

ANNALES DE L'INSTITUT FOURIER

MARIE-NICOLE GRAS

Classes et unités des extensions cycliques réelles de degré 4 de \mathbb{Q}

Annales de l'institut Fourier, tome 29, n° 1 (1979), p. 107-124

http://www.numdam.org/item?id=AIF_1979__29_1_107_0

© Annales de l'institut Fourier, 1979, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

**CLASSES ET UNITÉS
DES EXTENSIONS CYCLIQUES RÉELLES
DE DEGRÉ 4 de \mathbf{Q}**

par Marie-Nicole GRAS

Dédié à Monsieur Claude Chabauty.

INTRODUCTION

Soit K une extension cyclique réelle de degré 4 de \mathbf{Q} . On note k le sous-corps quadratique de K . Ces extensions ont été étudiées par H. Hasse dans un article ([6]) antérieur à celui de H.W. Leopoldt sur l'interprétation arithmétique du nombre de classes des corps abéliens réels ([8]). Partant de la formule analytique ([5]) qui permet d'exprimer le nombre de classes h de K comme quotient d'un régulateur convenable d'unités cyclotomiques de K par le régulateur du corps, H. Hasse détermine un système de générateurs du groupe des unités de K et obtient ainsi par un calcul d'indices le nombre de classes h de K . L'algorithme utilisé par H. Hasse pour déterminer un système d'unités fondamentales de K repose sur la recherche d'une solution, vérifiant une condition de minimalité, d'une équation diophantienne dont les solutions ne sont pas bornées a priori ; cet algorithme se révèle impraticable sur ordinateur ; il a cependant permis à H. Hasse de dresser la table des nombres de classes et des unités pour les corps K de conducteur inférieur à 100 (soit 23 corps au total).

Notre travail est constitué des deux parties suivantes :

Dans la première partie, nous appliquons au cas cyclique réel de degré 4 la nouvelle méthode de calcul du nombre de classes et des unités que nous avons développée dans un article en commun avec G. Gras ([2]). Par cette méthode, nous déterminons simultanément le nombre de classes et le groupe des unités de K . Nous

avons obtenu une table de ces résultats pour tous les corps K de conducteur inférieur à 4000 (soit 1536 corps).

La deuxième partie est consacrée à l'étude de la "capitulation" dans K des classes de k . On sait que si une extension est partout non ramifiée, alors il existe une classe non triviale du corps de base qui devient principale par extension. Compte tenu du fait que ici K/k est toujours ramifiée, il n'est pas question de pouvoir illustrer ce théorème ; cependant, nous avons constaté que dans certains cas une classe d'ordre 2 de k devenait principale dans K malgré la ramification. L'étude de ce phénomène repose sur les mêmes techniques que celles permettant de démontrer le théorème 94 de Hilbert. Nous montrons que le noyau de l'homomorphisme extension des classes de k à K est d'ordre 1 ou 2 et que la connaissance du groupe des unités de K suffit à le déterminer (théorème (II, § 5)). Nous avons inclus ces résultats dans une table qui paraîtra intégralement dans [4] ; nous en donnons un extrait à la fin de cet article.

Nous n'avons pas étudié les extensions analogues imaginaires. En effet, dans ce cas, le problème de la détermination des unités et du nombre de classes est complètement résolu (cf. [6] par exemple). Par ailleurs, il n'est pas difficile de vérifier qu'aucune classe de k ne devient principale dans K lorsque K est imaginaire.

I. NOMBRE DE CLASSES ET UNITES

Soit K une extension cyclique réelle de degré 4 de \mathbf{Q} ; soit f le conducteur de K et soit $G = \langle \sigma \rangle$ le groupe de Galois de K/\mathbf{Q} . On note k le sous-corps quadratique de K et m le conducteur de k .

1. Rappel des résultats de Leopoldt.

Les notations et les résultats de ce paragraphe se trouvent dans [8] ; ils ont été rappelés aussi dans [2].

Le corps K de conducteur f est cyclique, donc il est de la forme K_χ , où χ est un caractère rationnel de $\mathbf{Q}^{(f)}$. Soit E_K le groupe des unités de K ; $|E_K|$ (groupe des valeurs absolues de E_K) est un \mathbf{Z} -module libre de rang 3 que l'on munit canoniquement d'une structure de $\mathbf{Z}[G]$ -module, en posant $|u|^\sigma = |u^\sigma|$ pour tout $u \in E_K$.

Si on applique la définition de H.W. Leopoldt pour les unités χ -relatives, on obtient qu'une unité w de K est χ -relative si et seulement si $w^{1+\sigma^2} = \pm 1$. Soit E_χ le groupe des unités χ -relatives; puisque $\mathbf{Z}[G]/(1 + \sigma^2)$ est isomorphe à $\mathbf{Z}[i]$, on considère $|E_\chi|$ comme un $\mathbf{Z}[i]$ -module; il est libre de dimension 1; donc $|E_\chi| \simeq \mathbf{Z}[i]$ et il existe une unité χ -relative ϵ_χ génératrice (dans l'isomorphisme $\mathbf{Z}[G]/(1 + \sigma^2) \simeq \mathbf{Z}[i]$, i correspond à σ ; ainsi tout élément u_χ de E_χ s'écrit de manière unique $u_\chi = \pm \epsilon_\chi^{\mu+\nu\sigma}$, $\mu, \nu \in \mathbf{Z}$). Soit E_k le groupe des unités de k . Soit E^K le sous G -module de E_K engendré par E_k et E_χ ; alors $|E^K| = |E_k| \oplus |E_\chi|$ et si ϵ_0 est un générateur de E_k , toute unité w de E^K s'écrit de façon unique $w = \pm \epsilon_0^\lambda \epsilon_\chi^{\mu+\nu\sigma}$, $\lambda, \mu, \nu \in \mathbf{Z}$. Soit $Q_K = (|E_K| : |E^K|)$; d'après les résultats de H. Hasse ([6]) on a $Q_K = 1$ ou 2, ce qui donne deux structures possibles pour le groupe des unités de K (voir § 4).

Soit η_χ l'unité cyclotomique χ -relative génératrice; on rappelle que η_χ se détermine de la manière suivante: soit \mathfrak{A} un système de représentants modulo f correspondant à $\text{Gal}(\mathbf{Q}_0^{(f)}/K)$; soit $\xi = \exp\left(\frac{i\pi}{f}\right)$ et soit $\Theta = \prod_{a \in \mathfrak{A}} (\xi^a - \xi^{-a})$. D'après ([8]), l'extension $K(\Theta)/\mathbf{Q}$ est abélienne et si $\bar{\sigma}$ est un prolongement de σ à $K(\Theta)$, alors $\eta = \Theta^{1-\bar{\sigma}}$ est une unité de K et $\eta_\chi = \eta^{1+\sigma}$ est une unité χ -relative de K . Soit F_χ le sous-module de E_χ engendré par η_χ ; alors F_χ est d'indice fini dans E_χ et $|F_\chi|$ est un sous $\mathbf{Z}[i]$ -module libre de dimension 1 de $|E_\chi|$; on a donc $\eta_\chi = \pm \epsilon_\chi^{\mu+\nu\sigma}$ et $(|E_\chi| : |F_\chi|) = \mu^2 + \nu^2$.

D'après [8], le nombre de classes h de K est donné par la formule: $h = \frac{Q_K}{2} h_\chi h_0$, où h_χ désigne l'indice de $|F_\chi|$ dans $|E_\chi|$, h_0 le nombre de classes de k et Q_K l'indice de $|E^K|$ dans $|E_K|$.

En ce qui nous concerne, le calcul de h se ramène essentiellement à celui de h_χ et Q_K , h_0 étant supposé connu.

2. Majoration de $h_x = (|E_x| : |F_x|)$.

En utilisant les techniques développées dans [2], nous obtenons la majoration suivante :

PROPOSITION 1. — Soit E_x le groupe des unités x -relatives de K ; soit F_x le sous-module de E_x engendré par l'unité cyclotomique η_x ; soit $h_x = (|E_x| : |F_x|)$; alors

$$h_x \leq H(F_x) \quad \text{où} \quad H(F_x) = 4 \frac{(\log |\eta_x|)^2 + (\log |\eta_x^\sigma|)^2}{\left(\log \frac{f-6}{2}\right)^2}.$$

Démonstration. — Soit Φ le polynôme résolvante de Lagrange ; pour tout $\alpha \in K^*$, on a

$$\begin{aligned} \Phi(\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \alpha^{\sigma^3}) &= (\alpha + i\alpha^\sigma - \alpha^{\sigma^2} - i\alpha^{\sigma^3})(\alpha - i\alpha^\sigma - \alpha^{\sigma^2} + i\alpha^{\sigma^3}) \\ &= (\alpha - \alpha^{\sigma^2})^2 + (\alpha^\sigma - \alpha^{\sigma^3})^2. \end{aligned}$$

On sait que si α est un entier de K n'appartenant pas à k , alors $\Phi(\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \alpha^{\sigma^3})$ est un entier rationnel non nul multiple de f . Soit u_x une unité x -relative de K autre que ± 1 ; alors

$$\begin{aligned} f &\leq (u_x - u_x^{\sigma^2})^2 + (u_x^\sigma - u_x^{\sigma^3})^2 = u_x^2 + u_x^{2\sigma} + u_x^{2\sigma^2} + u_x^{2\sigma^3} \pm 4 \\ &\leq 6 + 2 \operatorname{Max}(u_x^2, u_x^{2\sigma}, u_x^{2\sigma^2}, u_x^{2\sigma^3}) \end{aligned}$$

puisque $u_x^{1+\sigma^2} = \pm 1$ et que parmi les quatre éléments $u_x^2, u_x^{2\sigma}, u_x^{2\sigma^2}$ et $u_x^{2\sigma^3}$, deux sont inférieurs à 1. Donc quelle que soit l'unité x -relative non triviale u_x de K , on a $\operatorname{Max}(u_x^2, u_x^{2\sigma}, u_x^{2\sigma^2}, u_x^{2\sigma^3}) \geq \frac{f-6}{2}$.

Le plus petit conducteur possible de K étant $f = 15$, on a toujours $\frac{f-6}{2} > 1$; en appliquant le théorème II.1 de [2], on obtient la ma-

ajoration voulue. En appliquant une méthode géométrique analogue à celle utilisée dans [3] pour les corps cubiques cycliques, on obtient encore la proposition 1 (pour cela, se reporter à [4] où l'on trouvera les détails des différents calculs).

3. Détermination de h_x et ϵ_x .

On détermine η_x numériquement (valeur approchée réelle). On applique alors la méthode de dévissage des unités cyclotomiques décrite dans [2], IV.1. Rappelons-en le principe :

(i) Soit $l = \mu^2 + \nu^2 \neq 2$ la norme absolue d'un élément premier de $\mathbf{Z}[i]$ ($l = p$, p premier si $p \equiv 1 \pmod{4}$, $l = q^2$, q premier si $q \equiv 3 \pmod{4}$). On sait que l divise h_x si et seulement s'il existe $u_x \in E_x$ telle que $\eta_x = u_x^{\mu+\nu\sigma}$; soit $s = N_{K/k}(\eta_x) = \pm 1$; alors $N_{K/k}(u_x) = s$ car $\mu + \nu$ est impair; on a alors $\eta_x^{\mu-\nu\sigma} = s^{\nu^2} u_x^{\mu^2+\nu^2} = s' u_x^l$; alors $u_x = s'(\eta_x^{\mu-\nu\sigma})^{1/l}$; soient $u'_x = s'(\eta_x^{\mu\sigma-\nu\sigma^2})^{1/l}$, $u''_x = s u_x^{-1}$ et $u'''_x = s u_x^{-1}$; une condition nécessaire et suffisante pour que $u_x \in K_x$ est que le polynôme $P = (X - u_x)(X - u'_x)(X - u''_x)(X - u'''_x)$ soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, on a $u_x^\sigma = u'_x$, $u_x^{\sigma^2} = u''_x$ et $u_x^{\sigma^3} = u'''_x$.

(ii) Le nombre premier $l = 2$ divise h_x si et seulement s'il existe $u_x \in E_x$ telle que $\eta_x = \pm u_x^{1-\sigma}$; il est donc nécessaire que $N_{K/k}(\eta_x) = +1$; soit $s = N_{K/k}(u_x)$; alors $\eta_x^{1+\sigma} = u_x^{1+\sigma^2} = s u_x^2$; donc 2 divise h_x si et seulement s'il existe $u_x \in E_x$ telle que $N_{K/k}(\epsilon_x) = s$ et $u_x = \pm \sqrt{s \eta_x^{1+\sigma}}$. Soient $v_x = \sqrt{s \eta_x^{1+\sigma}}$, $v'_x = \sqrt{s \eta_x^{\sigma+\sigma^2}}$, $v''_x = s v_x^{-1}$ et $v'''_x = s v_x^{-1}$; une condition nécessaire et suffisante pour que $v_x \in K_x$ est qu'il existe des nombres $\delta, \delta' \in \{-1, +1\}$ tels que le polynôme $P = (X - \delta v_x)(X - \delta' v'_x)(X - \delta v''_x)(X - \delta' v'''_x)$ soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, on a $u_x = \delta v_x$, $u_x^\sigma = \delta' v'_x$, $u_x^{\sigma^2} = \delta v''_x$ et $u_x^{\sigma^3} = \delta' v'''_x$.

L'algorithme de "dévissage" proprement dit est alors le suivant :

- On effectue d'abord le dévissage en 2 : on sait d'après [8] que h_x est pair si et seulement si f est composé; dans ce dernier cas, on cherche la plus grande puissance 2^d de 2 qui divise h_x par dévissages successifs de l'unité cyclotomique (cf. (ii)). On obtient alors dans tous les cas $\eta_x = \varphi_x^\omega$, $\omega \in \mathbf{Z}[i]$ de norme 2^d et si F désigne le sous-G-module de E_x engendré par φ_x , alors $(|F| : |F_x|) = 2^d$ et $(|E_x| : |F|) = h_x/2^d$. On a donc $(|E_x| : |F|) \leq H(F)$, avec $H(F) = H(F_x)/2^d$.

- On part ensuite de l'unité φ_x engendrant F . On teste la divisibilité de $(E_x : F)$ par les nombres l impairs de la forme p ou

q^2 (cf. (i)) classés par ordre croissant. On obtient ainsi une suite finie (qui peut être vide) de nombres non nécessairement distincts $l_1 \leq l_2 \leq \dots \leq l_n$, une suite strictement croissante $F = F_0 \subsetneq F_1 \subsetneq \dots \subsetneq F_n = E_x$ de sous-G-modules de E_x et une suite strictement décroissante $H(F_0) > H(F_1) > \dots > H(F_n)$ de nombres tels que $H(F_i) = H(F_{i-1})/l_i$. On a $F_n = E_x$ si le test de divisibilité par les l tels que $l_{n-1} \leq l \leq H(F_n)$ est toujours négatif. On a alors $h_x = 2^d l_1 \dots l_n$ et la dernière unité obtenue est ϵ_x . On remarque que $s = N_{K/k}(\epsilon_x) = N_{K/k}(\varphi_x)$.

Remarque 1. — La longueur maximum de l'algorithme correspond au cas où $h_x = 2^d$ car alors on doit tester tous les dévisages relatifs aux l compris entre 5 et $H(F)$.

Remarque 2. — Cet algorithme est efficace dans la pratique, car la constante $H(F_x)$ n'est pas très grande numériquement. Par exemple, il y a 198 corps K dont le conducteur f est tel que $2000 < f < 2500$; on a alors $H(F_x) < 500$; il y a seulement 8 corps pour lesquels $H(F_x) \geq 300$ et pour 150 corps on a $H(F_x) < 100$.

4. Etude de l'indice $Q_K = (|E_K| : |E_x| \oplus |E_k|)$.

PROPOSITION 2. —

- a) On a $Q_K = 1$ ou 2 et $Q_K = 2$ si et seulement s'il existe une "unité de Minkowski" ϵ pour E_K ;
- b) Soient ϵ_0 un générateur de E_k et ϵ_x un générateur de E_x . Les conditions suivantes sont équivalentes :
- (i) $Q_K = 2$,
 - (ii) il existe $u \in E_K$ telle que $u^{1+\sigma^2} = \pm \epsilon_0$,
 - (iii) il existe $v \in E_K$ telle que $v^{1+\sigma} = \pm \epsilon_x$,
 - (iv) il existe $w \in E_K$ telle que $w^2 = \pm \epsilon_0 \epsilon_x^{1-\sigma}$.

Lorsque ces conditions sont réalisées, on peut choisir u, v et w de telle sorte que $u = v = w = \epsilon$.

Cette propriété est démontrée par H. Hasse ([6]). Elle est aussi démontrée dans ([1]) comme cas particulier d'un résultat plus général.

Nous avons retrouvé directement ce résultat en montrant de plus que les seules structures de $\mathbb{Z}[G]$ -modules (a priori possibles pour le groupe des unités d'un corps K cyclique réel de degré 4) étaient les deux structures ci-dessus caractérisées par la valeur de Q_K (voir [4]).

II. CLASSES DE k QUI DEVIENNENT PRINCIPALES DANS K

1. Enoncé du problème.

Plaçons nous tout d'abord dans un cadre plus général : soit k un corps de nombres, K une extension cyclique, supposée totalement réelle, de degré premier p de k et soit τ un générateur de $H = \text{Gal}(K/k)$. Soient E_K le groupe des unités de K , $E_K^* = \{u \in E_K, N_{K/k}(u) = 1\}$ et E_k le groupe des unités de k ; on note j' l'homomorphisme "extension" des idéaux, qui est injectif, et j l'homomorphisme, du groupe des classes de k dans celui de K , qui s'en déduit. Si on désigne par P^H le groupe des idéaux principaux de K invariants par H , et par P_0 le groupe des idéaux principaux de k , on sait ([7]) que $P^H/j'P_0$ est canoniquement isomorphe à $E_K^*/E_K^{\tau-1}$ qui est non trivial d'après le théorème 92 de Hilbert. Si de plus, K/k est non ramifiée pour toute valuation, alors $P^H/j'P_0$ s'identifie à $\ker j$ et on obtient le théorème 94 de Hilbert, à savoir que $\ker j$ est isomorphe à $E_K^*/E_K^{\tau-1}$ et est donc non trivial. On montre de toute façon facilement que, sans hypothèse sur la ramification, $\ker j$ est seulement isomorphe à un sous-groupe de $E_K^*/E_K^{\tau-1}$ ce qui alors n'implique rien sur sa trivialité ou sa non trivialité et l'on peut se poser le problème de la détermination effective de $\ker j$.

Dans notre cas, où l'extension K/k est toujours ramifiée, nous allons montrer que $\ker j$ est isomorphe à un sous-groupe d'ordre 1 ou 2 de $E_K^*/E_K^{\tau-1}$ et que la connaissance de l'unité χ -relative génératrice ϵ_χ (ou plus simplement de l'unité φ_χ dévisée au maximum en 2) permet de le déterminer.

2. Construction d'un homomorphisme injectif θ de $\ker j$
dans $\mathcal{E} = E_K^*/E_K^{\sigma^2-1}$ et caractérisation de $\text{Im } \theta$.

On désigne par A_K l'anneau des entiers de K , par $\mathcal{H}(K)$ (resp. $\mathcal{H}(k)$) le 2-groupe des classes au sens ordinaire de K (resp. k). Soit \mathfrak{b} un idéal de k et soit $\mathfrak{b} A_K$ l'idéal étendu à K ; on considère l'homomorphisme j extension des classes qui à $cl_k(\mathfrak{b})$ de $\mathcal{H}(k)$ fait correspondre $cl_K(\mathfrak{b} A_K)$ de $\mathcal{H}(K)$. Alors $\ker j$ est l'ensemble des classes des idéaux \mathfrak{b} de k pour lesquels il existe $\beta \in K^*$ tel que $\mathfrak{b} A_K = \beta A_K$; c'est un 2-groupe d'exposant 2.

PROPOSITION 3. — Soit E_K^* l'ensemble des $w \in E_K$ telles que $N_{K/k}(w) = +1$. Il existe un homomorphisme injectif θ de $\ker j$ dans $\mathcal{E} = E_K^*/E_K^{\sigma^2-1}$.

Démonstration. — Soit $cl_k(\mathfrak{b}) \in \ker j$; alors $\mathfrak{b} A_K = \beta A_K$, $\beta \in K^*$; on a $(\mathfrak{b} A_K)^{\sigma^2-1} = \mathfrak{b}^{\sigma^2-1} A_K = (1)$ puisque $\mathfrak{b} \subset k$; donc $\mathfrak{b}^{\sigma^2-1} A_K = (1)$, soit $\mathfrak{b}^{\sigma^2-1} = u$, u unité de K ; alors $u \in E_K^*$ et on associe à $cl_k(\mathfrak{b})$ l'image \bar{u} de u dans \mathcal{E} . On vérifie que l'on obtient un homomorphisme injectif.

PROPOSITION 4. — L'image de θ est l'ensemble des classes dans \mathcal{E} des unités w de K telles qu'il existe un élément α de K^* et un idéal α de k vérifiant les relations $\alpha^{\sigma^2-1} = u$ et $\alpha A_K = \alpha A_K$.

Démonstration. — Soit $\bar{u} \in \mathcal{E}$, $\bar{u} \neq \bar{1}$, $u \in E_K^*$; d'après le théorème 90 de Hilbert, u est de la forme α^{σ^2-1} , $\alpha \in K^*$, α défini modulo k^* . On étudie la décomposition en idéaux premiers de αA_K ; αA_K est un idéal principal invariant puisque $\alpha^{\sigma^2-1} = u$; il s'écrit donc de façon unique sous la forme $\alpha A_K = \alpha A_K \times \mathfrak{P}_1 \times \dots \times \mathfrak{P}_n$ où α est un idéal de k et où $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ ($n \geq 0$) sont des idéaux premiers ramifiés dans K/k que l'on peut supposer distincts.

On vérifie que si l'on change u modulo $E_K^{\sigma^2-1}$, αA_K ne change pas modulo les idéaux principaux de k . D'après la définition de θ , \bar{u} sera un élément de $\text{Im } \theta$ si et seulement si $\alpha A_K = \alpha A_K$ (c'est-à-dire $n = 0$) d'où la proposition.

Remarque 3. — Si $u \in E_K^*$, $u \neq -1$, alors $\alpha = 1 + u$ est tel que $\alpha^{1-\sigma^2} = u$.

En effet $\alpha^{\sigma^2} = 1 + u^{\sigma^2} = 1 + \frac{1}{u}$ et $\alpha^{1-\sigma^2} = u$.

Remarque 4. — En pratique, on aura $\ker j \neq 1$ si et seulement s'il existe $u \in E_K^*$, $u \notin E_K^{\sigma^2-1}$ telle que dans la décomposition en idéaux premiers de αA_K ($\alpha = 1 + u$ par exemple), aucun idéal premier ramifié dans K/k n'intervienne à une puissance impaire.

3. Détermination de $\mathcal{E} = E_K^*/E_K^{\sigma^2-1}$ et d'un sous-groupe de \mathcal{E} contenant $\text{Im } \theta$.

Soit ϵ_χ un générateur du groupe E_χ des unités χ -relatives de K et soit $s = N_{K/k}(\epsilon_\chi) = \pm 1$. On a alors les deux propositions dont les démonstrations sont élémentaires :

PROPOSITION 5. — Si $s = +1$, $E_K^* = E_\chi$. Si $s = -1$, E_K^* est engendré par -1 et $\epsilon_\chi^{1-\sigma}$.

PROPOSITION 6. — Le groupe $\mathcal{E} = E_K^*/E_K^{\sigma^2-1}$ est formé des éléments suivants :

- 1) Si $Q_K = 1$ et $s = +1$, alors $\mathcal{E} = \{\overline{\pm 1}, \overline{\pm \epsilon_\chi}, \overline{\pm \epsilon_\chi^\sigma}, \overline{\pm \epsilon_\chi^{1-\sigma}}\}$,
- 2) Si $Q_K = 1$ et $s = -1$, alors $\mathcal{E} = \{\overline{\pm 1}, \overline{\pm \epsilon_\chi^{1-\sigma}}\}$,
- 3) Si $Q_K = 2$ et $s = +1$, alors $\mathcal{E} = \{\overline{\pm 1}, \overline{\pm \epsilon_\chi}\}$,
- 4) Si $Q_K = 2$ et $s = -1$, alors $\mathcal{E} = \{\overline{\pm 1}\}$.

PROPOSITION 7. — Lorsque $N_{K/k}(\epsilon_\chi) = +1$, aucun des éléments $\overline{\epsilon_\chi}, \overline{\epsilon_\chi^\sigma}, \overline{-\epsilon_\chi}, \overline{-\epsilon_\chi^\sigma}$ n'appartient à $\text{Im } \theta$.

Démonstration. — Puisque $\epsilon_\chi \in E_K^*$, $\alpha = 1 + \epsilon_\chi$ vérifie $\epsilon_\chi = \alpha^{1-\sigma^2}$; supposons que $\overline{\epsilon_\chi}$ appartienne à $\text{Im } \theta$; alors $\alpha A_K = a A_K$, a idéal de k ; il en résulte que

$$\alpha^{1+\sigma} A_K = a^{1+\sigma} A_K = \rho A_K, \quad \rho \in \mathbf{Q};$$

donc il existe v unité de K telle que $\alpha^{1+\sigma} = \rho v$; alors $\alpha^{1-\sigma^2} = (\rho v)^{1-\sigma} = v^{1-\sigma}$; on a donc $\epsilon_\chi = v^{1-\sigma}$; mais alors l'unité v est nécessairement χ -relative : en effet

$$N_{K/\mathbf{Q}}(\alpha) = \alpha^{(1+\sigma)(1+\sigma^2)} = \rho^{1+\sigma^2} v^{1+\sigma^2} = \rho^2 v^{1+\sigma^2};$$

mais $N_{K/\mathbf{Q}}(\alpha) = \pm \rho^2$; donc $N_{K/k}(v) = \pm 1$ et $v \in E_x$. Donc l'hypothèse $\epsilon_x \in \text{Im } \theta$ entraîne qu'il existe $v \in E_x$ telle que $\epsilon_x = v^{1-\sigma}$, ce qui est en contradiction avec ϵ_x générateur de E_x . Donc $\bar{\epsilon}_x \notin \text{Im } \theta$. Le raisonnement est le même pour $\overline{\epsilon_x^\sigma}$, $-\bar{\epsilon}_x$ et $-\overline{\epsilon_x^\sigma}$.

PROPOSITION 8. — Soit $u_x \neq \pm 1$ une unité x -relative. Alors $-u_x^{1-\sigma}$ n'appartient pas à $\text{Im } \theta$.

Démonstration. — L'unité $-u_x^{1-\sigma}$ appartient à E_K^* ; donc si $u_x \neq \pm 1$, $\alpha = 1 - u_x^{1-\sigma}$ vérifie $\alpha^{1-\sigma^2} = -u_x^{1-\sigma}$; soit $\psi = \sqrt{\sqrt{mg} \frac{\sqrt{m+a}}{2}}$ (avec $g = \frac{f}{m}$ et $m = a^2 + b^2$, $a > 0$, b pair) ; alors $\psi^{\sigma^2} = -\psi$ et $\psi^{1-\sigma^2} \alpha^{1-\sigma^2} = u_x^{1-\sigma}$; il en résulte que $(\psi\alpha)^{1+\sigma} = \rho'u_x$, $\rho' \in \mathbf{Q}$. Supposons de plus que $\alpha A_K = a A_K$, a idéal de k ; alors il existe $v \in E_K$ et $\rho \in \mathbf{Q}$ tels que $\alpha^{1+\sigma} = \rho v$; on a donc $\psi^{1+\sigma} \rho v = \rho'u_x$, c'est-à-dire que $\psi^{1+\sigma} = \rho''w$, $\rho'' \in \mathbf{Q}$, $w \in E_K$; or $\psi\psi^\sigma = \pm \sqrt{mg} \frac{b}{2}$; ceci est donc impossible.

COROLLAIRE. — Les deux éléments $\overline{-1}$ et $-\overline{\epsilon_x^{1-\sigma}}$ de \mathcal{E} n'appartiennent pas à $\text{Im } \theta$.

Démonstration. — La proposition 8 appliquée à $u_x = \epsilon_x$ entraîne le résultat pour $-\overline{\epsilon_x^{1-\sigma}}$. Pour l'appliquer à $\overline{-1}$, on remarque que :

si $N_{K/k}(\epsilon_x) = 1$, $\overline{-1} = -\overline{\epsilon_x^2}$ et $u_x = \epsilon_x^{1+\sigma}$ vérifie $-u_x^{1-\sigma} = -\epsilon_x^2$,

si $N_{K/k}(\epsilon_x) = -1$, $\overline{-1} = -\overline{\epsilon_x^{2(1-\sigma)}}$ et $u_x = \epsilon_x^{1-\sigma^2}$ vérifie $-u_x^{1-\sigma} = -\epsilon_x^{2(1-\sigma)}$.

On a donc démontré :

PROPOSITION 9. — On a $\text{Im } \theta \subset \{1, \overline{\epsilon_x^{1-\sigma}}\}$.

La proposition 6 entraîne que si $Q_K = 2$, alors $\ker j = (1)$. Il reste à étudier, lorsque $Q_K = 1$, si $\overline{\epsilon_x^{1-\sigma}}$ appartient ou non à $\text{Im } \theta$.

4. Etude du cas $Q_K = 1$.

Soit ϵ_x une unité χ -relative génératrice de E_x ; posons $s = N_{K/k}(\epsilon_x)$, $t = \text{Tr}_{K/\mathfrak{Q}}(\epsilon_x)$ et

$$r = \epsilon_x^{1+\sigma} + \epsilon_x^{1+\sigma^2} + \epsilon_x^{1+\sigma^3} + \epsilon_x^{\sigma+\sigma^2} + \epsilon_x^{\sigma+\sigma^3} + \epsilon_x^{\sigma^2+\sigma^3}.$$

On vérifie que le polynôme minimal sur \mathfrak{Q} de ϵ_x est égal à $X^4 - tX^3 + rX^2 - sX + 1$ et que celui de $\epsilon_x^{1-\sigma}$ se met alors sous la forme $X^4 - TX^3 + RX^2 - TX + 1$, avec $T = sr - 2$ et $R = st^2 - 2sr + 2$. On trouve alors facilement la relation $N_{K/\mathfrak{Q}}(1 + \epsilon_x^{1-\sigma}) = R + 2T + 2 = st^2$, que nous écrivons sous forme de proposition.

PROPOSITION 10. — Soit ϵ_x l'unité χ -relative génératrice de E_x ; soient $s = N_{K/k}(\epsilon_x)$ et $t = \text{Tr}_{K/\mathfrak{Q}}(\epsilon_x)$; alors $N_{K/\mathfrak{Q}}(1 + \epsilon_x^{1-\sigma}) = st^2$.

Pour savoir si $\overline{\epsilon_x^{1-\sigma}}$ appartient ou non à $\text{Im } \theta$, on est amené à étudier la décomposition en idéaux premiers de l'idéal invariant αA_K , où $\alpha = 1 + \epsilon_x^{1-\sigma}$. On étudie le problème localement (c'est-à-dire en un p ramifié dans K/k , p fixé); on peut écrire de façon unique :

(i) si p est inerte ou ramifié dans k/\mathfrak{Q} : $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^x$,

(ii) si p est décomposé dans k/\mathfrak{Q} : $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^x \mathfrak{P}'^y$,

en appelant \mathfrak{P} (resp. \mathfrak{P} et \mathfrak{P}') l'idéal premier au-dessus de p dans K (resp. les deux idéaux premiers conjugués par σ au-dessus de p dans K) et où \mathfrak{M}_p est un idéal ambige premier à p .

Il est clair que dans la décomposition $\alpha A_K = \alpha A_K \mathfrak{P}_1 \times \dots \times \mathfrak{P}_n$ (α idéal de k , $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ ($n \geq 0$) idéaux premiers distincts ramifiés dans K/k), une condition nécessaire et suffisante pour que $n = 0$ est que pour tout p ramifié dans K/k on ait :

$$x \equiv 0 \pmod{2} \text{ dans le cas (i),}$$

$$x \equiv y \equiv 0 \pmod{2} \text{ dans le cas (ii).}$$

L'appartenance de $\overline{\epsilon_x^{1-\sigma}}$ à $\text{Im } \theta$ se ramène donc à un nombre fini de conditions de valuations que nous allons expliciter de façon complète et immédiatement utilisable en pratique.

a) Cas où p (ramifié dans K/k) est ramifié dans k/\mathfrak{Q} .

La condition $N_{K/\mathbf{Q}}(\alpha) = \pm t^2$ entraîne $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^{2x}$.

b) Cas où p (ramifié dans K/k) est inerte dans k/\mathbf{Q} .

Soit $c = v_p(t)$, c'est-à-dire que $t = p^c t'$, $(t', p) = 1$; la condition $N_{K/\mathbf{Q}}(\alpha) = \pm p^{2c} r'^2$, $(t', p) = 1$ entraîne que $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^c$. On vérifie en particulier que :

(i) si $p \equiv 1 \pmod{4}$, alors $c = 0$: en effet, il existe $\omega \in k^*$ ($\omega^\sigma \equiv \omega^p(p)$) tel que $\epsilon_x \equiv \omega(\mathfrak{P})$; en utilisant le fait que $\epsilon_x^{1+\sigma^2} \equiv \omega^2 \equiv s(p)$ et que $p \equiv 1 \pmod{4}$, on en déduit que $\omega^\sigma \equiv \omega \pmod{p}$ et que $\text{Tr}_{K/k}(\epsilon_x) \equiv 4\omega \pmod{p}$;

(ii) si $N_{K/k}(\epsilon_x) = 1$, alors $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^{2x}$: en effet $\epsilon_x \in E_K^*$; donc $\epsilon_x = \beta^{1-\sigma^2}$, $\beta \in K^*$ et $\alpha^{1-\sigma^2} = \epsilon_x^{1-\sigma}$; la décomposition de αA_K se déduit de celle de βA_K .

c) Cas où p (ramifié dans K/k) est décomposé dans k/\mathbf{Q} .

Soient $c = v_p(t)$ et $e = v_p(sr + 2)$, c'est-à-dire que $t = p^c t'$, $(t', p) = 1$ et $sr + 2 = p^e r'$, $(r', p) = 1$. Si $c = 0$, alors $\alpha A_K = \mathfrak{M}_p$; si $c \neq 0$, alors on montre que $e \neq 0$. La connaissance de la norme de α sur \mathbf{Q} n'est plus suffisante pour déterminer la décomposition de αA_K . On la déduit de l'étude de $\text{Irr}(\alpha^2, \mathbf{Q})$. On vérifie que $\alpha A_K = \mathfrak{M}_p \mathfrak{P}^{\min(c,e)} \mathfrak{P}^{2c-\min(c,e)}$.

5. Conclusion.

Les résultats démontrés dans les paragraphes précédents se résument en le théorème suivant :

THEOREME. — Soit K une extension cyclique réelle de degré 4 de \mathbf{Q} de sous-corps quadratique k . Soit ϵ_x l'unité χ -relative génératrice de E_x et soit $Q_K = (|E_K| : |E_k| \oplus |E_x|)$. Soit $s = N_{K/k}(\epsilon_x)$ et soit $\text{Irr}(\epsilon_x, \mathbf{Q}) = X^4 - tX^3 + rX^2 - sX + 1$; pour tout nombre premier p , on pose $c = v_p(t)$ et $e = v_p(sr + 2)$. On a les propriétés suivantes :

a) Il existe au plus une classe non triviale de k devenant principale dans K et lorsqu'une telle classe existe, on a $(1 + \epsilon_x^{1-\sigma}) A_K = \alpha A_K$, où α idéal non principal de k représente la classe en question.

b) Si $Q_K = 2$ alors aucune classe non triviale de k ne devient principale dans K .

c) Si $Q_K = 1$, une condition nécessaire et suffisante pour qu'une classe non triviale de k devienne principale dans K est que tout nombre premier p ramifié dans K/k vérifie l'une des trois conditions suivantes :

- (i) p est ramifié dans k/\mathbf{Q} ,
- (ii) p est inerte dans k/\mathbf{Q} et c est pair,
- (iii) p est décomposé dans k/\mathbf{Q} et $\min(c, e)$ est pair.

Remarque 5. — Soit p (ramifié dans K/k) et inerte dans k/\mathbf{Q} ; la condition $c \equiv 0 \pmod{2}$ est vérifiée si

- (i) $p \equiv 1 \pmod{4}$
- ou
- (ii) $s = +1$.

Remarque 6. — Pour déterminer si une classe de k devient principale dans K (y compris le calcul de Q_K et de s) il suffit de connaître l'unité φ_x dévissée au maximum en 2 à la place de ϵ_x .

Remarque 7. — Nous avons démontré dans [4] le fait suivant : soit p ramifié dans K/k :

- (i) Si $s = -1$ et si $p \equiv 3 \pmod{4}$, alors p est inerte dans k/\mathbf{Q} et c est impair.
- (ii) Si $s = -1$ et si $g = 4g'$, g' impair, alors 2 est inerte dans k/\mathbf{Q} et $c = 1$.

III. RESULTATS NUMERIQUES

Les tables numériques ont été établies sur l'ordinateur IRIS 50 du centre de calcul de l'Université de Besançon. Nous avons calculé une valeur approchée de toutes les quantités avec une double précision réelle (15 chiffres significatifs). Pour certains corps, nous avons dû utiliser l'ordinateur du C.I.R.C.E. muni de la quadruple précision. Ces tables numériques qui paraîtront intégralement dans [4] donnent pour chaque extension K cyclique réelle de degré 4 de \mathbf{Q} et de

conducteur inférieur à 4000 :

- le conducteur f de K ,
- la décomposition en facteurs premiers de f ,
- le conducteur m du sous-corps quadratique k de K ,
- les entiers a et b ($a, b > 0$, b pair) tels que $m = a^2 + b^2$, définissant le corps K parmi ceux de conducteur égal à f ,
- la norme dans k/\mathbf{Q} du générateur ϵ_0 de E_k , notée s_0 ,
- la norme dans K/k du générateur ϵ_x de E_x , notée s ,
- $t = \epsilon_x + \epsilon_x^\sigma + \epsilon_x^{\sigma^2} + \epsilon_x^{\sigma^3}$,
- $r = \epsilon_x \epsilon_x^\sigma + \epsilon_x \epsilon_x^{\sigma^2} + \epsilon_x \epsilon_x^{\sigma^3} + \epsilon_x^\sigma \epsilon_x^{\sigma^2} + \epsilon_x^\sigma \epsilon_x^{\sigma^3} + \epsilon_x^{\sigma^2} \epsilon_x^{\sigma^3}$,
- l'indice $Q_K = (|E_K| : |E_x| \oplus |E_k|)$ (égal à 1 ou 2),
- l'indice $h_x = (|E_x| : |F_x|)$,
- le nombre de classes h_0 de k ,
- le nombre de classes h de K (on a $h = \frac{Q_K}{2} h_0 h_x$),
- le symbole $*$ lorsqu'une classe non triviale de k devient principale dans K .

En annexe 1, nous donnons la fin de la table ($3950 \leq f \leq 4000$).

A notre connaissance, la seule table existante exclusivement consacrée aux corps cycliques de degré 4 est celle déterminée par H. Hasse ([6]) qui donne le nombre de classes et les unités pour les corps K du conducteur inférieur à 100.

Les principales remarques que l'on peut déduire de l'étude de notre table sont les suivantes :

a) Il y a 1536 corps K de conducteur $f \leq 4000$. Dans cet intervalle il y a exactement :

81	corps pour lesquels h_x est divisible par	5,
4	"	9
8	"	13
3	"	17.

Dans l'annexe 2, nous donnons les extraits de la table concernant les corps K de plus petit conducteur tels que 5, 9, 13 ou 17 divise h_x ; nous donnons également deux exemples (hors table) pour lesquels 25 puis 29 divise h_x .

b) Les 1536 corps K de conducteur $f \leq 4000$ se répartissent en :

- (i) 130 corps pour lesquels f est premier (ou $f = 16$) ; alors $m = f$ (ou $m = 8$), $Q_K = 2$, $s_0 = s = -1$, h_0 , h_x et h sont impairs.
- (ii) 892 corps pour lesquels f est composé et m est premier (ou égal à 8). Alors h_0 est impair et h_x est pair. Parmi ces corps, on constate que $Q_K = 2$ pour 95 d'entre eux.
- (iii) 514 corps pour lesquels f et m sont composés. Alors h_0 et h_x sont pairs. Parmi ces corps, on constate que $Q_K = 2$ pour 81 d'entre eux. Le problème de l'existence d'une classe de k qui devient principale dans K ne se pose que pour ces corps. Parmi ces 514 corps, on constate que pour 231 d'entre eux une classe de k devient principale dans K (pour 181 corps, la raison en est que $Q_K = 1$ et tous les p_i ramifiés dans K sont totalement ramifiés (théorème c) (i)).

c) Supposons f et m fixés et soit $m = p_0 p_1 \dots p_n$, $p_i \equiv 1 \pmod{4}$ (p_0 pouvant être égal à 8) la décomposition de m en facteurs premiers ; alors le nombre de tels corps est égal à 2^n . En général, on constate que de tels corps ont des propriétés analogues (valeur de Q_K , 2-valeur de h_x , capitulation ou non capitulation de classes de k dans K) ; il y a pourtant des exceptions ; nous en donnons la liste dans l'annexe 3.

ANNEXE I

f	m	a	b	s_0	s	t	h	Q_K	h_x	h_0	h
3952	16.13.19	104	10	2	-1	+1	30988772				4
3952	16.13.19	104	2	10	-1	+1	42332	2385768742			4
3952	16.13.19	8	2	2	-1	-1	1766772	-17655866			4
3955	5.7.11.3	565	23	6	-1	-1	84066297	-4420006			2
3955	5.7.11.3	565	9	22	-1	-1	2772	100605417019			4
3955	5.7.11.3	5	1	2	-1	-1	159383	-6488466			4
3959	37.10.7	37	1	6	-1	+1	39697	-4412091			2
3961	17.23.3	3961	45	44	-1	-1	5016	4231955			2
3961	17.23.3	3961	19	60	-1	-1	351314028	-47538			4
3961	17.23.3	233	13	8	-1	-1	857328059242609928	1012881470569			4
3961	17.23.3	17	1	4	-1	-1	250598	-8139469583914491175554			2
3965	5.13.61	793	27	8	+1	+1	3839	-871986429			2
3965	5.13.61	793	3	28	+1	+1	97065608634284	71376			4
3965	5.13.61	305	17	4	+1	-1	5971379992	64227873647273561651366			4
3965	5.13.61	305	7	16	+1	-1	227	365814594571134			8
3965	5.13.61	65	7	4	-1	+1	247229584	-6			8
3965	5.13.61	65	1	8	-1	+1	3904	-12124771874			8
3973	29.13.7	137	11	4	-1	-1	23026166254124553904	-91319			8
3977	41.97	3977	61	16	-1	-1	9216474608056	53591816641378876959294			2
3977	41.97	3977	29	56	-1	-1	4468904739702197288	-561877349426591490			2
3977	41.97	97	9	4	-1	-1	110223534	349655872425034714838089086			2
3977	41.97	41	5	4	-1	-1	80519	-1190448809845301			2
3979	23.17.3	173	13	2	-1	+1	6236473	142505618			2
3984	16.3.83	8	2	2	-1	-1	22908	16368437391			1
3985	5.797	3985	63	4	-1	-1	63	-207950854			2
3985	5.797	3985	41	48	-1	-1	2594103432	-6			26
3988	4.997	997	31	6	-1	-1	1617962617314	70876973720503294			10
3991	13.307	13	3	2	-1	-1	445764	-16171856753192848406			1
3995	5.17.47	85	9	2	-1	-1	22860760473	-28380306			1
3995	5.17.47	85	7	6	-1	-1	4183	-1186056663941			4
3995	5.17.47	5	1	2	-1	-1	3735513	13679			4
								-3342121			2

ANNEXE 2

f	m	a	b	s_0	s	t	r	Q_K	h_x	h_0	h
212	53	7	2	-1	-1	14	-6	1	10	1	5
1465	1465	21	32	-1	-1	1792	-41026	1	18	2	18 *
1172	293	17	2	-1	-1	34	-6	1	26	1	13
1697	1697	41	4	-1	-1	41	-6	2	17	1	17
4916	1229	35	2	-1	-1	70	-6	1	50	3	75
5492	1373	37	2	-1	-1	74	-6	1	58	3	87

ANNEXE 3

f	m	a	b	s_0	s	t	r	Q_K	h_x	h_0	h
1480	185	13	4	-1	-1	272	-6	1	16	2	16
1480	185	11	8	-1	-1	172	-4446	1	8	2	8 *
1780	445	21	2	-1	-1	42	-6	1	16	4	32
1780	445	11	18	-1	+1	716	-16014	1	16	4	32 *
1808	904	30	2	-1	-1	13500	42625402	2	8	8	64
1808	904	2	30	-1	-1	60	-6	1	8	8	32 *
2960	296	14	10	-1	-1	172	-6	1	16	2	16 *
2960	296	10	14	-1	-1	172	-1243206	1	8	2	8 *
2960	40	6	2	-1	-1	72372	232954	1	16	2	16
2960	40	2	6	-1	-1	468	-6	1	8	2	8 *
3120	104	10	2	-1	+1	100	-1242	1	32	2	32
3120	104	2	10	-1	-1	228	10394	1	16	2	16
3536	1768	42	2	-1	+1	1025852	-218595046170	1	8	8	32 *
3536	1768	38	18	-1	+1	412	14150	1	8	8	32 *
3536	1768	18	38	-1	-1	84	-141446	1	16	8	64 *
3536	1768	2	42	-1	-1	84	-6	1	32	8	128 *
3848	481	15	16	-1	-1	1014906276	-11785065662	1	8	2	8 *
3848	481	9	20	-1	-1	864	169306	1	16	2	16

BIBLIOGRAPHIE

- [1] L. BOUVIER et J.J. PAYAN, Modules sur certains anneaux de Dedekind. Application à la structure du groupe des classes et à l'existence d'unités de Minkowski, *J. reine angew. Math.*, 274/275 (1975), 278-286.
- [2] G. GRAS et M.N. GRAS, Calcul du nombre de classes et des unités des extensions abéliennes réelles de \mathbf{Q} , *Bull. Sc. Math.* 2^{ème} série, 101 (1977), 97-129.
- [3] M.N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbf{Q} , *J. reine angew. Math.*, 277 (1975), 89-116.
- [4] M.N. GRAS, Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de \mathbf{Q} , *Publ. Math. Univ. Besançon*, 1977-78, fasc. 2.
- [5] H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
- [6] H. HASSE, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Abh. Deutsch. Akad. Wiss. Berlin, Math.* (1948), n° 2, 1-95.
- [7] K. IWASAWA, A note on the group of units of an algebraic number field, *Journ. Math. Pures Appl.*, 35 (1956), 189-192.
- [8] H.W. LEOPOLDT, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, *Abh. Deutsche Akad. Wiss. Berlin, Math.* (1953), n° 2, 1-48.

Manuscrit reçu le 16 mars 1978.

Marie-Nicole GRAS,
(Equipe de Recherche associée au
C.N.R.S. n° 07 0654)
Faculté des Sciences
Mathématiques
25030 Besançon Cedex.