TABLE DES 2-RANG, 4-RANG ET 8-RANG DU 2-GROUPE DES CLASSES D'IDÉAUX AU SENS RESTREINT DE $\mathbf{Q}(\sqrt{m})$ m ÉTANT UN ENTIER RELATIF SANS FACTEUR CARRÉ TEL QUE $1 < |m| < 10\,000$

par Lyliane Bouvier

Cette table a été établie en utilisant les méthodes de détermination du 4-rang et du 8-rang du 2-groupe des classes au sens restreint d'une extension quadratique de $\mathbf{Q}$ exposées par L. Redei et H. Reichardt dans [3], [4], [5] et [6], méthodes dont je résume ci-dessous les étapes essentielles. Les calculs numériques ont été effectués par l'ordinateur IBM 40-65 de Grenoble.

Soit m un entier relatif sans facteur carré, on note k l'extension $\mathbf{Q}(\sqrt{m})$ de $\mathbf{Q}$ et D son discriminant. Soit $\mathscr{H}$ le sous-groupe du groupe des classes d'idéaux au sens restreint engendré par les éléments dont l'ordre est une puissance de 2, $\mathscr{H}$ est encore appelé le 2-groupe des classes d'idéaux au sens restreint. On appelle 2^n-rang de $\mathscr{H}$ — on le désigne par R_n — la dimension du $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel $\mathscr{H}^{2n-1}/\mathscr{H}^{2n}$ — cf. [1] —, c'est aussi le nombre de composantes d'ordre supérieur ou égal à 2^n qui interviennent dans une décomposition de $\mathscr{H}$ en produit direct de sous-groupes cycliques. On remarque alors que le nombre de sous-groupes d'ordre 2 de $\mathscr{H}$ qui sont contenus dans un sous-groupe cyclique d'ordre $\geqslant 2^n$ de $\mathscr{H}$, est égal à $2^{R_n} - 1$. Par suite, $\mathscr{H}$ étant isomorphe à son groupe dual, on montre que le nombre d'extensions quadratiques non ramifiées de k qui sont contenues dans une extension non ramifiée cyclique de degré 2^n de k est égal à $2^{R_n} - 1$. C'est en déterminant ce nombre pour $n = 2$ et $n = 3$ que l'on déterminera le 4-rang et le 8-rang de $\mathscr{H}$.

L'ensemble des extensions quadratiques non ramifiées de k est l'ensemble des extensions $\mathbf{Q}(\sqrt{D_1}, \sqrt{D_2})$ où D_1 et D_2 sont des nombres discriminants d'extensions quadratiques de $\mathbf{Q}$ (i.e.: $D_i \equiv 1 \pmod 4$ ou $D_i \equiv 8 \pmod{16}$ ou $D_i \equiv 12 \pmod{16}$ pour $i = 1, 2$) tels que $D_1 D_2 = D$ et que $D_i \neq 1$ pour $i = 1, 2$.

Définition 1 : On appelle *D-décomposition* un couple (D_1, D_2) d'entiers relatifs tels que D_1 et D_2 soient des nombres discriminants d'extensions quadratiques de $\mathbf{Q}$ et que $D_1 D_2 = D$.

En identifiant les couples (D_1, D_2) et (D_2, D_1), on voit que le nombre de D-décompositions est égal à 2^{R1}. La D-décomposition $(1, D)$ est appelée D-décomposition triviale.

Définition 2: Une D-décomposition (D_1, D_2) non triviale est appelée *D-décomposition de n-ième espèce* (n entier > 1) si et seulement si $\mathbf{Q}(\sqrt{D_1}, \sqrt{D_2})$ est contenue dans une extension non ramifiée cyclique de degré 2^n de k.

Par convention, la D-décomposition $(1, D)$ est considérée comme une D-décomposition de n-ième espèce, quel que soit $n > 1$. On voit alors que le nombre de D-décomposition de n-ième espèce est égal à 2^{Rn}.

Pour déterminer R_2 (resp. R_3) il suffit donc de dénombrer les D-décompositions de 2^e-espèce (resp. 3^e-espèce). Pour cela nous allons utiliser la propriété caractéristique suivante démontrée par H. Reichardt dans [6].

Définition 2' : Soit n un entier naturel > 1, *une D-décomposition non triviale* (D_1, D_2) *est une D-décomposition de n-ième espèce si et seulement si* $\mathbf{Q}(\sqrt{D_1}, \sqrt{D_2})$ *est contenue dans une extension non ramifiée cyclique de degré* 2^{n-1} *de k, dans laquelle tout idéal premier de k divisant D est totalement décomposé.*

Dans le cas $n = 2$, nous obtenons en corollaire la proposition suivante:

Proposition 1: Une D-décomposition non triviale (D_1, D_2) est une D-décomposition de 2^e-espèce si et seulement si $\left(\frac{D_1}{q}\right) = +1$ quel que soit q premier divisant D_2 et $\left(\frac{D_2}{q}\right) = +1$ quel que soit q premier divisant D_1 (le symbole $\left(\frac{\ }{\ }\right)$ désignant le symbole de Legendre-Jacobi-Kronecker).

Or si (D_1, D_2) est une D-décomposition de 2^e-espèce non triviale, il existe des entiers relatifs non nuls x, y et z tels que x, yD_1 et zD_2 soient premiers entre eux deux à deux, que y soit pair et que $x^2 = y^2 D_1 + Z^2 D_2$ (si D est pair, y étant pair, D_1 est l'élément pair du couple (D_1, D_2)). En choisissant les signes de x et de y tels que

$$x + y \equiv 1 \pmod 4 \text{ si } D \text{ est impair}$$

et

$$x \equiv 1 \pmod 4 \text{ si } D \text{ est pair,}$$

on peut alors montrer la proposition suivante, démontrée par L. Redei dans [4]:

(N.B.: les conditions ci-dessus vérifiées par x, y et z seront désignées par la suite par conditions (1)).

Proposition 2 : Une D-décomposition de 2^e-espèce (D_1, D_2) non triviale est une D-décomposition de 3^e-espèce si et seulement si il existe une D-décomposition $\mathscr{E} = (E_1, E_2)$ telle que

si $D \equiv 1 \pmod 4$ ou $D \equiv 8 \pmod{16}$

$$\left(\frac{2x\,\mathscr{E}}{q_2}\right) = +1 \qquad \text{et} \qquad \left(\frac{x\,\mathscr{E}}{q_1}\right) = +1$$

si $D \equiv 12 \pmod{16}$

$$\left(\frac{2x\,\mathscr{E}}{q_2}\right) = +1\,, \quad \left(\frac{x\,\mathscr{E}}{q_1}\right) = +1 \qquad \textit{pour} \qquad q_1 \neq 2$$

$$\text{et} \qquad \left(\frac{(x+2y)\,\mathscr{E}}{2}\right) = +1$$

où q_i parcourt les diviseurs premiers de Di $(i=1, 2)$ avec $\left(\frac{a\,\mathscr{E}}{q}\right) = \left(\frac{a\,E_1}{q}\right)$ $\left(\text{resp. } \left(\frac{a\,E_2}{q}\right)\right)$ si q divise E_2 (resp. E_1).

Une méthode pour évaluer R_2 et R_3 consiste donc à déterminer l'ensemble des D-décompositions, puis parmi celles-ci l'ensemble des D-décompositions de 2^e-espèce et enfin, parmi ces dernières celles qui sont de 3^e-espèce.

Mais on peut aussi procéder de façon plus « mécanique » — cf. [3] et [4] —:

Soit t le nombre de diviseurs premiers de D que l'on désigne par P_i $(i=1, 2, ..., t)$ avec, si D est pair, $P_t = 2$. On sait que $R_1 = t - 1$. Notons $P_i^* = (-1)^{\frac{P_i - 1}{2}} P_i$ pour tout $i \in \{1, 2, ..., t\}$ tel que $P_i \neq 2$.

a. Considérons la matrice M_k suivante

$$M_k = \begin{bmatrix} \left(\frac{D/P_1^*}{P_1}\right) & \left(\frac{P_2^*}{P_1}\right) & \cdots & \left(\frac{P_i^*}{P_2}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_2}\right) \\ \left(\frac{P_1^*}{P_2}\right) & \left(\frac{D/P_2^*}{P_2}\right) & \cdots & \left(\frac{P_i^*}{P_2}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_2}\right) \\ \vdots & \vdots & \ddots & & & \vdots \\ \left(\frac{P_1^*}{P_i}\right) & \left(\frac{P_2^*}{P_i}\right) & \cdots & \left(\frac{D/P_i^*}{P_i}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_i}\right) \\ \vdots & & & & \ddots & \vdots \\ \left(\frac{P_1^*}{P_t}\right) & \left(\frac{P_2^*}{P_t}\right) & \cdots & \left(\frac{P_i^*}{P_t}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_t}\right) \end{bmatrix}$$

C'est une matrice à $t-1$ colonnes et t lignes dont les éléments sont égaux à $+1$ ou -1. On dit que la i-ème colonne $(i=1, \ldots, t-1)$ « appartient à P_i », avec $d = P_1^{*\varepsilon 1} P_2^{*\varepsilon 2} \ldots P_{t-1}^{*\varepsilon t-1}$ où les ε_i $(i=1, \ldots, t-1)$ sont non tous nuls et appartiennent à $\mathbf{Z}/2\mathbf{Z}$, on appelle « produit des colonnes appartenant à d» la colonne de t lignes dont l'élément de la j-ème ligne $(j=1, 2, \ldots, t)$ est égal au produit des éléments de la j-ème ligne des colonnes appartenant aux P_i $(i=1, 2, \ldots, t-1)$ qui divisent d. On appelle aussi « colonne unité », la colonne de t lignes dont tous les éléments sont égaux à $+1$.

On voit alors que la D-décomposition non triviale (D_1, D_2) est une D-décomposition de 2e-espèce si et seulement si le produit des colonnes appartenant à D_1 (ou à D_2 si P_t divise D_1) est la colonne unité. En conséquence:

Proposition 1' : 2^{R2} *est égal au nombre d'éléments* $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-1})$ *de* $(\mathbf{Z}/2\mathbf{Z})^{t-1}$ *tels que le produit des colonnes appartenant à* $d = P_1^{*\varepsilon 1} P_2^{*\varepsilon 2} \ldots P_{t-1}^{*\varepsilon t-1}$ *soit égal à la colonne unité,* en associant, par convention, la colonne unité à $d = P_1^{*0} P_2^{*0} \ldots P_{t-1}^{*0}$.

b. Soient (D_1, D_2) une D-décomposition de 2e-espèce non triviale et x, y et z des entiers relatifs vérifiant les conditions (1). Considérons la matrice $M_k(x)$ suivante:

$$
M_k(x) = \begin{bmatrix}
\left(\frac{D/P_1^*}{P_1}\right) & \left(\frac{P_2^*}{P_1}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_1}\right) & \left(\frac{a}{P_1}\right) \\
\left(\frac{P_2^*}{P_2}\right) & \left(\frac{D/P_2^*}{P_2}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_2}\right) & \left(\frac{a}{P_2}\right) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\left(\frac{P_1^*}{P_t}\right) & \left(\frac{P_2^*}{P_t}\right) & \cdots & \left(\frac{P_{t-1}^*}{P_t}\right) & \left(\frac{a}{P_t}\right)
\end{bmatrix}
$$

C'est une matrice à t lignes et t colonnes telle que, si D est impair, P_t divise D_1 et où

$$
\left(\frac{a}{P_i}\right) = \begin{cases}
\left(\frac{2x}{P_i}\right) & \text{si } P_i \text{ divise } D_2 \\
\left(\frac{x}{P_i}\right) & \text{si } P_i \text{ divise } D_1 \text{ et } i \neq t \\
\left(\frac{x+2y}{P_t}\right) & \text{si } D \equiv 12 \pmod{16}, \left(\frac{x}{q_t}\right) \text{ sinon.}
\end{cases}
$$

En utilisant les mêmes conventions que précédemment et en désignant la dernière colonne de $M_k(x)$ par « la colonne appartenant à P_t », on obtient la proposition suivante:

Proposition 2' : La D-décomposition de 2e-espèce non triviale (D_1, D_2) *est une D-décomposition de 3e-espèce si et seulement si il existe* $d = P_1^{*\varepsilon 1} P_2^{*\varepsilon 2} \ldots P_{t-1}^{*\varepsilon t-1}$ *avec* $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-1})$ *appartenant à* $(\mathbf{Z}/2\mathbf{Z})^{t-1}$ *tel que le produit des colonnes appartenant à* $d.p_t$ *soit la colonne unité.*

Le programme employé pour déterminer R_2 et R_3 a été établi en utilisant les propositions $1'$ et $2'$ et écrit en Algol 60.

L'entier $m > 0$ étant sans facteur carré, on détermine successivement le 4-rang $\tilde{R}_2$ et le 8-rang $\tilde{R}_3$ correspondant à $\tilde{k} = \mathbf{Q}(\sqrt{-m})$, puis le 4-rang R_2 et le 8-rang R_3 correspondant à $k = \mathbf{Q}(\sqrt{m})$. Ceci non seulement pour utiliser le fait que les éléments des tableaux $M_{\tilde{k}}$ et M_k sont presque tous identiques mais aussi pour tenir compte de l'inégalité $\tilde{R}_2 \geqslant R_2$ démontrée par P. Domey et J. J. Payan — cf. [2] —, et qui permet de simplifier le programme.

Schéma du programme :

1. Introduction de $m > 0$ dans la machine.
2. Test pour savoir si m est sans facteur carré.
3. Détermination des facteurs premiers de m.
4. a. Remplissage du tableau $M_{\tilde{k}}$.
   b. Recherche des quantités D_2 qui correspondent à des produits de colonnes égaux à la colonne unité et détermination de $\tilde{R}_2$ (si $\tilde{R}_2 = 0$, alors $\tilde{R}_3 = R_2 = R_3 = 0$).
   c. Avec chacune des quantités D_2:
      1. Recherche d'une solution $dX^2 = Y^2 D_1 + Z^2 D_2$ vérifiant les conditions (1).
      2. Remplissage de $M_{\tilde{k}}(x)$.
      3. Test pour savoir si (D_1, D_2) est une D-décomposition de 3e-espèce et détermination de $\tilde{R}_3$.
5. a. Modification de $M_{\tilde{k}}$ pour obtenir M_k.
   b. Cf. 4.b.
   c. Cf. 4.c.

Pour déterminer une solution de l'équation $X^2 = Y^2 D_1 + Z^2 D_2$, on se ramène d'abord à résoudre l'équation équivalente du type $a\alpha^2 = b\beta^2 + c\gamma^2$ où a, b et c sont des entiers strictement positifs. On fait ensuite calculer une solution en entiers α, β et γ de l'équation $a\alpha^2 = b\beta^2 + c\gamma^2$ en programmant des essais méthodiques, dans l'ordre croissant, pour l'entier α, puis, α étant fixé, pour l'entier β: on prend pour valeur initiale de α la partie entière de $\dfrac{b + c}{a}$ et, pour une valeur de α fixée, on fait balayer par β les valeurs comprises entre 1 et $\sqrt{\dfrac{a\alpha^2 - c}{b}}$; on itère le procédé jusqu'à ce que l'on obtienne une solution.

Bien que les calculs aient été faits à la machine pour $1 < |m| < 10\,000$, nous ne donnons ici qu'un extrait des tables ainsi obtenues [1]). Cet extrait

[1]) Un exemplaire roneotypé complet de ces tables peut être obtenu à l'Institut de mathématiques pures, Boîte postale 116, 38 — Saint-Martin d'Hères, France.

correspond à $4600 < |m| < 5200$, cette tranche de nombres est telle que l'on trouve la plupart des valeurs obtenues pour (R_1, R_2, R_3) et $(\tilde{R}_1, \tilde{R}_2, \tilde{R}_3)$ lorsque $|m|$ varie de 1 à 10 000.

On peut noter cependant que, pour les valeurs de $|m|$ inférieures à 10 000, deux extensions seulement ont un 8-rang du 2-groupe des classes d'idéaux au sens restreint strictement supérieur à 1; il s'agit de $\mathbf{Q}(\sqrt{-6497})$ et $\mathbf{Q}(\sqrt{-7966})$, pour lesquelles $\tilde{R}_3$ est égal à 2.

On peut aussi remarquer que, alors que la différence $\tilde{R}_2 - R_2$ est toujours positive ou nulle — cf. [2] —, il n'en est pas de même pour $\tilde{R}_3 - R_3$ par exemple pour $\mathbf{Q}(\sqrt{-4705})$ et $\mathbf{Q}(\sqrt{4705})$, $\tilde{R}_3 - R_3 = -1$.

Tableau I: R_1, R_2, R_3 pour $\mathbf{Q}(\sqrt{m})$.

m	R_1	R_2	R_3	m	R_1	R_2	R_3	m	R_1	R_2	R_3	m	R_1	R_2	R_3
4607	2	1	1	4767	3	1	0	4899	3	1	1	5066	2	1	0
4614	2	1	0	4777	1	1	0	4902	3	1	0	5069	1	1	0
4633	1	1	0	4786	1	1	0	4930	3	1	0	5105	1	1	1
4645	1	1	0	4807	3	1	1	4939	2	1	0	5109	2	1	0
4658	2	2	0	4810	3	2	0	4946	1	1	0	5134	2	1	0
4669	2	1	1	4827	2	1	0	4953	2	1	0	5135	3	1	0
4674	3	1	0	4830	4	1	0	4971	2	1	1	5138	2	1	0
4705	1	1	1	4834	1	1	0	4981	1	1	1	5141	1	1	0
4711	2	1	0	4838	2	1	0	5002	2	1	1	5181	2	1	0
4715	3	1	0	4849	1	1	0	5017	1	1	0	5183	2	1	1
4717	1	1	0	4882	1	1	0	5026	2	1	0	5186	1	1	1
4718	2	1	0	4890	3	1	0	5037	2	1	0	5190	3	1	0
4738	2	1	1	4891	2	1	0	5042	1	1	0				
4754	1	1	0	4895	3	1	0	5045	1	1	0				
4763	2	1	0	4898	2	1	0	5057	1	1	0				

TABLEAU II: $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$ pour $\mathbf{Q}(\sqrt{-m})$.

m	$\tilde{R}_1$	$\tilde{R}_2$	$\tilde{R}_3$	m	$\tilde{R}_1$	$\tilde{R}_2$	$\tilde{R}_3$	m	$\tilde{R}_1$	$\tilde{R}_2$	$\tilde{R}_3$	m	$\tilde{R}_1$	$\tilde{R}_2$	$\tilde{R}_3$
4602	3	1	1	4754	1	1	0	4899	2	1	1	5069	2	1	0
4605	3	1	1	4763	1	1	0	4902	3	1	1	5073	3	1	0
4607	1	1	1	4766	1	1	1	4907	1	1	0	5074	2	1	0
4613	2	1	0	4767	2	1	1	4917	3	1	0	5079	1	1	1
4614	2	1	0	4771	1	1	0	4921	3	1	0	5081	1	1	0
4619	1	1	0	4777	2	2	1	4930	3	1	1	5083	2	1	0
4622	1	1	0	4781	2	1	1	4935	3	1	0	5086	1	1	1
4631	1	1	0	4786	1	1	1	4937	1	1	0	5089	2	1	1
4633	2	2	1	4790	2	1	1	4939	1	1	1	5095	1	1	1
4634	2	1	0	4791	1	1	0	4942	2	1	0	5102	1	1	1
4641	4	1	1	4793	1	1	1	4946	1	1	1	5105	2	1	0
4642	2	1	0	4794	3	1	1	4953	3	1	1	5106	3	1	0
4645	2	1	1	4798	1	1	1	4955	1	1	0	5109	3	1	1
4646	2	1	0	4801	1	1	1	4962	2	1	1	5113	1	1	0
4647	1	1	1	4807	2	1	0	4963	1	1	0	5115	3	1	0
4649	1	1	1	4810	3	2	0	4965	3	1	0	5117	3	1	1
4657	1	1	1	4817	1	1	1	4966	2	1	0	5129	2	1	0
4658	2	2	1	4818	3	1	1	4969	1	1	1	5134	2	2	1
4665	3	1	0	4821	2	1	0	4971	1	1	1	5135	2	1	0
4669	3	1	1	4823	2	1	1	4978	2	1	0	5138	2	1	1
4673	1	1	0	4826	2	1	0	4981	2	1	1	5141	2	1	0
4674	3	1	0	4827	1	1	0	4982	2	1	0	5143	1	1	1
4677	2	1	0	4829	2	1	0	4985	2	1	0	5153	1	1	0
4681	2	1	1	4830	4	1	0	4993	1	1	1	5154	2	1	0
4683	2	1	1	4834	1	1	0	4994	2	1	1	5155	1	1	0
4687	1	1	1	4838	2	1	0	5002	2	1	1	5159	2	1	0
4690	3	1	1	4841	2	1	1	5005	4	1	0	5161	2	1	0
4699	1	1	0	4843	1	1	1	5006	1	1	0	5173	2	1	0
4702	1	1	1	4845	4	1	0	5007	1	1	0	5174	2	1	0
4705	2	1	0	4846	1	1	0	5009	1	1	0	5177	2	1	0
4710	3	1	1	4849	2	1	1	5010	3	1	0	5178	2	1	1
4711	1	1	0	4853	2	1	1	5015	2	1	0	5181	3	1	0
4715	2	1	0	4855	1	1	0	5017	2	1	1	5182	1	1	1
4717	2	1	0	4858	2	1	0	5026	2	1	0	5183	1	1	1
4718	2	2	1	4863	1	1	0	5033	2	1	0	5185	3	1	1
4721	1	1	1	4866	2	1	0	5034	2	1	0	5186	1	1	1
4722	2	1	0	4867	1	1	1	5037	3	2	0	5187	3	1	0
4729	1	1	1	4882	1	1	1	5042	1	1	0	5190	3	2	1
4730	3	1	0	4889	1	1	1	5045	2	1	0	5191	1	1	1
4738	2	1	1	4890	3	1	1	5053	2	1	0	5195	1	1	1
4741	2	1	0	4891	1	1	0	5057	2	1	1	5198	2	1	0
4745	3	1	0	4894	1	1	1	5063	1	1	0				
4747	1	1	1	4895	2	2	1	5065	2	1	0				
4749	2	1	1	4898	2	1	0	5066	2	1	0				

N.B.: Dans le tableau I ne sont pas mentionnées les valeurs de m telles que, pour $\mathbf{Q}(\sqrt{m})$, $R_2 = 0$. De même, les valeurs de m telles que, pour $\mathbf{Q}(\sqrt{-m})$, $\tilde{R}_2 = 0$ ne sont pas mentionnées dans le tableau II.

BIBLIOGRAPHIE

[1] Bourbaki, N. *Algèbre*, chap. VII, §4, exercice.

[2] Damey, P. et J. J. Payan. Existence et construction des extensions galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique différente de 2. *J. reine angew. Math. 244* (1970), 37-54.

[3] Redei, L. Arithmetischer Beweis des Satzes über die Anzhal der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. reine angew. Math. 171* (1934), 55-64.

[4] —— Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. reine angew. Math. 171* (1934), 131-148.

[5] —— und H. Reichardt. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. reine angew. Math. 170* (1933), 69-74.

[6] Reichardt, H. Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. reine angew. Math. 170* (1933), 75-82.

(Reçu le 26 octobre 1971)

Lyliane Bouvier
Institut de mathématiques pures
Boîte postale 116
F-38 — Saint-Martin d'Hères