(V) - d(V, (-1)^{n+1})} \epsilon^*(V) C(V)^{-n} \tilde{\Lambda}(V, 2-n).$$

$$\text{On remarque que } i^{-md(V)/2 + nd(V) - d(V, (-1)^{n+1})} \epsilon^*(V) \sim_{\mathbb{Q}} \gamma_{\infty}(V)^{-1}.$$

On a en effet

$$i^{md(V)/2 - nd(V) + d(V, (-1)^{n+1})} = i^{md(V)/2 + (-1)^n d(V, -)}_{(-1)} [n/2] d(V).$$

Dans la théorie p -adique, on étudie un motif V en même temps que ses tordus par un caractère de Dirichlet de conducteur une puissance de p , ce qui demande de définir des motifs avec coefficients.

Soit χ un caractère de Dirichlet de conducteur M à valeurs dans une extension algébrique finie E de \mathbb{Q} . Soit $\tilde{\chi}$ le caractère de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associé défini par

$$\tilde{\chi}(\text{Frob}_r) = \chi(r)$$

pour tout nombre premier r premier à M . On associe à χ un motif $[\chi]$ à coefficients dans E dont les différentes réalisations se décrivent ainsi :

$H^B(\chi)$ est un E -espace vectoriel de dimension 1. On le munit d'une action de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ par

$$\rho_B(\sigma)x = \tilde{\chi}(\sigma)^{-1}x$$

pour $x \in H^B(\chi)$ et $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. En particulier, la conjugaison complexe agit par $\chi(-1)$.

Si λ est une place de E au-dessus de ℓ , on construit une représentation λ -adique (à valeurs dans un E_λ -espace vectoriel) par

$$H^\lambda(\chi) = H^B(\chi) \otimes_E E_\lambda.$$

On pose

$$H_{dR}(\chi) = \text{Hom}_E(H^B(\chi), E \otimes_{\mathbb{Q}} \bar{\mathbb{Q}})^{\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}$$

où $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ agit sur $E \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$ par l'identité sur E et de manière naturelle sur $\bar{\mathbb{Q}}$. C'est un E -espace vectoriel de dimension 1. On le munit de la filtration triviale $F^0 H_{dR}(\chi) = H_{dR}(\chi)$ et on munit $H^B(\chi)$ de la structure de Hodge triviale (de poids 0).

Donnons une base de $H_{dR}(\chi)$. Il s'agit de trouver un élément ω de $E \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$ vérifiant

$$\sigma\omega/\omega = \tilde{\chi}(\sigma)^{-1}$$

pour tout $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Un tel ω correspond en effet à un E -homomorphisme f de $H^B(\chi)$ dans $E \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$ par $f(1) = \omega$; le fait que f est invariant par $\text{Gal}(\mathbb{Q}/\bar{\mathbb{Q}})$ se traduit par

$$\sigma(f(1)) = f(\sigma(1)) = f(\tilde{\chi}(\sigma)^{-1} \cdot 1) = \tilde{\chi}(\sigma)^{-1} f(1).$$

On vérifie que, si ζ est une racine de l'unité d'ordre M ,

$$\omega = (\Sigma \tilde{\chi}(a) \otimes \zeta^a) = G(\chi)$$

(où a parcourt les classes modulo M) convient. On en déduit que

$$\text{discr } (H^B(\chi), H_{dR}(\chi)) \sim G(\chi).$$

La fonction L associée au motif $[\chi]$ est la fonction L usuelle associée au caractère χ^{-1} , c'est-à-dire

$$L([\chi], s) = \Sigma_{(n,M)=1} \bar{\chi}(n) n^{-s}.$$

Le motif $V(\chi)$ est alors formellement le produit tensoriel de V et de $[\chi]$. Les périodes de $V(\chi)$ sont

$$\Omega(V(\chi))^{\epsilon} = \Omega(V)^{\epsilon \sigma(\chi)} G(\chi)^{-d(V, -\epsilon \sigma(\chi))}$$

où $\sigma(\chi)$ est la parité du caractère de χ .

On vérifiera aisément la compatibilité formelle de la notion d'entier critique à la définition suivante : un couple (n, χ) formé d'un entier n et d'un caractère de Dirichlet est critique pour V si et seulement si

$$F^n H_{dR}(V) = F^{(-1)^{n+1}\sigma(\chi)} H_{dR}(V).$$

Pour tout couple (n, χ) critique pour V , on pose $\sigma(n, \chi) = \sigma(\chi)(-1)^{n+1}$ vu comme élément de $\{+, -\}$.

La conjecture de Deligne devient alors

Si (n, χ) est critique pour V , alors

$$G(\chi)^{d(V, -\sigma(n, \chi))} \tilde{\Lambda}(V(\chi), n)/\Omega_\infty(V)^{\sigma(n, \chi)} \in \bar{\mathbb{Q}}.$$

De plus, l'action sur le membre de gauche d'un élément g de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ est obtenue en changeant χ en χ^g .

Donnons maintenant une définition conjecturale des fonctions L p -adiques dans le cas où V est une représentation p -adique ordinaire (cf. [2]). Soit \mathcal{F} l'ensemble des racines réciproques de $L_p(V, X)$ de valuation $\geq s$ pour tout entier s tel que $F^\epsilon H_{dR}(V) = F^s H_{dR}(V)$ (cet ensemble ne dépend bien sûr pas du choix de s). On a donc d'après les hypothèses

$$\#(\mathcal{F}) = d(V, \epsilon).$$

Identifions $\underline{\Omega}_p$ et $\underline{\Omega}_\infty$. On suppose que, si m est pair, le motif $\mathbb{Q}(m/2)$ de réalisations ℓ -adiques $H^\ell(\mathbb{Q}(m/2)) = \mathbb{Q}_\ell(m/2)$ n'est pas facteur direct dans V .

CONJECTURE.— *Il existe une unique mesure μ_V sur \mathbb{Z}_p^\times à valeurs dans $\underline{\Omega}_p$ telle que pour tout couple (n, χ) critique pour V où χ est un caractère de Dirichlet de conducteur $p^{m(\chi)}$*

$$\int_{\mathbb{Z}_p^\times} \chi x^{n-1} d\mu_V = \prod_{\substack{\alpha \notin J^\sigma(n, \chi) \\ \alpha \in J^\sigma(n, \chi)}} p^{n-1/\alpha} \prod_{\alpha \notin J^\sigma(n, \chi)} \alpha^{(1-\chi(p)p^{n-1}/\alpha)} \\ \prod_{\alpha \in J^\sigma(n, \chi)} (1 - \chi^{-1}(p)\alpha/p^n) G(\chi)^d(V, -\sigma(n, \chi)) \tilde{\Lambda}(V(\chi), n).$$

Remarque. L'hypothèse que V est spécial est équivalente au fait qu'il existe des valeurs critiques.

On pose alors

$$L_p(\rho) = \int_{\mathbb{Z}_p^\times} \rho d\mu_V$$

où ρ est un caractère de $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ que l'on a identifié à \mathbb{Z}_p^\times par l'isomorphisme d'Artin. C'est la fonction L p -adique attachée à V vue comme fonction sur les caractères de $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. Elle ne dépend d'aucun choix de périodes mais est à valeurs dans $\Omega_p \subset B_{\text{cris}}$.

2.4.— Structure sur \mathbb{Z} . Variation de la période p -adique.

Nous allons maintenant introduire une structure supplémentaire sur V qui revient à considérer le choix des réseaux comme une donnée et non comme un intermédiaire de calcul. Par exemple, dans le cas des courbes elliptiques, ce choix revient à choisir une courbe elliptique dans sa classe d'isogénie. On pourra alors associer à V muni de sa *structure entière* une fonction à valeurs dans \mathbb{Q}_p dépendant de la *structure entière* de V . On suppose toujours que V a bonne réduction en p .

(H.5) _{\mathbb{Z}} Il existe un réseau L_B de $H^B(V)$ stable par ρ_B tel que les réseaux $L_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ de $H^\ell(V)$ soient stables par $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et un réseau M_{dR} de $H_{dR}(V)$ tel que $M_{dR} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ soit adapté au φ -module filtré $H_{dR}(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ et tel que

$$V_{\text{cris}}^*(T_p(M_{dR} \otimes_{\mathbb{Z}} \mathbb{Z}_p)) = L_B \otimes_{\mathbb{Z}} \mathbb{Z}_p \\ T_\infty(M_{dR} \otimes_{\mathbb{Z}} \mathbb{R}) = \text{Hom}(L_B \otimes_{\mathbb{Z}} \mathbb{C}, \mathbb{C})^{\text{Gal}(\mathbb{C}/\mathbb{R})}.$$

On posera alors $L_p = L_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ et $M_p = M_{dR} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Remarque. Si les nombres de Hodge de V appartiennent à un intervalle de longueur strictement inférieure à $p-1$, le lemme 1.6 affirme que $D_{cris}^*(L_B \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ est un réseau adapté de $D_{cris}^*(H_B^B(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p)$. De plus, les résultats de [9] impliquent que l'on a

$$T_p(M_{dR} \otimes_{\mathbb{Z}} \mathbb{Z}_p)) = D_{cris}^*(L_B \otimes_{\mathbb{Z}} \mathbb{Z}_p).$$

Soient

$$\begin{aligned} L_B^\epsilon &= \{x \in L_B \mid t.q \rho_B x = \epsilon x\}, \\ F^\epsilon M_{dR} &= M_{dR} \cap F^\epsilon H_{dR}(V), \end{aligned}$$

On a alors

$$\dim_{\mathbb{Z}_p} L_p^\epsilon = \dim_{\mathbb{Q}} H_B(V)^\epsilon = \dim_{\mathbb{Z}_p} F^\epsilon M_p.$$

On pose

$$\begin{aligned} \Omega_\infty(V, L_B)^\epsilon &= \epsilon^*(V)^{-1} i^{-md(V)/2 - \epsilon d(V, -)} (2i\pi)^{-t} H^{(V, \epsilon)} \text{discr } \Theta_\infty(L_B^\epsilon, M_{dR}^\epsilon) \\ \Omega_p(V, L_B)^\epsilon &= \epsilon^*(V)^{-1} i^{-md(V)/2 - \epsilon d(V, -)} (2i\pi)^{-t} H^{(V, \epsilon)} \text{discr } \Theta_p(L_B^\epsilon, M_{dR}^\epsilon) \end{aligned}$$

où l'on rappelle que L_B et M_{dR} sont maintenant liés par (H.5) $_{\mathbb{Z}}$.

Les nombres $\Omega_\infty(V, L_B)^\epsilon$ et $\Omega_p(V, L_B)^\epsilon$ appartiennent bien sûr à la classe de $\Omega_\infty(V)^\epsilon$ et $\Omega_p(V)^\epsilon$ dans $(\mathbb{C} \times B_{dR})/\mathbb{Q}^\times$. Mais les réseaux ayant été fixés, ils sont alors déterminés à $\{+1, -1\}$ près. Nous allons maintenant étudier la variation de $\Omega_p(V, L_B)^\epsilon$ par isogénie, mais seulement à une unité de \mathbb{Z}_p près, ce qui nous permettra de faire un parallèle avec la théorie d'Iwasawa arithmétique comme l'a transformée Greenberg dans [10]. Cette étude est extrêmement facile, mais c'est son lien avec [14] qui est intéressant.

Soient deux réseaux $L_{B,1}$ et $L_{B,2}$ de $H^B(V)$ vérifiant toujours (H.5) $_{\mathbb{Z}}$. On note $\text{Fil}^i L_B$ la filtration de $H^p(V)$ induite sur $L_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

PROPOSITION.— *Si V a bonne réduction ordinaire en p et si les nombres de Hodge de V appartiennent à un intervalle de longueur strictement inférieure à $p-1$, on a*

$$\Omega_p(V, L_{B,1})^\epsilon / \Omega_p(V, L_{B,2})^\epsilon \sim_p^{\mu(L_{B,2}/L_{B,1})}$$

(à une unité de \mathbb{Z}_p près) avec

$$\mu(L_{B,2}/L_{B,1}) = \text{ord}_p([L_{B,2}^\epsilon : L_{B,1}^\epsilon]) - \text{ord}_p([\text{Fil}^s L_{B,2} : \text{Fil}^s L_{B,1}])$$

si s est un entier tel que $F^s H_{dR}(V) = F^\epsilon H_{dR}(V)$.

A toute représentation p -adique V_p de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ordinaire en p , à tout réseau L_p de V_p stable par $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et à tout entier s , Greenberg associe un module $X^{(s)}(L_p)$ sur l'algèbre $\Lambda = \mathbb{Z}_p[[\Gamma]]$ où Γ est le groupe de Galois de la \mathbb{Z}_p -extension cyclotomique de \mathbb{Q} , module qui est compact et de type fini. Lorsque V_p est la représentation p -adique attachée à un motif V comme précédemment, il conjecture que ce module $X^{(s)}(L_p)$ est de torsion dès que s est un entier critique pour V . Notons dans ce cas $F_p^{(s)}(L, \rho)$ sa série caractéristique (définie à une unité près de Λ) vue comme fonction sur le groupe des caractères continus de Γ . Cette fonction dépend du choix du réseau L_p . Sa variation est calculée dans [14] et est donnée par la formule inverse de celle de la proposition. On en déduit donc que la fonction

$$F_p^{(s)}(V, \rho) = F_p^{(s)}(L_B, \rho) \Omega_p(V, L_B)^\epsilon$$

ne dépend pas du réseau L_B choisi, ce qui permet de rêver à un lien entre $F_p^{(s)}(V, \rho)$ et la fonction L p -adique construite par interpolation.

Revenons-en à la démonstration de la proposition. Pour simplifier les notations, posons $L_k = L_{B,k} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$ etc. Soit

$$C = L_2 / L_1.$$

C'est un groupe fini muni d'une structure de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -module. Si C^ϵ est défini par la suite exacte

$$0 \rightarrow L_{p,1}^\epsilon \rightarrow L_{p,2}^\epsilon \rightarrow C^\epsilon \rightarrow 0,$$

C^ϵ est un sous-groupe de C car L_j^ϵ est facteur direct dans L_j . De même, posons

$$\text{Fil}^i C = \text{Fil}^i L_2 / \text{Fil}^i L_1.$$

C'est un sous-groupe de C et le groupe d'inertie en p agit sur $\text{Fil}^i C$ par χ^i .

On commence par utiliser un argument d'algèbre linéaire. On notera ici $F^i M_j$ la filtration naturelle de M_j . Soit Δ le conoyau de $M_2 \rightarrow M_1$:

$$0 \rightarrow M_2 \rightarrow M_1 \rightarrow \Delta \rightarrow 0.$$

et soit $F^i \Delta$ le groupe fini défini par

$$0 \rightarrow F^i M_2 \rightarrow F^i M_1 \rightarrow F^i \Delta \rightarrow 0.$$

Soit $\underline{\omega}$ une \mathbb{Q}_p -base de $F^\epsilon H_{dR}(V) \otimes \mathbb{Q}_p$. On a

$$\text{disc}(L_1^\epsilon, \underline{\omega}) = \#(C^\epsilon) \text{disc}(L_2^\epsilon, \underline{\omega}).$$

Choisissons pour $\underline{\omega}$ une \mathbb{Z}_p -base de $F^\epsilon M_1$. On a alors

$$\text{disc}(L_1^\epsilon, F^\epsilon M_1) = \text{disc}(L_1^\epsilon, \underline{\omega}) = (\#(C^\epsilon) / \#(F^\epsilon \Delta)) \text{disc}(L_2^\epsilon, F^\epsilon M_2).$$

Il s'agit donc simplement de montrer que

$$\#(F^\epsilon \Delta) = \#(\text{Fil}^s C).$$

Cela se déduit du lemme suivant.

LEMME.— *Soit U une représentation cristalline dont les poids de Hodge-Tate appartiennent à un intervalle de longueur strictement inférieure à $p-1$. Soient M_1 et M_2 deux réseaux adaptés tels que $M_2 \subset M_1$. Alors*

$$[M_1 : M_2] = [V_{\text{cris}}^*(M_2) : V_{\text{cris}}^*(M_1)].$$

Démonstration. On commence par se ramener par torsion au cas où les poids de Hodge-Tate sont positifs. C'est alors une conséquence directe de [9]. Donnons rapidement l'idée de la démonstration. On introduit la catégorie MF des $W(k)$ -modules de Dieudonné filtrés définis dans [9]. On a alors par définition $V_{\text{cris}}^*(M) = \text{Hom}_{MF}(M, A_{\text{cris}})$. Soit $\Delta = M_2/M_1$. On a la suite exacte

$$\begin{aligned} 0 \rightarrow \text{Hom}_{MF}(M_1, A_{\text{cris}}) &\rightarrow \text{Hom}_{MF}(M_2, A_{\text{cris}}) \rightarrow \text{Ext}_{MF}^1(\Delta, A_{\text{cris}}) \\ &\rightarrow \text{Ext}_{MF}^1(M_1, A_{\text{cris}}). \end{aligned}$$

Sous l'hypothèse sur les poids de Hodge-Tate, il est démontré dans [9] la nullité de $\text{Ext}_{MF}^1(M_1, A_{\text{cris}})$ et l'égalité des cardinaux de Δ et de $\text{Ext}_{MF}^1(\Delta, A_{\text{cris}})$. On en déduit le lemme.

On applique ce lemme à la représentation ordinaire $\text{Fil}^s W$. De l'égalité $V_{\text{cris}}^*(M) = L$ et de la remarque suivant la proposition 1.3, on déduit facilement que

$$V_{\text{cris}}^*(M/\oplus_{j < s} M_{[j]}) = \text{Fil}^s L.$$

On a donc

$$\#(\text{Fil}^s C) = [M_1/\oplus_{j < s} M_{1,[j]} : M_2/\oplus_{j < s} M_{2,[j]}].$$

Posons $\Delta_{[j]} = M_{1[j]}/M_{2[j]}$. C'est un sous-groupe de Δ . On vérifie alors facilement que l'on a la suite exacte

$$0 \rightarrow M_2 / \oplus_{j < s} M_{2[j]} \rightarrow M_1 / \oplus_{j < s} M_{1[j]} \rightarrow \Delta / \oplus_{j < s} \Delta_{[j]} \rightarrow 0$$

et que

$$\Delta = F^s \Delta \oplus (\oplus_{j < s} \Delta_{[j]}),$$

ce qui termine la démonstration.

Manuscrit reçu le 12 avril 1989

BIBLIOGRAPHIE

- [1] D. Bernardi, C. Goldstein et N. Stephens.— *Notes p -adiques sur les courbes elliptiques*, J. für die reine und ang. Math. 351 (1984), 129–170.
- [2] J. Coates et B. Perrin-Riou.— *On p -adic L -functions attached to motives over \mathbb{Q}* , Advanced studies in Pure Math. 17 (1989), 23–54.
- [3] P. Deligne.— *Valeurs de fonctions L et périodes d'intégrales*, Proc. Symp. Pure Math. vol. 33, 2 (1979), 313–346.
- [4] J.-M. Fontaine.— *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate*, Astérisque 63 (1979), 3–80.
- [5] J.-M. Fontaine.— *Sur certains types de représentations p -adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate*, Ann. Math. 115 (1982), 529–577.
- [6] J.-M. Fontaine.— *Représentations p -adiques*, Proc. Int. C. Math. (1983), Vaszawa, 475–486.
- [7] J.-M. Fontaine.— *Cohomologie de de Rham, cohomologie cristalline et représentations p -adiques*, L.N. 1016, Springer-Verlag, Berlin (1983), 86–108.
- [8] J.-M. Fontaine.— *Lettre à U. Jannsen* (décembre 1987).
- [9] J.-M. Fontaine et G. Lafaille.— *Construction de représentations p -adiques*, Ann. Scient. Ec. Norm. Sup. 15, 4ème série (1982), 547–608.
- [10] R. Greenberg.— *Iwasawa theory for p -adic representations*, Advanced studies in Pure Math. 17 (1989).
- [11] N. Katz.— *Slope filtration of F -crystals*, Astérisque 63 (1979), 113–164.
- [12] B. Mazur.— *Frobenius and the Hodge filtration*, Bull. AMS 78 (1972), 653–667.

- [13] B. Perrin–Riou.– *Périodes p-adiques*, C.R. Acad. Sci. Paris 300 (1985), 455–457.
- [14] B. Perrin–Riou.– *Variation de la fonction L p-adique par isogénie*, Advanced studies in Pure Math. 17 (1989).
- [15] J.-P. Serre.– *Facteurs locaux de fonctions zeta des variétés algébriques (définitions et conjectures)*. Séminaire Delange–Pisot–Poitou 1969/70, exp. 19.
- [16] J. Tate.– *p-divisible groups*, Proc. of a conference on local fields, Nuffic Summer School at Driebergen, 158–183, Springer, Berlin (1967).
- [17] Séminaire *Périodes p-adiques* (1988), IHES.
- [18] S. Bloch et K. Kato.– *L functions and Tamagawa numbers of motives*.
- [19] J. Coates.– *p-adic L functions*, Séminaire Bourbaki, exposé 701 (1988).

LMF, UER 48
 45–46 3ème étage
 Université P. et M. Curie
 4, place Jussieu
 75230 Paris Cedex 05
 France
 et
 URA D0752
 Université de Paris–Sud

*Séminaire de Théorie des Nombres
Paris 1987-88*

RAISING THE LEVELS OF MODULAR REPRESENTATIONS

Kenneth A. RIBET

1.— Introduction

Let ℓ be a prime number, and let \mathbb{F} be an algebraic closure of the prime field \mathbb{F}_ℓ . Suppose that

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}(2, \mathbb{F})$$

is an irreducible (continuous) representation. We say that ρ is *modular of level N*, for an integer $N \geq 1$, if ρ arises from cusp forms of weight 2 and trivial character on $\Gamma_0(N)$.

The term "arises from" may be interpreted in several equivalent ways. For our present purposes, it is simplest to work with maximal ideals of the Hecke algebra for weight-2 cusp forms on $\Gamma_0(N)$. Namely, let $S(N)$ be the \mathbb{C} -vector space consisting of such forms, and for each $n \geq 1$ let $T_n \in \mathrm{End} S(N)$ be the n^{th} Hecke operator. Let $\mathbb{T} = \mathbb{T}_N$ be the subring of $\mathrm{End} S(N)$ generated by these operators. As is well known ([3], th. 6.7 and [7], § 5), for each maximal ideal m of \mathbb{T} , there is a semi-simple representation

$$\rho_m : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}(2, \mathbb{T}/m),$$

unique up to isomorphism, satisfying

$$\mathrm{tr} \rho_m(\mathrm{Frob}_r) = T_r \pmod{m}, \quad \det \rho_m(\mathrm{Frob}_r) = r \pmod{m}$$

for almost all primes r . (Here Frob_r is a Frobenius element in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ for the prime r .) This representation is in fact unramified at every prime r prime to ℓN , and the indicated relations hold for all such primes. We understand that

ρ is modular of level N if there is a maximal ideal m of \mathbb{T} , together with an inclusion $w : \mathbb{T}/m \hookrightarrow \mathbb{F}$, so that the representations ρ and $\rho_m \otimes_w \mathbb{F}$ are isomorphic (cf. [7], § 5.)

The representations ρ_m are nothing other than the Galois representations attached to mod ℓ eigenforms of weight 2 on $\Gamma_0(N)$. Indeed, let \mathcal{L} be the space of forms in $S(N)$ which have integral q -expansions. As is well known, \mathcal{L} is a lattice in $S(N)$, cf. [3], Proposition 2.7. The space $\bar{\mathcal{L}} = \mathcal{L}/\ell\mathcal{L}$ is the space of mod ℓ cusp forms on $\Gamma_0(N)$. The \mathbb{F}_ℓ -algebra \mathcal{A} generated by the Hecke operators T_n in $\text{End } \bar{\mathcal{L}}$ may be identified with $\mathbb{T}/\ell\mathbb{T}$ (see, for example, [7], § 5). To give a pair (m, w) as above is to give a character (i.e., homomorphism)

$$\epsilon : \mathcal{A} \longrightarrow \mathbb{F}.$$

If f is a non-zero element of $\bar{\mathcal{L}} \otimes_{\mathbb{F}_\ell} \mathbb{F}$ which is an eigenvector for all T_n , the action of \mathcal{A} on the line generated by f defines such a character ϵ . It is an elementary fact that all characters ϵ arise in this manner.

Assume now that ρ is modular of level Np , where p is a prime number not dividing N . We say that ρ is p -new (of level pN) if ρ arises in a similar manner from the p -new subspace $S(pN)_{p\text{-new}}$ of $S(pN)$. Recall that there are two natural inclusions (or degeneracy maps) $S(N) \rightrightarrows S(pN)$ and dually two trace maps $S(pN) \rightarrowtail S(N)$. (See [1] for the former maps.) The two maps $S(N) \rightrightarrows S(pN)$ combine to give an inclusion $S(N) \oplus S(N) \hookrightarrow S(pN)$, whose image is known as the p -old subspace $S(pN)_{p\text{-old}}$ of $S(pN)$. The space $S(pN)_{p\text{-new}}$ is defined as the orthogonal complement to $S(pN)_{p\text{-old}}$ in $S(pN)$, under the Petersson inner product on $S(pN)$. It may also be characterized algebraically as the intersection of the kernels of the two trace maps; this definition is due to Serre. The space $S(pN)_{p\text{-new}}$ is \mathbb{T}_{pN} -stable.

The image of \mathbb{T}_{pN} in $\text{End } S(pN)_{p\text{-new}}$ is the p -new quotient

$$\bar{\mathbb{T}}_{pN} = \mathbb{T}_{pN/p\text{-new}}$$

of \mathbb{T}_{pN} . We say that ρ is p -new if $m \in \mathbb{T}_{pn}$ and ω may be found, as above, in such a way that the maximal ideal m of \mathbb{T}_{pN} is the inverse image of a maximal ideal of \mathbb{T}_{pn} , under the canonical quotient map $\mathbb{T}_{pN} \rightarrow \mathbb{T}_{pn}$. On a concrete level, this means that the character

$$\epsilon : \mathbb{T}_{pN} \rightarrow \mathbb{F}$$

coming from (m, ω) is defined by an eigenform in the mod ℓ reduction of the space $S(pN)_{p\text{-new}}$, i.e., in the \mathbb{F} -vector space $\Lambda \otimes_{\mathbb{Z}} \mathbb{F}$, where Λ is the lattice in $S(pN)_{p\text{-new}}$ consisting of forms with integral coefficients.

THEOREM 1.— *Let ρ be modular of level N . Let $p \nmid \ell N$ be a prime satisfying one or both of the identities*

$$(1) \quad \text{tr } \rho(\text{Frob}_p) = \pm(p+1) \pmod{\ell}.$$

Then ρ is p -new of level pN .

Remarks.

1. In the Theorem, and in the discussion below, we assume that ρ is irreducible, as above.
2. A slightly stronger conclusion may be obtained if one assumes that ρ is q -new of level N , where q is a prime number which divides N , but not N/q . Under this hypothesis, plus the hypothesis of Theorem 1, one may show that ρ is pq -new of level pN , in a sense which is easy to make precise as above. (See [7], § 7, where a theorem to this effect is proved, under the superfluous additional hypothesis $p \equiv -1 \pmod{\ell}$.) The interest of Theorem 1 is that no hypothesis is made about the existence of a prime number q .
3. The case $p = \ell$ can be included in the Theorem if its hypothesis (1) is reformulated. Namely, (1) tacitly relies on the fact that ρ is unramified outside the primes dividing ℓN . Choose a maximal ideal m for ρ as in the definition of "modular of level N ." Then (1) may be re-written as the congruence

$$T_p \equiv \pm (p+1) \pmod{m}.$$

Assuming simply that p is prime to N , but permitting the case $p = \ell$, one proves that ρ is p -new of level pN if this congruence is satisfied (with at least one choice of \pm).

COROLLARY.— *Let ρ be modular of level N . Then there are infinitely many primes p , prime to ℓN , such that ρ is p -new of level pN .*

Indeed, suppose that p is prime to ℓN . Then p is unramified in ρ , so that a Frobenius element Frob_p is well defined, up to conjugation, in the image of ρ .

By the Cebotarev Density Theorem, there are infinitely many such p such that Frob_p is conjugate to $\rho(c)$, where c is a complex conjugation in $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Both sides of the congruence (1) are then 0, so that (1) is satisfied. (Cf. [7], Lemma 7.1.)

Our corollary is stated (in terms of mod ℓ eigenforms) as "Théorème (A)" in a recent preprint of Carayol [2]. Carayol cites his Théorème (A) as having been proved in preliminary versions of [7], as an application of results in [6]. In later versions of [7], Théorème (A) was replaced by a theorem involving pq -new forms (alluded to above), which is proved by methods involving Shimura curves. The aim of this present note is to resurrect Théorème (A).

Our derivation of Theorem 1 is based on the results of [6]. Although we couch our results in the language of Jacobians of modular curves, it should be clear to the reader that we use no fine arithmetic properties of these Jacobians: the argument is entirely cohomological. As F. Diamond has recently shown [4], an elaboration of these methods leads to results for cusp forms of weight $k \geq 2$.

2.— Summary of [6]

First let N be a positive integer, and consider the modular curve $X_0(N)_{\mathbb{C}}$, along with its Jacobian $J_0(N) = \text{Pic}^0(X_0(N))$. The curve $X_0(N)$ comes equipped with standard Hecke correspondences T_n , which induce endomorphisms of $J_0(N)$ by Pic functoriality (cf. [7], § 3). These endomorphisms, in turn, act on the space of holomorphic differentials on the abelian variety dual to $J_0(N)$, which is the Albanese variety of $X_0(N)$. This space of differentials is canonically identified with $S(N)$, and via this identification the endomorphism T_n of $J_0(N)$ acts on the space of differentials

as the usual Hecke operator T_n of $S(N)$. Since the action of $\text{End}(J_0(N))$ on $S(N)$ is faithful, it follows that the subring of $\text{End}(J_0(N))$ generated by the T_n is "nothing other" than the ring \mathbb{T}_N .

We now choose a prime p prime to N and consider $X_0(pN)$ and $J_0(pN)$, to which the same remarks apply. The two curves $X_0(pN)$ and $X_0(N)$ are linked by a pair of natural degeneracy maps $\delta_1, \delta_p : X_0(pN) \rightarrow X_0(N)$, with the following (naive) modular interpretation. The curve $X_0(pN)$ is associated to the moduli problem of classifying elliptic curves E which are furnished with cyclic subgroups C_N and C_p of order N and p , respectively. Similarly, $X_0(N)$ classifies elliptic curves with cyclic subgroups of order N . The degeneracy map δ_1 maps (E, C_N, C_p) to (E, C_N) , while δ_p maps (E, C_N, C_p) to $(E/C_p, C'_N)$, where C'_N is the image of C_N on E/C_p .

In a similar vein, we recall the modular interpretation of the correspondences T_p on $X_0(N)$ and on $X_0(pN)$. First, for $X_0(N)$ we have

$$T_p : (E, C_N) \longmapsto \sum_D (E/D, (C_N \oplus D)/D),$$

where the sum is taken over the $(p+1)$ different subgroups D of order p in E . For $X_0(pN)$, we have a sum of p terms

$$T_p : (E, C_N, C_p) \longmapsto \sum_{D \neq C_p} (E/D, (C_N \oplus D)/D, E[p]/D),$$

where $E[p]$ is the group of p -division points on E . (This latter group is the direct sum $C_p \oplus D$.) These formulas lead immediately to the relations among correspondences

$$\delta_1 \circ T_p = T_p \circ \delta_1 - \delta_p, \quad \delta_p \circ T_p = p \cdot \delta_1.$$

The map δ_1 and δ_p combine to induce a map on Jacobians

$$\alpha : J_0(N) \times J_0(N) \rightarrow J_0(pN), \quad (x,y) \mapsto \delta_1^*(x) + \delta_p^*(y).$$

The image of this map is by definition the p -old subvariety A of $J_0(pN)$; the kernel of α is a certain finite group which is calculated in [6].

Namely, let Sh be the Shimura subgroup of $J_0(N)$, i.e., the kernel of the map $J_0(N) \rightarrow J_1(N)$ which is induced by the covering of modular curves $X_1(N) \rightarrow X_0(N)$. The group Sh is a finite group which may be calculated in the following way: Consider the maximal unramified subcovering $X \rightarrow X_0(N)$ of $X_1(N) \rightarrow X_0(N)$, and let \mathcal{G} be the covering group of this subcovering. Then \mathcal{G} and Sh are canonically \mathbb{G}_m -dual.

Let $\Sigma \subset J_0(N) \times J_0(N)$ be the image of Sh under the antidiagonal embedding

$$J_0(N) \rightarrow J_0(N) \times J_0(N), \quad x \mapsto (x, -x).$$

According to [6], Theorem 4.3, we have

PROPOSITION 1.— *The kernel of α is the group Σ .*

The map α is equivariant with respect to Hecke operators T_n with $(n,p) = 1$. Namely, we have $\alpha \circ T_n = T_n \circ \alpha$ for all n prime to p , with the understanding that the endomorphism T_n of $J_0(N)$ acts diagonally on the product $J_0(N) \times J_0(N)$. On the other hand, this formula must be modified when n is replaced by p , as one sees from (2).

Before recording the correct formula for T_p , we introduce the notational device of reserving the symbol T_p for the p^{th} Hecke operator at level N , and the symbol U_p for the p^{th} Hecke operator at level pN . With this notation, we have (as a consequence of (2)) the formula

$$(3) \quad U_p \circ \alpha = \alpha \circ \begin{pmatrix} T_p & p \\ -1 & 0 \end{pmatrix},$$

in which the matrix refers to the natural left action of $M(2, \mathbb{T}_N)$ on the product $J_0(N) \times J_0(N)$.

Concerning the behavior of Sh and Σ under Hecke operators, the following (easy) result is noted briefly in [6] and proved in detail in [8].

PROPOSITION 2.— *The Shimura subgroup Sh of $J_0(N)$ is annihilated by the endomorphisms*

$$\eta_r = T_r - (r+1)$$

of $J_0(N)$ for all primes $r \nmid N$.

COROLLARY.— *The subgroup Σ of $J_0(N) \times J_0(N)$ lies in the kernel of the endomorphism $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$ of $J_0(N) \times J_0(N)$. It is annihilated by the operators $T_r - (r+1)$ for all prime numbers r not dividing pN .*

The significance of the endomorphism introduced in the corollary appears when we note the formula $\beta \circ \alpha = \begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$, in which $\beta : J_0(Np) \rightarrow J_0(N) \times J_0(N)$ is the map induced by the two degeneracy maps $X_0(Np) \rightrightarrows X_0(N)$ and Albanese functoriality of the Jacobian. (The map β becomes the dual of α when we use "autoduality of the Jacobian" to identify the Jacobians with their own duals.) The formula results from the fact that the two degeneracy maps are each of degree $p+1$, and from the usual definition of T_p as a correspondence in terms of degeneracy maps.

Let $\Delta \subset J_0(N) \times J_0(N)$ be the kernel of $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$. Then Δ is a finite subgroup of $J_0(N) \times J_0(N)$. Indeed, Δ differs only by 2-torsion from the direct sums of the kernels of $T_p^{\pm(p+1)}$ on $J_0(N)$. These latter kernels are finite

because neither number $\pm(p+1)$ can be an eigenvalue of T_p on $S(N)$, in view of Weil's Riemann hypothesis, which bounds T_p 's eigenvalues by $2\sqrt{p}$. Further, the group Δ comes equipped with a perfect G_m -valued skew-symmetric pairing, in view of its interpretation as the kernel $K(L)$ of a polarization map

$$\phi_L : J_0(N) \times J_0(N) \rightarrow (J_0(N) \times J_0(N))^\vee.$$

(One takes L to be the pullback by α of the "theta divisor" on the Jacobian $J_0(pN)$.)

The subgroup Σ of Δ is self-orthogonal under the pairing on Δ . In other words, if we let Σ^\perp be the annihilator of Σ in the pairing, we have a chain of groups

$$\Delta \supset \Sigma^\perp \supset \Sigma.$$

Note also that Δ/Σ is naturally a subgroup of the abelian variety A , since A and Σ are the image and kernel of α , respectively. Thus the subquotient Σ^\perp/Σ of Δ is in particular a subgroup of A .

On the other hand, the quotient Δ/Σ^\perp is canonically the Cartier (i.e., G_m) dual Σ^* of Σ . It is naturally a subgroup of A^\vee . Indeed, Σ is the kernel of the isogeny $J_0(N) \times J_0(N) \rightarrow A$ induced by α . The kernel of the dual homomorphism $A^\vee \rightarrow (J_0(N) \times J_0(N))^\vee$ may be identified with Σ^* .

To state the final result that we need, we introduce the p -new abelian subvariety B of $J_0(pN)$. To define it, consider the map

$$J_0(pN)^\vee \rightarrow A^\vee$$

which is dual to the inclusion $A \hookrightarrow J_0(pN)$. Its kernel is an abelian subvariety Z of $J_0(pN)^\vee$. Using the autoduality of $J_0(pN)$ to transport Z back to $J_0(pN)$, we obtain B . This subvariety of $J_0(pN)$ is a complement to A in the sense that $J_0(pN) = A + B$ and $A \cap B$ is finite. It is p -new in that \mathbb{T}_{pN}

stabilizes B and acts on B through its p -new quotient $\overline{\mathbb{T}}_{pN}$ (which acts faithfully on B). The following main result of [6] is a formal consequence of Proposition 2 :

THEOREM 2.— *The finite groups $A \cap B$ and Σ^\perp / Σ are equal.*

In the notation of [6], $A \cap B$ is the group Ω , which can be described directly in terms of Δ and the kernel of α ([6], pp. 508–509). Once this kernel is identified, the description of Theorem 2 is immediate.

3.— Proof of Theorem 1

We assume from now on that ρ is modular of level N , and choose an ideal m of \mathbb{T}_N , plus an embedding $\omega : \mathbb{T}_N/m \hookrightarrow \mathbb{F}$ as in the definition of "modular of level N ." Assuming that one of the two congruences (1) is satisfied, we will construct

1. A maximal ideal \mathcal{M} of $\overline{\mathbb{T}}_{pN}$, and
2. An isomorphism $\mathbb{T}_N/m \approx \overline{\mathbb{T}}_{pN}/\mathcal{M}$ which takes T_r to T_r for all primes $r \neq p$.

This is enough to prove the theorem, since the representations ρ_m and $\rho_{\mathcal{M}}$ will necessarily be isomorphic, in view of the T_r -compatible isomorphism between the residue fields of m and \mathcal{M} . Our procedure is to construct \mathcal{M} first as a maximal ideal of \mathbb{T}_{Np} and then to verify that \mathcal{M} in fact arises by pullback from a maximal ideal of $\overline{\mathbb{T}}_{pN}$.

It might be worth pointing out explicitly that our construction of \mathcal{M} depends on the sign \pm in (1). If $p \not\equiv -1 \pmod{\ell}$, then there is a unique sign \pm which makes (1) true, under the hypothesis of the theorem, and our construction proceeds in a mechanical way. In case $p \equiv -1 \pmod{\ell}$, both congruences (1) are satisfied under the hypothesis of the theorem, and the construction requires us to decide whether (1) should read $0 \equiv +0$ or $0 \equiv -0$. The two choices of sign lead to different ideals \mathcal{M} , at least when ℓ is odd, since our construction shows that $U_p \equiv \pm 1 \pmod{\mathcal{M}}$, with the same sign \pm as in (1).

Before beginning the construction, we introduce the following abbreviations :

$$R = \mathbb{T}_N, \quad k = \mathbb{T}_N/m, \quad \mathbb{T} = \mathbb{T}_{pN}, \quad \overline{\mathbb{T}} = \overline{\mathbb{T}}_{pN}.$$

Also, let

$$V = J_0(N)[m]$$

be the kernel of m on $J_0(N)$, i.e., the intersection of the kernels on $J_0(N)$ of the various elements of m . This group is a finite k -vector space which is easily seen to be non-zero (cf. [5], or [7], Theorem 5.2). The group $V \times V$ is then a finite subgroup of $J_0(N) \times J_0(N)$. This subgroup has zero intersection with $\text{Sh} \times \text{Sh}$, in view of the irreducibility of ρ_m , Proposition 2 above, and [7], Theorem 5.2 (c). In particular, α maps $V \times V$ isomorphically into A . Therefore, we can (and will) regard $V \times V$ as a subgroup of that abelian variety.

We now assume that one of the two congruences (1) is satisfied. To fix ideas we will treat only the case

$$\text{tr } \rho(\text{Frob}_p) \equiv -(p+1) \pmod{\ell}.$$

Using the isomorphism between ρ and $\rho_m \otimes_{\omega} \mathbb{F}$, we restate this congruence in the form

$$(4) \quad T_p \equiv -(p+1) \pmod{m}.$$

(The left-hand side of (4) is the trace of $\rho_m(\text{Frob}_p)$.) We embed V in $V \times V$ via the *diagonal* embedding ; the antidiagonal embedding would be used instead if T_p were $p + 1$ modulo m . We have

$$V \hookrightarrow V \times V \hookrightarrow A.$$

LEMMA 1.— *The subgroup V of A is stable under \mathbb{T} . The action of \mathbb{T} on V is summarized by a homomorphism $\gamma : \mathbb{T} \rightarrow k$ which takes T_n to T_n modulo m for $(n,p) = 1$ and takes U_p to -1 .*

Proof: That $T_n \in \mathbb{T}$ acts on V in the indicated way, for n prime to p , follows from the equivariance of a with respect to such T_n . The statement relative to U_p then follows from (3) and (4). \square

Define $\mathcal{M} = \ker \gamma$, so that we have an inclusion $\mathbb{T}/\mathcal{M} \hookrightarrow k = R/m$. This map is in fact an *isomorphism* since k is generated by the images of the T_n with n prime to p . Indeed, T_p lies in the prime field \mathbb{F}_ℓ of k because of (4).

To conclude our proof of Theorem 1, we must show that the maximal ideal \mathcal{M} of \mathbb{T} arises by pullback from $\bar{\mathbb{T}}$. For this, it suffices to show that \mathbb{T} acts on V through its quotient $\bar{\mathbb{T}}$. This fact follows from

LEMMA 2.— *The subgroup V of A lies in the intersection $A \cap B$.*

Proof : We first note that V , considered diagonally as a subgroup of $J_0(N) \times J_0(N)$, lies in the group Δ . Indeed, $V \subset J_0(N)$ is killed by $T_p + p + 1$ by virtue of (4). The isomorphic image of V in $J_0(pN)$ therefore lies in Δ/Σ . To prove the lemma, we must show that this image lies in the subgroup $A \cap B = \Sigma^\perp/\Sigma$ of Δ/Σ . In other words, we must show that the image of V in Δ/Σ^\perp is 0.

A somewhat painless way to see this is to view the varieties $J_0(N)$, $J_0(Np)$, A, \dots as being defined over \mathbb{Q} . The group Δ/Σ^\perp is canonically the G_m -dual of Σ , which may be identified $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -equivariantly with the Shimura subgroup Sh of $J_0(N)$. This latter group is in turn the G_m -dual of the covering group \mathcal{G} introduced above. It follows that the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on Δ/Σ^\perp is trivial. (We note in passing that the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on Sh is given by the cyclotomic character $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \hat{\mathbb{Z}}^*$.) Hence if V maps non-trivially to Δ/Σ^\perp , the semisimplification of V (as a $\mathbb{F}_\ell[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -module) contains the trivial representation. This semisimplification may be constructed by the following recipe : find the semisimplification W on V as a $k[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -module,

and consider W as an \mathbb{F}_ℓ -module. (A simple representation over k remains semisimple after "restriction of scalars" from k to \mathbb{F}_ℓ .) Hence W contains $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -invariant vectors, if V maps non-trivially to Δ/Σ^\perp . This conclusion is absurd, since W is the direct sum of a number of copies of the k -simple 2-dimensional representation ρ_m ([5], Chapter II, Proposition 14.2). \square

Manuscrit reçu le 18 février 1989

BIBLIOGRAPHY

- [1] A.O.L. Atkin and J. Lehner.— *Hecke operators on $\Gamma_0(m)$* , Math. Ann. 185, (1970), 134–160.
- [2] H. Carayol.— *Sur les représentations Galoisiennes modulo ℓ attachées aux formes modulaires*, Preprint.
- [3] P. Deligne and J.-P. Serre.— *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. 7, 507–530 (1974).
- [4] F.I. Diamond.— *Congruence primes for cusp forms of weight $k \geq 2$* , to appear.
- [5] B. Mazur.— *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47, (1977), 33–186.
- [6] K. Ribet.— *Congruence relations between modular forms*, Proc. International Congress of Mathematicians 1983, 503–514.
- [7] K. Ribet.— *On modular representations of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Preprint.
- [8] K. Ribet.— *On the component groups and the Shimura subgroup of $J_0(N)$* , Séminaire de Théorie des Nombres, Université de Bordeaux, 1987/88.

K.A. Ribet
 Mathematics Department
 University of California
 Berkeley CA 94720
 U.S.A.

*Séminaire de Théorie des Nombres
Paris 1987-88*

MATRICES DONT LES COEFFICIENTS SONT DES FORMES LINÉAIRES

D. ROY

I.— Introduction.

Soit L le \mathbb{Q} -sous-espace de \mathbb{C} constitué des logarithmes des nombres algébriques. Soient n et d des entiers vérifiant $0 \leq n \leq d$, et soit V un sous-espace de \mathbb{C}^d de dimension n . En se basant sur un théorème de transcendance de Michel Waldschmidt ([6], thm. 1.1), Michel Emsalem a montré que si $V \cap \mathbb{Q}^d = 0$, la dimension sur \mathbb{Q} de $V \cap L^d$ est $\leq nd$, tandis qu'elle est infinie sinon ([1], thm. 2). M. Waldschmidt a amélioré cette borne en montrant $\dim_{\mathbb{Q}}(V \cap L^d) \leq n(n+1)$ sous la même hypothèse $V \cap \mathbb{Q}^d = 0$ ([4], thm. 1.1). La question demeure, de déterminer la valeur maximale de $\dim_{\mathbb{Q}}(V \cap L^d)$, lorsque V parcourt les sous-espaces de \mathbb{C}^d de dimension n vérifiant $V \cap \mathbb{Q}^d = 0$. Des exemples montrent qu'elle est $\geq \frac{1}{2}n(n+1)$ ([4], § 1). Au paragraphe 2 de l'introduction de son cours [5], M. Waldschmidt conjecture qu'elle vaut $\frac{1}{2}n(n+1)$. Il demande si cela peut se déduire du cas particulier de la conjecture de Schanuel ([2], ch. III, Historical note) suivant lequel des éléments de L qui sont linéairement indépendants sur \mathbb{Q} sont algébriquement indépendants sur \mathbb{Q} . Au paragraphe 2, on montre que tel est le cas.

Un autre problème concerne les matrices dont les coefficients appartiennent à L . On cherche à estimer leur rang en considérant l'ensemble des matrices qui leur sont \mathbb{Q} -équivalentes, c'est-à-dire qui s'en déduisent par multiplication à gauche et à droite par des matrices inversibles à coefficients dans \mathbb{Q} . Ainsi, si M est une matrice de format $d \times l$ à coefficients dans L , M. Waldschmidt montre que son rang est $\geq d\theta/(1+\theta)$, où θ désigne le minimum des rapports $(l-l_1)/(d-d_1)$ lorsque (d_1, l_1) parcourt les couples d'entiers ≥ 0 avec $d_1 < d$, pour lesquels il existe une matrice \mathbb{Q} -équivalente à M de la forme $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec B de format $d_1 \times l_1$ ([4], § 7, cor. 7.1). Au

paragraphe 2, on montre comment ce résultat peut se déduire de la conjecture de Schanuel. Ce problème m'avait été proposé par M. Waldschmidt. Il est à espérer que des travaux plus approfondis dans cette direction permettront d'obtenir des conjectures utiles concernant les matrices à coefficients dans L .

Enfin au paragraphe 3, on démontre un résultat donné sans démonstration dans [3] (lemme 1, § 2), et on en déduit une nouvelle démonstration de la proposition centrale du travail présent (prop. 1, § 2), dans le cas où le corps k qui intervient est de cardinalité infinie.

2.— Matrices dont les coefficients sont des formes linéaires.

Soient k un corps, K une extension de k , et L un k -sous-espace de K engendré par une famille d'éléments de K algébriquement indépendants sur k . L'espace vectoriel L possède les propriétés suivantes :

- (i) Des éléments de L qui sont linéairement indépendants sur k sont algébriquement indépendants sur k .
- (ii) Si L' est un sous-espace de L , et si x est un élément de L qui n'appartient pas à L' , alors x est transcendant sur $k(L')$.

Lorsque $k = \mathbb{Q}$ et $K = \mathbb{C}$, la conjecture de Schanuel permet de prendre pour L le \mathbb{Q} -sous-espace de \mathbb{C} constitué des logarithmes des nombres algébriques.

DEFINITION. *On dit que deux matrices à coefficients dans K sont k -équivalentes si elles ont même format, et si l'une s'obtient de l'autre en la multipliant à gauche et à droite par des matrices inversibles à coefficients dans k .*

Si M_1, M_2 sont deux matrices k -équivalentes à coefficients dans K , de même format $d \times l$, elles ont le même rang, et les k -sous-espaces de K^l (resp. K^d) engendrés par leurs lignes (resp. leurs colonnes) ont même dimension sur k .

DEFINITION. Soit M une matrice $d \times l$ à coefficients dans K . On définit le coefficient θ de M par

$$\theta(M) = \min\left(\frac{l-l_1}{d-d_1}\right)$$

où (d_1, l_1) parcourt les couples d'entiers ≥ 0 avec $d_1 < d$, pour lesquels il existe une matrice k -équivalente à M de la forme $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec B de format $d_1 \times l_1$.

Lorsque $k = \mathbb{Q}$, on retrouve le coefficient θ défini par M. Waldschmidt dans [6], § 7a.

PROPOSITION 1. Toute matrice à coefficients dans L est k -équivalente à une matrice de la forme $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec A inversible.

Démonstration : Soit M une matrice à coefficients dans L , et soit L_0 le k -sous-espace de L engendré par les coefficients de M . On démontre la proposition par récurrence sur la dimension de L_0 .

Si elle est nulle, alors $M = 0$, et la proposition est vérifiée. Sinon, L_0 contient un élément $x \neq 0$, et s'écrit $L_0 = \langle x \rangle_k \oplus L_1$ pour un certain sous-espace L_1 de dimension moindre. Parallèlement à cette décomposition de L_0 , M s'écrit $xN + M_1$ où N est une matrice à coefficients dans k , et M_1 une matrice à coefficients dans L_1 . Soit r le rang de N , et soient P , Q des matrices inversibles à coefficients dans k , pour lesquelles

$$PNQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$

où I_r désigne la matrice identité de format $r \times r$. En multipliant M par les mêmes matrices P , Q , on trouve :

$$PMQ = \begin{pmatrix} xI_r + A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$$

pour certaines matrices A_1, B_1, C_1, D_1 à coefficients dans L_1 . Par récurrence, on peut supposer la proposition vérifiée pour D_1 . Cela signifie l'existence de matrices inversibles P', Q' à coefficients dans k telles que $P'D_1Q'$ s'écrit $\begin{pmatrix} A' & B' \\ C' & 0 \end{pmatrix}$ avec A' inversible à coefficients dans L_1 . En multipliant PMQ à gauche par $\begin{pmatrix} I_r & 0 \\ 0 & P' \end{pmatrix}$ et à droite par $\begin{pmatrix} I_r & 0 \\ 0 & Q' \end{pmatrix}$, elle prend la forme $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec

$$A = \begin{pmatrix} xI_r + A_1 & B'' \\ C'' & A' \end{pmatrix},$$

pour certaines matrices B'' et C'' à coefficients dans L_1 . Le déterminant de A est un polynôme en x à coefficients dans $k(L_1)$, dont le coefficient de x^r est le déterminant de A' . Or x est transcendant sur $k(L_1)$ puisque $x \notin L_1$, et ce coefficient n'est pas nul puisque A' est inversible. Donc le déterminant de A n'est pas nul non plus, et A est inversible. La proposition est démontrée.

On en déduit le corollaire ci-dessous qui, sous l'hypothèse que la conjecture de Schanuel est vraie, généralise le résultat de M. Waldschmidt cité dans l'introduction.

COROLLAIRE. Soit M une matrice $d \times l$ à coefficients dans L . Son rang est $\geq d\theta(M)/(1+\theta(M))$.

Démonstration : Si le rang de M est d , c'est immédiat. Sinon, M est équivalente à $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$, avec A inversible de rang $r < d$. On en tire $\theta(M) \leq r/(d-r)$, donc $r \geq d\theta(M)/(1+\theta(M))$. Comme le rang de M est $\geq r$, la conclusion suit.

Remarque : Lorsque $k = \mathbb{Q}$, ce corollaire se déduit du résultat de M. Waldschmidt. En effet, soient M une matrice $d \times l$ à coefficients dans L , L_0 le sous-espace de L engendré par les coefficients de M , et x_1, \dots, x_t une base de L_0 sur \mathbb{Q} . La matrice M s'écrit $M = x_1M_1 + \dots + x_tM_t$ pour certaines matrices M_1, \dots, M_t à coefficients dans \mathbb{Q} . On choisit des

logarithmes de nombres algébriques $\log \alpha_1, \dots, \log \alpha_t$ qui sont linéairement indépendants sur \mathbb{Q} , et on pose $M' = (\log \alpha_1)M_1 + \dots + (\log \alpha_t)M_t$. Puisque x_1, \dots, x_t sont algébriquement indépendants sur \mathbb{Q} et que M' s'obtient de M via la spécialisation $(x_1, \dots, x_t) \rightarrow (\log \alpha_1, \dots, \log \alpha_t)$, le rang de M' est au plus égal à celui de M . Comme M et M' ont le même coefficient θ , la conclusion suit en appliquant le résultat en question. Cet argument est dû à M. Waldschmidt.

PROPOSITION 2. *Soit M une matrice $d \times l$ à coefficients dans L , dont les colonnes sont linéairement indépendantes sur k , et soit V le K -sous-espace de K^d qu'elles engendrent. Si $V \cap k^d = 0$, on a $l \leq \frac{1}{2}n(n+1)$ en désignant par n le rang de M .*

Démonstration : On procède par récurrence sur d . Si $d = 1$, la condition $V \cap k = 0$ entraîne $l = 0$, et la proposition est vérifiée. Supposons $d > 1$, $V \cap k^d = 0$ et $l \neq 0$. Alors la dimension de V , égale à n , vérifie $n < d$. Suivant la proposition précédente, M est équivalente à une matrice de la forme $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec A inversible. Notons $d_1 \times l_1$ le format de B , n_1 son rang, et V_1 le K -sous-espace de K^{d_1} engendré par ses colonnes. Comme V contient $V_1 \times 0$, on a $V_1 \cap k^{d_1} = 0$. De plus les colonnes de B sont linéairement indépendantes sur k . Alors, par récurrence, on peut supposer $l_1 \leq \frac{1}{2}n_1(n_1+1)$. L'égalité $V_1 \cap k^{d_1} = 0$ implique $n_1 < d_1$. On a aussi $d_1 \leq n$ puisque A est inversible de rang d_1 . On en déduit

$$l \leq d_1 + \frac{1}{2}n_1(n_1+1) \leq n + \frac{1}{2}(n-1)n = \frac{1}{2}n(n+1).$$

COROLLAIRE 1. *Soient n et d des entiers ≥ 0 , et soit V un K -sous-espace de K^d de dimension n . Si $V \cap k^d = 0$, alors la dimension de $V \cap L^d$ sur k est $\leq \frac{1}{2}n(n+1)$.*

Démonstration : Supposons $V \cap k^d = 0$, et soit M une matrice de format $d \times l$, dont les colonnes sont des éléments de $V \cap L^d$ linéairement indépendants

sur k . Le K -sous-espace V_1 de K^d qu'elles engendent est contenu dans V . Il vérifie donc $V_1 \cap k^d = 0$, et le rang de M , égal à la dimension de V_1 sur K , est $\leq n$. D'après la proposition 2, cela implique $l \leq \frac{1}{2}n(n+1)$. Donc la dimension de $V \cap L^d$ sur k est finie et $\leq \frac{1}{2}n(n+1)$.

Cela fournit une réponse à la question posée par M. Waldschmidt dans l'introduction de [5], § 2 :

COROLLAIRE 2. *Soient n et d des entiers ≥ 0 , et soit V un sous-espace de \mathbb{C}^d de dimension n . Si la conjecture de Schanuel est vraie, et si $V \cap \mathbb{Q}^d = 0$, les points de V dont les coordonnées sont des logarithmes de nombres algébriques constituent un \mathbb{Q} -sous-espace de V de dimension $\leq \frac{1}{2}n(n+1)$.*

3.— Espaces vectoriels de transformations linéaires.

Soit k un corps de cardinalité infinie. Pour chaque entier $n > 0$ on munit k^n de la topologie de Zariski dans laquelle les fermés sont les ensembles des zéros des idéaux de $k[X_1, \dots, X_n]$. Dans cette topologie les automorphismes k -linéaires de k^n sont des homéomorphismes. Donc si V est un espace vectoriel sur k de dimension n , il existe une unique topologie de V pour laquelle les k -isomorphismes de V dans k^n sont des homéomorphismes. On l'appelle la topologie de Zariski de V . Chaque espace vectoriel de dimension finie sur k est muni d'une telle topologie, et toute application k -linéaire entre de tels espaces est continue relativement à leurs topologies de Zariski.

PROPOSITION 3. *Soient U et V des espaces vectoriels sur k de dimension finie, et T un k -sous-espace de $\text{Hom}_k(U, V)$. L'ensemble des éléments de T de rang maximal constitue un ouvert (de Zariski) de T . Si θ appartient à cet ouvert, alors $\xi(\ker(\theta)) \subset \text{Im}(\theta)$ pour tout $\xi \in T$.*

Démonstration : Soient l et d les dimensions respectives de U et V , et soit $\text{Mat}_{d \times l}(k)$ l'espace vectoriel sur k constitué des matrices de format $d \times l$ à coefficients dans k . On choisit des bases de U et de V , et on considère l'isomorphisme de $\text{Hom}_k(U, V)$ dans $\text{Mat}_{d \times l}(k)$, qui à une transformation linéaire de U dans V associe sa matrice relative à ces bases. Cet isomorphisme

est aussi un homéomorphisme, et il préserve le rang. Soit s un entier positif. L'ensemble des éléments de $\text{Mat}_{d \times l}(k)$ de rang $\geq s$ est ouvert, car il consiste des matrices dont au moins un des mineurs d'ordre s n'est pas nul. Donc l'ensemble des éléments de $\text{Hom}_k(U, V)$ de rang $\geq s$ est aussi ouvert. Alors l'ensemble des éléments de T de rang $\geq s$ est ouvert, car il est l'image réciproque de cet ouvert de $\text{Hom}_k(U, V)$ via l'inclusion de T dans $\text{Hom}_k(U, V)$, et l'inclusion étant linéaire est continue. Comme l'entier $s \geq 1$ est arbitraire, on en déduit que l'ensemble des éléments de T de rang maximal est ouvert.

Soient θ un élément de cet ouvert, r son rang, et $u \in \ker \theta$. On choisit un complément W de $\ker \theta$ dans U et une base u_1, \dots, u_r de W . Pour tout $a \in k$ et $\xi \in T$, on trouve

$$(\theta + a\xi)(u_1) \wedge \dots \wedge (\theta + a\xi)(u_r) \wedge (\theta + a\xi)(u) = 0$$

dans $\bigwedge_k^{r+1}(V)$, car le rang de $\theta + a\xi$ est $\leq r$. Comme la cardinalité de k est infinie, chacun des coefficients du membre de gauche développé suivant les puissances de a doit être nul. Considérant celui de a , on obtient

$$\theta(u_1) \wedge \dots \wedge \theta(u_r) \wedge \xi(u) = 0.$$

Cela montre que $\xi(u)$ appartient au k -sous-espace de V engendré par $\theta(u_1), \dots, \theta(u_r)$, c'est-à-dire à $\text{Im } \theta$.

Remarque : Soient k , K et L comme au paragraphe 2. En supposant la cardinalité de k infinie, cette proposition permet de donner une nouvelle démonstration de la proposition 1 du paragraphe 2. En effet soient d et l des entiers positifs, M une matrice $d \times l$ à coefficients dans L , L_0 le k -sous-espace de L engendré par les coefficients de M , et x_1, \dots, x_t une base de L_0 sur k . On obtient $M = x_1 M_1 + \dots + x_t M_t$ pour certaines matrices $M_1, \dots, M_t \in \text{Mat}_{d \times l}(k)$. Soit W le k -sous-espace de $\text{Mat}_{d \times l}(k)$ engendré par les M_i . Étant donné l'isomorphisme entre $\text{Mat}_{d \times l}(k)$ et $\text{Hom}_k(k^l, k^d)$, la proposition ci-dessus montre que l'ensemble des éléments de W de rang

maximal constituent un ouvert de W , et que pour un élément N de cet ouvert, on a $M_i(\ker N) \subset \text{Im } N$ pour $i = 1, \dots, t$. Soient N une telle matrice, r son rang, et P, Q des matrices inversibles à coefficients dans k telles que $PNQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$, où I_r désigne la matrice identité $r \times r$. D'après la relation $M_i(\ker N) \subset \text{Im } N$, la matrice PM_iQ s'écrit $\begin{pmatrix} A_i & B_i \\ C_i & 0 \end{pmatrix}$ pour certaines matrices A_i, B_i, C_i à coefficients dans k , avec A_i de format $r \times r$. On en déduit que PMQ s'écrit $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ avec $A = x_1A_1 + \dots + x_tA_t$ de format $r \times r$. Puisqu'une spécialisation de (x_1, \dots, x_t) dans k^t applique M sur N , la même spécialisation applique A sur I_r . Donc le rang de A est r , et la proposition est vérifiée.

Manuscrit reçu le 7 novembre 1988

BIBLIOGRAPHIE

- [1] M. Emsalem.— *Sur les idéaux dont l'image par l'application d'Artin dans une \mathbb{Z}_p -extension est triviale*, J. reine angew. Math., 382 (1987), 181–198.
- [2] S. Lang.— *Introduction to transcendental numbers*, Addison-Wesley, Reading, Mass., 1966.
- [3] D. Roy.— *Sous-groupes minimaux de \mathbb{R}^n* , C.R. Acad. Sc. Paris, Série I, 307 (1988), 423–426.
- [4] M. Waldschmidt.— *Dependance of logarithms of algebraic points*, Coll. Math. Soc. Janos Bolyai, 1987, à paraître.
- [5] M. Waldschmidt.— *Quelques aspects transcendants de la théorie des nombres algébriques*, cours de troisième cycle donné à Paris VI en 1987, à paraître dans les publications de l'Université Paris VI.
- [6] M. Waldschmidt.— *Transcendance et exponentielles en plusieurs variables*, Invent. Math., 63 (1981), 97–127.

Damien Roy
 Problèmes diophantiens
 Institut Henri Poincaré
 11, rue Pierre et Marie Curie
 75231 PARIS CEDEX 05

*Séminaire de Théorie des Nombres
Paris 1987-88*

SOME NEW HASSE PRINCIPLES FOR CONIC BUNDLE SURFACES

P. SALBERGER

0.— Introduction

Let k be a number field and let X be a smooth projective geometrically integral variety defined over k . If K is an overfield of k , denote by $X(K)$ the set of K -points on X .

To decide if $X(k) \neq \emptyset$ one first studies the much easier question whether $X(k_v) \neq \emptyset$ for the v -adic completions k_v of k associated to the places v of k .

In particular, if v is non-archimedean and X has good reduction at v , then one may often use the Weil conjectures as proved by Deligne and Hensel's lemma to show that $X(k_v) \neq \emptyset$. After having studied the local questions one is then confronted with the following problem.

Question : Suppose that $X(k_v) \neq \emptyset$ at each place v of k . Is then $X(k) \neq \emptyset$?

If the answer is positive, then X is said to satisfy the Hasse principle. This terminology is motivated by Hasse's theorem that the question above has a positive answer for quadratic hypersurfaces. Other positive results have been obtained by the Hardy–Littlewood circle method (cf. e.g. [Sc]).

There are also counterexamples to the Hasse principle among for example curves of genus one (cf. [Si, ch. X, 4.11]) and cubic surfaces (cf. [CKS]). It seems however that all the known counterexamples can be explained by means of an obstruction to the Hasse principle introduced by Manin (cf. [Ma₂], [CS₃, § 3]). This obstruction vanishes if the natural map from $\mathrm{Br} k := H_{\acute{e}t}^2(k, G_m)$ to $\mathrm{Br} X := H_{\acute{e}t}^2(X, G_m)$ is surjective.

Now let k' be an algebraic closure of k and $X' := X \times_k k'$. Then X is said to be rational (resp. k -rational) if the function field of X' (resp. X) is

purely transcendental over k' (resp. k). It is easy to show that a smooth projective curve X is rational if and only if X' is isomorphic to the projective line $\mathbb{P}_{k'}^1$. It is much more difficult to give a k -birational classification of rational surfaces. This depends on the fact that the Cremona group of birational automorphisms of $\mathbb{P}_{k'}^2$ is much bigger than the group of biregular automorphisms. To describe what is known we shall need the following definition.

(0.1) DEFINITION.— *Let Y be a smooth geometrically integral curve defined over a perfect field K . Let X be a smooth surface over K equipped with a K -morphism $f : X \rightarrow Y$ satisfying the following condition :*

(*) *There is an open affine covering $Y = \bigcup_i Y_i$; $Y_i = \text{Spec } R_i$ and quadratic homogeneous polynomials $q_i(T_0, T_1, T_2) \neq 0$ with coefficients in R_i such that $X_i := X \times_Y Y_i$ is isomorphic to $\text{Proj}(R_i[T_0, T_1, T_2]/(q_i))$ as an Y_i -scheme for each i .*

Then $f : X \rightarrow Y$ is said to be a conic bundle and X a conic bundle surface over Y .

The following result of Iskovskikh (cf. [Is]) improves upon earlier results of Enriques and Manin.

(0.2.) THEOREM.— *Let X be a (smooth projective) rational surface defined over a perfect field K . Then X is K -birational to a conic bundle surface over a rational curve over K or to a K -surface X for which the anticanonical sheaf is ample (i.e. to a del Pezzo surface over K).*

In our discussion of the arithmetic of rational surfaces we shall also need the notion of degree.

(0.3) DEFINITION.— *The degree of a rational surface X (always smooth and projective) is the self intersection number of the canonical class.*

One can show that the degree of a rational surface X is at most nine with equality if and only if X' is isomorphic to $\mathbb{P}_{k'}^2$. If X is a conic bundle surface over \mathbb{P}_k^1 with n geometric degenerate fibres, then the degree of X is $8 - n$.

The following result tells us that the arithmetic of rational surfaces of high degree is similar to the arithmetic of rational curves.

(0.4) **THEOREM.**— *Let X be a rational surface of degree at least five over a number field k . Then the Hasse principle holds for X . Moreover, if $X(k) \neq \emptyset$ then X is k -rational.*

This theorem summarizes the positive results about the arithmetic of rational surfaces which were known around 1970. The most important contributions were made by Manin [Ma₁] (cf. also [Co], [MT, § 7] and [Sw]).

The arithmetic of (minimal) rational surfaces of lower degree is much more complicated. There are counterexamples to both statements in (0.4) already for the so called Châtelet surfaces. To define these, let $P(t)$ be a separable polynomial of degree 3 or 4 and let U be the k -subvariety of $\mathbb{P}_k^2 \times \mathbb{A}_k^1$ with coordinates $(x,y,z;t)$ defined by the equation

$$(0.5) \quad x^2 + by^2 = P(t)z^2$$

for some $b \in k \setminus k^2$. The projection $(x,y,z;t) \mapsto t$ defines a conic bundle morphism $U \rightarrow \mathbb{A}_k^1$ which may be extended to a conic bundle morphism $X \rightarrow \mathbb{P}_k^1$ with 4 degenerate geometric fibres (cf. [CSS, § 7]). Such k -surfaces are called (generalized) Châtelet surfaces.

In [CSS] Colliot-Thélène, Sansuc and Swinnerton-Dyer proved that certain descent varieties (universal torsors) over Châtelet surfaces satisfy the conclusions of (0.4). From this they deduced that the Manin obstruction is the only obstruction to the Hasse principle for Châtelet surfaces.

If $P(t)$ is irreducible then $\text{Br } X / \text{Im Br } k = 0$. Hence there is no Manin obstruction and one obtains the following result (cf. [CSS, § 8]):

(0.6) **THEOREM.**— *Let X be a Châtelet surface over a number field k defined by means of an equation (0.5) in which $P(t)$ is irreducible. Then the Hasse principle holds for X .*

In [Sal₂], [Sal₃] we showed that the Hasse principle holds for some other classes of conic bundle surfaces with four degenerate geometric fibres. To prove this, we used descent varieties which were constructed by means of K -theory. In

[CS₂] Colliot–Thélène and Sansuc noticed that these descent varieties were essentially the universal torsors over X . Thus our method was still related to the one used in [CSS] for studying Châtelet surfaces.

To study the arithmetic of conic bundle surfaces with five or more degenerate geometric fibres by means of descent theory seems difficult. The problem is that there are no methods available to prove that the Hasse principle holds for the universal torsors over such conic bundle surfaces. The following result (cf. [Sal₄]) was obtained by means of an entirely different method :

(0.7) **THEOREM.**— *Let X/\mathbb{P}_k^1 be a conic bundle for which $\text{Br } X/\text{Im Br } k = 0$. Then there is a closed point of odd degree on X if and only if there are such points on $X_v := X \times k_v$ for each place v of k .*

One can reformulate this theorem in terms of 0–cycles. A 0–cycle on X is a formal linear sum $\Sigma n_P[P]$ with integer coefficients, over a finite set of closed points P on X . The degree of the 0–cycle is defined to be $\Sigma n_P[k(P):k]$. Now since there are points of degree two on a conic bundle surface over \mathbb{P}_k^1 we obtain that (0.7) is equivalent to the following result.

(0.8) **THEOREM.**— *Let X/\mathbb{P}_k^1 be a conic bundle for which $\text{Br } X/\text{Im Br } k = 0$. Then there is a 0-cycle of degree one on X if and only if there are such 0-cycles on X_v for each place v of k .*

This was conjectured by Colliot–Thélène and Sansuc (cf. [CS₁, § 4]) for all rational surfaces with $\text{Br } X/\text{Im Br } k = 0$. There are counterexamples to the conclusion of (0.8) for rational surfaces with $\text{Br } X/\text{Im Br } k \neq 0$ but one can introduce a *Manin obstruction* (cf. e.g. [Sai]) which explains all the known counterexamples. One can also deduce from [Sal₄] that the conclusion of (0.8) holds for all conic bundle surfaces over \mathbb{P}_k^1 for which this obstruction vanishes.

The following result is due to Colliot–Thélène and Coray [CC, th. B] (cf. also [Sal₁ , part b] and the appendix of this paper).

(0.9) **THEOREM.**— *Let K be a perfect field and let X/\mathbb{P}_K^1 be a conic bundle with n degenerate geometric fibres. Suppose there is a point of odd degree on X . Then there is a point of odd degree $d \leq n/2$ on X .*

If we combine (0.7) with (0.9) then we obtain :

(0.10) COROLLARY.— *Let X/\mathbb{P}_k^1 be a conic bundle with four degenerate geometric fibres and such that $\text{Br } X/\text{Im Br } k = 0$. Then the Hasse principle holds for X .*

Thus from (0.7) we recover the known Hasse principles of conic bundle surfaces. In particular, we obtain a new proof of the Hasse principle for Châtelet surfaces in (0.6). From (0.7) and (0.9) we also deduce the following generalization of (0.6) :

(0.11) COROLLARY.— *Let $P(t)$ be an irreducible polynomial of degree n with coefficients in k and b an element in k^* . Let U be the k -subvariety of $\mathbb{P}_k^2 \times \mathbb{A}_k^1$ with coordinates $(x,y,z;t)$ defined by the equation*

$$x^2 + by^2 = P(t)z^2$$

and let X/\mathbb{P}_k^1 be an extension to a conic bundle over \mathbb{P}_k^1 of the conic bundle U over $\mathbb{A}_k^1 = \text{Spec } k[t]$. Suppose there are points of odd degree on $X_v = X \times k_v$ at each place v of k . Then there is a point of odd degree $d \leq n/2$ on X .

To see this, use the fact that $\text{Br } X/\text{Im Br } k = 0$ for k -surfaces as in (0.11) (cf. [San₂]).

The proof of (0.7) in [Sal₄] depends heavily on the K -theory developed by the author in [Sal₃] (cf. also [Sal₁]). This theory enables one to reduce to a concrete problem concerning approximation of certain polynomials with coefficients in the local fields k_v by means of certain polynomials with coefficients in k .

If one is only interested in (0.11), then it is possible to reduce directly to an approximation problem for polynomials without using K -theory. The aim of this paper is to present such a proof of (0.11). To solve the approximation problem we will use the same method as in [Sal₄] based on Dirichlet's theorem on primes in arithmetical progressions and the reciprocity law in class field theory. There are some technical simplifications however, since we only consider conic bundle surfaces of a special type.

We hope that this paper will make it easier to understand the proofs of the more general results obtained in [Sal4]. The proof of (0.11) is given in the first three sections. Section four contains an elementary proof of (0.9) for the conic bundle surfaces introduced in (0.11). This proof, which first appeared in a letter from J.-L. Colliot-Thélène to D. Coray, makes our paper selfcontained and independent of [CC].

We would like to thank J.-L. Colliot-Thélène for his interest in this paper and for his permission to include his proof of (4.1).

1.— Distinguished polynomials

In this section we introduce a class of polynomials which we will call distinguished. We also show how (0.11) would follow from a certain approximation property for these polynomials.

In the sequel we will use the following notations. k will denote a number field, b an element in $k^* = k \setminus \{0\}$ and $P(t)$ an irreducible polynomial in $k[t]$. By U we denote the k -subvariety of $\mathbb{P}_k^2 \times \mathbb{A}_k^1$ with coordinates $(x,y,z;t)$ defined by the equation

$$(1.1) \quad x^2 + by^2 = P(t)z^2$$

The projection $(x,y,z;t) \mapsto t$ defines a conic bundle morphism from U to $\text{Spec } k[t]$. We shall in the sequel write U/\mathbb{A}_k^1 for this conic bundle and U_K/\mathbb{A}_k^1 for the corresponding conic bundle over an extension field K of k .

If the degree of $P(t)$ is odd, then there is a point of odd degree on U with $x = y = P(t) = 0$. We assume therefore from now on that the degree n of $P(t)$ is even.

(1.2) **DEFINITION.**— *Let K be an overfield of k and $Q(t)$ be a polynomial in $K[t]$. Then $Q(t)$ is said to be K -distinguished or distinguished over K if the following conditions hold :*

- (i) *$Q(t)$ is separable and relatively prime to $P(t)$.*
- (ii) *If $Q_i(t)$ is an irreducible factor of $Q(t)$ in $K[t]$ and F_i the fibre of U_K/\mathbb{A}_k^1 defined by $Q_i(t)$, then there is a point on F_i defined over the residue field of $Q_i(t)$ in $K[t]$.*

The following result explains our interest in these polynomials.

(1.3) PROPOSITION.— (a) Suppose there exists a distinguished polynomial $Q(t) \in K[t]$ of odd degree over a field $K \supset k$. Then there exist points of odd degree on $U_K = U \times_k K$.

(b) Let v be a place of k and X_v an extension of $U_v := U \times_k k_v$ to a conic bundle surface over $\mathbb{P}_{k_v}^1$. Suppose there exists a point of odd degree on X_v .

Then there exists a distinguished polynomial over k_v of degree $n + 1$.

Proof (a) : Let $Q_1(t)$ be an irreducible factor of odd degree of $Q(t)$. Then there are points of odd degree on the fibre of U_K/\mathbb{A}_k^1 defined by $Q_1(t)$.

(b) We conclude from (0.9) that there is a point x of odd degree $d \leq n + 1$ on X_v . By applying the implicit function theorem (cf. [CCS, 3.1.2]) we may further assume that x lies on a smooth fibre F_0 of $U_v/\mathbb{A}_{k_v}^1$. Let $Q_0(t) \in k_v[t]$ be the monic irreducible polynomial for which $Q_0(x) = 0$. The fibre F_0 defined by $Q_0(t)$ is then a smooth projective curve of genus 0 containing a point x of odd degree and hence isomorphic to a projective line. We have therefore proved that there is a k_v -distinguished polynomial $Q_0(t)$ of odd degree $d_0 \leq n + 1$. But it is easy to show that there are infinitely many monic k_v -distinguished polynomials of degree two (cf. [Sal₄, § 5]). We may therefore find a k_v -distinguished polynomial of degree $n + 1$ which is the product of $Q_0(t)$ and $\frac{1}{2}(n+1-d_0)$ of these quadratic polynomials.

By using this proposition and the theorem of Colliot-Thélène and Coray (cf. (4.1)) one obtains that (0.11) would follow from a proof of the following statement :

(1.4) ASSERTION.— Suppose there exist k_v -distinguished polynomials $Q_v(t)$ of degree $n + 1$ at each place v of k . Then there exists a k -distinguished polynomial of degree $n + 1$.

The rest of this paper will be devoted to a proof of this assertion. The following criterion will be used to verify that a polynomial $Q(t) \in k[t]$ is distinguished over k .

(1.5) LEMMA.— Let $Q(t)$ be a polynomial with coefficients in k . Then $Q(t)$ is distinguished over k if and only if $Q(t)$ is distinguished over k_v for each place v of k .

Proof : If $Q(t)$ is k -distinguished, then it is trivial to see that $Q(t)$ is distinguished over any overfield of k . Conversely, if $Q(t)$ is K -distinguished over some field K containing k , then $Q(t)$ is separable and relatively prime to $P(t)$. We have therefore reduced to prove that an irreducible polynomial $Q(t) \in k[t]$ relatively prime to $P(t)$ is k -distinguished if it is k_v -distinguished at each place v of k . But this follows from the fact that the Hasse principle holds for the smooth fibre of U/\mathbb{A}_k^1 defined by $Q(t)$.

Before one can construct k -distinguished polynomials, it is essential to have a good supply of k_v -distinguished polynomials at each place v of k . To find these, we shall use different methods at the archimedean places and at the places where U/\mathbb{A}_k^1 has *bad reduction* then at the places where U/\mathbb{A}_k^1 has *good reduction*. It will therefore be convenient to make the following precise definitions.

(1.6) DEFINITION.— Let v be a non-archimedean place of k and \mathcal{o}_v be the valuation ring of k_v . Then we will say that U/\mathbb{A}_k^1 has *bad reduction* at v if (at least) one of the following conditions hold :

- (i) b is not a unit in \mathcal{o}_v or $k \subset k(\sqrt{-b})$ ramifies at v .
- (ii) $P(t)$ has some coefficient which does not belong the \mathcal{o}_v .
- (iii) $P(t)$ has coefficients in \mathcal{o}_v but reduces to a non-separable polynomial over the residue field of \mathcal{o}_v
- (iv) $P(t)$ has a leading coefficient which is not a unit in \mathcal{o}_v .

Moreover, if none of these conditions hold, then we say that U/\mathbb{A}_k^1 has *good reduction* at v .

We now describe the two methods that we will use to construct distinguished polynomials over local fields.

(1.7) THE IMPLICIT FUNCTION METHOD.— Let v be a place of k and $Q(t)$ be a polynomial in $k_v[t]$ of the same degree as a k_v -distinguished polynomial $Q_v(t)$. Then $Q(t)$ is distinguished over k_v if the coefficients of $Q(t) - Q_v(t)$ are sufficiently small.

Proof: Let \bar{k}_v be an algebraic closure of k_v and let $\alpha_1, \alpha_2, \dots, \alpha_m$ be the zeroes of $Q_v(t)$ in \bar{k}_v . Then, for $Q(t) \in k_v[t]$ sufficiently close to $Q_v(t)$, we conclude from Krasner's lemma (cf. [La, Ch. II, § 2]) that $Q(t)$ is separable with zeroes $\beta_1, \beta_2, \dots, \beta_m \in \bar{k}_v$ satisfying $k_v(\alpha_i) = k_v(\beta_i)$ for $i = 1, \dots, m$.

Now apply the implicit function theorem to a suitable smooth restriction of the conic bundle morphism from $U \times_{k_v} k_v(\alpha_i)$ to the affine line over $k_v(\alpha_i)$ for $i = 1, \dots, m$. We then obtain neighbourhoods N_i of α_i in $k_v(\alpha_i)$ such that the fibres of the conic bundle at any $t \in N_i$ have points in $k_v(\alpha_i)$. This yields the desired conclusion since $\beta_i \in N_i$ for $i = 1, \dots, n$ if $Q(t)$ is close enough to $Q_v(t)$.

(1.8) THE GOOD REDUCTION METHOD : Let v be a non-archimedean place of k for which U has good reduction at v (cf. (1.6)). Let o_v be the valuation ring of k_v and let $Q(t)$ be a separable polynomial with coefficients in o_v for which the leading coefficient C is a unit. Suppose that the resultant of $P(t)$ and $Q(t)$ is a unit in o_v . Then $Q(t)$ is distinguished over k_v .

Proof: Let \bar{k}_v be an algebraic closure of k_v and let β_1, \dots, β_m be the zeroes of $Q(t)$ in \bar{k}_v . Then, it follows from the assumptions on $Q(t)$ that β_1, \dots, β_m are integral over o_v . In particular, since $P(t) \in o_v[t]$ (cf. (1.6)(ii)) we conclude that $P(\beta_i)$ is integral over o_v for each zero β_i of Q . But we also know from the assumption on the resultant of P and Q that $C^m \prod_{i=1}^m P(\beta_i)$ is a unit in o_v . Hence $P(\beta_i)$ must be a unit in the local field $k_v(\beta_i)$ for $i = 1, \dots, m$. This combined with the assumption that $k \subset k(\sqrt{-b})$ is unramified at v (cf. (1.6)(i)) implies that $P(\beta_i)$ is represented by $x^2 + by^2$ over $k_v(\beta_i)$, thereby completing the proof.

We may now describe the main idea behind the construction of k -distinguished polynomials. Let S be the union of the following places of k :

- (1.9) (a) archimedean places
- (b) places where U/\mathbb{A}_k^1 has bad reduction

Our goal is then to construct a polynomial $Q(t) \in k[t]$ of degree $n+1$ for which we can apply the implicit function method at places $v \in S$ and the good reduction method at places $v \notin S$ to show that $Q(t)$ is k_v -distinguished at each place v of k . We then need to approximate the $Q_v(t)$ given in (1.4) at $v \in S$ by a polynomial $Q(t) \in k[t]$ for which $Q(t) \in o_v[t]$ at $v \notin S$ and such that the leading coefficient of $Q(t)$ and the resultant of $P(t)$ and $Q(t)$ are units in o_v at each $v \notin S$. It turns out, however, that in practice it is impossible to find polynomials with all these properties. What we will do in the next two sections is to carry out a modified version of this program.

2.— An approximation by means of Dirichlet's theorem.

In this section we use Dirichlet's theorem on primes in arithmetical progressions to construct a candidate $Q(t)$ for a k -distinguished polynomial of degree $n+1$. It will be clear from our construction that we may apply the implicit function method on $Q(t)$ at all places in S (cf. (1.9)) except at one archimedean place and that we may apply the good reduction method on $Q(t)$ at all places outside S except at two non-archimedean places. These exceptional places will later be handled by other methods.

We will keep the notations of the previous section. In particular, we let $Q_v(t)$ be the k_v -distinguished polynomials introduced in (1.4) and S be the finite set of places in (1.9) (but cf. (2.6)). For each place v of k we shall also define $C_v \in k_v^*$, $D_v \in k_v$ and a polynomial $R_v(t) \in k_v[t]$ by means of the following conditions.

$$(2.1) \quad Q_v(t) = (C_v t + D_v) P(t) + R_v(t); \quad \deg R_v(t) < \deg P(t)$$

Now fix an archimedean place v_∞ of k . Then, by a suitable version of Dirichlet's theorem on primes in arithmetical progression (cf. [La, p. 317]), we obtain the following result.

(2.2) LEMMA.— *There exists $C \in k^*$ arbitrarily close to $C_v \in k_v^*$ for each $v \in S \setminus \{v_\infty\}$ such that*

- (i) *C is integral with respect to places outside S*
- (ii) *There exists a place v_0 of k such that C is a unit with respect to places outside $S \cup \{v_0\}$*
- (iii) *C is a uniformizing parameter at v_0 .*

To approximate D_v we shall only need strong approximation.

(2.3) LEMMA.— *There exists $D \in k$ arbitrarily close to $D_v \in k_v$ for each $v \in S \setminus \{v_\infty\}$ such that*

- (i) *D is integral with respect to places outside S*

We now want to approximate the polynomials $R_v(t)$, $v \in S \setminus \{v_\infty\}$ by a polynomial $R(t)$ with coefficients in k . To do this, we shall need some further notations. We will denote by E the field $k[t]/(P(t))$ and by θ the image of t in E . Moreover, we denote by S_E the set of places w of E such that the restriction of w to k belongs to S .

(2.4) LEMMA.— *There exist polynomials $R(t) \in k[t]$ of degree less than n , arbitrarily close to $R_v(t)$ for each $v \in S \setminus \{v_\infty\}$ and such that :*

- (i) *the coefficients of $R(t)$ are integral with respect to places outside S*
- (ii) *there exists a place w_1 of E such that $w_1 \nmid v_0$ (with v_0 as in (2.2)) and such that $R(\theta)$ is a unit in E with respect to places of E outside $S_E \cup \{w_1\}$*
- (iii) *$R(\theta) \in E$ is a uniformizing parameter at w_1 .*

Proof : Let v be a place of k . Then there is a natural isomorphism (algebraical and topological) between $k_v[\theta]$ and $\prod_{w|v} E_w$ where w runs over all places of E dividing v . Denote by $\prod_{w|v} \alpha_w$ the element of $\prod_{w|v} E_w$ corresponding to $R_v(\theta)$ and observe that $\alpha_w \neq 0$ for each w since $P(t)$ and $Q_v(t)$ are relatively prime.

Next, let o_v be the valuation ring of a non-archimedean local field k_v and Λ_v be the maximal o_v -order of $k_v[\theta]$. We then obtain from the definition of S (cf. (1.6), (1.9)) that the o_v -lattice Λ_v has a basis consisting of $1, \theta, \dots, \theta^{n-1}$ at places v outside S .

Now let w_∞ be a place of E dividing v_∞ . Then by Dirichlet's theorem (compare (2.2)) there exists $\alpha \in E^*$ arbitrarily close to α_w for $w \in S_E \setminus \{w_\infty\}$ such that :

- (i') α is integral with respect to places outside S_E
- (ii') there exists a place w_1 of E such that $w_1 \nmid v_0$ and such that α is a unit with respect to the places of E outside $S_E \cup \{w_1\}$
- (iii') α is a uniformizing parameter at w_1

(it is clear from Dirichlet's theorem there are such α for infinitely many primes w_1 of E and hence that we may choose w_1 such that $w_1 \nmid v_0$).

Now define $R(t) \in k[t]$ to be the unique polynomial satisfying

$$(2.5) \quad R(\theta) = \alpha, \quad \deg R < n$$

Then, we conclude from (i') that $R(\theta) \in \Lambda_v = \prod_{i=0}^{n-1} o_v \theta^i$ for v not in S .

Hence, since there is only one polynomial satisfying (2.5) we obtain that $R(t) \in o_v[t]$ for these v . It is also clear that if only α is close enough to α_w at $w \in S_E \setminus \{w_\infty\}$ then we obtain $R(t)$ arbitrarily close to $R_v(t)$ for $v \in S \setminus \{w_\infty\}$.

We have therefore shown that there exist $R(t)$ with all the desired properties.

(2.6) **Remark.**— Note that the proofs of (2.2)–(2.4) also work for any finite set S of places containing the archimedean places and the places for which U/\mathbb{A}_k^1 have bad reduction. We shall in the sequel, if k has only one archimedean place and U/\mathbb{A}_k^1 has good reduction at all non-archimedean places, change the definition of S and add one non-archimedean place to S .

From now on let $Q(t) = (Ct+D) + R(t)$ for $C, D, R(t)$ as in (2.2)–(2.4). By applying the implicit function method we then obtain that $Q(t)$ is k_v -distinguished at each $v \in S \setminus \{w_\infty\}$ if $C, D, R(t)$ are chosen close enough to $C_v, D_v, R_v(t)$ at these v . In particular, since $S \setminus \{w_\infty\} \neq \emptyset$ (cf. (2.6)) we see that $Q(t)$ is separable.

Next, let v_1 be the restriction of w_1 to k . We shall then show that the good reduction method may be applied to $Q(t)$ at places outside $S \cup \{v_0\} \cup \{v_1\}$. To begin with, recall that U/\mathbb{A}_k^1 has good reduction at places outside S (cf. (1.9), (2.6)). We know therefore that $P(t) \in o_v[t]$ and that the leading coefficient A of $P(t)$ is a unit in o_v at these v . This combined with (i) of (2.2)–(2.4) (resp. (2.2)(ii)) implies that $Q(t) \in o_v[t]$ at v outside S (resp. that the leading coefficient AC of $Q(t)$ is a unit with respect to v outside $S \cup \{v_0\}$).

We now consider the resultant of P and Q . It is easily shown that this is equal to $A^{n+1} N_{E/k}(Q(\theta)) = A^{n+1} N_{E/k}(R(\theta))$. We therefore obtain from (2.4) (ii) that the resultant of P and Q in k is a unit at places outside $S \cup \{v_1\}$.

We may now apply the good reduction method at places outside $S \cup \{v_0\} \cup \{v_1\}$ and conclude that $Q(t)$ is k_v -distinguished at these places.

It still remains to show that $Q(t)$ is k_v -distinguished at v_0, v_1 and v_∞ . To simplify the treatment of v_∞ we exclude from now on the case where k is totally real. We may then assume that v_∞ is complex and use the fact that \mathbb{C} is algebraically closed to conclude that $Q(t)$ is k_v -distinguished at $v = v_\infty$.

(2.7) **Remark.**— There are two methods to treat the case where k is totally real. In [Sal₄] we used a modified version of Dirichlet's theorem due to Sansuc [San₁, Cor. 4.4]. His result is based on a deep theorem of Waldschmidt in transcendence theory. One can also avoid transcendence theory by using another refinement of Dirichlet's theorem due to Hecke (cf. [CCS, § 2]). This second method can be used to prove (0.7) and (0.11) but is not suitable for the finer theory developed in [Sal₄].

3.— Some reciprocity arguments

In this section we complete the proof of (1.4) by showing that the polynomial $Q(t) = (Ct+D)P(t) + R(t)$ constructed in § 2 is k_v -distinguished also at v_0 and v_1 . To prove this, we shall essentially use the good reduction method. It is clear, however, that it cannot be used in the same way as for the other places outside S since the resultant of P and Q (resp. C) is not a unit at v_1 (resp. v_0). These difficulties will be overcome by means of the reciprocity law in class field theory and a reciprocity formula for rational function fields.

We first treat v_1 . The following result will make it possible to apply the good reduction method at v_1 .

(3.1) **LEMMA.**— *Let $Q(t) = (Ct+D)P(t) + R(t)$ be a polynomial as in § 2 which is k_v -distinguished at each place v different from v_0 and v_1 . Then w_1 splits in $E(\sqrt{-b})$.*

Proof: Let A be the leading coefficient of $P(t)$ and let $\beta_1, \dots, \beta_{n+1}$ be the zeroes of $Q(t)$ in an algebraic closure of k . We then have the following reciprocity formula

$$(3.2) \quad A^n C^n \prod_{i=1}^{n+1} P(\beta_i) = A^{n+1} N_{E/k}(Q(\theta))$$

obtained by calculating the resultant of P and Q in two different ways.

We now use the assumption that Q is k_v -distinguished at $v \neq v_0, v_1$.

We then obtain from (1.1) and (1.2) (ii) that the multiplicative quadratic form

$x^2 + by^2$ represents $\prod_{i=1}^{n+1} P(\beta_i)$ over k_v at each $v \neq v_0, v_1$. But C^n is a square in k since n is even by assumption. We therefore conclude from (3.2) that $x^2 + by^2$ represents $A N_{E/k}(Q(\theta)) = A N_{E/k}(R(\theta))$ over k_v at each place v different from v_0 and v_1 .

The following formula (cf. [La, p. 39]) relates $N_{E/k}(R(\theta))$ to local norms $N_w(R(\theta))$ from E_w to k_v for places w of E dividing v .

$$(3.3) \quad N_{E/k}(R(\theta)) = \prod_{w|v} N_w(R(\theta)).$$

By using this formula for $v = v_0$ together with (2.4)(ii) we obtain that $N_{E/k}(R(\theta))$ is a unit at v_0 . Moreover, since U/\mathbb{A}_k^1 has good reduction outside S we find that A is a unit at v_0 and that $k \subset k(\sqrt{-b})$ is unramified at v_0 . We therefore conclude from Hensel's lemma that $x^2 + by^2$ represents $A N_{E/k}(R(\theta))$ over k_{v_0} .

We are now in a position to apply the reciprocity law in class field theory (cf. e.g. [CCS, 4.1]). We then obtain that $x^2 + by^2$ represents $A N_{E/k}(R(\theta))$ over k_{v_1} . But it is also clear from the argument used for v_0 that $x^2 + by^2$ represents A over k_{v_1} . We have therefore shown that $x^2 + by^2$ represents $N_{E/k}(R(\theta))$ over k_{v_1} .

Next, note that (cf. (2.4) (ii)) $N_w(R(\theta))$ is a unit at v_1 for each place $w \neq w_1$ dividing v_1 . This implies that all the local norms $N_w(R(\theta))$ defined by places $w \neq w_1$ dividing v_1 are represented by $x^2 + by^2$ over k_{v_1} .

We now apply (3.3) for $v = v_1$. We then obtain that $x^2 + by^2$ represents $N_{w_1}(R(\theta))$ over k_{v_1} and hence by a standard result in local class field theory (cf. [Se, ch. XIII, § 4 Ex]) that $x^2 + by^2$ represents $R(\theta)$ over E_{w_1} . But we also

know from (2.3) (iii) that $R(\theta)$ is a uniformizing parameter of E_{w_1} . Thus, since w_1 does not ramify in $E(\sqrt{-b})$ (cf. (1.6)(i)), we obtain that w_1 splits in $E(\sqrt{-b})$.

(3.4) LEMMA.— *Let $Q(t) \in k[t]$ be a polynomial as in (3.1). Then $Q(t)$ is k_v -distinguished at $v = v_1$.*

Proof : Let $p_1(t)$ be a monic irreducible factor of $P(t)$ corresponding to w_1 under the canonical isomorphism between $k_{v_1}[t]/(P(t))$ and $\prod_{w|v_1} E_w$. Then, since w_1 splits in $E(\sqrt{-b})$, we conclude that $p_1(t)$ is a product of two monic irreducible polynomials in $k_{v_1}(\sqrt{-b})[t]$. Let $f(t)$ be one of these and define $g(t)$, $h(t) \in k_{v_1}[t]$ by means of the equality $f(t) = g(t) + \sqrt{-b} h(t)$. We then have the following identity between $p_1(t)$, $g(t)$ and $h(t)$.

$$(3.5) \quad p_1(t) = g(t)^2 + b h(t)^2.$$

Next, let $\tilde{k} = k_{v_1}$ and $\tilde{P}(t) = P(t)/p_1(t)$. Define a conic bundle $\tilde{U}/\mathbb{A}_{\tilde{k}}^1$ as in (1.1) by means of the equation

$$(3.6) \quad \tilde{x}^2 + b\tilde{y}^2 = \tilde{P}(t)\tilde{z}^2.$$

Then, by (3.5) there is an isomorphism between the restrictions of $\tilde{U}/\text{Spec } \tilde{k}[t]$ and $U_{v_1}/\text{Spec } \tilde{k}[t]$ to conic bundles over $\text{Spec } \tilde{k}[t]_{P(t)}$ given by

$$(x, y, z) = (g(t)\tilde{x} - bh(t)\tilde{y}, h(t)\tilde{x} + g(t)\tilde{y}, z).$$

Thus, since $Q(t)$ is relatively prime to $P(t)$ we conclude that $Q(t)$ is \tilde{k} -distinguished with respect to $U_{v_1}/\mathbb{A}_{\tilde{k}}^1$ (cf. (1.2)) if and only if $Q(t)$ is \tilde{k} -distinguished with respect to $\tilde{U}/\mathbb{A}_{\tilde{k}}^1$.

The idea is now to apply the good reduction method on $\tilde{U}/\mathbb{A}_{\tilde{k}}^1$ instead of $U_{v_1}/\mathbb{A}_{\tilde{k}}^1$. To begin with, we note that since $U_{v_1}/\mathbb{A}_{\tilde{k}}^1$ has good reduction and $P(t) = \tilde{P}(t)p_1(t)$ with p_1 monic, then $\tilde{U}/\mathbb{A}_{\tilde{k}}^1$ must also have good reduction. We next observe that the leading coefficient AC of $Q(t)$ is a unit in \tilde{k} since $v_0 \neq v_1$ (cf. (2.2)(ii), (2.4)(ii)). Thus, to complete the proof we only have to verify the last assumption in (1.8) concerning the resultant of $\tilde{P}(t)$ and $Q(t)$. This is up to a sign given by $A^{n+1} \prod_{w \neq w_1} N_w(Q(\theta))$ where A as before is the leading coefficient of $P(t)$ and $\tilde{P}(t)$ and where w runs over all places of E dividing v_1 different from w_1 . We may now apply (2.4)(ii) to show that $N_w(Q(\theta))$ is a unit in \tilde{k} for these w , thereby completing the proof.

We now turn to v_0 . We have already observed at the end of § 2 that $Q(t) \in o_{v_0}[t]$ at each place v of k outside S . We also know from the assumption that U/\mathbb{A}_k^1 has good reduction outside S and from (2.2) that the leading coefficient of $Q(t) = (Ct+D)P(t) + R(t)$ is a uniformizing parameter at v_0 . This implies that we may find an irreducible factor $q(t)$ of $Q(t)$ in $k_{v_0}[t]$ such that $q(t)$ and $\tilde{Q}(t) := Q(t)/q(t)$ have integral coefficients and such that $\tilde{Q}(t)$ is monic. It is now straightforward to see that we may apply the good reduction method to $U_{v_0}/\mathbb{A}_{k_{v_0}}^1$ and $\tilde{Q}(t)$ in the same way as it was applied to $U_v/\mathbb{A}_{k_v}^1$ and $Q(t)$ at places outside $S \cup \{v_0\} \cup \{v_1\}$. We then obtain that $\tilde{Q}(t)$ and all its factors in $k_{v_0}[t]$ are distinguished over k_{v_0} .

Let $Q_1(t)$ be an irreducible factor of $Q(t)$ in $k[t]$ which is divisible by $q(t)$ in $k_{v_0}[t]$, and let F be the fibre of U/\mathbb{A}_k^1 defined by $Q_1(t)$. F is then a smooth conic over $K := k[t]/(Q_1(t))$.

Now note that for each place v of k , there is a natural bijection between the monic irreducible factors $Q_{1u}(t)$ of $Q_1(t)$ in $k_v[t]$ and the places u of K

dividing v . This bijection is such that $Q_{1u}(t)$ is distinguished over k_v if and only if $F(K_u) \neq \emptyset$. But we know from our previous results that $Q(t)$ and hence $Q_1(t)$ is k_v -distinguished at each $v \neq v_0$ and that $Q_1(t)/q(t) \in k_{v_0}[t]$ is k_{v_0} -distinguished. We conclude therefore that $F(K_u) \neq \emptyset$ at all places u of K different from the place u_0 corresponding to the monic factor $q(t)/AC$ of $Q_1(t)$ in $k_{v_0}[t]$.

We now apply the reciprocity law. This implies that $F(K_u) \neq \emptyset$ also at $u = u_0$ and hence that $q(t) \in k_{v_0}[t]$ is k_{v_0} -distinguished. We have therefore shown that $Q(t)$ is k_v -distinguished at each place v of k and hence by (1.5) that $Q(t)$ is distinguished over k . This completes the proof of (1.4) and (0.11).

(3.7) **Remark.**— The assertion (1.4) is false for an arbitrary separable polynomial $P(t) \in k[t]$. To see where the irreducibility is used, let $P(t) = A \prod_{i=1}^m p_i(t)$ be a factorization of $P(t)$ in $k[t]$ such that $A \in k^*$ and $p_1(t), \dots, p_m(t)$ are monic and irreducible. Further, let $P_i(t) = P(t)/Ap_i(t)$, $E_i = k[t]/(p_i(t))$ and θ_i be the image of t in E_i . Then there are unique elements $C_v \in k_v^*$, $D_v \in k_v$ and unique polynomials $R_{i,v}(t) \in k_v[t]$, $i > 1, \dots, m$ such that :

$$Q_v(t) = (C_v t + D_v)P(t) + \sum_{i=1}^m R_{i,v}(t)P_i(t), \quad \deg R_{i,v} < \deg p_i$$

We now try to approximate $Q_v(t)$ by a polynomial

$$Q(t) = (Ct + D)P(t) + \sum_{i=1}^m R_i(t)P_i(t), \quad \deg R_i < \deg p_i$$

as in § 2. We then obtain for each $i = 1, \dots, m$ an exceptional place w_i of E_i (cf. (2.4)(iii)) for which $R_i(\theta_i)$ is a uniformizing parameter at w_i and such that the restriction v_i of w_i to k is outside S . To apply the good reduction method at these places (cf. (3.4)) we then have to show that w_i splits in $E_i(\sqrt{-b})$ for each i . But the proof of (3.1) does not work if $m > 1$ unless we

put further conditions on $Q_v(t)$. What one needs is the hypothesis that there is no Brauer–Manin obstruction to the existence of 0–cycles of degree 1 on X (cf. [Sai]). This hypothesis is always satisfied if $m = 1$ and has been used in an implicit form in the proof of (3.1). One may then assume that the images of $Q_v(\theta_i)$ in $k_v(\theta)^*/N(k_v(\theta\sqrt{-b})^*)$ come from a fixed element η in $k(\theta)^*/N(k(\theta\sqrt{-b})^*)$ and use the reciprocity law to show that $Q(t)$ is k_{v_i} –distinguished (see [Sa₄, § 6] for further details).

4.– Appendix

This section is nothing but a free translation of a letter from J.-L. Colliot–Thélène to D. Coray dated 29.08.1980. It gives a short and very elementary proof of (0.9) for the conic bundle surfaces considered in § 1, § 2 and § 3.

(4.1) THEOREM.— *Let K be a field, b an element in K^* and $P(t)$ be a polynomial of degree n with coefficients in K . Let U be the K -subvariety of $\mathbb{P}_K^2 \times \mathbb{A}_K^1$ with coefficients $(x,y,z;t)$ defined by the equation $x^2 + by^2 - P(t)z^2 = 0$ and let X/\mathbb{P}_K^1 be an extension of U/\mathbb{A}_K^1 to a conic bundle over \mathbb{P}_K^1 . Suppose there exists a point of odd degree on X . Then there exists a point of odd degree $d \leq n/2$ on X .*

Proof : One may assume that the following conditions hold :

- (i) there is a (closed) point u on U such that $[K(u):K]$ is odd for the residue field $K(u)$ of u
- (ii) n is even
- (iii) the K –form $x^2 + by^2$ does not represent the leading coefficient of $P(t)$.

If one of (i), (ii) or (iii) is false, then it is easily seen that there is a K –point on $X \setminus U$. We also note that (iii) implies that the following condition holds :

- (iv) the K –form $x^2 + by^2$ is anisotropic.

Now let $R(t) \in K[t]$ be an irreducible polynomial such that $R(u) = 0$ (cf. (i)) and let a be the image of t in the residue field $K[t]/(R(t))$. We then obtain from (i) that $[K(u):K(a)]$ and $[K(a):K]$ are odd and that the $K(a)$ -form $x^2 + by^2 - P(a)z^2 = 0$ becomes isotropic over $K(u)$. We may therefore apply Springer's theorem [Sp] twice to show that $x^2 + by^2 - P(a)z^2$ is isotropic and $x^2 + by^2$ anisotropic (cf. (iv)) over $K(a)$. This implies that there exist polynomials $X(t), Y(t) \in K[t]$ of degree less than $r := \deg R(t)$ for which $X(a)^2 + bY(a)^2 - P(a) = 0$ and hence that

$$(4.2) \quad X(t)^2 + bY(t)^2 - P(t) = R(t)S(t)$$

for some $S(t) \in K[t]$.

Let $m \leq 2r-2$ be the degree of $X(t)^2 + bY(t)^2$. We then deduce from (iv) that m is even and from (iii) that $X(t)^2 + bY(t)^2 - P(t)$ is of degree $\sup(m, n)$. We also know from (i) (resp. (ii)) that r (resp. n) is odd (resp. even). We therefore conclude from (4.2) that $s := \deg S(t) = \sup(m, n) - r$ is odd.

Next, note that $(x, y, z; t) = (X(a), Y(a), 1; a)$ defines a point of odd degree r . We may thus assume that $r > n/2$ and hence by (ii) that $n \leq 2r-2$. Then we have that $s = \sup(m, n) - r \leq r-2$ and an irreducible factor $S_1(t)$ of $S(t)$ of odd degree $s_1 \leq s \leq r-2$.

Let a_1 be the image of t in $K[t]/(S_1(t))$. Then $(x, y, z; t) = (X(a_1), Y(a_1), 1; a_1)$ defines a point of odd degree $s_1 \leq r-2$ on U . We have therefore a descent process which finally will give us a point of odd degree $d \leq n/2$.

Manuscrit reçu le 8 octobre 1988

BIBLIOGRAPHY

- [Co] J.-L. Colliot–Thélène.— *Quelques propriétés arithmétiques des surfaces rationnelles (d’après Manin)*, Séminaire de Théorie des Nombres, Bordeaux 1972–72, Exp. 13, Lab. Théorie des Nombres, C.N.R.S., Talence 1972.
- [CC] J.-L. Colliot–Thélène, D. Coray.— *L’équivalence rationnelle sur les points fermés des surfaces rationnelles fibrées en coniques*, Compositio Math. 39 (1979), 301–332.
- [CCS] J.-L. Colliot–Thélène, D. Coray, J.-J. Sansuc.— *Descente et principe de Hasse pour certaines variétés rationnelles*, J. reine angew. Math., 320 (1980), 150–191.
- [CKS] J.-L. Colliot–Thélène, D. Kanevsky, J.-J. Sansuc.— *Arithmétique des surfaces cubiques diagonales*, in Diophantine Approximation and Transcendence Theory, G. Wüstholz ed., Springer Lecture Notes in Mathematics 1290 (1987), 1–108.
- [CS₁] J.-L. Colliot–Thélène, J.-J. Sansuc.— *On the Chow group of certain rational surfaces : a sequel to a paper of S. Bloch*, Duke Math. J. 48 (1981), 421–447.
- [CS₂] J.-L. Colliot–Thélène, J.-J. Sansuc.— *La descente sur les surfaces rationnelles fibrées en coniques*, C.R. Acad. Sci. Paris 303, Série I 1986, 303–306.
- [CS₃] J.-L. Colliot–Thélène, J.-J. Sansuc.— *La descente sur les variétés rationnelles*, II, Duke Math. J. 54 (1987), 375–492.
- [CSS] J.-L. Colliot–Thélène, J.-J. Sansuc, Sir Peter Swinnerton–Dyer.— *Intersections of two quadrics and Châtelet surfaces*, J. reine angew. Math. 373 (1987), 37–107 et 374 (1987), 72–168.

- [Is] V.A. Iskovskih.— *Minimal models of rational surfaces over arbitrary fields*, Izv. Ak. Nauk. SSSR Ser. Mat. 43 (1979), 19–43 (engl. transl. : Math. USSR—Izv. 14 (1980), 17–39).
- [La] S. Lang.— *Algebraic number theory*, Addison–Wesley, Reading 1970.
- [Ma₁] Yu.I. Manin.— *Rational surfaces over perfect fields* (Russian), Inst. des Hautes Etudes Sci., Publ. Math. 30 (1966), 55–113 (engl. transl. : Translations AMS (2) 84 (1969) 137–186).
- [Ma₂] Yu.I. Manin.— *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, in Actes du congrès intern. math. Nice 1 (1970), 401–411, Gauthier–Villars, Paris 1971.
- [MT] Yu.I. Manin, M.A. Tsfasman.— *Rational varieties : Algebra, geometry and arithmetic*, Uspekhi Mat. Nauk 41 (1986), 43–94 (engl. transl. : Russian Math. Surveys 41 (1986), 51–116).
- [Sai] S. Saito.— *Some observations on motivic cohomologies of arithmetical schemes*, preprint.
- [Sal₁] P. Salberger.— *K-theory of orders and their Brauer-Severi schemes*, Thesis, Department of Mathematics, University of Göteborg 1985.
- [Sal₂] P. Salberger.— *Sur l'arithmétique de certaines surfaces de del Pezzo*, C.R. Acad. Sci. Paris 303, série I (1986), 273–276.
- [Sal₃] P. Salberger.— *On the arithmetic of conic bundle surfaces*, in Séminaire de Théorie des Nombres Paris 1985–86, Progr. Math. 71, Birkhäuser, Basel Boston 1987, 175–197 (cf. also the Errata in this volume).
- [Sal₄] P. Salberger.— *Zero-cycles on rational surfaces over number fields*, Invent. Math. 91 (1988), 505–524.

- [San₁] J.-J. Sansuc.— *Descente et principe de Hasse pour certaines variétés rationnelles*, in Séminaire de Théorie des Nombres, Paris 1980–81, Progr. Math. 22, Birkhäuser, Basel Boston 1982, 253–271.
- [San₂] J.-J. Sansuc.— *A propos d'une conjecture arithmétique sur le groupe de Chow d'une surface rationnelle*, Séminaire de Théorie des Nombres, Bordeaux 1981–81, Exp. 33 Lab. Théorie des Nombres, C.N.R.S., Talence 1972.
- [Sc] W.M. Schmidt.— *The density of integer points on homogeneous varieties*, Acta Math. 154 (1985), 243–296.
- [Se] J.-P. Serre.— *Corps locaux*, deuxième éd., Hermann, Paris 1968.
- [Si] J. Silverman.— *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, Springer–Verlag, Berlin Heidelberg New York 1986.
- [Sp] T.A. Springer.— *Sur les formes quadratiques d'indice zero*, C.R. Acad. Sci. 234, 1517–1519 (1952).
- [Sw] H.P.F. Swinnerton–Dyer.— *Rational points on del Pezzo surfaces of degree 5*, in Algebraic geometry Oslo 1970 (Proc. 5th Nordic Summer School in Math.), Wolters and Noordhoff, Groningen 1972, 287–290.

Per SALBERGER
 C.N.R.S. Mathématiques
 URA D0752
 Bâtiment 425
 Université de Paris–Sud
 F–91405 ORSAY CEDEX

*Séminaire de Théorie des Nombres
Paris 1987-88*

**VALEURS DES FORMES QUADRATIQUES
INDÉFINIES IRRATIONNELLES**
(d'après G.A. Margulis)
J.-C. SIKORAV

Introduction.

Nous allons exposer la preuve du résultat suivant, obtenue par G.A. Margulis en 1987 ([6], [7], [8]) :

THEOREME A. *Soit B une forme quadratique sur \mathbb{R}^n , $n \geq 3$, indéfinie, non dégénérée et irrationnelle (non multiple d'une forme entière). Alors $|B|$ prend des valeurs arbitrairement petites sur $\mathbb{Z}^n \setminus \{0\}$.*

Ceci résout une conjecture faite par A. Oppenheim en 1929. On peut en déduire que les valeurs de $B|_{\mathbb{Z}^n}$ sont denses dans \mathbb{R} . Ce résultat a depuis été amélioré par G. Dani et G.A. Margulis[4] : l'ensemble des valeurs prises par la forme quadratique sur les points entiers primitifs est déjà dense.

Avant Margulis, les meilleurs résultats avaient été obtenus par H. Davenport et ses collaborateurs de 1946 à 1959 [5], qui avaient démontré la conjecture (a) pour $n \geq 21$; (b) pour $n = 5$ et B diagonale.

Alors que le problème avait été attaqué essentiellement par la méthode du cercle, Margulis prend une voie totalement différente, déduisant le théorème A du

THEOREME B. *Soient $G = \mathrm{Sl}(3, \mathbb{R})$, $\Gamma = \mathrm{Sl}(3, \mathbb{Z})$, et $\Omega = G/\Gamma$. Soient B_0 la forme $2x_1x_3 - x_2^2$ sur \mathbb{R}^3 et $H = 0(B_0)$ son groupe d'isométries, que l'on fait agir sur Ω . Alors, si l'orbite Hz est relativement compacte, H/H_z est compact, où H_z est le stabilisateur de z (de façon équivalente : toute orbite relativement compacte est compacte).*

Les théorèmes A et B ont été généralisés au cas d'un corps de nombres par A. Borel et G. Prasad [2].

Plan. Suivant de près [6], on démontre d'abord l'implication (facile) de A sur B. Ensuite (section 2), raisonnant par l'absurde, on réduit le théorème B à quatre lemmes (démontrés dans les sections 3 à 5) sur l'action de G et de certains de ses sous-groupes sur Ω :

— Les lemmes 1 et 2 sont des énoncés tout à fait généraux sur les actions d'un groupe de Lie sur un espace homogène.

— Le lemme 3 est le cœur de la preuve : il dit que, sous certaines conditions, une partie de Ω invariante et minimale pour l'action d'un sous-groupe unipotent est en fait invariante par un sous-groupe plus gros. Ceci est lié à une conjecture générale de M.S. Raghunathan ([3], [8]) : *Si G est un groupe de Lie (semi-simple ?), Γ un réseau et U un sous-groupe fermé unipotent connexe, alors l'adhérence d'une orbite de U dans $G\Gamma$ est toujours homogène, c'est-à-dire est l'orbite d'un sur-groupe de U .* Dans la preuve de ce lemme, le point clé (proposition (*)) porte sur l'existence de chemins de points fixes pour un sous-groupe unipotent du groupe linéaire.

— Le lemme 4 est une conséquence facile de la proposition (*).

1.— Le théorème B entraîne le théorème A.

Il suffit de montrer le théorème A pour $n = 3$, et l'on peut alors supposer $B = B_0 \circ g$, $g \in G$. Notons $z = B\mathbb{Z}^3$, alors :

— H/H_z , qui est homéomorphe à $O(B)/O(B) \cap \Gamma$, est non compact. En effet, l'irrationalité de B implique que $O(B) \cap \Gamma$ préserve une forme non multiple de B donc n'est pas Zariski-dense dans $O(B)$. Il suffit alors d'appliquer le théorème de densité de Borel [1].

— Supposons par l'absurde que $|B| \mathbb{Z}^3 \setminus \{0\}$ est minoré. Il en est alors de même pour $|B_0| z \setminus \{0\}$, donc pour $|B_0| hz \setminus \{0\}$ pour tout $h \in H$. On en déduit que les éléments de $hz \setminus \{0\}$ sont uniformément éloignés de 0, et le critère de compacité de Mahler implique alors que Hz est compact, ce qui contredit le théorème B. \square

2.- Réduction du théorème B.

Nous aurons besoin des sous-groupes suivants de G :

$$V_1 = \{v_1(t) = \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}, t \in \mathbb{R}\}, D = \{d(a) = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a^{-1} \end{pmatrix}, a > 0\}$$

$$V_2 = \{v_2(u) = \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, u \in \mathbb{R}\}, V = V_1 V_2.$$

Notons V_2^+ et V_2^- les sous-ensembles définis par $u > 0$ ou $u < 0$.

Propriétés.

- V est commutatif, D normalise V_1 , V_2 et V
- $N_G(V_1) = DV \approx \{\text{homothéties-translations de } \mathbb{R}^2\}$
- DV_1 est contenu dans H
- V_1 , V_2 et V sont unipotents. □

Dans les lemmes 1 et 2 suivants, G est un groupe localement compact, séparable pour le lemme 2, agissant sur un espace homogène Ω , et H est un sous-groupe fermé. Dans les lemmes 3 et 4, G , Ω et H reprennent leur signification antérieure.

LEMME 1. Soit $y \in \Omega$ tel que \overline{Hy} est compact et H -minimal et H/H_y n'est pas compact. On pose $M = \{g \in G \setminus H \mid gy \in \overline{Hy}\}$. Alors l'adhérence de M contient id.

LEMME 2. Soient F , P et P' des sous-groupes fermés de G tels que $F \subset P \cap P'$. Soient Y et Y' des parties fermées de Ω et M une partie de G . On suppose que :

- $PY = Y$ et $P'Y' = Y'$
- Y est compact et F -minimal
- $mY \cap Y' \neq \emptyset$ pour tout $m \in M$.

Alors pour tout $h \in N_G(F) \cap P'MP$ on a $hY \subset Y'$.

LEMME 3. Soit $Y = V_1y$ un compact V_1 -minimal tel que \overline{Hy} soit compact. Alors DY est contenu dans Y .

LEMME 4. Soit M une partie de $G \setminus H$ dont l'adhérence contient id . Alors $HMDV_1$ contient V_2^+ ou V_2^- .

Preuve du théorème B modulo les lemmes 1–4. Supposons par l'absurde qu'il existe z tel que \overline{Hz} est compact mais pas H/H_z . Alors X contient un fermé H -invariant minimal Y' , qui à son tour contient $Y = \overline{V_1y}$ V_1 -minimal. Il est clair que $\overline{Hy} = Y'$ est compact mais H/H_y ne l'est pas.

— Définissant M comme dans le lemme 1, on a donc $M \ni id$. D'après le lemme 4, on en déduit $HMDV_1 \supset V_2^+$ ou V_2^- , disons V_2^+ .

— Donc V_2^+ est contenu dans $N_G(V_1) \cap HMDV_1$; de plus, $DV_1Y \subset Y$ d'après le lemme 3, donc on peut appliquer le lemme 2 avec $F = V_1$, $P = DV_1$, $P' = H$. Il vient $V_2^+y \subset Y'$, donc Y' contient $DV_1V_2^+y$.

— Or $DV_1V_2^+y$ n'est jamais relativement compact : en effet, y contient un élément $u = (x_1, x_2, x_3)$ tel que $B_0(u) < 0 < x_3$. Posons $g(a) = d(a)v_2(-B_0(u)/2x_3^2)v_1(-x_2/x_3)$: c'est un élément de $DV_1V_2^+$ et le réseau $g(a)y$ contient $g(a)u = (0, 0, ax_3)$. Faisant tendre a vers 0, on voit que le critère de compacité de Mahler n'est pas vérifié.

On en déduit une contradiction puisque Y' est compact. □

3.— Preuve des lemmes 1 et 2.

1) Soit $U \subset G$ un ouvert relativement compact contenant id . On va montrer $U \cap M \neq \emptyset$:

— Soit $x \in \overline{Hy}$: la minimalité implique $y \in \overline{Hx}$, donc Uy rencontre Hx , soit $x \in HUy$. Ainsi $\overline{Hy} \subset HUy = \bigcup_{h \in H} hUy$.

— Par compacité, \overline{Hy} est recouvert par $\bigcup_{1 \leq i \leq N} h_i Uy$, $h_i \in H$.

— $K = \bigcup_{1 \leq i \leq N} h_i U$ est compact, donc il existe $h \in H \setminus KH_y$. Alors $hy \in \overline{Hy}$ donc il existe $i \in [1, N]$ et $u \in U$ tels que $hy = h_i u y$.

— Pour terminer la preuve, il suffit de montrer $u \in M$: d'abord, $uy = h_i^{-1}hy \in Hy$; ensuite, $u \notin H$, sinon on aurait $(h_i u)^{-1}h \in H_y$ et puisque $h_i u \in K$ on en déduirait $h \in KH_y$. □

2) Par hypothèse, on a $h = \lim p'_n m_n p_n$, où $p'_n \in P'$, $m_n \in M$, $p_n \in P$, et il existe $y_n \in Y$ tel que $m_n y_n \in Y'$. Alors $p_n^{-1} y_n \in PY \subset Y$. Comme Y est compact, on peut supposer que $p_n^{-1} y_n$ converge vers $z \in Y$, d'où

$$hz = \lim p'_n m_n p_n \cdot p_n^{-1} y_n = \lim p'_n m_n y_n \in Y'.$$

Enfin, la minimalité de Y implique $y \in Fz$, et $h \in N_G(F)$ implique $hy \in Fhz$. On en déduit $hy \in FY' = Y'$. \square

4.— Preuve du lemme 3.

Soient $M_1 = \{g \in G \setminus V_1 \mid gy \notin Y\}$, $A = N_G(V_1) \cap \overline{V_1 M_1 V_1}$ et $\Psi \subset G$ le sous-groupe fermé engendré par A . Notons que Ψ contient V_1 .

- 1) $\overline{M_1} \ni id$: en effet, d'après le lemme 1 il suffit de prouver que $V_1/(V_1)_y$ n'est pas compact, c'est-à-dire que $(V_1)_y = \{id\}$. Si au contraire $v_1(t)y = y$ avec $t \neq 0$, alors $(v_1(t)^2 - id)y \in y$, donc y contient un vecteur non nul de la forme $x_3 e_3$, ce qui contredit la compacité de Dy ($d(a)y \ni ax_3 e_3$, a aussi petit qu'on veut).
- 2) $\overline{\Psi y} \subset \overline{V_1 y}$: en effet, il suffit d'appliquer le lemme 2 avec $F = P = P' = V_1$, $Y' = Y$. On en déduit que :

- $\overline{\Psi y}$ est compact : en effet, il est contenu dans \overline{Hy} .
- Pour prouver le lemme 3, il suffit de prouver que Ψ contient D .

- 3) **Affirmation.** Si M_1 est une partie de $G \setminus N_G(V_1)$ telle que $\overline{M_1} \ni id$, alors l'adhérence de $(N_G(V_1) \cap \overline{V_1 M_1 V_1}) \setminus V_1$ contient id .

COROLLAIRE. $\overline{A \setminus V_1}$ contient id : en effet, d'après 1) il existe une suite $m_n \in M_1$ convergeant vers id . Si $m_n \in N_G(V_1)$ pour une infinité de n , c'est terminé, sinon on peut appliquer l'affirmation.

La preuve de l'affirmation (qui est en fait vraie pour tous les sous-groupes unipotents de G) repose sur les deux énoncés suivants :

a) *il existe une représentation de G dans un \mathbb{R} -espace vectoriel de dimension finie E et un point $p_0 \in E$ tels que $g \mapsto gp_0$ induit un plongement localement propre φ de G/V_1 dans E : il suffit de prendre $E = \mathbb{R}^3 \times \Lambda^2 \mathbb{R}^3 \times \mathfrak{q}$ ($\mathfrak{q} =$ formes quadratiques sur \mathbb{R}^3) avec l'action naturelle de G et $p_0 = (e_1, e_1 \wedge e_2, B_0)$.*

b) **PROPOSITION (*).** *Soient E un \mathbb{R} -espace vectoriel de dimension finie, $U \subset \mathrm{GL}(E)$ un sous-groupe unipotent connexe, L l'espace des points fixes de U . Soient $Y \subset E \setminus L$ et $p_0 \in L \cap Y$. Alors $UY \cap L$ contient un chemin polynomial non constant passant par p_0 .*

Preuve de la proposition (*). Nous nous restreindrons au cas où U est à un paramètre, le cas général étant tout à fait analogue : $U = \{u(t) = \exp(tN) \mid t \in \mathbb{R}\}$, où N est un endomorphisme nilpotent. Alors il existe des sous-espaces $L_0 = L, L_1, \dots, L_k$ tels que

$$\ker N^{i+1} = L_0 \oplus \dots \oplus L_i \quad (0 \leq i \leq k), \quad L_0 \oplus \dots \oplus L_k = E$$

$$N^i \text{ injecte } L_i \text{ dans } L \quad (0 \leq i \leq k).$$

Donc tout $x \in E$ s'écrit $x = \ell_0 + \dots + \ell_k$, $\ell_i \in L_i$, d'où

$$u(t)x = \ell_0 + tN(\ell_1) + \dots + (t^k/k!)N^k(\ell_k) + o(\max_{i \geq 1} t^i \|\ell_i\|),$$

où le o est uniforme pour $|t| \rightarrow \infty$.

Ensuite, par hypothèse il existe une suite $x_n \in Y$ qui tend vers p_0 :

– Ecrivant $x_n = \ell_{n,0} + \dots + \ell_{n,k}$, le fait que $Y \subset E \setminus L$ implique $\max_{i \geq 1} \|\ell_{n,i}\| > 0$, donc $\max_{i \geq 1} \|(t^i/i!)N^i(\ell_{n,i})\| = f_n(t)$ croît strictement de 0 à $+\infty$ pour $t \geq 0$. De plus, les $\ell_{n,i}$ tendent vers 0 pour $i \geq 1$ donc $\lim_{n \rightarrow \infty} f_n(t) = 0$ uniformément sur tout compact.

– Donc il existe un unique $\tau_n > 0$ tel que $f_n(\tau_n) = 1$, et l'on a $\lim \tau_n = +\infty$. En passant à une suite extraite, on peut supposer

$$(\forall i \in [0, k]) (\tau_n^i / i!) N^i(\ell_{n,i}) \rightarrow \ell_i \in L, \max_{1 \leq i \leq k} \|\ell_i\| = 1.$$

Il en résulte que $(\forall t \in \mathbb{R}) \lim u(t\tau_n)x_n = p_0 + t\ell_1 + \dots + t^k\ell_k$, donc ce chemin est à valeurs dans $UY \cap L$. \square

Preuve de l'affirmation. Considérant la représentation donnée par a), soit U l'image de V_1 et $Y = M_1 p_0 = \varphi(M_1 V_1 / V_1)$:

– On a $\varphi^{-1}(L) = N_G(V_1) / V_1$. En effet, l'injectivité de φ implique $G_{p_0} = V_1$, donc

$$[g] \in \varphi^{-1}(L) \Leftrightarrow (\forall v \in V_1) vgp_0 = gp_0 \Leftrightarrow g \in N_G(V_1).$$

– Donc $\varphi^{-1}(L)$ est disjoint de $M_1 V_1 / V_1$, et l'injectivité de φ implique que Y ne rencontre pas L . On peut donc appliquer la proposition (*), trouvant ainsi $p(t) \in \overline{V_1 Y} \cap L = \varphi(\overline{V_1 M_1 V_1 / V_1}) \cap L$.

– Comme φ est un plongement localement propre, on a $p(t) \in \varphi(V_1 M_1 V_1 / V_1)$ et l'on peut trouver un chemin continu $g(t) \in V_1 M_1 V_1$, $|t| < \epsilon$, tel que $g(0) = id$ et $g(t)p_0 = p(t)$. Comme $p(t) \in L$, on a $g(t) \in N_G(V_1)$ donc $g(t) \in A$.

– Si t est non nul et assez petit, on a $p(t) \neq p_0$ donc $g(t) \notin V_1$: donc $g(t) \in A \setminus V_1$ et comme $\lim_{t \rightarrow 0} g(t) = p_0$ l'affirmation est démontrée.

4) **Fin de la preuve du lemme 3.** Ψ est un sous-groupe fermé de DV contenant V_1 , et d'après 3) la composante connexe de l'identité contient strictement V_1 . Interprétant DV comme le groupe des homothéties-translations de \mathbb{R}^2 , on en déduit que l'un des deux cas suivants se produit :

- a) $\Psi = V$: c'est impossible car $D\Psi y$ est compact mais pas \overline{DVy} .
- b) Ψ contient $v_2(u_0)Dv_2(u_0)^{-1}$ pour un certain $u_0 \in \mathbb{R}$. Si $u_0 = 0$, Ψ contient D donc c'est terminé. Sinon, disons si $u_0 > 0$, on a

$$(\forall t > 0) D\Psi \ni d(-t)v_2(u_0)d(t)v_2(-u_0) = v_2(u_0/t^2 - u_0).$$

Donc $D\Psi$ contient V_2^* . Comme Ψ contient V_1 , il vient $D\Psi \supset DV_1V_2^*$ ce qui contredit la compacité de $\overline{D\Psi y}$. \square

5.— Preuve du lemme 4. L'application $g \mapsto B_0 \circ g^{-1}$ induit un isomorphisme d'espaces G -homogènes de G/H sur \mathfrak{q} , espace des formes quadratiques de signature $(1,2)$ et de déterminant 1. Il s'agit donc de prouver que $\overline{B_0 \circ MDV_1}$ contient $B_0 \circ V_2^*$ ou $B_0 \circ V_2^-$:

Remarquons d'abord que $B_0 \circ V_2^\pm = B_0 + \mathbb{R}^\pm x_3^2$ et que l'espace L des points fixes de V_1 dans \mathfrak{q} est engendré par B_0 et x_3^2 .

Ensuite, par hypothèse on a une suite $m_n \in M$ qui tend vers id , donc $B_0 \circ m_n$ est différent de B_0 et tend vers B_0 . Il y a deux cas :

- Si $B_0 \circ m_n \notin L$ pour tout n , alors $\overline{B_0 \circ M \setminus L}$ contient id . Appliquons la proposition (*) à $E = \mathfrak{q}$, $U = V_1$ (ou plutôt son image dans $GL(E)$) et $Y = B_0 \circ M \setminus L$: elle dit que $\overline{B_0 \circ MV_1}$ contient un chemin polynomial passant par B_0 , non constant, de la forme $a(t)B_0 + b(t)x_3^2$. Comme le déterminant est 1, on a $a(t) \equiv 1$ et les propriétés ($b(0) = 0$, b non constant) impliquent que $im(b)$ contient \mathbb{R}_+ ou \mathbb{R}_- , donc que $\overline{B_0 \circ MV_1}$ contient $B_0 + \mathbb{R}_+x_3^2$ ou $B_0 + \mathbb{R}_-x_3^2$.

- Sinon, il existe n tel que $B_0 \circ m_n = B_0 + \epsilon_n x_3^2$ avec $\epsilon_n \neq 0$. Donc $B_0 \circ MD$ contient $B_0 + \mathbb{R}_+x_3^2$ ou $B_0 + \mathbb{R}_-x_3^2$. \square

BIBLIOGRAPHIE

- [1] A. Borel.— *Density properties of certain subgroups of semisimple groups*, Annals of Math. 72 (1960), 179–188.
- [2] A. Borel et G. Prasad.— *Valeurs de formes quadratiques aux points entiers*, C.R.A.S. Paris, t. 307, Série I (1988), 217–220.
- [3] G. Dani.— *Orbits of horospherical flows*, Duke Math. J. 53 (1986), 178–188.
- [4] G. Dani et G.A. Margulis.— *Valeurs de formes quadratiques aux points entiers primitifs*, note aux C.R.A.S., (à paraître).
- [5] H. Davenport.— *Collected Works*, Acad. Press, London 1977, vol. III, 1004–1117.
- [6] G.A. Margulis.— *Formes quadratiques indéfinies et flots unipotents sur les espaces homogènes*, C.R.A.S. Paris, t. 304, Série I (1987), 249–252.
- [7] G.A. Margulis.— *Indefinite quadratic forms and unipotent flows on homogeneous spaces*, Semester on Dynamical Systems and Ergodic Theory, Banach Center Publ., Varsovie 1986 (à paraître).
- [8] G.A. Margulis.— *Lie groups and ergodic theory*, in Algebra : Some Current Trends, Varna 1986, Springer Lect. Notes 1352 (1988), 130–146.

Jean-Claude SIKORAV
UA 41169 Topologie
Mathématique, bât. 425,
Université Paris-Sud
91405 Orsay cedex 05

*Séminaire de Théorie des Nombres
Paris 1987-88*

p-ADIC HEIGHTS ON ABELIAN VARIETIES

Yuri G. ZARHIN

It has recently become clear that the construction of a *p*-adic height on an Abelian variety A eventually reduces to a splitting of the Hodge filtration of its de Rham cohomology. The present paper provides a natural description of this connection, based on the study of the universal vectorial extension of A , and of rigidified extensions of algebraic groups. Following a request of the editor, a detailed introduction to these topics has been included, in order to make the text as self-contained as possible.

0.— Notations.

Let k be a number field, i.e. a finite algebraic extension of the field \mathbb{Q} of rational numbers. If \mathfrak{p} is a place of k we write $k_{\mathfrak{p}}$ for the completion of k in the \mathfrak{p} -adic topology. If G is an algebraic k -group we write $G_{\mathfrak{p}}$ for the corresponding algebraic $k_{\mathfrak{p}}$ -group $G \otimes k_{\mathfrak{p}}$. Let \mathfrak{p} be a non-Archimedean place of k . Then we write $\mathcal{O}_{\mathfrak{p}}$ for the ring of all \mathfrak{p} -adic integers in $k_{\mathfrak{p}}$ and $\ell(\mathfrak{p})$ for the characteristic of the residue field at \mathfrak{p} . We write

$$\text{ord}_{\mathfrak{p}} : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}$$

for the discrete valuation map attached to \mathfrak{p} and normalized by the condition $\text{ord}_{\mathfrak{p}}(\ell(\mathfrak{p})) = 1$. Clearly, $\text{ord}_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}^*) = 0$ and $k_{\mathfrak{p}}$ is a finite algebraic extension of the field \mathbb{Q}_{ℓ} of ℓ -adic numbers where $\ell = \ell(\mathfrak{p})$. Clearly, $\mathcal{O}_{\mathfrak{p}}^*$ and $\ell = \ell(\mathfrak{p})$ generate the multiplicative subgroup of finite index in $k_{\mathfrak{p}}^*$.

The multiplicative group $k_{\mathfrak{p}}^*$ and the additive group $k_{\mathfrak{p}}$ have natural structures of one-dimensional commutative $k_{\mathfrak{p}}$ -Lie groups [1]. In particular, their Lie algebras $\text{Lie}(k_{\mathfrak{p}}^*)$ and $\text{Lie}(k_{\mathfrak{p}})$ are one-dimensional $k_{\mathfrak{p}}$ -vector spaces and we will identify them with $k_{\mathfrak{p}} t \frac{d}{dt}$ and $k_{\mathfrak{p}} \frac{d}{dt}$ respectively. Here the basis elements $t \frac{d}{dt}$ and $\frac{d}{dt}$ are canonical invariant derivations on $k_{\mathfrak{p}}^*$ and $k_{\mathfrak{p}}$ respectively. We write

$$\log : k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$$

for a branch of p -adic logarithm (recall that \mathfrak{p} is non-Archimedean). It is a local isomorphism of the $k_{\mathfrak{p}}$ -Lie groups, whose tangent map

$$d \log : \text{Lie}(k_{\mathfrak{p}}^*) = k_{\mathfrak{p}} t \frac{d}{dt} \rightarrow \text{Lie}(k_{\mathfrak{p}}) = k_{\mathfrak{p}} \frac{d}{dt}$$

transforms $t \frac{d}{dt}$ into $\frac{d}{dt}$ [1]. The branch \log is uniquely determined by the value $\log(\ell(\mathfrak{p}))$. If $\text{Log} : k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$ is another branch of the logarithm then $\text{Log} = \log + (\text{Log}(\ell(\mathfrak{p})) - \log(\ell(\mathfrak{p}))) \text{ord}_{\mathfrak{p}}$. Conversely, $\log + c \text{ord}_{\mathfrak{p}}$ is a branch of the logarithm for each $c \in k_{\mathfrak{p}}$.

1. – p -adic characters.

Let p be a prime and $\chi : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$ be a p -adic character, i.e. a continuous homomorphism from the multiplicative group $k_{\mathfrak{p}}^*$ to the additive group \mathbb{Q}_p . If \mathfrak{p} is Archimedean then, clearly, $\chi = 0$.

Let us assume that \mathfrak{p} is non-Archimedean. The character χ is called **unramified** if

$$\chi(\mathcal{O}_{\mathfrak{p}}^*) = 0.$$

Unramified χ is determined uniquely by the value $\chi(\ell(\mathfrak{p}))$; more precisely,

$$\chi = \chi(\ell(\mathfrak{p})) \text{ord}_{\mathfrak{p}}.$$

Notice, that if $\ell(\mathfrak{p}) \neq p$ then all $\chi : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$ are unramified.

1.1.— Now, let us assume that $\ell(\mathfrak{p}) = p$, i.e. $k_{\mathfrak{p}}$ is a p -adic field. Then $k_{\mathfrak{p}}^*$ and $k_{\mathfrak{p}}$ have natural structures of finite-dimensional commutative p -adic Lie groups, whose p -adic Lie algebras coincide with $\text{Lie}(k_{\mathfrak{p}}^*)$ and $\text{Lie}(k_{\mathfrak{p}})$ respectively; of course these algebras should be viewed as the \mathbb{Q}_p -vector spaces. Let $\chi : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$ be a p -adic character. Then it is a morphism of the P -adic Lie groups [1] and its (\mathbb{Q}_p -linear) tangent map

$$d\chi : \text{Lie}(k_{\mathfrak{p}}^*) = k_{\mathfrak{p}} t \frac{d}{dt} \rightarrow \text{Lie}(\mathbb{Q}_p) = \mathbb{Q}_p \frac{d}{dt}$$

is **not** zero if and only if χ is ramified.

Let us assume that χ is ramified. Then there exists a non-zero \mathbb{Q}_p -linear map $\delta : k_{\mathfrak{p}} \rightarrow \mathbb{Q}_p$ such that

$$d\chi(c t \frac{d}{dt}) = \delta(c) \frac{d}{dt} \text{ for } c \in k_{\mathfrak{p}}.$$

Since \mathbb{Q}_p is the one-dimensional \mathbb{Q}_p -vector space, δ is surjective.

Let us choose $u \in k_{\mathfrak{p}}$ such that $\delta(u) = \chi(p)$. And now, let us choose the branch

$$\log : k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$$

of the p -adic logarithm, such that $\log(p) = u$. I claim that

$$\chi = \delta \log.$$

Indeed, χ and $\delta \log$ are morphism $k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$, whose tangent maps coincide.

Clearly, this implies that $\chi = \delta \log$ on $\mathcal{O}_{\mathfrak{p}}^*$ because each open subgroup in the compact group $\mathcal{O}_{\mathfrak{p}}^*$ is of finite index, and \mathbb{Q}_p is uniquely divisible. On the other

side $\chi(P) = \delta \log(p)$. One has only to recall that \mathcal{O}_p^* and p generate a multiplicative subgroup of finite index in k_p^* , and \mathbb{Q}_p is uniquely divisible.

1.2.— Let $\rho = (\rho_{\mathfrak{p}})$ be a collection of p -adic characters $\rho_{\mathfrak{p}} : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$ where \mathfrak{p} runs through the set of all places of k . Clearly, $\rho_{\mathfrak{p}}$ is unramified for all but finitely many \mathfrak{p} ; this implies that if $c \in k^*$ then $\rho_{\mathfrak{p}}(c) = 0$ for all but finitely many \mathfrak{p} . We call ρ admissible if *the sum formula*

$$\sum_{\mathfrak{p}} \rho_{\mathfrak{p}}(c) = 0$$

holds for all $c \in k^*$; here the sum is taken over all places of k . One may view ρ as a continuous homomorphism from the idèle group of k into \mathbb{Q}_p ; clearly, ρ is admissible if and only if it kills the group of principal ideles.

2.— Main results.

Let A be an Abelian variety over k , A^t its dual Abelian variety, \mathcal{I} the universal extension of A^t by the vector group [14, 16]. Let $\rho = (\rho_{\mathfrak{p}})$ be an admissible collection of local p -adic characters.

The aim of this paper is to construct a canonical biadditive pairing

$$(1) \quad h = h(\rho) : \mathcal{I}(k) \times A(k) \rightarrow \mathbb{Q}_p.$$

The pairing h depends \mathbb{Q}_p -linearly on ρ .

Let us fix a splitting of the Hodge filtration of the first de Rham cohomology $H_{DR}^1(A_{\mathfrak{p}})$ for all \mathfrak{p} with ramified $\rho_{\mathfrak{p}}$. This data set allows us to construct *usual* P -adic biadditive height pairing [5, 9]

$$(2) \quad h' = h'(\rho) : A^t(k) \times A(k) \rightarrow \mathbb{Q}_p.$$

For A be the jacobian of a smooth projective curve with good reduction at all \mathfrak{p} with ramified $\rho_{\mathfrak{p}}$ the pairing (2) is also constructed in [2].

I learned from N. Katz and D. Bertrand the following two cases when a canonical choice of splittings of Hodge filtrations is possible.

I) $A_{\mathfrak{p}}$ has ordinary good reduction at all \mathfrak{p} with ramified $\rho_{\mathfrak{p}}$: one ought to take the unit root subspace for the action of Frobenius as the complement to the differentials of first kind (cf. Katz [12]).

II) A is of CM -type over k : one ought to take splittings invariant under the action of complex multiplications (see the work of Gross quoted in [15] in the elliptic case).

So, in both these cases we have canonical p -adic height pairing. The existence of this pairing is known in the case of ordinary reductions [5, 9], and, probably, the pairing (2) coincides with the pairing described in [5, 9]; see also [13]. The existence of canonical p -adic height pairing for Abelian varieties of CM -type seems to be a new result (except, may be, the elliptic curve case [8]).

This paper grows up from an attempt to translate Néron's article [7] into the language of author's paper [11]; the latter in turn, arised from an answer to a question, posed by Manin's article [4]. The results of the present paper were obtained in 1984 and reported on the Shafarevich Seminar in Autumn of 1984. I am deeply grateful to Yu. I. Manin, I.R. Shafarevich, A.N. Parshin, D. Bertrand, L. Breen, N. Katz and C. Goldstein for their interest to this paper, helpful discussions and encouragement. This publication is a result of author's stay in Orsay in January–February of 1988 and I am very happy to be able to thank the University of Orsay for the hospitality.

3.– Rigidified extensions.

In order to construct the pairing (1) we need to work out the notion of rigidified extension of algebraic and Lie groups.

Let K be a commutative field of characteristic zero, B an Abelian variety over K , B^t its dual Abelian variety. Recall [3, 6, 10] that a connected commutative algebraic K -group X is called an extension of B by the multiplicative group \mathbb{G}_m if X contains \mathbb{G}_m as a closed subgroup and we have an isomorphism $X/\mathbb{G}_m \simeq B$ of algebraic K -groups. In other words, X sits in a short exact sequence

$$(3) \quad 0 \longrightarrow \mathbb{G}_m \longrightarrow X \xrightarrow{\pi} B \longrightarrow 0$$

where $\mathbb{G}_m = \text{Ker } \pi$ and π induces an isomorphism $X/\mathbb{G}_m \xrightarrow{\sim} B$.

This implies that the sequence of the corresponding Lie algebras

$$(4) \quad 0 \longrightarrow \text{Lie}(\mathbb{G}_m) \longrightarrow \text{Lie}(X) \xrightarrow{d\pi} \text{Lie}(B) \longrightarrow 0$$

induced by (3), is also exact. Hereafter, if G is a commutative algebraic K -group, we write $\text{Lie}(G)$ for its Lie algebra ; if u is a morphism of commutative algebraic K -groups, we write du for the corresponding K -linear map of their Lie algebras. Clearly, $\text{Lie}(G)$ is just a finite-dimensional K -vector space. For example, $\text{Lie}(\mathbb{G}_m)$ is a one-dimensional K -vector space, and we will identify it with $K t \frac{d}{dt}$ where $t \frac{d}{dt}$ is the canonical invariant derivation on $\mathbb{G}_m = \text{spec } K[t, t^{-1}]$.

A **rigidification** of the extension (3) is, by definition [6], a splitting of the short exact sequence (4) of the K -vector spaces. Of course, these splittings exist and constitute a torsor over the K -vector space

$$\text{Hom}_K(\text{Lie}(B), \text{Lie}(\mathbb{G}_m)).$$

There are two equivalent ways to define a splitting of (4). The first one [6] is to define a section, i.e. a K -linear map $r : \text{Lie}(B) \rightarrow \text{Lie}(X)$ such that the composition

$$d\pi \circ r : \text{Lie}(B) \rightarrow \text{Lie}(X) \rightarrow \text{Lie}(B)$$

is the identity map. Clearly, r is an injection and $\text{Im } r \cap \text{Lie}(\mathbb{G}_m) = \{0\}$. Hereafter, we view $\text{Lie}(\mathbb{G}_m)$ as the one-dimensional K -vector subspace of $\text{Lie}(X)$. Clearly, we have $\text{Lie}(X) = \text{Lie}(\mathbb{G}_m) \oplus \text{Im } r$.

The second way is to define a projection, i.e. a K -linear map $w : \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{G}_m)$, whose restriction to $\text{Lie}(\mathbb{G}_m)$ is the identity map. Clearly, w is surjective, $\text{Ker } w \cap \text{Lie}(\mathbb{G}_m) = \{0\}$ and $\text{Lie}(X) = \text{Lie}(\mathbb{G}_m) \oplus \text{Ker } w$. Of course, these two ways are related by the formula $\text{Im } r = \text{Ker } w$.

Now, we describe the *third* way.

Dividing w by $t \frac{d}{dt}$ we obtain a K -linear functional $\varphi : \text{Lie}(X) \rightarrow K$ such that $\varphi(t \frac{d}{dt}) = 1$ for $t \frac{d}{dt} \in \text{Lie}(\mathbb{G}_m) \subset \text{Lie}(X)$ and

$$\varphi(v) t \frac{d}{dt} = w(v) \quad \text{for } v \in \text{Lie}(X).$$

Recall that the K -vector space of all K -linear functionals on $\text{Lie}(X)$ is just $\Omega^1(X)$. Hereafter, if G is a commutative algebraic K -group, we write $\Omega^1(G)$ for the K -vector space of all invariant differentials on G ; one may naturally identify $\Omega^1(G)$ with the space of all K -linear functionals on $\text{Lie}(G)$. For example, $\Omega^1(\mathbb{G}_m) = K \frac{dt}{t}$ and the basic invariant differential $\frac{dt}{t}$ defines the K -linear map $\frac{dt}{t} : \text{Lie}(\mathbb{G}_m) = K t \frac{d}{dt} \rightarrow K$, $ct \frac{d}{dt} \mapsto c$, i.e. $\frac{dt}{t}(t \frac{d}{dt}) = 1$. For B the space $\Omega^1(B)$ is just the space of all differentials of first kind on B .

So, $\varphi \in \Omega^1(X)$ and the value $\varphi(t \frac{d}{dt}) = 1$. This implies that the restriction of φ to \mathbb{G}_m coincides with $\frac{dt}{t} \in \Omega^1(\mathbb{G}_m)$. Clearly, φ uniquely determined the rigidification w . Conversely, each invariant differential $\varphi \in \Omega^1(X)$, whose restriction to \mathbb{G}_m coincides with $\frac{dt}{t}$, defines certain rigidification

$$w : \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{G}_m), \quad v \mapsto \varphi(v) t \frac{d}{dt}.$$

Let X' be an extension of B by \mathbb{G}_m , sitting in the short exact sequence

$$(5) \quad 0 \longrightarrow \mathbb{G}_m \longrightarrow X' \xrightarrow{\pi'} B \longrightarrow 0$$

and

$$(6) \quad 0 \longrightarrow \text{Lie}(\mathbb{G}_m) \longrightarrow \text{Lie}(X') \xrightarrow{d\pi'} \text{Lie}(B) \longrightarrow 0$$

is the corresponding exact sequence of the Lie algebras. Let $X \wedge X'$ be the Baer sum of the extensions (3) and (5), sitting in the short exact sequence

$$(7) \quad 0 \longrightarrow \mathbb{G}_m \longrightarrow X \wedge X' \xrightarrow{\pi \wedge \pi'} B \longrightarrow 0$$

(see [6, 3, 10].

Then the corresponding extension of the Lie algebras

$$(8) \quad 0 \longrightarrow \text{Lie}(\mathbb{G}_m) \longrightarrow \text{Lie}(X \wedge X') \xrightarrow{d(\pi \wedge \pi')} \text{Lie}(B)$$

is the Baer sum of the extensions (4) and (6). In particular,

$$(9) \quad \text{Lie}(X \wedge X') = \{(u, c') \in \text{Lie}(X) \oplus \text{Lie}(X') \mid d\pi(u) = d\pi'(u')\} / \{(v, -v) \mid v \in \text{Lie}(\mathbb{G}_m)\}.$$

Let

$$w : \text{Lie}(X) \longrightarrow \text{Lie}(\mathbb{G}_m), \quad w' : \text{Lie}(X') \longrightarrow \text{Lie}(\mathbb{G}_m)$$

be the rigidifications of X and X' respectively. Clearly, the map

$$(u, u') \mapsto w(u) + w'(u'), \quad (u, u') \in \text{Lie}(X) \oplus \text{Lie}(X'), \quad d\pi(u) = d\pi'(u')$$

induces certain rigidification

$$w \wedge w' : \text{Lie}(X \wedge X') \longrightarrow \text{Lie}(\mathbb{G}_m),$$

which we will call the Baer sum of w and w' .

Since all \mathbb{G}_m -torsors are trivial, the sequences (3), (5) and (7) induce short exact sequences of the groups of K -points

$$(10) \quad 0 \longrightarrow K^* \longrightarrow X(K) \longrightarrow B(K) \longrightarrow 0$$

$$(11) \quad 0 \longrightarrow K^* \longrightarrow X'(K) \xrightarrow{\pi'} B(K) \longrightarrow 0$$

$$(12) \quad 0 \longrightarrow K^* \longrightarrow X \wedge X'(K) \xrightarrow{\pi \wedge \pi'} B(K) \longrightarrow 0.$$

Using once more the triviality of \mathbb{G}_m -torsors and explicit description of $X \wedge X'$, one easily obtains that the extension (12) is the Baer sum of the extensions (10) and (11). In particular,

$$(13) \quad X \wedge X'(K) = \{(x, x') \in X'(K) | \pi x = \pi' x'\} / \{(c, c^{-1}) | c \in K^*\}.$$

A pair (X, w) , consisting of an extension (3) and its rigidification w , is called a **rigidified extension** of B by \mathbb{G}_m . The set $\text{Ext Rig}(B, \mathbb{G}_m)$ of all isomorphism classes of rigidified extensions forms a commutative group with the Baer sum as group law [6]. The forgetful map $(X, w) \mapsto X$ induces the surjective homomorphism $\text{Ext Rig}(B, \mathbb{G}_m) \rightarrow \text{Ext}(B, \mathbb{G}_m)$ into the commutative group $\text{Ext}(B, \mathbb{G}_m)$ of all isomorphism classes of extensions of B by \mathbb{G}_m . This homomorphism sits in the short exact sequence

$$(14) \quad 0 \rightarrow \Omega^1(B) \rightarrow \text{Ext Rig}(B, \mathbb{G}_m) \rightarrow \text{Ext}(B, \mathbb{G}_m) \rightarrow 0$$

of commutative groups [6]. Here

$$\Omega^1(B) = \text{Hom}_K(\text{Lie}(B), K) \simeq \text{Hom}_K(\text{Lie}(B), \text{Lie}(\mathbb{G}_m))$$

is canonically isomorphic to the set of all rigidifications of the trivial extension $X = B \times \mathbb{G}_m$. Namely, to $\psi \in \Omega^1(B)$ corresponds the rigidification

$$\text{Lie}(X) = \text{Lie}(B) \oplus \text{Lie}(\mathbb{G}_m) \rightarrow \text{Lie}(\mathbb{G}_m), (u, v) \mapsto \psi(u)t \frac{d}{dt} + v.$$

Recall [6] that the universal extension of B^t by a vector group is a connected commutative algebraic K -group I , sitting in the short exact sequence of commutative algebraic K -groups.

$$(15) \quad 0 \rightarrow \underline{\omega}_B \rightarrow I \rightarrow B^t \rightarrow 0,$$

where $\underline{\omega}_B$ is the K -vector group attached to $\Omega^1(B)$. This means that the K -algebraic group $\underline{\omega}_B$ is isomorphic to $\mathbb{G}_a^{\dim(B)}$, where \mathbb{G}_a is the additive

K -group, and $\underline{\omega}_B(K) = \Omega^1(B)$. The corresponding sequence of Lie algebras is also exact and coincide with the Hodge filtration [6]

$$(16) \quad 0 \rightarrow \Omega^1(B) \rightarrow H_{DR}^1(B) \rightarrow \text{Lie}(B^t) \rightarrow 0$$

of the first de Rham cohomology group of B (recall that $\text{Lie}(I) = H_{DR}^1(B)$ [6] and $\text{Lie}(B^t) = H^1(B, \mathcal{O}_B)$).

Since all \mathbb{G}_a -torsors are trivial, the sequence (15) induces a short exact sequence of the groups of K -points

$$(17) \quad 0 \rightarrow \Omega^1(B) \rightarrow I(K) \rightarrow B^t(K) \rightarrow 0,$$

and it is known [6] that the sequence (17) is canonically isomorphic to the sequence (14), i.e., there is the canonical commutative diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & \Omega^1(B) & \rightarrow & \text{Ext Rig } (B, \mathbb{G}_m) & \rightarrow & \text{Ext}(B, \mathbb{G}_m) \rightarrow 0 \\ & & \parallel & & | \wr & & | \wr \\ 0 & \rightarrow & \Omega^1(B) & \rightarrow & I(K) & \rightarrow & B^t(K) \rightarrow 0. \end{array}$$

Here $\text{Ext}(B, \mathbb{G}_m) \simeq B^t(K)$ is the canonical Weil–Barsotti isomorphism [10, 3]. So, we may and will identify $I(K)$ with $\text{Ext Rig}(B, \mathbb{G}_m)$.

3.1.— Rigidified extensions of Lie groups.

Now, assume that K is complete with respect to a non-discrete non-Archimedean absolute value. If G is a commutative algebraic K -group, then $G(K)$ has a natural structure of finite-dimensional commutative K -Lie group and one may naturally identify $\text{Lie}(G)$ with the Lie algebra $\text{Lie}(G(K))$ of $G(K)$. Hereafter, if H is a finite-dimensional commutative K -Lie group, then we write $\text{Lie}(H)$ for its Lie algebra. If u is a morphism of commutative K -Lie groups, then we write du for the corresponding K -linear map of their Lie algebras (if u is induced by a morphism of algebraic K -groups, then algebraic and analytic definitions of du coincide. Until the end of Section 3 all the Lie groups will be finite-dimensional commutative K -Lie groups, and we will write just ...Lie group... instead of ...finite-dimensional commutative K -Lie group...).

A Lie group H is called **good** if for each open subgroup $H' \subset H$ the quotient H/H' is a torsion group. For example, each compact H is good ; indeed, H/H' is a compact discrete group, and, therefore, finite.

The following assertion will be proved in Section 6.

3.1.1.– LEMMA. *Let H and D be Lie groups, $\text{Mor}(H,D)$ the commutative group of all morphisms $u : H \rightarrow D$. If H is good and D is uniquely divisible, then the natural map*

$$d : \text{Mor}(H,D) \rightarrow \text{Hom}_K(\text{Lie}(H), \text{Lie}(D)) , \quad u \mapsto du$$

is bijective.

3.1.2.– Let

$$(18) \quad 0 \rightarrow F \rightarrow E \xrightarrow{\pi} H \rightarrow 0$$

be an exact sequence of Lie groups, i.e. one may identify F with a closed Lie subgroup of E , and π induces an isomorphism of Lie groups $E/F \cong H$.

The sequence (18) induces a short exact sequence of the corresponding Lie algebras

$$(19) \quad 0 \longrightarrow \text{Lie}(F) \longrightarrow \text{Lie}(E) \xrightarrow{d\pi} \text{Lie}(H) \longrightarrow 0$$

which is just a sequence of K -vector spaces. We define a rigidification of the extension (18) as a splitting of the short exact sequence (19). Of course, such splittings exist and constitute a torsor over the K -vector space $\text{Hom}_K(\text{Lie}(H), \text{Lie}(F))$. As above, there are two equivalent ways to describe a splitting of (19) :

I) to choose a K -linear section $r : \text{Lie}(H) \rightarrow \text{Lie}(E)$ such that the composition $d\pi r$ is the identity map on $\text{Lie}(H)$;

II) to choose a K -linear projection $w : \text{Lie}(E) \rightarrow \text{Lie}(F)$, whose restriction to $\text{Lie}(F)$ is the identity map. Here we identify $\text{Lie}(F)$ with its image in $\text{Lie}(E)$.

Of course, we have $\text{Im } r = \text{Ker } w$ and

$$\text{Lie}(E) = \text{Lie}(F) \oplus \text{Im } r = \text{Lie}(F) \oplus \text{Ker } w .$$

Remark : Each (algebraic) rigidification of (3) is an (analytic) rigidification of (10).

The following theorem will be proved in Section 6. See Lemma 1 of [15] for results of a similar nature.

3.1.3.—THEOREM. *Let us assume that H is good and F is uniquely divisible. Then :*

a) the sequence (18) of Lie groups splits ;

b) let Spl be the set of all splittings $q : E \rightarrow F$ of the extension (18), i.e. the set of all morphisms of Lie groups $q : E \rightarrow F$ such that the restriction of q to F is the identity map. Then Spl is a torseur over

$$\text{Mor}(H, F) \xrightarrow{\sim} \text{Hom}_K(\text{Lie}(H), \text{Lie}(F)) ;$$

c) the map

$$q \mapsto w = dq : \text{Lie}(E) \rightarrow \text{Lie}(F)$$

defines a bijection between Spl and the set Rig of all rigidifications $w : \text{Lie}(E) \rightarrow \text{Lie}(F)$. This bijection is an isomorphism of $\text{Hom}_K(\text{Lie}(H), \text{Lie}(F))$ -torseurs.

3.1.4.—Remark : Let q be as in Theorem 3.1.3. Then $\text{Ker } q$ is a closed Lie subgroup in E and the restriction of π to $\text{Ker } q$ defines an isomorphism of Lie groups $\pi : \text{Ker } q \xrightarrow{\sim} H$. Its inverse $R : H \xrightarrow{\sim} \text{Ker } q \subset E$ is a section of (18) and the corresponding tangent map $dR : \text{Lie}(E) \rightarrow \text{Lie}(E)$ is a section of (19) attached to the rigidification $w = dq$, i.e., $\text{Im } dR = \text{Ker } w$.

3.1.5.—Example : Let us assume that K is locally compact (e.g., $K = k_{\mathfrak{p}}$ for some non-Archimedean place of k). Since the Abelian variety B^t is projective, $B^t(K)$ is compact and, therefore, a good Lie group. So, (17) is the extension of good $B^t(K)$ by the uniquely divisible K -vector space $\Omega^1(B)$. Applying Theorem 3.1.3 and Remark 3.1.4 to the extensions (17) and (16) we obtain that each splitting of the Hodge filtration (16) on $H_{DR}^1(B)$ defines a certain splitting $B^t(K) \rightarrow I(K)$ of the extension (17).

3.1.6. Remark : Let us assume that F is discrete, i.e. $\text{Lie}(F) = 0$. Then there is exactly one splitting of the extension (19). So, under assumptions of Theorem 3.1.3 we obtain a unique canonical splitting of the extension (18).

The following assertion is a generalization of Theorem 3.1.3, (see also [15], Lemma 1).

3.1.7.— THEOREM. Let us assume that H is good and F is an arbitrary finite-dimensional commutative K -Lie group. Let D be uniquely divisible Lie group and $\chi : F \rightarrow D$ be a morphism of Lie groups. Then one can extend uniquely χ to a morphism

$$\gamma(\chi, w) : E \rightarrow D$$

of Lie groups, in such a way that

$$d\gamma(\chi, w) = d\chi w : \text{Lie}(E) \rightarrow \text{Lie}(F) \rightarrow \text{Lie}(D).$$

If $\chi' : F \rightarrow D$ is a morphism of Lie groups then $\gamma(\chi + \chi', w) = \gamma(\chi, w) + \gamma(\chi', w)$, (we write the group law in D additively).

We will prove this Theorem in Section 6. Notice only that the equality

$$\gamma(w, \chi + \chi') - \gamma(w, \chi) - \gamma(w, \chi') = 0$$

is an immediate corollary of the uniqueness of $\gamma(\cdot, w)$, applied to the zero morphism $F \rightarrow D$.

3.1.8.— Remark : Let us assume that D is discrete, i.e. $\text{Lie}(D) = 0$. Then $d\chi = 0$ for all $\chi : F \rightarrow D$. This implies that $d\gamma(\chi, w) = d\chi w = 0$ for all rigidifications w . In particular, $d\gamma(\chi, w)$ does not depend on the choice of w . Now, the uniqueness of $\gamma(\chi, w)$, claimed by Theorem 3.1.7, implies that $\gamma(\chi, w)$ also does not depend on the choice of w .

3.1.9. In the last part of this section we will briefly discuss Baer sums of rigidified extensions of Lie groups. Let

$$(20) \quad 0 \longrightarrow F \longrightarrow E' \xrightarrow{\pi'} H \longrightarrow 0$$

be an extension of Lie groups, and

$$(21) \quad 0 \longrightarrow \text{Lie}(F) \longrightarrow \text{Lie}(E') \xrightarrow{d\pi'} \text{Lie}(H) \longrightarrow 0$$

the corresponding exact sequence of their Lie algebras. Let

$$(22) \quad 0 \longrightarrow F \longrightarrow E \wedge E' \xrightarrow{\pi \wedge \pi'} H \longrightarrow 0$$

be the Baer sum of the extensions (18) and (20), and

$$(23) \quad 0 \rightarrow \text{Lie}(F) \rightarrow \text{Lie}(E \wedge E') \xrightarrow{d(\pi \wedge \pi')} \text{Lie}(H) \rightarrow 0$$

be the corresponding exact sequence of Lie algebras, which, in turn, is the Baer sum of the extensions (19) and (21). More precisely

$$E \wedge E' = \{(e, e') \in E \oplus E' \mid \pi e = \pi' e'\} / \{(f, f^{-1}) \mid f \in F\}$$

(we write group law in F multiplicatively),

$$\text{Lie}(E \wedge E') = \frac{\{(u, u') \in \text{Lie}(E) \oplus \text{Lie}(E') \mid d\pi(u) = d\pi'(u')\}}{\{(v, -v) \mid v \in \text{Lie}(F)\}}$$

If

$$w : \text{Lie}(E) \rightarrow \text{Lie}(F), \quad w' : \text{Lie}(E') \rightarrow \text{Lie}(F)$$

are rigidifications of E and E' respectively, then the map $(u, u') \mapsto w(u) + w'(u')$, $(u, u') \in \text{Lie}(E) \oplus \text{Lie}(E')$, $d\pi(u) = d\pi'(u')$ induces certain rigidification $w \wedge w' : \text{Lie}(E \wedge E') \rightarrow \text{Lie}(F)$, which we call the Baer sum of w and w' .

Remark : Let

$$w : \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{G}_m), \quad w' : \text{Lie}(X') \rightarrow \text{Lie}(\mathbb{G}_m)$$

be rigidifications of the extensions (3) and (5) respectively. Then w and w' are also rigidifications of the extensions (10) and (11) of the Lie groups and K -points. So, we have algebraic definition of the Baer sum $w \wedge w'$ as the rigidification of the extension (7) and the analytic one as the rigidification of the corresponding extension (12) of the Lie groups of K -points. Clearly, these two definitions of $w \wedge w'$ coincide.

Now, assume that H is good and $\chi : F \rightarrow D$ be a morphism in the uniquely divisible Lie group D . Then, in notations of Theorem 3.1.3, applied to E and E' the map

$$(e, e') \rightarrow \gamma(\chi, w)e + \gamma(\chi, w')e' , \quad (e, e') \in E \oplus E' , \quad \pi e = \pi' e'$$

induces the morphism $d : E \wedge E' \rightarrow D$, coinciding with χ on F and with the tangent map

$$d\alpha = d\chi(w \wedge w') : \text{Lie}(E \wedge E') \rightarrow D .$$

Now, the uniqueness, claimed by Theorem 3.1.7, implies that $\alpha = \gamma(\chi, \omega \wedge \omega')$.

4.— Local results.

Throughout this section \mathfrak{p} is a non-Archimedean place of k and $K = k_{\mathfrak{p}}$. Let B be an Abelian variety over $K = k_{\mathfrak{p}}$, X an extension (3) of B by \mathbb{G}_m . Recall that we have exact sequences of the commutative $k_{\mathfrak{p}}$ -Lie groups

$$(24) \quad 0 \rightarrow k_{\mathfrak{p}}^* \rightarrow X(k_{\mathfrak{p}}) \rightarrow B(k_{\mathfrak{p}}) \rightarrow 0$$

and of the corresponding $k_{\mathfrak{p}}$ -Lie algebras

$$(25) \quad 0 \longrightarrow \text{Lie}(\mathbb{G}_m) \longrightarrow \text{Lie}(X) \xrightarrow{d\pi} \text{Lie}(B) \longrightarrow 0$$

Recall also that

$$\text{Lie}(\mathbb{G}_m) = \text{Lie}(k_{\mathfrak{p}}^*) = k_{\mathfrak{p}} t \frac{d}{dt} , \quad \text{Lie}(X) = \text{Lie}(X(k_{\mathfrak{p}})) , \quad \text{Lie}(B) = \text{Lie}(B(k_{\mathfrak{p}})) .$$

Since B is projective, $B(k_{\mathfrak{p}})$ is compact and, therefore, good.

4.1.— THEOREM. *One can uniquely extend the discrete valuation map $\text{ord}_{\mathfrak{p}} : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}$ to a continuous homomorphism $X(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}$, which we will also denote by $\text{ord}_{\mathfrak{p}}$ and consider as a morphism $\text{ord}_{\mathfrak{p}} : X(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}$ of the $k_{\mathfrak{p}}$ -Lie group $X(k_{\mathfrak{p}})$ into the discrete $k_{\mathfrak{p}}$ -Lie group \mathbb{Q} .*

Proof : One has only to choose a rigidification of the extension (24) and to apply Theorem 3.1.7 and Remark 3.1.8 to $\chi = \text{ord}_{\mathfrak{p}} : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}$.

Remark : Of course, Theorem 4.1 is just the existence and uniqueness theorem for Néron pairings over $k_{\mathfrak{p}}$ (see [11], [3], [5]).

4.2.—LEMMA. *Let us assume that there exists an extension*

$$(26) \quad 0 \rightarrow \mathbb{G}_m \rightarrow \underline{X} \rightarrow \underline{B} \rightarrow 0$$

of commutative group schemes over $\text{spec } \mathcal{O}_{\mathfrak{p}}$, whose generic fiber coincides with the extension (3)

$$0 \rightarrow \mathbb{G}_m \rightarrow X \rightarrow B \rightarrow 0.$$

Here \mathbb{G}_m is the multiplicative group scheme over $\text{spec } \mathcal{O}_{\mathfrak{p}}$. Then $\underline{X}(\mathcal{O}_{\mathfrak{p}})$ is an open subgroup of $X(k_{\mathfrak{p}})$ and $\text{ord}_{\mathfrak{p}}$ kills $\underline{X}(\mathcal{O}_{\mathfrak{p}})$.

Proof : Since $\mathcal{O}_{\mathfrak{p}}$ is open in $k_{\mathfrak{p}}$, $\underline{X}(\mathcal{O}_{\mathfrak{p}})$ is an open subgroup of $X(k_{\mathfrak{p}})$. Notice that

$$\underline{X}(\mathcal{O}_{\mathfrak{p}}) \cap k_{\mathfrak{p}}^* = \mathbb{G}_m(\mathcal{O}_{\mathfrak{p}}) = \mathcal{O}_{\mathfrak{p}}^* \subset \text{Ker } \text{ord } \mathfrak{p}.$$

Since $\text{ord}_{\mathfrak{p}} : X(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}$ is the morphism into the discrete \mathbb{Q} , its kernel $\text{Ker } \text{ord}_{\mathfrak{p}}$ is an open subgroup of $X(k_{\mathfrak{p}})$. Let us put

$$U := k_{\mathfrak{p}}^* \underline{X}(\mathcal{O}_{\mathfrak{p}}) = \{cx \mid c \in k_{\mathfrak{p}}^*, x \in \underline{X}(\mathcal{O}_{\mathfrak{p}})\} \subset X(k_{\mathfrak{p}})$$

(we write the group law in $X(k_{\mathfrak{p}})$ multiplicatively). Clearly, U is open in $X(k_{\mathfrak{p}})$. I claim that $X(k_{\mathfrak{p}})/U$ is a torsion group. Indeed, since U is open, πU is open in $B(k_{\mathfrak{p}})$, because

$$d\pi : \text{Lie}(X(k_{\mathfrak{p}})) = \text{Lie}(X) \rightarrow \text{Lie}(B) = \text{Lie}(B(k_{\mathfrak{p}}))$$

is surjective (the sequence (25) is exact). Since $B(k_p)$ is compact, $B(k_p)/\pi U$ is a torsion group. Now, one has only to use the exactness of the sequence (24) and inclusion $k_p^* \subset U$.

Let us define a morphism of the k_p -Lie groups $\gamma : U \rightarrow \mathbb{Q}$ by the formula

$$\gamma(cx) = \text{ord}_p(c) \quad \text{for } c \in k_p^*, \quad x \in \underline{X}(\mathcal{O}_p).$$

Clearly, γ kills $\underline{X}(\mathcal{O}_p)$.

Since $X(k_p)/U$ is a torsion group and \mathbb{Q} is uniquely divisible, one can extend uniquely γ to a morphism $\gamma' : X(k_p) \rightarrow \mathbb{Q}$. Clearly, the restriction of γ' to k_p^* coincides with $\text{ord}_p : k_p^* \rightarrow \mathbb{Z}$ and γ' kills $\underline{X}(\mathcal{O}_p)$. Now, the uniqueness, claimed by Theorem 4.1, implies that $\gamma' = \text{ord}_p$. So, ord_p kills $\underline{X}(\mathcal{O}_p)$.

Remark : Compare Lemma 4.1 and its proof with ([5], Case 1.5.2, pp. 202–203).

4.3.—THEOREM. *Let us assume that $\ell(p) = p$ and let us fix a branch*

$$\log : k_p^* \rightarrow k_p$$

of the p -adic logarithm. Let

$$w : \text{Lie}(X(k_p)) = \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{G}_m) = \text{Lie}(k_p^*)$$

be a rigidification of the extensions (3) and (24). Then one can uniquely extend \log to a morphism of k_p -Lie groups $\gamma(\log, w) : X(k_p) \rightarrow k_p$ in such a way that

$$d\gamma(\log, w) = d \log w : \text{Lie}(X(k_p)) \rightarrow \text{Lie}(k_p^*) \rightarrow \text{Lie}(k_p).$$

Proof : One has only to apply Theorem 3.1.7 to the extension (24) and $\chi = \log : k_p^* \rightarrow k_p$.

4.3.1.– Remark : If $\text{Log} : k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$ is another branch of \mathfrak{p} -adic logarithm, then one may easily check that

$$\gamma(\text{Log}, w) = \gamma(\log, w) + (\text{Log}(p) - \log(p))\text{ord}_{\mathfrak{p}}.$$

(apply the uniqueness for $\gamma(\text{Log}, w)$ claimed by Theorem 3.1.7).

4.3.2.– Example. Let $X = B \times \mathbb{G}_m$ be the trivial extension of B by \mathbb{G}_m and

$$w : \text{Lie}(X) = \text{Lie}(B) \oplus \text{Lie}(\mathbb{G}_m) \rightarrow \text{Lie}(\mathbb{G}_m),$$

be the rigidification attached to $\psi \in \Omega^1(B)$. Then

$$\gamma(\log, w) : X(k_{\mathfrak{p}}) = B(k_{\mathfrak{p}}) \times k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$$

is defined by the formula

$$(b, c) \mapsto \psi(\log_{B(k_{\mathfrak{p}})}(b)) + \log(c)$$

where

$$\log_{B(k_{\mathfrak{p}})} : B(k_{\mathfrak{p}}) \rightarrow \text{Lie}(B(k_{\mathfrak{p}}))$$

is the everywhere defined logarithm map [1] on the compact \mathfrak{p} -adic Lie group $B(k_{\mathfrak{p}})$.

4.3.3.– Let $\ell(\mathfrak{p}) = p$ and $\chi : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$ be a **ramified** p -adic character. Then (Sect. 2) there exist a branch $\log : k_{\mathfrak{p}}^* \rightarrow k_{\mathfrak{p}}$ of the \mathfrak{p} -adic logarithm and a \mathbb{Q}_p -linear map $\delta : k_{\mathfrak{p}} \rightarrow \mathbb{Q}_p$ such that

$$\chi = \delta \log.$$

Let us put

$$\gamma(\chi, w) := \delta\gamma(\log, w) : X(k_{\mathfrak{p}}) \rightarrow k_{\mathfrak{p}} \rightarrow \mathbb{Q}_p .$$

Remark 4.3.1. implies that

$$\gamma(\chi, w) : X(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}_p$$

does not depend on the choice of the branch \log . Clearly, $\gamma(\chi, w)$ coincides with χ on $k_{\mathfrak{p}}^*$.

4.3.4.– Remark. If we consider $\gamma(\chi, w)$ as a morphism of p -adic Lie groups then its tangent map

$$d\gamma(\chi, w) : \text{Lie}(X(k_{\mathfrak{p}})) = \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{Q}_p) = \mathbb{Q}_p t \frac{d}{dt}$$

is the composition

$$d\chi \circ w : \text{Lie}(X) \rightarrow \text{Lie}(\mathbb{G}_m) = \text{Lie}(k_{\mathfrak{p}}^*) \rightarrow \text{Lie}(\mathbb{Q}_p) .$$

(see the definition of δ in Section 2).

So, one may construct $\gamma(\chi, w)$, applying Theorem 3.1.7 to $K = \mathbb{Q}_p$, the extension (24) of p -adic Lie groups and $\chi : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$.

5.– Global construction.

The aim of this section is to give an explicit construction of the pairing (1)

$$h = h(\rho) : \mathcal{I}(k) \times A(k) \rightarrow \mathbb{Q}_p ,$$

where $\rho = (\rho_{\mathfrak{p}})$ is an admissible collection of local \mathfrak{p} -adic characters $\rho_{\mathfrak{p}} : k_{\mathfrak{p}}^* \rightarrow \mathbb{Q}_p$. We start with a point $j \in \mathcal{I}(k)$ of the universal extension \mathcal{I} of A^t by a vector group, and a point $a \in A(k)$. Recall (Sect. 3) that j is a pair (Y, w) , consisting of an extension

$$(27) \quad 0 \rightarrow \mathbb{G}_m \rightarrow Y \rightarrow A \rightarrow 0$$

of A by \mathbb{G}_m and its rigidification $w : \text{Lie}(Y) \rightarrow \text{Lie}(\mathbb{G}_m)$.

Recall that the sequence (27) induces the exact sequence of the groups of k -points

$$(28) \quad 0 \rightarrow k^* \rightarrow Y(k) \rightarrow A(k) \rightarrow 0.$$

Let us choose a point y in $A(k)$ lying above a .

For each non-Archimedean place \mathfrak{p} of k the pair (Y, w) induces the extension $Y_{\mathfrak{p}} = Y \otimes k_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ by \mathbb{G}_m and its rigidification $w_{\mathfrak{p}}$. We have natural inclusions $Y(k) \subset Y_{\mathfrak{p}}(k_{\mathfrak{p}})$.

Let us put

$$h_{unr}(Y, y) = \sum_{\mathfrak{p}} \rho_{\mathfrak{p}}(\ell(\mathfrak{p})) \text{ord}_{\mathfrak{p}}(y) \in \mathbb{Q}_p$$

where the sum is taken over all non-Archimedean places \mathfrak{p} with unramified $\rho_{\mathfrak{p}}$.

Here $\text{ord}_{\mathfrak{p}} : Y(k_{\mathfrak{p}}) \rightarrow \mathbb{Q}$ is the morphism described in Theorem 4.1. Notice, that Lemma 4.2 implies that this sum is finite (compare with [5], p. 214).

The ramified part $h_r(j, a)$ is defined by the formula

$$h_r(j, y) = \sum_{\mathfrak{p}} \gamma(\rho_{\mathfrak{p}}, w_{\mathfrak{p}})(y) \in \mathbb{Q}_p$$

where the sum is taken over all non-Archimedean \mathfrak{p} with ramified $\rho_{\mathfrak{p}}$ (clearly, all such \mathfrak{p} constitute a finite set and $\ell(\mathfrak{p}) = p$ for all such \mathfrak{p}). Now, let us put

$$h(j, a) := h_{unr}(Y, y) + h_r(j, y)$$

The sum formula for ρ implies that $h(j, a)$ does not depend on the choice of y . Clearly, $h(j, a)$ depends additively on a . In order to check that $h(j, a)$ depends additively on j , one has only to apply results of Section 3.1.9.

5.1.— Recall that $\mathcal{I}(k)$ sits in the short exact sequence

$$(29) \quad 0 \rightarrow \Omega^1(A) \rightarrow \mathcal{I}(k) \rightarrow A^t(k) \rightarrow 0$$

and $\mathcal{I}(k) \rightarrow A^t(k)$ is just the forgetful map $(Y, w) \mapsto Y$. Notice, that the unramified part $h_{unr}(Y, y)$ depends only on Y and does not depend on w . In contrast, the ramified part of h depends on rigidification w_p of Y_p for all p with ramified ρ_p . Notice, that (Y_p, w_p) is a point of $\mathcal{I}_p(k_p)$ where \mathcal{I}_p is the universal extension of A_p by a vector group. The group $\mathcal{I}_p(k_p)$ sits in the short exact sequence of commutative k_p -Lie groups

$$(30) \quad 0 \rightarrow \Omega^1(A_p) \rightarrow \mathcal{I}_p(k_p) \rightarrow A_p^t(k_p) \rightarrow 0$$

Recall that $A_p^t(k_p) = A^t(k_p) \supset A^t(k)$.

Let us fix a splitting of the Hodge filtration on $H_{DR}^1(A_p)$ for all p with ramified ρ_p . According to Example 3.1.5 this choice defines splittings

$$r_p : A_p^t(k_p) \rightarrow \mathcal{I}_p(k_p)$$

of the extensions (30) for all p with ramified ρ_p . Now, we are ready to define a height pairing

$$h' = h'(\rho) : A^t(k) \times A(k) \rightarrow \mathbb{Q}_p.$$

Let a^t be a point of $A^t(k)$ and Y be the extension of A by \mathbb{G}_m attached to a^t . Then $r_p(a^t) \in \mathcal{I}_p(k_p)$ is a pair, consisting of the extension Y_p of A_p by \mathbb{G}_m and one of its rigidification w'_p (ρ_p is ramified). Now, we put

$$h'(a^t, a) = h_{unr}(Y, y) + \sum_p \gamma(\rho_p, w'_p)(y)$$

where the sum is taken over all p with ramified ρ_p .

6.— Lie groups : proofs.

The aim of this section is to prove results, announced in Sect. 3.1 (see also [15]).

6.1.— Proof of Lemma 3.1.1.

Surjectiveness of d . Let $v : \text{Lie}(H) \rightarrow \text{Lie}(D)$ be a K -linear map. Then [1] there exists an open subgroup H' of H and a morphism $u' : H' \rightarrow D$ with $du = v$. Since H is good, H/H' is a torsion group. Since D is uniquely divisible, one could extend uniquely u' to a morphism $u : H \rightarrow D$. Clearly, $du = du' = v$.

Injectiveness of d . Let $u : H \rightarrow D$ be a morphism with $du = 0$. Then there exists an open subgroup H' of H such that $u = 0$ on H' . Since H/H' is a torsion group and D is uniquely divisible, $u = 0$.

6.2.— Proof of Theorem 3.1.7. Existence. There is an open subgroup E' of E and a morphism $\gamma : E' \rightarrow D$ with $d\gamma = d\chi w$. Replacing, if necessary, E' by its open subgroup, we may and will assume that $\gamma = \chi$ on $E' \cap F$, because

$$d\gamma = d\chi \circ = d\chi \text{ on } \text{Lie}(F) \subset \text{Lie}(E).$$

Let us put

$$U = E' F = \{ef \mid e \in E', f \in F\} \subset E$$

(we write the group law on E multiplicatively). Clearly, U is an open subgroup of E , containing E' and F . Let us extend γ to U by the formula

$$\gamma(ef) = \gamma(e)\chi(f) \quad \text{for } e \in E', f \in F.$$

Clearly, $\gamma : U \rightarrow D$ is a morphism of the Lie groups and $d\gamma = d\chi w$. I claim that E/U is a torsion group. Indeed, since U is open, πU is open in H , because $d\pi : \text{Lie}(E) \rightarrow \text{Lie}(H)$ is surjective. Since H is good, $H/\pi U$ is a torsion group. Now, one has only to use the exactness of the sequence (18) and inclusion $F \subset E'$.

So, E/U is a torsion group. Since D is uniquely divisible, one could extend uniquely $\gamma : U \rightarrow D$ to a morphism of Lie groups $\gamma(\chi, w) : E \rightarrow D$. Clearly, $d\gamma(\xi, w) = d\gamma = d\chi w$.

Uniqueness. Let $\gamma' : E \rightarrow D$ be a morphism of Lie groups such that $d\gamma' = d\chi|_w$ and $\gamma' = \chi$ on F . Then the difference

$$\gamma' - \gamma(\chi, w) : E \rightarrow D$$

(we write the group law on D additively) factors through H and has tangent map

$$d(\gamma' - \gamma(\chi, w)) = 0.$$

Applying Lemma 3.1.1, we obtain that

$$\gamma' - \gamma(\chi, w) = 0, \text{ i.e., } \gamma' = \gamma(\chi, w).$$

6.3.— Proof of Theorem 3.1.3. The assertion χ is a special case of Theorem 3.1.7 for $F = D$ and χ the identity map. The assertion a is an immediate corollary of the assertion e .

The assertion b is trivial.

Manuscrit reçu le 30 août 1988

BIBLIOGRAPHY

- [1] N. Bourbaki.— *Groupes et algèbres de Lie*, Chapitre 3, Hermann, Paris, 1972.
- [2] R. Coleman and B. Gross.— *p-adic heights on curves*, Preprint, MSRI, Berkeley, August, 1987.
- [3] S. Lang.— *Fundamentals of diophantine geometry*, Springer—Verlag, 1983.
- [4] Yu.I. Manin.— *The refined structure of the Néron-Tate height*, Math. Sbornik 83 (1970), 332–248 (Math. USSR Sbornik 12 (1971), 325–342).
- [5] B. Mazur and J. Tate.— *Canonical height pairings via biextensions*, Arithmetic and Geometry (vol. 1), Progress in Mathematics (Birkhäuser) 35 (1983), 195–238.
- [6] W. Messing.— *The universal extension of an abelian variety by a vector group*. Symposia Mathematica 11 (1973), 359–372.
- [7] A. Néron.— *Hauteurs et fonctions theta*, Rend. Sci. Mat. Milano 46 (1976), 111–135.
- [8] B. Perrin-Riou.— *Hauteurs p-adiques*, Séminaire de théorie des nombres, Paris 1982–83, Progress in Mathematics (Birkhäuser) 51 (1984), 233–257.
- [9] P. Schneider.— *p-adic height pairings*, I, II, Invent. Math. 69 (1982), 401–409 ; 79 (1985), 329–374.
- [10] J.-P. Serre.— *Groupes algébriques et corps de classes*, Hermann, Paris, 1958.
- [11] Yu.G. Zarhin.— *Néron pairing and quasicharacters*, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 497–509 (Math. USSR Izvestija, 6 (1972), 491–503).
- [12] N. Katz (with an appendix by L. Illusie).— *Internal reconstruction of the unit root F-crystal via expansion coefficients*, Annales Sci. ENS (4), 18 (1985), 245–268 (269–285).

- [13] H. Imai.— *On the p -adic heights of some abelian varieties*, Proc. Amer. Math. Soc. 100 (1987), 1–7.
- [14] M. Rosenlicht.— *Extensions of vector groups by Abelian varieties*, Amer. J. of Math. 80 (1958), 685–714.
- [15] J. Oesterlé.— *Constructions de hauteurs archimédiennes et p -adiques suivant la méthode de Bloch*, Séminaire de Théorie des Nombres, Paris 1980–81, Birkhäuser Prog. Math., 22, 1982, 175–192.

Yu.G. Zarhin
The USSR Academy of Sciences
Research Computing Center
Pushchino Moscow Region
142292 USSR

ERRATUM A

Diagonale de fractions rationnelles

par G. Christol

(Séminaire de Théorie des Nombres 1986–87)

La démonstration de la proposition 5.1 comporte une erreur, signalée et rectifiée par Yves André. Voici une version corrigée de la fin de cette démonstration (à partir de la page 84, ligne 15).

On constate que $f(0, \dots, 0)$ est le "résidu en \mathcal{P} " de la forme différentielle $\omega^{\wedge} f^*(d\pi/\pi)$. Maintenant, en notant \mathcal{R} l'application résidu de Poincaré (cf. [24] p. 232) on obtient une application :

$$\theta : \Omega_{X/\mathcal{C}}^r < Y > \xrightarrow{\hat{f}^*(d\pi/\pi)} \Omega_X^{r+1} < Y > \xrightarrow{\mathcal{R}} (a_{r+1})_* \Omega_Y^0 (r+1)$$

qui s'annule sur $d(\Omega_{X/\mathcal{C}}^{r-1} < Y >)$ et se prolonge donc en une application :

$$\Omega_{X/\mathcal{C}}^r < Y > \xrightarrow{\theta} (a_{r+1})_* \Omega_Y^r (r+1)$$

qui donne une application :

$$\mathbb{R}^r f_*(\Omega_{X/\mathcal{C}}^r < Y >) \xrightarrow{\theta} \mathbb{R}^0 f_*((a_{r+1})_* \Omega_Y^r (r+1)) = (fa_{r+1})_* \Omega_Y^0 (r+1).$$

On voit alors que $\delta_{\mathcal{P}}(\bar{\omega})$ est non nul si l'en est ainsi de $\theta(\bar{\omega})$. Maintenant le faisceau $\mathbb{R}^p f_*(\Omega_{X/\mathcal{C}}^r < Y >)$ est localement libre, ([24] théorème 2.18), on a donc l'isomorphisme suivant :

$$\mathbb{H}^r(Y, \Omega_{X/\mathcal{C}}^r < Y > \otimes \mathcal{O}_Y) \cong \mathbb{R}^r f_*(\Omega_{X/\mathcal{C}}^r < Y >) \otimes \mathcal{O}_P / \mathcal{M}_P$$

et on obtient une application :

$$\mathbb{H}^r(Y, \Omega_{X/\mathcal{G}}^{<Y>} \otimes \mathcal{O}_Y) \xrightarrow{\theta} H^0(\tilde{Y}^{(r+1)})$$

pour laquelle on trouve :

$$\dim \mathcal{S} \geq \text{Im}(\theta) .$$

Pour aller plus loin, nous utilisons les résultats de [24]. Considérons le complexe double de faisceaux sur Y :

$$A^{p,q} = \Omega_X^{p+q+1} < Y > / W_q \Omega_X^{p+q+1} < Y >$$

muni des différentielles :

$$d' : A^{p,q} \rightarrow A^{p+1, q+1} \text{ induite par la différentielle extérieure,}$$

$$d'' : A^{p,q} \rightarrow A^{p+1, q} \text{ induite par } {}^{\wedge}f^*(d\pi/\pi) .$$

On munit le complexe simple A^{\cdot} correspondant d'une filtration (encore notée W) en posant :

$$W_k A^{p,q} = W_{2q+k+1} \Omega_X^{p+q+1} < Y > / W_q \Omega_X^{p+q+1} < Y > .$$

On constate que ${}^{\wedge}f^*(d\pi/\pi)$ envoie $W_k A^{\cdot}$ dans $W_{k+1} A^{\cdot}$ si bien que :

$$Gr_k^w A^{\cdot} = \bigoplus_q Gr_k^w A^{\cdot, q}[-q] .$$

En particulier en utilisant le fait que X est de dimension $r+1$, on trouve :

$$Gr_k^w A^{\cdot} = 0 \text{ pour } k > r \text{ et } k < -r .$$

L'application $\wedge f^*(d\pi/\pi)$ définit une surjection de $\Omega_{X/\mathcal{C}}^p \wedge Y \otimes \mathcal{O}_Y$ dans $A^{p,0}$ de telle sorte que $A^{p,0}$ est une résolution de $\Omega_{X/\mathcal{C}}^p \wedge Y \otimes \mathcal{O}_Y$. On en déduit une suite spectrale :

$$E_1^{-k, q+k} = H^q(Y, Gr_k^w A^\cdot) \Rightarrow H^q(Y, A^\cdot) = H^q(Y, \Omega_{X/\mathcal{C}}^\cdot \wedge Y \otimes \mathcal{O}_Y)$$

telle que $E_1^{-k, \cdot} = 0$ et donc $E_\infty^{-k, \cdot} = 0$ pour $k > r$. Comme cette suite est dégénérée en E_2 ([24], 4.20), elle nous fournit, par passage au gradué associé, une surjection :

$$H^r(Y, \Omega_{X/\mathcal{C}}^\cdot \wedge Y \otimes \mathcal{O}_Y) \xrightarrow{\Phi} E_\infty^{-r, 2r} = E_2^{-r, 2r} = \ker(E_1^{-r, 2r} \rightarrow E_1^{-r+1, 2r}).$$

Maintenant, en utilisant le résidu de Poincaré, on trouve ([24] lemme 4.18) :

$$Gr_k^w A^\cdot \underset{\substack{q \geq -k \\ q \geq 0}}{\cong} \bigoplus_{q \geq 0} a_* \Omega_{\tilde{Y}(2q+k+1)}^\cdot [-k-2q].$$

En particulier on a :

$$\begin{aligned} Gr_r^w A^\cdot &\cong (a_{r+1})_* \Omega_{\tilde{Y}(r+1)}^\cdot [-r] \\ Gr_{r-1}^w A^\cdot &\cong (a_r)_* \Omega_{\tilde{Y}(r)}^\cdot [1-r] \end{aligned}$$

si bien que :

$$\begin{aligned} E_1^{-r, 2r} &= H^r(Y, Gr_r^w A^\cdot) \cong H^0(Y, (a_{r+1})_* \Omega_{\tilde{Y}(r+1)}^\cdot) = H^0(\tilde{Y}^{(r+1)}) \\ E_1^{-r+1, 2r} &= H^{r+1}(Y, Gr_{r-1}^w A^\cdot) \cong H^2(Y, (a_r)_* \Omega_{\tilde{Y}(r)}^\cdot) \\ &= H^2(\tilde{Y}^{(r)}, \Omega_{\tilde{Y}(r)}^\cdot) = H^0(\tilde{Y}^{(r)}, \Omega_{\tilde{Y}(r)}^\cdot)^* = H^0(\tilde{Y}^{(r)})^* \end{aligned}$$

que les applications Φ et θ_φ se déduisent l'une de l'autre par ces isomorphismes résulte de la construction même de la suite spectrale. Nous avons donc :

$$\dim \mathcal{S} \geq \dim \ker(E_1^{-r, 2r} \rightarrow E_1^{-r+1, 2r}).$$

Il suffit alors de remarquer que l'application d de la suite spectrale est la duale de l'application cobord d de $H^0(\tilde{Y}^{(r+1)})/d(H^0(\tilde{Y}^{(r)})) = H^r(\Gamma)$.

ERRATUM

to *On the arithmetic of conic bundle surfaces*

Per SALBERGER

In Séminaire de Théorie des Nombres de Paris 1985–86, Birkhäuser (175–197)

Page 193 : Dr. A.N. Skorobogatov has kindly informed me that the proof of (5.3) contains a mistake. More precisely he points out that one cannot expect any exact sequence such as the first one on p. 193.

It is easy to correct this mistake. To begin with, note that $U(k_v)$ is dense in $X(k_v)$ for each place v of k by the implicit function theorem. It is therefore sufficient to show that the hypothesis in (5.2) is satisfied for any set $\{P_v\}$ of k_v -points on U . Thus, we have to show that $\prod_{\text{all } v} \epsilon_v = \prod_{\text{all } v} \mathcal{C}(P_v)$ belongs to $\text{Im}(H^1(k, S) \rightarrow \prod_{\text{all } v} H^1(k_v, S))$. To see this, we use the following commutative diagram with exact rows :

$$\begin{array}{ccccccc} H^1(k, T) & \longrightarrow & H^1(k, S) & \xrightarrow{\delta} & Br k \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{\text{all } v} H^1(k_v, T) & \longrightarrow & \prod_{\text{all } v} H^1(k_v, S) & \xrightarrow{(\delta_v)} & \prod_{\text{all } v} Br k_v \end{array}$$

Here T is the k -torus for which $T(\bar{k}) = \text{Pic } \bar{X} \otimes_{\mathbb{Z}} \bar{k}^*$ and the rows are those on p. 194 (op. cit.). The surjectivity of the first vertical map is clear from class field theory, since $H^1(\text{Gal}(\bar{k}/k), \text{Pic } \bar{X}) = 0$ by assumption. Thus, to complete the proof we only have to prove that $\prod_{\text{all } v} \delta_v \mathcal{C}_v(P_v)$ belongs to $\text{Im}(\text{Br } k \rightarrow \prod_{\text{all } v} Br k_v)$. But this is clear from lemma (2.10) of my article

Zero-cycles on rational surfaces over number fields, Inventiones Math. 91 (1988), pp. 505–524.

Liste des conférenciers

5 octobre	1987	K. Ribet.— Opérateurs de Hecke pour les courbes modulaires et les courbes de Shimura
12 octobre	1987	A.-M. Bergé.— Minorations géométriques de régulateurs
19 octobre	1987	L. Clozel.— Algébricité des opérateurs de Hecke opérant sur certaines formes de Maass (travail commun avec D. Blasius et D. Ramakrishnan).
26 octobre	1987	J.-J. Sansuc.— Sur les nombres de Tamagawa, d'après R. Kottwitz.
9 novembre	1987	J.-L. Nicolas.— Partitions sans petits sommants
16 novembre	1987	J. Tilouine.— Critères de Kummer en théorie d'Iwasawa anticyclotomique
23 novembre	1987	A. Movahhedi.— Corps p -rationnels
30 novembre	1987	J.-F. Mestre.— Courbes de genre 2 à multiplications réelles par $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.
7 décembre	1987	P. Kaplan.— Parité des solutions de l'équation $T^2 - DU^2 = 4$ pour $D \equiv 5 \pmod{8}$.
14 décembre	1987	E. Friedman.— Analytic formulas for the regulator of a number field.
4 janvier	1988	Ph. Robba [†] .— Une démonstration p -adique du théorème de Lindeman–Weierstrass.
11 janvier	1988	P. Salberger.— Some new Hasse principles for rational surfaces.

- 18 janvier 1988 M. Balazard.— Sur le nombre de facteurs premiers des entiers.
- 25 janvier 1988 G. Anderson.— A cocycle defining an Extension of the Taniyama Group.
- 1er février 1988 J.-P. Serre.— $x^4+y^4+z^4=t^4$ d'après N. Elkies.
J. Zarhin.— Informal talk on Kolyvagin's proof of the finiteness of \prod for some elliptic curves.
- 15 février 1988 N. Boston.— Explicit deformation of Galois representations
- 22 février 1988 S. Louboutin.— Arithmétique des corps quadratiques réels.
- 29 février 1988 M. Hindry.— Minorations de hauteurs de Néron—Tate.
- 7 mars 1988 M. Laurent.— Quelques nouveaux résultats sur la conjecture de Leopoldt.
- 14 mars 1988 S. Lichtenbaum.— Les valeurs en $\sigma = 1$ des fonctions zêta pour les surfaces ouvertes.
- 21 mars 1988 P. Vojta.— A refinement of Schmidt's Subspace Theorem.
- 11 avril 1988 J.C. Sikorav.— Preuve de la conjecture de Davenport sur les valeurs des formes quadratiques indéfinies (d'après Margulis).
- 18 avril 1988 J.-P. Serre.— Groupes de Galois des points de torsion des courbes elliptiques : bornes effectives.
- 25 avril 1988 H. Carayol.— Le conducteur analytique des représentations modulo p de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- 2 mai 1988 K. Rubin.— On the main conjecture of Iwasawa theory for imaginary quadratic fields.

Progress in Mathematics

Edited by:

J. Oesterlé
Departement des Mathematiques
Université de Paris VI
4, Place Jussieu
75230 Paris Cedex 05
France

A. Weinstein
Department of Mathematics
University of California
Berkeley, CA 94720
U.S.A.

Progress in Mathematics is a series of books intended for professional mathematicians and scientists, encompassing all areas of pure mathematics. This distinguished series, which began in 1979, includes authored monographs and edited collections of papers on important research developments as well as expositions of particular subject areas.

All books in the series are “camera-ready”, that is they are photographically reproduced and printed directly from a final-edited manuscript that has been prepared by the author. Manuscripts should be no less than 100 and preferably no more than 500 pages.

Proposals should be sent directly to the editors or to: Birkhäuser Boston, 675 Massachusetts Avenue, Suite 601, Cambridge, MA 02139, U.S.A.

A complete list of titles in this series is available from the publisher.

- | | |
|---|--|
| 19 ODA. Periods of Hilbert Modular Surfaces | 32 BOOKS/GRAY/REINHART. Differential Geometry |
| 20 STEVENS. Arithmetic on Modular Curves | 33 ZUILY. Uniqueness and Non-Uniqueness in the Cauchy Problem |
| 21 KATOK. Ergodic Theory and Dynamical Systems II | 34 KASHIWARA. Systems of Microdifferential Equations |
| 22 BERTIN. Séminaire de Théorie des Nombres. Paris 1980–81 | 35 ARTIN/TATE. Arithmetic and Geometry: Papers Dedicated to I.R. Shafarevich on the Occasion of His Sixtieth Birthday, Vol. 1 |
| 23 WEIL. Adeles and Algebraic Groups | 36 ARTIN/TATE. Arithmetic and Geometry: Papers Dedicated to I.R. Shafarevich on the Occasion of His Sixtieth Birthday. Vol. II |
| 24 LE BARZ/HERVIER. Enumerative Geometry and Classical Algebraic Geometry | 37 DE MONVEL. Mathématique et Physique |
| 25 GRIFFITHS. Exterior Differential Systems and the Calculus of Variations | 38 BERTIN. Séminaire de Théorie des Nombres, Paris 1981–82 |
| 26 KOBLITZ. Number Theory Related to Fermat’s Last Theorem | 39 UENO. Classification of Algebraic and Analytic Manifolds |
| 27 BROCKETT/MILLMAN/SUSSMAN. Differential Geometric Control Theory | 40 TROMBI. Representation Theory of Reductive Groups |
| 28 MUMFORD. Tata Lectures on Theta I | 41 STANELY. Combinatorics and Commutative Algebra |
| 29 FRIEDMAN/MORRISON. Birational Geometry of Degenerations | 42 JOUANOLOU. Théorèmes de Bertini et Applications |
| 30 YANO/KON. CR Submanifolds of Kaehlerian and Sasakian Manifolds | |
| 31 BERTRAND/WALDSCHMIDT. Approximations Diophantiennes et Nombres Transcendants | |

- 43 MUMFORD. Tata Lectures on Theta II
- 44 KAC. Infinite Dimensional Lie Algebras
- 45 BISMUT. Large Deviations and the Malliavin Calculus
- 46 SATAKE/MORITA. Automorphic Forms of Several Variables Taniuchi Symposium, Katata, 1983
- 47 TATE. Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$
- 48 FRÖHLICH. Classgroups and Hermitian Modules
- 49 SCHLICHTKRULL. Hyperfunctions and Harmonic Analysis on Symmetric Spaces
- 50 BOREL, ET AL. Intersection Cohomology
- 51 BERTIN/GOLDSTEIN. Séminaire de Théorie des Nombres. Paris 1982–83
- 52 GASQUI/GOLDSCHMIDT. Déformations Infinitesimales des Structures Conformes Plates
- 53 LAURENT. Théorie de la Deuxième Microlocalisation dans le Domaine Complèxe
- 54 VERDIER/LE POTIER. Module des Fibres Stables sur les Courbes Algébriques Notes de l'Ecole Normale Supérieure, Printemps, 1983
- 55 EICHLER/ZAGIER. The Theory of Jacobi Forms
- 56 SHIFFMAN/SOMMESE. Vanishing Theorems on Complex Manifolds
- 57 RIESEL. Prime Numbers and Computer Methods for Factorization
- 58 HELFFER/NOURIGAT. Hypoellipticité Maximale pour des Opérateurs Polynomes de Champs de Vecteurs
- 59 GOLDSTEIN. Séminaire de Théorie des Nombres, Paris 1983–84
- 60 PROCESI. Geometry Today: Giornate Di Geometria, Roma. 1984
- 61 BALLMANN/GROMOV/SCHROEDER. Manifolds of Nonpositive Curvature
- 62 GUILLOU/MARIN. A la Recherche de la Topologie Perdue
- 63 GOLDSTEIN. Séminaire de Théorie des Nombres, Paris 1984–85
- 64 MYUNG. Malcev-Admissible Algebras
- 65 GRUBB. Functional Calculus of Pseudo-Differential Boundary Problems
- 66 CASSOU-NOGUÈS/TAYLOR. Elliptic Functions and Rings and Integers
- 67 HOWE. Discrete Groups in Geometry and Analysis: Papers in Honor of G.D., Mostow on His Sixtieth Birthday
- 68 ROBERT. Antour de L'Approximation Semi-Classique
- 69 FARAUT/HARZALLAH. Deux Cours d'Analyse
- 70 ADOLPHSON/CONREY/GHOSH/YAGER. Number Theory and Diophantine Problems: Proceedings of a Conference at Oklahoma State University
- 71 GOLDSTEIN. Séminaire de Théories des Nombres, Paris 1985–1986
- 72 VAISMAN. Symplectic Geometry and Secondary Characteristics Classes
- 73 MOLINO. Riemannian Foliations
- 74 HENKIN/LEITERER. Andreotti–Grauert Theory by Integral Formulas
- 75 GOLSTEIN. Séminaire de Théories des Nombres, Paris 1986–87
- 76 COSSEC/DOLGACHEV. Enriques Surfaces I
- 77 REYSAAT. Quelques Aspects des Surfaces de Riemann
- 78 BORHO/BRYLINSKI/MACPHERSON. Nilpotent Orbits, Primitive Ideals, and Characteristic Classes
- 79 MCKENZIE/VALERIOTE. The Structure of Decidable Locally Finite Varieties
- 80 KRAFT/PETRIE/SCHWARZ. Topological Methods in Algebraic Transformation Groups
- 81 GOLDSTEIN. Séminaire de Théorie des Nombres, Paris 1987–1988