

ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS

Sur les Z_2 -extensions d'un corps quadratique imaginaire

Annales de l'institut Fourier, tome 33, n° 4 (1983), p. 1-18

http://www.numdam.org/item?id=AIF_1983__33_4_1_0

© Annales de l'institut Fourier, 1983, 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/>

SUR LES \mathbf{Z}_2 -EXTENSIONS D'UN CORPS QUADRATIQUE IMAGINAIRE

par Georges GRAS

0. Introduction et rappels.

Soit k une extension quadratique totalement imaginaire d'un corps totalement réel k_0 vérifiant la conjecture de Leopoldt pour $p = 2$, et soit $H = \{1, s\}$ le groupe de Galois de k/k_0 . Soit \tilde{k} le composé des \mathbf{Z}_2 -extensions de k , et soit \bar{k} le 2-corps de classes de Hilbert de k . Dans [5] nous avons apporté une solution aux problèmes suivants :

- (i) description de type corps de classes de $\text{Gal}(\tilde{k} \cap \bar{k}/k)$;
- (ii) détermination de la $\mathbf{Z}_2[H]$ -structure de $\text{Gal}(\tilde{k}/k)$.

Comme on nous l'a fait remarquer, les deux points ci-dessus ne sont pas totalement indépendants; dans cet article, nous étudions de façon générale cette dépendance, et donnons, dans le cas particulier où k est un corps quadratique imaginaire, une classification complète (cf. théorèmes 2.1, 2.2) montrant par exemple que, sauf si le complété en 2 de k est $\mathbf{Q}_2(\sqrt{-3})$ ou $\mathbf{Q}_2(\sqrt{-14})$, \tilde{k} est le composé *direct* de la \mathbf{Z}_2 -extension cyclotomique de k par la \mathbf{Z}_2 -extension de k prodiédrale sur \mathbf{Q} , si et seulement si $\tilde{k} \cap \bar{k} \neq k$. Nous donnons enfin la liste des corps quadratiques imaginaires pour lesquels on a $\tilde{k} \subset \bar{k}$ (théorème 2.3).

Redonnons brièvement les notations ainsi que la définition des logarithmes qui ont été introduits dans [5], § 1, 2, relativement à un corps de nombres k quelconque et un nombre premier p quelconque :

Soit \hat{k} la p -extension abélienne p -ramifiée maximale du corps de nombres k , et soient $\mathcal{A} = \text{Gal}(\hat{k}/k)$, $\tilde{\mathcal{A}} = \text{Gal}(\hat{k}/\tilde{k})$; on a $\mathcal{A}/\tilde{\mathcal{A}} \simeq \mathcal{H}$, le p -groupe des classes de k .

Il existe sur \mathcal{A} une application logarithme continue de la forme $\text{Log} : \mathcal{A} \rightarrow \mathcal{P}/\Lambda$, où $\mathcal{P} = \prod_{\mathfrak{p}|p} k_{\mathfrak{p}}$ est le produit des complétés en $\mathfrak{p}|p$ du corps k , où Λ est le \mathbf{Q}_p -espace vectoriel engendré par l'image du groupe des unités de k par le logarithme usuel $\ell\text{og} : \mathcal{U} \rightarrow \mathcal{P}$ ⁽¹⁾. On rappelle que l'on a le diagramme commutatif suivant de groupes, où α désigne l'application d'Artin $I \rightarrow \mathcal{A}$ définie sur l'ensemble I des idéaux premiers à p de k :

$$\begin{array}{ccc} I & \xrightarrow{\text{Log}} & \mathcal{P}/\Lambda \\ \alpha \downarrow & & \nearrow \text{Log} \\ \mathcal{A} & & \end{array}$$

l'application $\text{Log} : I \rightarrow \mathcal{P}/\Lambda$ étant définie par $\text{Log}(\mathfrak{A}) = n^{-1} \ell\text{og}(a)$ modulo Λ ,

où $\mathfrak{A}^n = (a)$, $a \in k$. Comme $\alpha(I)$ est dense dans \mathcal{A} , on a $\text{Log}(\mathcal{A}) = \overline{\text{Log}(I)}$, l'adhérence de $\text{Log}(I)$ dans \mathcal{P}/Λ . On vérifie que $\text{Log}(\mathcal{U})$ est l'image de $\ell\text{og}(\mathcal{U})$ dans \mathcal{P}/Λ ; par analogie on la note $\text{Log}(\mathcal{U})$ (on écrit, par abus, $\text{Log}(u) = \ell\text{og}(u)$ modulo Λ pour tout $u \in \mathcal{U}$). On sait ([5], théorème 2.1) que $\text{Ker}(\text{Log}) = \mathcal{C} = \text{Gal}(\bar{k}/k)$, le p -groupe de torsion de \mathcal{A} , ce qui établit un isomorphisme canonique de \mathbf{Z}_p -modules, de la forme

$$\text{Gal}(\bar{k}/k) \rightarrow \text{Log}(\mathcal{A}) = \overline{\text{Log}(I)}.$$

On pose $\mathcal{B} = \text{Gal}(\bar{k}/k)$, $\mathcal{B}' = \text{Gal}(\bar{k}/k \cap \bar{k})$, et

$$\mathcal{X} = \text{Gal}(\bar{k} \cap \bar{k}/k) \simeq \mathcal{B}/\mathcal{B}';$$

dans l'isomorphisme $\mathcal{B} \rightarrow \overline{\text{Log}(I)}$, \mathcal{B}' a pour image $\text{Log}(\mathcal{U})$, d'où

$$\mathcal{X} \simeq \overline{\text{Log}(I)}/\text{Log}(\mathcal{U}).$$

On a aussi défini dans [5], § 1, des applications $\text{Res}_{L/K}$ et $\text{Cor}_{L/K}$ dans une extension L/K de corps de nombres. Comme on a

$$\text{Res}_{L/K}(\mathcal{C}(L)) \subset \mathcal{C}(K) \quad \text{et} \quad \text{Cor}_{L/K}(\mathcal{C}(K)) \subset \mathcal{C}(L),$$

(1) Où \mathcal{U} est le groupe des unités principales de \mathcal{P} .

il en résulte que l'on peut définir des applications, notées encore $\text{Res}_{L/K}$ et $\text{Cor}_{L/K}$,

$$\text{Res}_{L/K} : \mathcal{B}(L) \rightarrow \mathcal{B}(K), \quad \text{Cor}_{L/K} : \mathcal{B}(K) \rightarrow \mathcal{B}(L);$$

la première n'est autre que la restriction des automorphismes

$$\text{Gal}(\tilde{L}/L) \rightarrow \text{Gal}(\tilde{K}/K),$$

son image est $\text{Gal}(\tilde{K}/\tilde{K} \cap L)$ et son noyau $\text{Gal}(\tilde{L}/\tilde{K}L)$; la seconde est injective car $\text{Res}_{L/K} \circ \text{Cor}_{L/K} = [L : K]$.

Soit $\text{Tr}_{L/K}$ (resp. $i_{L/K}$) la trace $\mathcal{P}(L)/\Lambda(L) \rightarrow \mathcal{P}(K)/\Lambda(K)$ (resp. l'injection canonique $\mathcal{P}(K)/\Lambda(K) \rightarrow \mathcal{P}(L)/\Lambda(L)$); comme on a

$$\text{Tr}_{L/K} \circ \text{Log} = \text{Log} \circ \text{Res}_{L/K} \quad \text{sur } \mathcal{A}(L),$$

et

$$i_{L/K} \circ \text{Log} = \text{Log} \circ \text{Cor}_{L/K} \quad \text{sur } \mathcal{A}(K) \text{ (cf. [5], § 2),}$$

il en résulte que l'on a ici les diagrammes commutatifs suivants, de \mathbb{Z}_p -modules :

$$\begin{array}{ccc} \mathcal{B}(L) & \xrightarrow{\text{Res}_{L/K}} & \mathcal{B}(K) \\ \cong \downarrow & & \downarrow \cong \\ \text{Log}(\mathcal{A}(L)) & \xrightarrow{\text{Tr}_{L/K}} & \text{Log}(\mathcal{A}(K)) \end{array} \quad \begin{array}{ccc} \mathcal{B}(K) & \xrightarrow{\text{Cor}_{L/K}} & \mathcal{B}(L) \\ \cong \downarrow & & \downarrow \cong \\ \text{Log}(\mathcal{A}(K)) & \xrightarrow{i_{L/K}} & \text{Log}(\mathcal{A}(L)) \end{array}$$

les isomorphismes étant induits par l'application Log .

Si L/K est galoisienne de groupe de Galois G , tous les groupes définis ci-dessus sont des $\mathbb{Z}_p[G]$ -modules, et toutes les applications des homomorphismes de $\mathbb{Z}_p[G]$ -modules. On a en outre dans ce cas

$$\text{Cor}_{L/K} \circ \text{Res}_{L/K} = \sum_{g \in G} g.$$

Enfin, la plus grande sous-extension F de \tilde{L}/L , normale sur K , telle que $\text{Gal}(F/L)$ soit \mathbb{Z}_p -libre et annulé par $\sum_{g \in G} g$, est le corps fixe par $\mathcal{B}(L)^G$.

Revenons au cas où k est un « CM-field » de sous-corps réel maximal k_0 de degré D_0 sur \mathbb{Q} ; on adopte pour k_0 des notations analogues : I_0 ,

LEMME. — Les quotients de Herbrand des H-modules $\check{\mathcal{B}}$ et \mathcal{B} sont égaux à 2^{1-D_0} . Les H-modules $\check{\mathcal{B}}^H/\check{\mathcal{B}}^{1+s}$ et $\mathcal{B}^H/\mathcal{B}^{1+s}$ sont d'ordre 1 ou 2, les H-modules $\check{\mathcal{B}}^*/\check{\mathcal{B}}^{1-s}$ et $\mathcal{B}^*/\mathcal{B}^{1-s}$ sont d'ordre 2^{D_0-1} ou 2^{D_0} .

Ceci résulte immédiatement de la méthode de calcul du quotient de Herbrand rappelée dans [1], p. XIX, compte tenu du fait que $\check{\mathcal{B}}$, \mathcal{B} sont \mathbf{Z}_2 -libres de dimension $D_0 + 1$, et $\check{\mathcal{B}}^H$, \mathcal{B}^H de dimension 1.

Dans [5] nous avons défini le nombre χ par

$$(\mathcal{B} : \mathcal{B}^H \mathcal{B}^*) = 2^\chi, \quad 0 \leq \chi \leq 1;$$

on rappelle qu'il caractérise la $\mathbf{Z}_2[\mathbf{H}]$ -structure de \mathcal{B} (cf. [5], corollaire 1 au théorème 3.2), et en particulier, \tilde{k} est le composé direct de la \mathbf{Z}_2 -extension cyclotomique k_∞ de k par une extension de k , normale sur k_0 , si et seulement si $\chi = 0$, ou encore si et seulement si le corps F fixe par \mathcal{B}^H est linéairement disjoint de k_∞ sur k .

Par analogie posons

$$(\check{\mathcal{B}} : \check{\mathcal{B}}^H \check{\mathcal{B}}^*) = 2^{\check{\chi}}, \quad 0 \leq \check{\chi} \leq 1;$$

on en déduit facilement les isomorphismes

$$\mathcal{B}^H/\mathcal{B}^{1+s} \simeq (\mathbf{Z}/2\mathbf{Z})^{1-\chi}, \quad \check{\mathcal{B}}^H/\check{\mathcal{B}}^{1+s} \simeq (\mathbf{Z}/2\mathbf{Z})^{1-\check{\chi}}.$$

Écrivons

$$\mathcal{K}^H/\mathcal{K}^{1+s} \simeq (\mathbf{Z}/2\mathbf{Z})^t, \quad t \geq 0;$$

alors la suite exacte ci-dessus a la forme suivante :

$$\begin{aligned} \xrightarrow{\partial} (\mathbf{Z}/2\mathbf{Z})^{1-\check{\chi}} &\rightarrow (\mathbf{Z}/2\mathbf{Z})^{1-\chi} \rightarrow (\mathbf{Z}/2\mathbf{Z})^t \xrightarrow{\partial'} \\ &\xrightarrow{\partial'} (\mathbf{Z}/2\mathbf{Z})^{D_0-\check{\chi}} \rightarrow (\mathbf{Z}/2\mathbf{Z})^{D_0-\chi} \rightarrow (\mathbf{Z}/2\mathbf{Z})^t \xrightarrow{\partial}. \end{aligned}$$

Posons enfin

$$\partial((\mathbf{Z}/2\mathbf{Z})^t) = (\mathbf{Z}/2\mathbf{Z})^\delta, \quad 0 \leq \delta \leq 1.$$

Remarque. — Si l'on pose $\partial'((\mathbf{Z}/2\mathbf{Z})^t) = (\mathbf{Z}/2\mathbf{Z})^\delta$, on a immédiatement $\delta' = t - \delta - \check{\chi} + \chi$; on peut donc baser la discussion sur les invariants $\check{\chi}$, δ , χ et t .

On a donc, tout d'abord, des relations de type algébrique entre les invariants $\check{\chi}$, δ , χ et t , qui proviennent de cette suite exacte :

PROPOSITION 1.1. — On a :

- (i) $\chi \leq \check{\chi} + \delta \leq 1$,
(ii) t vérifie les inégalités suivantes :

$\check{\chi}$	δ	$\chi = 0$	$\chi = 1$
0	0	$0 \leq t \leq D_0$	
0	1	$1 \leq t \leq D_0 + 1$	$1 \leq t \leq D_0$
1	0	$1 \leq t \leq D_0$	$0 \leq t \leq D_0 - 1$

Remarque. — Le premier point résulte aussi de la suite exacte

$$1 \rightarrow \check{\mathcal{B}}^H \cap \mathcal{B}^{1+s} / \check{\mathcal{B}}^{1+s} \rightarrow \check{\mathcal{B}}^H / \check{\mathcal{B}}^{1+s} \rightarrow \check{\mathcal{B}}^H / \check{\mathcal{B}}^H \cap \mathcal{B}^{1+s} \rightarrow 1,$$

et de l'injection

$$\check{\mathcal{B}}^H / \check{\mathcal{B}}^H \cap \mathcal{B}^{1+s} \rightarrow \mathcal{B}^H / \mathcal{B}^{1+s}.$$

Comme nous le disons dans l'introduction, la question de la structure de $\text{Gal}(\check{k} \cap \check{k} / k)$ n'est pas indépendante de celle de la disjonction linéaire sur k de k_∞ et F ; on a en effet obtenu le résultat suivant :

THÉORÈME 1.1. — Si k est un « CM-field » de sous-corps réel maximal k_0 vérifiant la conjecture de Leopoldt pour $p = 2$, alors on a, relativement aux invariants χ et t , les deux obstructions suivantes :

- (i) si $t = D_0 + \delta$, alors $\chi = 0$;
(ii) si $t = 0$, alors $\chi = \check{\chi}$.

Nous allons montrer que l'invariant δ est, comme $\check{\chi}$, un invariant local (i.e. ne dépendant que de \mathcal{P}), et en donner une méthode de calcul.

DÉFINITION. — On appelle 2^R l'indice ($\text{res}(\mathcal{B}) : \text{res}(\check{\mathcal{B}}) \text{res}(\mathcal{B}^2)$); on a $0 \leq R \leq 1$.

PROPOSITION 1.2. — On a $R = 0$ si et seulement si $k_\infty \cap \check{k} = k$. On a la relation $\delta = R(1 - \check{\chi})$.

Le premier point résulte du fait que

$$(\text{res}(\mathcal{B}) : \text{res}(\check{\mathcal{B}})) = [\check{k}_0 \cap \check{k} : k_0] = [k_\infty \cap \check{k} : k].$$

Si $\check{\chi} = 1$, la proposition 1.1, (i), donne $\delta = 0$. Supposons alors $\check{\chi} = 0$; on a $\check{\mathcal{B}} = \check{\mathcal{B}}^H \check{\mathcal{B}}^*$ par définition. On obtient alors

$$\begin{aligned} \text{res}(\mathcal{B})/\text{res}(\check{\mathcal{B}})\text{res}(\mathcal{B}^2) &= \text{res}(\mathcal{B})/\text{res}(\check{\mathcal{B}})\text{res}(\mathcal{B}^{1+s}) \\ &\simeq \mathcal{B}/\check{\mathcal{B}}\mathcal{B}^{1+s}\mathcal{B}^* = \mathcal{B}/\check{\mathcal{B}}^H\mathcal{B}^{1+s}\mathcal{B}^*, \end{aligned}$$

soit $2^R = (\mathcal{B}:\check{\mathcal{B}}^H\mathcal{B}^{1+s}\mathcal{B}^*)$, et on a la suite exacte

$$1 \rightarrow \check{\mathcal{B}}^H/\check{\mathcal{B}}^H \cap \mathcal{B}^{1+s} \rightarrow \mathcal{B}/\mathcal{B}^{1+s}\mathcal{B}^* \rightarrow \mathcal{B}/\check{\mathcal{B}}^H\mathcal{B}^{1+s}\mathcal{B}^* \rightarrow 1$$

(en effet, le noyau est $\check{\mathcal{B}}^H/\check{\mathcal{B}}^H \cap (\mathcal{B}^{1+s}\mathcal{B}^*)$, mais comme $\mathcal{B}^H \cap \mathcal{B}^* = (1)$, $\check{\mathcal{B}}^H \cap (\mathcal{B}^{1+s}\mathcal{B}^*) = \check{\mathcal{B}}^H \cap \mathcal{B}^{1+s}$). Comme on a aussi $(\check{\mathcal{B}}^H:\check{\mathcal{B}}^{1+s}) = 2$ et $(\check{\mathcal{B}}^H \cap \mathcal{B}^{1+s}:\check{\mathcal{B}}^{1+s}) = 2^\delta$, il vient $(\check{\mathcal{B}}^H:\check{\mathcal{B}}^H \cap \mathcal{B}^{1+s}) = 2^{1-\delta}$, et la suite exacte conduit à $(\mathcal{B}:\mathcal{B}^{1+s}\mathcal{B}^*) = 2^{1-\delta+R}$; or

$$\mathcal{B}/\mathcal{B}^{1+s}\mathcal{B}^* \simeq \text{res}(\mathcal{B})/(\text{res}(\mathcal{B}))^2 \text{ qui est d'ordre } 2,$$

d'où $R = \delta$ dans ce cas. D'où la formule donnant δ .

Il est commode d'introduire l'invariant (local) suivant :

DÉFINITION. — On appelle 2^r l'indice $(\check{\mathcal{B}}_0 : \text{res}(\check{\mathcal{B}})) = [\check{k}_0 \cap \check{k} : \check{k}_0 \cap k_0]$; on a $0 \leq r \leq 1$.

THÉORÈME 1.2. — On a les formules suivantes (où $2^{n_0} = [\mathbf{Q}_\infty \cap k_0 : \mathbf{Q}]$) :

(i) $[k_\infty \cap \check{k} : k] = 2^r |\mathcal{X}_0| = 2^{-n_0} (4\mathbf{Z}_2 : \ell \log(N\mathcal{U}))$,

$$|\mathcal{X}_0| = 2^{-n_0} (4\mathbf{Z}_2 : \ell \log(N_0\mathcal{U}_0)),$$

$$2^r = (\ell \log(N_0\mathcal{U}_0) : \ell \log(N\mathcal{U}));$$

(ii) $[F \cap \check{k} : k] = 2^{x-\check{x}} \times \frac{|\mathcal{X}|}{2^r |\mathcal{X}_0|}$, où F est le sous-corps de \check{k} fixe par \mathcal{B}^H et où $|\mathcal{X}| = (\text{Log}(\mathbf{I}) : \text{Log}(\mathcal{U}))$.

COROLLAIRE 1. — Le corps $\check{k} \cap k$ est de degré $2^{(R-1)x+\check{x}}$ sur le composé des corps $k_\infty \cap \check{k}$ et $F \cap \check{k}$; ce degré est 1 ou 2.

COROLLAIRE 2. — On a $R = 0$ si et seulement si $(4\mathbf{Z}_2 : \ell \log(\mathcal{N}\mathcal{U})) = 2^{n_0}$. L'invariant $\delta = R(1 - \check{\chi})$ est donc de nature locale.

On a $[k_\infty \cap \check{k} : k] = (\text{res}(\mathcal{B}) : \text{res}(\check{\mathcal{B}}))$; or l'application $\text{Res}_0 : \mathcal{B}_0 \rightarrow \mathbf{Q}_2$ est injective, et comme $\text{Res}_0 \circ \text{res} = \text{Res}$, on a donc

$$[k_\infty \cap \check{k} : k] = (\text{Res}(\mathcal{B}) : \text{Res}(\check{\mathcal{B}})) = (\text{Tr} \circ \text{Log}(\mathcal{A}) : \text{Tr} \circ \text{Log}(\check{\mathcal{A}})) \\ = (\ell \log \circ \text{Res}(\mathcal{A}) : \ell \log(\mathcal{N}\mathcal{U})) = (4 \times 2^{n_0} \mathbf{Z}_2 : \ell \log(\mathcal{N}\mathcal{U}))$$

puisque $\text{Res}(\mathcal{A}) = \text{Gal}(\mathbf{Q}_\infty : k \cap \mathbf{Q}_\infty)$.

On a

$$|\mathcal{X}_0| = [\check{k}_0 \cap k_0 : k_0] = (\mathcal{B}_0 : \check{\mathcal{B}}_0) = (\text{Res}_0(\mathcal{B}_0) : \text{Res}_0(\check{\mathcal{B}}_0)) \\ = (\text{Tr}_0 \circ \text{Log}(\mathcal{A}_0) : \text{Tr}_0 \circ \text{Log}(\check{\mathcal{A}}_0)) = (\ell \log \circ \text{Res}_0(\mathcal{A}_0) : \ell \log(\mathcal{N}_0 \mathcal{U}_0)) \\ = (4 \times 2^{n_0} \mathbf{Z}_2 : \ell \log(\mathcal{N}_0 \mathcal{U}_0)).$$

Ceci démontre (i).

Comme on a $\text{Gal}(\check{k}/k \cap \check{k}) = \check{\mathcal{B}}$ et $\text{Gal}(\check{k}/F) = \mathcal{B}^H$, il en résulte que l'on a $\text{Gal}(\check{k}/F \cap \check{k}) = \check{\mathcal{B}} \mathcal{B}^H$; on a alors $[F \cap \check{k} : k] = (\mathcal{B} : \check{\mathcal{B}} \mathcal{B}^H)$. On a l'isomorphisme $\mathcal{B}/\check{\mathcal{B}} \mathcal{B}^H \simeq \mathcal{B}^{1-1}/\check{\mathcal{B}}^{1-s}$, ce qui conduit, compte tenu des inclusions

$$\check{\mathcal{B}}^{1-s} \subset \mathcal{B}^{1-s} \subset \mathcal{B}^* \quad \text{et} \quad \check{\mathcal{B}}^{1-s} \subset \check{\mathcal{B}}^* \subset \mathcal{B}^*,$$

à

$$(\mathcal{B}^{1-s} : \check{\mathcal{B}}^{1-s}) = \frac{(\mathcal{B}^* : \check{\mathcal{B}}^*)(\check{\mathcal{B}}^* : \check{\mathcal{B}}^{1-s})}{(\mathcal{B}^* : \mathcal{B}^{1-s})} = (\mathcal{B}^* : \check{\mathcal{B}}^*) 2^{r-\check{\chi}}.$$

On a la suite exacte

$$1 \rightarrow \mathcal{B}^*/\check{\mathcal{B}}^* \rightarrow \mathcal{B}/\check{\mathcal{B}} \rightarrow \text{res}(\mathcal{B})/\text{res}(\check{\mathcal{B}}) \rightarrow 1;$$

d'où (ii) en utilisant l'expression de $(\text{res}(\mathcal{B}) : \text{res}(\check{\mathcal{B}}))$ donnée dans (i), et le fait que $(\mathcal{B} : \check{\mathcal{B}}) = |\mathcal{X}|$.

Remarque. — Les invariants $\check{\chi}$ et δ sont donc des invariants locaux; quant à χ et t , ce sont des invariants globaux liés à des propriétés fines des classes d'idéaux. Cependant on a la relation $\chi \leq \rho$, où ρ , $0 \leq \rho \leq 1$, est

l'invariant global (élémentaire) défini dans [5] (cf. corollaire 2 au théorème 3.2; voir aussi [2] et [3]); si $(\mathcal{H} : \mathcal{H}^2) = 2^c$, on a aussi la relation $t \leq c$.

2. Le cas des corps quadratiques imaginaires.

Dans ce cas, certaines simplifications ont lieu : comme $k_0 = \mathbf{Q}$, Λ est réduit à zéro, et on peut confondre les applications Log et ℓog en un sens évident; on a alors

$$\mathcal{B} \simeq \overline{\ell\text{og}(\mathbf{I})}, \quad \check{\mathcal{B}} \simeq \ell\text{og}(\mathcal{U}).$$

De plus on a

$$\mathcal{H}^{1+s} = (1), \quad \mathcal{H}^* = \mathcal{H}, \quad \mathcal{H}^{1+s} = (1), \quad \mathcal{H}^* = \mathcal{H}, \quad \mathcal{H}^{1-s} = \mathcal{H},$$

$\mathcal{H}^{\text{H}} = \mathcal{H}^{(2)}$ (noyau de l'élévation au carré), ce qui donne la suite exacte :

$$\xrightarrow{\partial} \check{\mathcal{B}}^{\text{H}} / \check{\mathcal{B}}^{1+s} \rightarrow \mathcal{B}^{\text{H}} / \mathcal{B}^{1+s} \rightarrow \mathcal{H}^{(2)} \xrightarrow{\partial'} \check{\mathcal{B}}^* / \check{\mathcal{B}}^{1-s} \rightarrow \mathcal{B}^* / \mathcal{B}^{1-s} \rightarrow \mathcal{H} / \mathcal{H}^2 \xrightarrow{\partial},$$

qui est donc de la forme ($D_0=1$)

$$\begin{aligned} \xrightarrow{\partial} (\mathbf{Z}/2\mathbf{Z})^{1-\check{\chi}} \rightarrow (\mathbf{Z}/2\mathbf{Z})^{1-\chi} \rightarrow (\mathbf{Z}/2\mathbf{Z})^t \xrightarrow{\partial'} \\ \xrightarrow{\partial'} (\mathbf{Z}/2\mathbf{Z})^{1-\check{\chi}} \rightarrow (\mathbf{Z}/2\mathbf{Z})^{1-\chi} \rightarrow (\mathbf{Z}/2\mathbf{Z})^t \xrightarrow{\partial}. \end{aligned}$$

Les invariants locaux $\check{\chi}$ et δ peuvent être explicités dans tous les cas :

On a $\check{\mathcal{B}}^{\text{H}} / \check{\mathcal{B}}^{1+s} \simeq (\ell\text{og}(\mathcal{U}))^{\text{H}} / \ell\text{og}(\text{N}\mathcal{U})$; dans le cas des corps quadratiques imaginaires, on peut déterminer $\ell\text{og}(\mathcal{U})$ facilement (cf. [4], chap. III), et en déduire $(\ell\text{og}(\mathcal{U}))^{\text{H}}$ et $\ell\text{og}(\text{N}\mathcal{U})$; d'où $\check{\chi}$.

On a $\partial(\mathcal{H} / \mathcal{H}^2) = \mathcal{B}^{1+s} / \check{\mathcal{B}}^{1+s}$ (car $\mathcal{B}^{1+s} \subset \check{\mathcal{B}}$); or $1+s = \text{cor} \circ \text{res}$, donc $\mathcal{B}^{1+s} / \check{\mathcal{B}}^{1+s} \simeq \text{res}(\mathcal{B}) / \text{res}(\check{\mathcal{B}})$ qui est d'ordre

$$[k_{\infty} \cap \check{k} : k] = (4\mathbf{Z}_2 : \ell\text{og}(\text{N}\mathcal{U}))$$

(cf. théorème 1.2, (i)); d'où δ .

D'où le tableau suivant, dans lequel la notation (a) désigne $a\mathbf{Z}_2$, le

\mathbf{Z}_2 -module engendré par a , et où \mathcal{O} est l'anneau des entiers de \mathcal{P} :

\mathcal{P}	\mathcal{U}	$\ell \log(\mathcal{U})$	$(\ell \log(\mathcal{U}))^H$	$\ell \log(\mathbf{N}\mathcal{U})$	$\tilde{\chi}$	δ
$\mathbf{Q}_2(\sqrt{-1})$	$1+(1+\sqrt{-1})\mathcal{O}$	$(4) \oplus (2+2\sqrt{-1})$	(4)	(4)	1	0
$\mathbf{Q}_2(\sqrt{-2})$	$1+\sqrt{-2}\mathcal{O}$	$(4) \oplus (2+\sqrt{-2})$	(4)	(4)	1	0
$\mathbf{Q}_2(\sqrt{-3})$	$1+2\mathcal{O}$	$(2) \oplus (2\sqrt{-3})$	(2)	(4)	0	0
$\mathbf{Q}_2(\sqrt{-5})$	$1+(1+\sqrt{-5})\mathcal{O}$	$(2) \oplus (2\sqrt{-5})$	(2)	(4)	0	0
$\mathbf{Q}_2(\sqrt{-6})$	$1+\sqrt{-6}\mathcal{O}$	$(4) \oplus (\sqrt{-6})$	(4)	(8)	0	1
$\mathbf{Q}_2 \times \mathbf{Q}_2$	$1+2\mathcal{O}$	$(4) \oplus (2+2(1,-1))$	(4)	(4)	1	0
$\mathbf{Q}_2(\sqrt{-10})$	$1+\sqrt{-10}\mathcal{O}$	$(4) \oplus (2+\sqrt{-10})$	(4)	(4)	1	0
$\mathbf{Q}_2(\sqrt{-14})$	$1+\sqrt{-14}\mathcal{O}$	$(4) \oplus (\sqrt{-14})$	(4)	(8)	0	1

Tableau I.

Les seules contraintes concernant l'invariant t , et qui ne proviennent pas de la proposition 1.1, (ii), concernent les cas $\mathcal{P} = \mathbf{Q}_2(\sqrt{-5})$ et $\mathcal{P} = \mathbf{Q}_2(\sqrt{-14})$ (elles sont de nature arithmétique) :

PROPOSITION 2.1. — Lorsque $\mathcal{P} = \mathbf{Q}_2(\sqrt{-5})$, on a $t = 1$.

Posons $k = \mathbf{Q}(\sqrt{-m})$, $m \equiv 5(8)$. Comme dans ce cas, on a $0 \leq t \leq 1$, il suffit de vérifier que $t \neq 0$. Ici 2 est ramifié : soit $\mathfrak{p}|2$ dans k , et soit \mathfrak{a} un idéal entier impair dans la classe de \mathfrak{p} ; on a

$$\mathfrak{a}\mathfrak{p} = (a), \quad a = u + v\sqrt{-m}, \quad u, v \text{ impairs,}$$

d'où $\mathfrak{a}^2(2) = (a^2)$, et $\mathfrak{a}^2 = (\alpha)$ avec

$$\alpha = \frac{u^2 - mv^2}{2} + uv\sqrt{-m}.$$

On a $u^2 - mv^2 \equiv -4(8)$, d'où $\alpha \equiv 2 \pm \sqrt{-m} \pmod{4\mathcal{O}}$, et

$$\ell \log(\mathfrak{a}) = \frac{1}{2} \ell \log(\alpha) \equiv \frac{1}{2} \ell \log(2 \pm \sqrt{-m}) \pmod{2\mathcal{O}};$$

or

$$\begin{aligned} \frac{1}{2} \ell \log(2 \pm \sqrt{-m}) &= \frac{1}{4} \ell \log(4 - m \pm 4\sqrt{-m}) \\ &\equiv \frac{1}{4} \ell \log(-1 \pm 4\sqrt{-m}) \pmod{2\mathcal{O}}, \end{aligned}$$

soit $\ell \log(a) \equiv \mp \sqrt{-m} \pmod{2\mathcal{O}}$. Or, d'après le tableau I précédent, on a $\ell \log(\mathcal{U}) = 2\mathcal{O}$; donc $\ell \log(a) \notin \ell \log(\mathcal{U})$, et $[\bar{k} \cap \bar{k} : k] \neq 1$.

PROPOSITION 2.2. — Lorsque

$$\mathcal{P} = \mathbf{Q}_2(\sqrt{-14}), \quad \rho = 1 \quad \text{et} \quad \chi = 0,$$

alors $t = 2$.

Posons $k = \mathbf{Q}(\sqrt{-m})$, $m = 2n$, $n \equiv 7(8)$. Comme on a $1 \leq t \leq 2$, il suffit de vérifier que le cas $t = 1$ est impossible. Comme $\rho = 1$, tout diviseur premier de n est congru à ± 1 modulo 8, donc n est norme (d'entier) dans $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, et il existe $a, b \in \mathbf{Z}$, $(a, b) = 1$, tels que $n = a^2 - 2b^2$; comme $n \equiv 7(8)$, a et b sont impairs. D'où

$$2a^2 = (2b)^2 + m, \quad \text{soit} \quad 2a^2 = N(2b + \sqrt{-m}),$$

ce qui implique immédiatement que

$$(2b + \sqrt{-m}) = a^2 p, \quad a \in \mathbf{I}, \quad p|2 \quad \text{dans } k.$$

En outre $C\ell(a)$ est d'ordre 4 car $C\ell(p)$ est d'ordre 2. On a

$$a^4(2) = 4b^2 - m + 4b\sqrt{-m},$$

soit $a^4 = (\alpha)$ avec $\alpha = 2b^2 - n + 2b\sqrt{-m}$. Comme b est impair, on a $2b^2 - n \equiv 3(8)$, et on en déduit facilement que

$$\ell \log(\alpha) \equiv 2\sqrt{-14} \pmod{(8)} \oplus (4\sqrt{-14}),$$

d'où

$$\ell \log(a) \equiv \frac{1}{2}\sqrt{-14} \pmod{(2)} \oplus (\sqrt{-14}).$$

Or l'hypothèse $\chi = 0$ signifie que $2 \in \overline{\ell \log(\mathbf{I})}$, donc ici $\frac{1}{2}\sqrt{-14} \in \overline{\ell \log(\mathbf{I})}$

puisque $\sqrt{-14} \in \ell \log(\mathcal{U})$ (cf. Tableau I), ce qui fait que

$$\overline{\ell \log(\mathbf{I})} / \ell \log(\mathcal{U}) = \overline{\ell \log(\mathbf{I})} / (4) \oplus (\sqrt{-14})$$

contient un sous-groupe isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$, et $t = 2$.

Les propositions 1.1, 2.1 et 2.2 conduisent au résultat suivant :

THÉORÈME 2.1. — *La classification des corps quadratiques imaginaires $\mathbf{Q}(\sqrt{-m})$, relativement aux invariants \mathcal{P} , ρ , χ , t , est constituée des 19 cas résumés dans le tableau suivant, où chaque cas est illustré par le plus petit m possible noté m_0 :*

\mathcal{P}	ρ	χ	t	$-m_0$
$\mathbf{Q}_2(\sqrt{-1})$	1	1	0	-1
	0	0	1	-33
	1	0	1	-41
$\mathbf{Q}_2(\sqrt{-2})$	1	1	0	-2
	0	0	1	-66
	1	0	1	-82
$\mathbf{Q}_2(\sqrt{-3})$	0	0	0	-3
	0	0	1	-155
$\mathbf{Q}_2(\sqrt{-5})$	0	0	1	-5
$\mathbf{Q}_2(\sqrt{-6})$	0	0	1	-6
	0	0	2	-310
$\mathbf{Q}_2 \times \mathbf{Q}_2$	1	1	0	-7
	0	0	1	-15
	1	0	1	-791
$\mathbf{Q}_2(\sqrt{-10})$	0	0	1	-10
$\mathbf{Q}_2(\sqrt{-14})$	1	1	1	-14
	0	0	1	-30
	0	0	2	-510
	1	0	2	-1582

Tableau II.

NOTE. — *Par commodité pour le lecteur, rappelons la signification des invariants \mathcal{P} , ρ , χ , t , dans le cas où $k = \mathbf{Q}(\sqrt{-m})$:*

- (i) \mathcal{P} est le produit des complétés de k pour les $p|2$,
- (ii) $\rho = 1$ si et seulement si tout diviseur premier impair de m est congru à ± 1 modulo 8,
- (iii) $\chi = 0$ si et seulement si la \mathbf{Z}_2 -extension de k , prodiédrale sur \mathbf{Q} , est linéairement disjointe de la cyclotomique (on a $\chi \leq \rho$),
- (iv) t est le nombre d'extensions quadratiques non ramifiées de k (indépendantes), contenues dans une \mathbf{Z}_2 -extension de k .

COROLLAIRE. — Si $\mathcal{P} \neq \mathbf{Q}_2(\sqrt{-3}), \mathbf{Q}_2(\sqrt{-14})$, on a $\chi = 1$ si et seulement si $\bar{k} \cap \check{k} = k$ (i.e. si et seulement si $\overline{\ell \text{og}(\mathbf{I})} = \ell \text{og}(\mathcal{U})$).

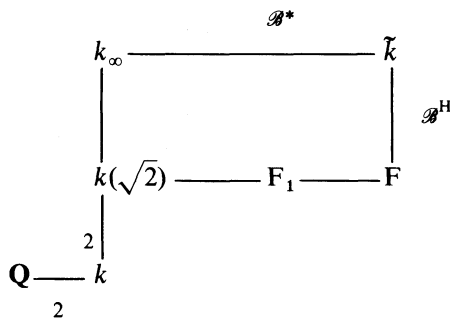
Remarque. — Pour \mathcal{P} fixé, le tableau est ordonné par χ décroissants, puis par ρ croissants, puis par t croissants; ceci semble refléter le degré de rareté du cas correspondant (cf. Table numérique de [4], à partir de laquelle nous avons déterminé les exemples numériques).

On peut alors, dans chaque cas, préciser la nature de l'intersection $\bar{k} \cap \check{k}$ au moyen du théorème 1.2 et de son corollaire 1. Appelons F_1 le corps $F \cap \check{k}$:

(i) Si $\chi = 1$, on vient de voir que $\bar{k} \cap \check{k} = k$ sauf si $\mathcal{P} = \mathbf{Q}_2(\sqrt{-14})$, auquel cas $\check{\chi} = 0$, $R = r = 1$, et $|\mathcal{X}| = [F_1 : k]$; autrement dit

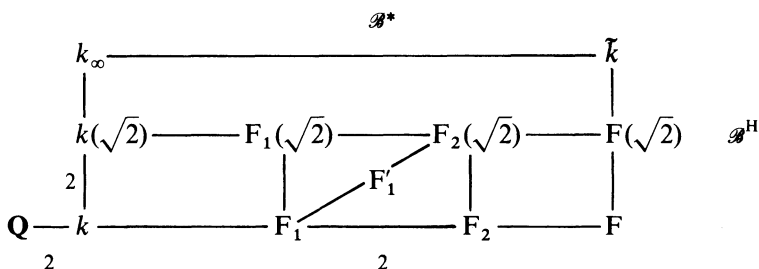
$$\bar{k} \cap \check{k} = F \cap \check{k} = F_1$$

dans ce cas :



$$\mathcal{P} = \mathbf{Q}_2(\sqrt{-14}), \quad \chi = 1$$

(ii) Si $\chi = 0$, appelons F_2 l'extension quadratique de F_1 contenue dans F , et F'_1 l'extension quadratique de F_1 contenue dans \bar{k} , distincte de $F_1(\sqrt{2})$ et de F_2 :



$$\chi = 0$$

Dans ce cas, le résultat ne va dépendre que de $\tilde{\chi}$ et r , via la formule $|\mathcal{H}| = 2^{\tilde{\chi}+r}[F_1:k]$.

Connaissant avec précision le corps $\bar{k} \cap \bar{k}$, et sachant que dans l'isomorphisme $\mathcal{B} \rightarrow \ell\text{og}(\text{I})$, $\text{Gal}(\bar{k}/\bar{k} \cap \bar{k})$ correspond à $\ell\text{og}(\mathcal{U})$ (donné par le Tableau I), on peut reconstituer $\overline{\ell\text{og}(\text{I})}$ facilement.

THÉORÈME 2.2. — Soit k un corps quadratique imaginaire, et soient \bar{k} le composé de ses \mathbf{Z}_2 -extensions et \check{k} son 2-corps de classes de Hilbert; on a le tableau suivant où l'on rappelle que $\bar{k} = k_\infty F$, où k_∞ (resp. F) est la \mathbf{Z}_2 -extension cyclotomique (resp. prodiédrale sur \mathbf{Q}) de k , que $[F \cap k_\infty : k] = 2^\chi$, que $[\bar{k} \cap \check{k} : k] = (\ell\text{og}(\text{I}) : \ell\text{og}(\mathcal{U}))$ noté κ , et que F'_1 est l'extension quadratique de $F_1 = F \cap \check{k}$ non contenue dans F ou $F_1 k_\infty$:

\mathcal{P}	χ	$k_\infty \cap \bar{k}$	$F \cap \bar{k}$	$\bar{k} \cap \check{k}$	$\overline{\ell\text{og}(\text{I})}$
$\mathbf{Q}_2(\sqrt{-1})$	1	k	k	k	$(4) \oplus (2+2\sqrt{-1})$
	0	k	F_1	F'_1	$(2) \oplus (4\kappa^{-1}\sqrt{-1})$
$\mathbf{Q}_2(\sqrt{-2})$	1	k	k	k	$(4) \oplus (2+\sqrt{-2})$
	0	k	F_1	F'_1	$(2) \oplus (2\kappa^{-1}\sqrt{-2})$
$\mathbf{Q}_2(\sqrt{-3})$	0	k	F_1	F_1	$(2) \oplus (2\kappa^{-1}\sqrt{-3})$
$\mathbf{Q}_2(\sqrt{-5})$	0	k	F_1	F_1	$(2) \oplus (2\kappa^{-1}\sqrt{-5})$
$\mathbf{Q}_2(\sqrt{-6})$	0	$k(\sqrt{2})$	F_1	$F_1(\sqrt{2})$	$(2) \oplus (2\kappa^{-1}\sqrt{-6})$
$\mathbf{Q}_2 \times \mathbf{Q}_2$	1	k	k	k	$(4) \oplus (2+2(1, -1))$
	0	k	F_1	F'_1	$(2) \oplus (4\kappa^{-1}(1, -1))$
$\mathbf{Q}_2(\sqrt{-10})$	0	k	F_1	F'_1	$(2) \oplus (2\kappa^{-1}\sqrt{-10})$
$\mathbf{Q}_2(\sqrt{-14})$	1	$k(\sqrt{2})$	$F_1 = F_1(\sqrt{2})$	$F_1 = F_1(\sqrt{2})$	$(4) \oplus (2+\kappa^{-1}\sqrt{-14})$
	0	$k(\sqrt{2})$	F_1	$F_1(\sqrt{2})$	$(2) \oplus (2\kappa^{-1}\sqrt{-14})$

Tableau III.

Remarque. — Dans ce tableau, κ est une puissance de 2 différente de 1, sauf pour $\mathcal{P} = \mathbf{Q}_2(\sqrt{-3})$ où κ peut prendre la valeur 1 (cf. Tableau II).

On se propose maintenant, à titre de complément, de caractériser les corps $k = \mathbf{Q}(\sqrt{-m})$ pour lesquels $\tilde{k} \subset \bar{k}$; le résultat est le suivant :

THÉORÈME 2.3. — *Le 2-corps de classes de Hilbert d'un corps quadratique imaginaire k est contenu dans le composé de ses \mathbf{Z}_2 -extensions si et seulement si k est l'un des corps suivants :*

- (i) $\mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{-2}),$
- (ii) $\mathbf{Q}(\sqrt{-\ell}), \ell$ premier, $\ell \equiv 3, 5, 7 \pmod{8},$
- (iii) $\mathbf{Q}(\sqrt{-2\ell}), \ell$ premier, $\ell \equiv 3, 5 \pmod{8},$
- (iv) $\mathbf{Q}(\sqrt{-\ell q}), \ell, q$ premiers, $\ell \equiv -q \equiv 3 \pmod{8}.$

D'après la formule démontrée dans [5], corollaire au théorème 2.1, on a $|\mathcal{C}| = \frac{|\mathcal{A}|}{|\mathcal{X}|} \times \frac{|\mu(\mathcal{U})|}{|\mu(k^\times)|}$; d'où $\tilde{k} \subset \bar{k}$ si et seulement si $|\mathcal{C}| = \frac{|\mu(\mathcal{U})|}{|\mu(k^\times)|}$, et deux cas sont à considérer :

(i) Cas $|\mu(\mathcal{U})| = |\mu(k^\times)|$. Dans ce cas, $\tilde{k} \subset \bar{k}$ équivaut à $|\mathcal{C}| = 1$, et le corollaire au théorème 5.2 de [5] montre que k est l'un des corps suivants :

$$\mathbf{Q}(\sqrt{-2}), \mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{-\ell}) \text{ ou } \mathbf{Q}(\sqrt{-2\ell}), \ell \text{ premier,} \\ \ell \equiv 3, 5 \pmod{8}.$$

(ii) Cas $|\mu(\mathcal{U})| = 4$ et $|\mu(k^\times)| = 2$. Dans ce cas, $\mathcal{P} = \mathbf{Q}_2(\sqrt{-1}), k \neq \mathbf{Q}(\sqrt{-1}),$ ou $\mathcal{P} = \mathbf{Q}_2 \times \mathbf{Q}_2,$ et $\tilde{k} \subset \bar{k}$ équivaut à $|\mathcal{C}| = 2$.

LEMME 1. — *Si $\mathcal{P} = \mathbf{Q}_2(\sqrt{-1}), k \neq \mathbf{Q}(\sqrt{-1}),$ alors $\tilde{k} \not\subset \bar{k}.$*

Soit $k = \mathbf{Q}(\sqrt{-m}), m \equiv 1 \pmod{8}, m \neq 1$. La classe de $\mathfrak{p}|2$ dans k est d'ordre 2 exactement; si \mathfrak{a} est un idéal entier impair dans la classe de \mathfrak{p} , on a $\mathfrak{a}\mathfrak{p} = (a), a = u + v\sqrt{-m}, u, v$ impairs, d'où $\mathfrak{a}^2(2) = (a^2)$, et $\mathfrak{a}^2 = (\alpha),$ avec $\alpha = \frac{u^2 - mv^2}{2} + uv\sqrt{-m}.$ Calculons $\ell \log(\mathfrak{a})$ modulo $\ell \log(\mathcal{U}) = 2\pi\mathcal{O},$ où $\pi = 1 + \sqrt{-1}$ (cf. Tableau I); on a $\ell \log(\mathfrak{a}) = \frac{1}{2}\ell \log(\alpha),$ et on peut donc calculer α modulo $4\pi\mathcal{O}.$ Quitte à changer u et v de signe et(ou) à conjuguer la relation $\mathfrak{a}\mathfrak{p} = (a),$ on peut supposer que $u = 1 + 4\lambda, v = 1 + 4\mu, \lambda, \mu \in \mathbf{Z}.$ Posons $m = 1 + 8s;$

il vient

$$\begin{aligned}\alpha &\equiv \frac{1 + 8\lambda - (1 + 8s)(1 + 8\mu)}{2} + (1 + 4\lambda + 4\mu)\sqrt{-m} \\ &\equiv 4\lambda - 4\mu - 4s + (1 + 4\lambda + 4\mu)\sqrt{-m} \pmod{4\pi\mathcal{O}};\end{aligned}$$

posons $\omega = 1 - \sqrt{-m}$, c'est une autre uniformisante de $\mathbf{Q}_2(\sqrt{-1})$, et on a

$$\begin{aligned}\alpha &\equiv 4\lambda - 4\mu - 4s + (1 + 4\lambda + 4\mu)(1 - \omega) \\ &\equiv 1 - \omega - 4s \pmod{4\pi\mathcal{O}}.\end{aligned}$$

Si l'on pose $\beta = 1 - \omega - 4s$, on vérifie que

$$\begin{aligned}\beta^2 &= (1 - \omega)^2 - 8s(1 - \omega) + 16s^2 \\ &= -1 - 16s + 16s^2 + 8s\omega \\ &= -1 \pmod{8\pi\mathcal{O}},\end{aligned}$$

donc $\ell \log(\beta) = \frac{1}{2} \ell \log(\beta^2) \equiv 0 \pmod{4\pi\mathcal{O}}$; par conséquent,

$$\ell \log(\alpha) \equiv 0 \pmod{4\pi\mathcal{O}}, \quad \text{et} \quad \ell \log(\alpha) \in \ell \log(\mathcal{U}).$$

D'après le corollaire au théorème 2.1 de [5], appliqué à $M = \tilde{k}$, l'idéal α est dans le groupe d'Artin de l'extension $\tilde{k} \cap \tilde{k}/k$; comme la classe de α est d'ordre 2, ceci implique $\tilde{k} \neq \tilde{k} \cap \tilde{k}$, d'où le lemme.

LEMME 2. — Si $m \equiv 7 \pmod{8}$, les conditions suivantes sont équivalentes :

- (i) $C\ell(\mathfrak{p}) \in \mathcal{H}^2$, où $\mathfrak{p}|2$ dans k ,
- (ii) pour tout ℓ premier, $\ell|m$, on a $\ell \equiv \pm 1(8)$.

Supposons que $C\ell(\mathfrak{p}) \in \mathcal{H}^2$; il existe un idéal entier impair \mathfrak{a} tel que $\mathfrak{a}^2\mathfrak{p} = (\mathfrak{a})$, $\mathfrak{a} = \frac{u + v\sqrt{-m}}{2}$, u, v impairs. Si $N\mathfrak{a} = w\mathbf{Z}$, il vient

$$u^2 + mv^2 = 8w^2 = 2(2w)^2,$$

soit $-mv^2 = u^2 - 2(2w)^2$, et $-m$ (donc m) est norme dans $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, ce qui implique que tout nombre premier $\ell|m$ est congru à ± 1 modulo 8.

Réciproquement, si cette propriété a lieu, $-m$ est norme dans $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, et on vérifie que l'on peut écrire $-mz^2 = x^2 - 8y^2$, $x, y, z \in \mathbf{Z}$, $(x, z) = (y, z) = 1$, x, z impairs, ce qui s'écrit encore

$$2y^2 = \mathbf{N}\left(\frac{x+z\sqrt{-m}}{2}\right).$$

L'idéal $\left(\frac{x+z\sqrt{-m}}{2}\right)$ de k est un idéal entier sans facteur rationnel, donc ceci implique $\left(\frac{x+z\sqrt{-m}}{2}\right) = \mathfrak{a}^2\mathfrak{p}$ dans I .

LEMME 3. — Si $\mathcal{P} = \mathbf{Q}_2 \times \mathbf{Q}_2$, alors $\bar{k} \subset \bar{k}$ si et seulement si $k = \mathbf{Q}(\sqrt{-\ell})$, ℓ premier, $\ell \equiv 7(8)$, ou $k = \mathbf{Q}(\sqrt{-\ell q})$, ℓ, q premiers, $\ell \equiv -q \equiv 3(8)$.

On utilise le théorème I.3 de [6], donnant la \mathbf{F}_2 -dimension de $\bar{\mathcal{C}}/\bar{\mathcal{C}}^2$: comme 2 est décomposé, et $|\bar{\mathcal{C}}| = 2$, il vient $\mathcal{H} = \langle \mathcal{C}\ell(\mathfrak{p}) \rangle$, où $\mathfrak{p}|2$ dans k ; donc \mathcal{H} doit être cyclique, ce qui implique $k = \mathbf{Q}(\sqrt{-\ell})$, $\ell \equiv 7(8)$, ou $k = \mathbf{Q}(\sqrt{-\ell q})$, $\ell q \equiv 7(8)$.

Le premier cas est solution puisqu'alors $\mathcal{H} = (1)$.

Dans le second, on a $\mathcal{H} \neq (1)$, et la condition $\mathcal{H} = \langle \mathcal{C}\ell(\mathfrak{p}) \rangle$ équivaut alors à $\mathcal{C}\ell(\mathfrak{p}) \notin \mathcal{H}^2$, et le lemme 2 conduit, par exemple, à $\ell \equiv 3(8)$, ce qui implique $q \equiv 5(8)$.

Réciproquement, soit $k = \mathbf{Q}(\sqrt{-\ell q})$, $\ell \equiv -q \equiv 3(8)$; on a $\mathcal{H} = \langle \mathcal{C}\ell(\mathfrak{p}) \rangle$. Soit I l'idéal premier au-dessus de ℓ dans k ; $\mathcal{C}\ell(I)$ est d'ordre 2, or $I^2 = (\ell)$, avec $\ell \equiv 3(8)$, donc $\ell \log(I) = 2u$, $u \in \mathbf{Z}_2^*$, et $\ell \log I \notin \ell \log \mathcal{U}$ (cf. Tableau 1); ceci veut dire que I n'est pas dans le groupe d'Artin de $\bar{k} \cap \bar{k}$, ce qui implique (puisque \mathcal{H} est cyclique et $\mathcal{C}\ell(I)$ d'ordre 2) $\bar{k} \cap \bar{k} = \bar{k}$, d'où le lemme, puis le théorème.

Remarques. — (i) Le cas non trivial illustrant l'inclusion $\bar{k} \subset \bar{k}$ est $k = \mathbf{Q}(\sqrt{-\ell q})$, $\ell \equiv -q \equiv 3(8)$, pour lequel $|\mathcal{H}|$ est arbitraire (pour tous les autres cas, $|\mathcal{H}| = 1$ ou 2 de façon canonique); par exemple, pour $k = \mathbf{Q}(\sqrt{-11 \times 37})$, la classe de $\mathfrak{p}|2$ est d'ordre 16.

(ii) Pour tous les corps donnés par le théorème 2.3, le 2-groupe des classes est engendré par la classe d'un idéal premier au-dessus de 2.

BIBLIOGRAPHIE

- [1] E. ARTIN and J. TATE, *Class field theory*, W. A. Benjamin, New-York (1967).
- [2] J. E. CARROLL, On determining the quadratic subfields of \mathbf{Z}_2 -extensions of complex quadratic fields, *Compositio Mathematica*, 30 (1975), 259-271.
- [3] J. E. CARROLL and H. KISILEVSKY, Initial layers of \mathbf{Z}_l -extensions of complex quadratic fields, *Compositio Mathematica*, 32 (1976), 157-168.
- [4] A. CHARIFI, Groupes de torsion attachés aux extensions abéliennes p -ramifiées maximales (cas des corps totalement réels et des corps quadratiques imaginaires), thèse de 3^e cycle, Besançon (1982).
- [5] G. GRAS, Logarithme p -adique et groupes de Galois, *Journal de Crelle*, 343 (1983), 64-80.
- [6] G. GRAS, Groupe de Galois de la p -extension abélienne p -ramifiée maximale d'un corps de nombres, *Journal de Crelle*, 333 (1982), 86-132.

Manuscrit reçu le 27 janvier 1983.

Georges GRAS,

Université de Franche-Comté
Laboratoire de Mathématiques
E.R.A. au C.N.R.S. n° 070654
25030 Besançon Cedex (France).
