Séminaire de Théorie des Nombres .

- Besançon -

Année 1974-1975

NOMBRE DE CLASSES ET UNITES DES EXTENSIONS CUBIQUES CYCLIQUES DE $\mathbb{Q}$.

Marie-Nicole GRAS
Faculté des Sciences. Mathématiques
25030 BESANCON CEDEX

NOMBRE DE CLASSES ET UNITES DES EXTENSIONS CUBIQUES CYCLIQUES DE $\mathbb{Q}$.

par Marie-Nicole GRAS

Introduction

Dans [2] , nous avons montré comment on pouvait calculer le nombre de classes des extensions cubiques cycliques de $\mathbb{Q}$ à partir de la seule connaissance du groupe des unités cyclotomiques . Cette méthode repose sur une majoration effective du nombre de classes de ces corps , majoration obtenue à l'aide de considérations de géométrie élémentaire . Dans [1] , nous avons obtenu (au moyen de méthodes classiques de géométrie des nombres) une majoration du nombre de classes des corps abéliens réels quelconques qui redonne pour le cas cubique une majoration meilleure que celle initialement obtenue . Le but de cet exposé est de montrer comment la méthode élémentaire de [2] permet d'obtenir la même majoration , à condition d'utiliser les meilleurs constantes possibles. On trouvera également dans [2] le détail des démonstrations des § 1 et 2 et des tables établies par ordinateur .

I

Groupe des unités .

Soit K une extension cubique cyclique de $\mathbb{Q}$ de conducteur m . Soit σ un générateur de $G = Gal(K/\mathbb{Q})$.

Soit E le groupe des unités de K . Ce groupe , modulo la torsion $\{\pm 1\}$, est un $\mathbb{Z}[G]/(1+\sigma+\sigma^2)$-module , donc un $\mathbb{Z}[j]$-module en posant $\varepsilon^j = \varepsilon^\sigma$, ($j^3 = 1$) ; il existe une $\mathbb{Z}[j]$-base de E notée ε_o , donc toute unité φ de E s'écrit de manière unique $\varphi = \pm \varepsilon_o^\omega$, $\omega = \lambda + \mu j$, $\lambda , \mu \in \mathbb{Z}$, où l'on vient de rappeler que $\varepsilon^{\lambda+\mu j} = \varepsilon^\lambda (\varepsilon^\mu)^\sigma$.

Pour raisonner modulo la torsion , Hasse [3] et Leopoldt [4], dans la formule analytique du nombre de classes , utilisent le $\mathbb{Z}[j]$-module des valeurs absolues des unités de E que l'on note $|E|$ et où $|\varepsilon|^{\sigma}$ est par définition $|\varepsilon^{\sigma}|$.

Soit F le groupe des unités cyclotomiques de K . Ce groupe F se détermine numériquement pour chaque corps . Il est engendré sur $\mathbb{Z}[j]$ par une unité η appelée unité cyclotomique de K ; η est une base de F , considérée comme $\mathbb{Z}[j]$-module .

Alors $h = (|E| : |F|)$ et si $|\eta| = |\varepsilon_o|^{\lambda+\mu\sigma} = |\varepsilon_o|^{\omega}$, $h = \lambda^2 - \lambda\mu + \mu^2$. En effet , on vérifie que $|E|/|F| \simeq \mathbb{Z}[j]/(\omega)$; son nombre d'éléments est $N_{\mathbb{Q}(j)/\mathbb{Q}}(\omega)$.

II

Principe de la méthode .

On part de F , donc de η ; on ne connaît pas ε_o . La méthode permet de déterminer en même temps le nombre de classes et l'unité fondamentale de K . En effet , dire que le nombre de classes de K est égal à h équivaut à dire qu'il existe un entier ω de $\mathbb{Z}[j]$ et une unité ε_o de K tels que $|\eta| = |\varepsilon_o|^{\omega}$.

On essaye toutes les normes , c'est-à-dire que pour tout entier r qui est norme d'entier dans $\mathbb{Q}(j)$, $r = \omega\bar{\omega}$, $\omega \in \mathbb{Z}[j]$, on cherche s'il existe $\varepsilon \in K$ tel que $|\eta| = |\varepsilon|^{\omega} = |\varepsilon|^{\lambda+\mu\sigma}$. Cette relation s'inverse , en considérant ε comme un entier algébrique pas forcément dans K à priori :

$$|\varepsilon| = |\eta|^{\frac{\lambda+\mu\sigma^2}{r}} \quad , \quad |\varepsilon^{\sigma}| = |\eta|^{\frac{\lambda\sigma+\mu}{r}} \quad , \quad |\varepsilon^{\sigma^2}| = |\eta|^{\frac{\lambda\sigma^2+\mu\sigma}{r}} \quad .$$

On sait tester si $\varepsilon \in K$ grâce à la propriété suivante :
$\varepsilon \in K$ si et seulement si $\varepsilon + \varepsilon^{\sigma} + \varepsilon^{\sigma^2}$ et $\varepsilon\varepsilon^{\sigma} + \varepsilon^{\sigma}\varepsilon^{\sigma^2} + \varepsilon^{\sigma^2}\varepsilon$ sont des entiers rationnels .

Le problème essentiel est donc de trouver un majorant des nombres r à essayer , sinon la méthode est sans intérêt pratique. Une majoration existe, car on a le phénomène suivant : si $|\varepsilon| = |\eta|^{\frac{\lambda+\mu\sigma^2}{r}}$,

$r = \lambda^2 - \lambda\mu + \mu^2$, $|\varepsilon|$, $|\varepsilon^\sigma|$ et $|\varepsilon^{\sigma^2}|$ tendent vers 1 quand $r \to +\infty$.

Or il existe des raisons arithmétiques qui contredisent le fait que l'on puisse trouver des conjugués tous voisins de 1 en valeur abso - lue . On considère par exemple :

(i) le <u>discriminant</u> $\Delta(\varepsilon) = (\varepsilon - \varepsilon^\sigma)(\varepsilon^\sigma - \varepsilon^{\sigma^2})(\varepsilon^{\sigma^2} - \varepsilon)$; c'est un entier non nul divisible par m si $\varepsilon \in K$; or au voisinage de $(\pm 1, \pm 1, \pm 1)$, il est peu différent de 0 .

(ii) la <u>résolvante de Lagrange</u> $N(\varepsilon) = (\varepsilon + j\varepsilon^\sigma + j^2\varepsilon^{\sigma^2})(\varepsilon + j^2\varepsilon^\sigma + j\varepsilon^\sigma)$; c'est un entier positif non nul divisible par m ; or au voisinage de $(\pm 1, \pm 1, \pm 1)$, elle est peu différente de 0 ou 4 .

III

<u>Majoration du nombre de classes de</u> K .

<u>Théorème</u> . Soit $\mathfrak{R}(\eta)$ le régulateur de l'unité cyclotomique de K ; soit h le nombre de classes de K ; alors on a

$$h \leq 4 \frac{\mathfrak{R}(\eta)}{\mathrm{Log}^2 \frac{m}{4}} .$$

La démonstration s'effectue en se servant de la résolvante de Lagrange ; on a d'abord le lemme suivant :

<u>Lemme</u> . Pour tout $x, y, z \in \mathbb{R}$,

$$0 < (x + jy + j^2 z)(x + j^2 y + jz) \leq 4 \, \mathrm{Max}(x^2, y^2, z^2) .$$

Soit $N(x,y,z) = (x + jy + j^2 z)(x + j^2 y + jz) = x^2 + y^2 + z^2 - xy - yz - zx$

et pour tout $(x,y,z) \neq (0,0,0)$ soit $\overline{N}(x,y,z) = N(x,y,z) / \mathrm{Max}(x^2, y^2, z^2)$.

Soit $C = \{(x,y,z) \in \mathbb{R}^3 , \mathrm{Max}(|x|, |y|, |z|) = 1\}$. La fonction $\overline{N}(x,y,z)$ étant homogène de degré 0 , on en déduit que

$\sup_{(x,y,z) \in \mathbb{R}^3} \overline{N}(x,y,z) = \sup_{(x,y,z) \in C} N(x,y,z)$. Comme N est continue et que C est compact , N atteint son maximum sur C . Montrons qu'en un point (x_o, y_o, z_o) où N atteint son maximum , $|x_o| = |y_o| = |z_o| = 1$.

En effet , supposons que l'une des composantes, x_o par exemple , est différente de ± 1 ; soit $\gamma(x) = x^2 + y_o^2 + z_o^2 - xy_o - y_o z_o - z_o x$ la fonction de la variable x ; on a $\gamma'(x_o) = 0$, puisque x_o est maximum local ; or $\gamma''(x_o) = 2$ et par conséquent , x_o ne peut représenter qu'un minimum de la fonction γ , donc on aura : $\underset{-1 \le x \le +1}{\text{Max}} \ \gamma(x) = \gamma(-1)$ ou $\gamma(1)$. Il est alors immédiat de vérifier que $\underset{\substack{|x_o|=1 \\ |y_o|=1 \\ |z_o|=1}}{\text{Max}} \ (x_o^2 + y_o^2 + z_o^2 - x_o y_o - y_o z_o - z_o x_o) = 4$

Démonstration du théorème .

Avec les notations du § 2 , montrons qu'il existe une constante M telle que si $r > M$, alors le nombre strictement positif $N(\varepsilon) = (\varepsilon + j\varepsilon^\sigma + j^2\varepsilon^{\sigma^2})(\varepsilon + j^2\varepsilon^\sigma + j\varepsilon^{\sigma^2})$ est inférieur à m . Il en résulte de manière évidente que $h \le M$.

Comme $0 < N(\varepsilon) \le 4 \ \text{Max} (\varepsilon^2, \varepsilon^{2\sigma} , \varepsilon^{2\sigma^2})$, il suffit de chercher M tel que $r > M$ entraîne $\text{Max} (\varepsilon^2, \varepsilon^{2\sigma}, \varepsilon^{2\sigma^2}) < \frac{m}{4}$. (1)

Or on a $|\varepsilon| = |\eta|^{\frac{\lambda+\mu\sigma^2}{r}}$, $|\varepsilon^\sigma| = |\eta|^{\frac{\lambda\sigma+\mu}{r}}$, $|\varepsilon^{\sigma^2}| = |\eta|^{\frac{\lambda\sigma^2+\mu\sigma}{r}}$,

donc $\text{Max} (\varepsilon^2, \varepsilon^{2\sigma}, \varepsilon^{2\sigma^2}) = |\eta_i|^{\frac{2\lambda}{r}} \ |\eta_i'|^{\frac{2\mu}{r}}$, $i = 1, 2$ ou 3 , $r = \lambda^2 - \lambda\mu + \mu^2$ et où $(\eta_1, \eta_1') = (\eta, \eta^\sigma)$, $(\eta_2, \eta_2') = (\eta^\sigma , \eta)$ et $(\eta_3 , \eta_3') = (\eta^{\sigma^2}, \eta)$.

L'inégalité (1) est donc équivalente aux trois inégalités

$$|\eta_i|^{\frac{2\lambda}{\lambda^2-\lambda\mu+\mu^2}} \ |\eta_i'|^{\frac{2\mu}{\lambda^2-\lambda\mu+\mu^2}} < \frac{m}{4} \ , \ i = 1,2,3 \ .$$

En prenant le logarithme de ces deux quantités positives , on obtient :

$$\frac{2\lambda}{\lambda^2 - \lambda\mu + \mu^2} \ \text{Log} \, |\eta_i| + \frac{2\mu}{\lambda^2 - \lambda\mu + \mu^2} \ \text{Log} \, |\eta_i'| < \text{Log} \frac{m}{4} \ ,$$

soit puisque $\lambda^2 - \lambda\mu + \mu^2 > 0$ et que $\text{Log}\,\frac{m}{4} > 0$ ($m \geq 7$) ,

$$\lambda^2 - \lambda\mu + \mu^2 - 2\ell_i\lambda - 2\ell_i'\mu > 0 \quad , \quad i = 1, 2, 3 ,$$

en posant $\ell_i = \dfrac{\text{Log}\,|\eta_i|}{\text{Log}^2\,\frac{m}{4}}$ et $\ell_i' = \dfrac{\text{Log}\,|\eta_i'|}{\text{Log}^2\,\frac{m}{4}}$.

Soient E_1 , E_2 , E_3 les trois ellipses d'équation

$$X^2 - XY + Y^2 - 2\ell_i X - 2\ell_i' Y = 0 \quad , \; i = 1, 2, 3$$

(cf. schéma) .

Si le point de coordonnées (λ,μ) est extérieur aux trois ellipses, alors la quantité $N(\varepsilon)$ est inférieure à m . On remarque qu'il suffit que ε ou ε^{-1} vérifie cette condition ; soient donc E_1' , E_2' et E_3' les trois ellipses symétriques par rapport à O de E_1 , E_2 et E_3 . Soient D_1 l'union des intérieurs de E_1 , E_2 , E_3 et D_1' l'union des intérieurs de E_1' , E_2' , E_3'. Si le point de coordonnées (λ,μ) est extérieur à D_1 ou D_1' , alors ou bien $0 < N(\varepsilon) < m$, ou bien $0 < N(\varepsilon^{-1}) < m$.

Or l'ellipse d'équation $X^2 - XY + Y^2 - 2\ell_i X - 2\ell_i' Y = 0$ a pour centre le point de coordonnées $X' = -(4\ell_i + 2\ell_i')/3$, $Y' = -(2\ell_i + 4\ell_i')/3$ et son équation au centre est :

$$(X - X')^2 - (X - X')(Y - Y') + (Y - Y')^2 = \frac{4}{3}(\ell_i^2 + \ell_i\ell_i' + \ell_i'^2)$$

avec $$X'^2 - X'Y' + Y'^2 = \frac{4}{3}(\ell_i^2 + \ell_i\ell_i' + \ell_i'^2) .$$

Mais , pour i = 1,2,3 , les six quantités $\ell_i^2 + \ell_i\ell_i' + \ell_i'^2$ et $(-\ell_i)^2 + (-\ell_i)(-\ell_i') + (\ell_i')^2$ sont égales à

$$\frac{\text{Log}^2\,|\eta_i| + \text{Log}\,|\eta_i|\;\text{Log}\,|\eta_i'| + \text{Log}^2\,|\eta_i'|}{\text{Log}^2\,\frac{m}{4}} = \frac{\Re(\eta)}{\text{Log}^2\,\frac{m}{4}} .$$

Les six ellipses E_1 , E_2 , E_3 , E_1' , E_2' , E_3' sont donc six ellipses égales passant par l'origine et centrées sur l'ellipse d'équation $X^2 - XY + Y^2 = \frac{4}{3}\,\Re(\eta)/\text{Log}^2\,\frac{m}{4}$. On vérifie qu'une ellipse E_i et une ellipse E_i' se coupent sur l'ellipse E d'équation $X^2 - XY + Y^2 = \dfrac{4\,\Re(\eta)}{\text{Log}^2\,\frac{m}{4}}$

et que si un point est extérieur à E , il est extérieur à D_1 ou à D_2 .

Donc , si $r > \frac{4\Re(\eta)}{\mathrm{Log}^2 \frac{m}{4}}$, $\mathrm{Max}(\varepsilon^2 , \varepsilon^{2\sigma} , \varepsilon^{2\sigma^2}) < \frac{m}{4}$ ou

$\mathrm{Max}(\varepsilon^{-2} , \varepsilon^{-2\sigma} , \varepsilon^{-2\sigma^2}) < \frac{m}{4}$, donc ε ne peut pas être un élément de K . On a donc trouvé une constante M ,

$$M = \frac{4\Re(\eta)}{\mathrm{Log}^2 \frac{m}{4}}$$

telle que $h \leq M$.

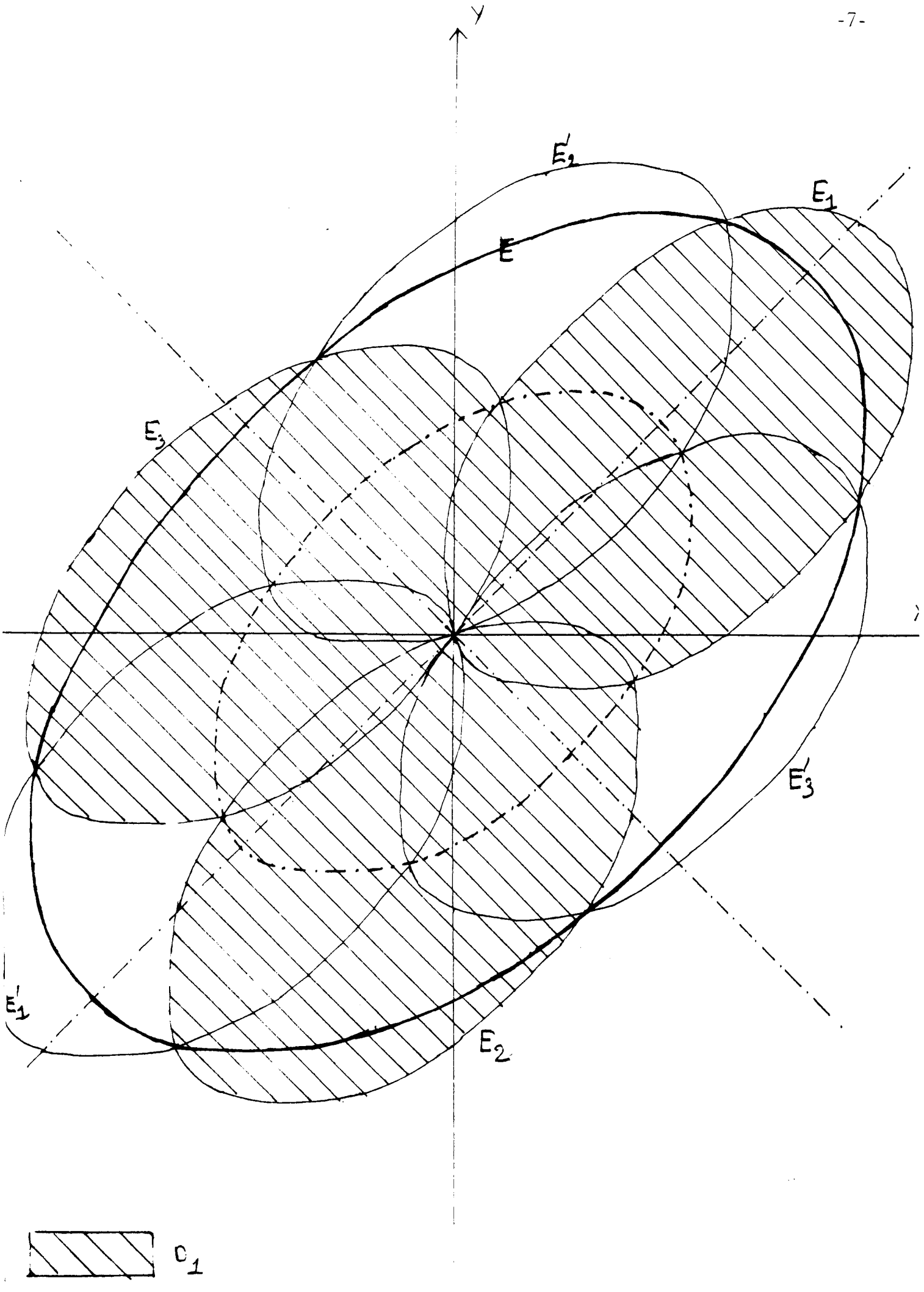
Bibliographie

[1] GRAS G.- GRAS M.N. :
Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbb{Q}$ (à paraître) .

[2] GRAS M.N. :
Méthodes et algorithmes pour le calcul du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$.
Journal de Crelle , Band 277, (1975) , p. 89 - 116 .

[3] HASSE H. :
Über die Klassenzahl abelscher Zahlkörper ,
Akademie-Verlag , Berlin (1952) .

[4] LEOPOLDT H.W. :
Über Einheitengruppe und Klassenzahl reeller abescher Zahlkörper , Abh. Deutsche Akad. Wiss. Berlin , Math. , 2 (1954) .


y
x
E'2
E1
E
E3
E'3
E'1
E2
D1