

# Chapitre premier. Ordres d'eichler ET IDÉAUX QUASI-NORMAUX

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **21 (1975)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

CHAPITRE PREMIER. ORDRES D'EICHLER  
ET IDÉAUX QUASI-NORMAUX

1. *Corps de quaternions totalement définis* [3]

Un corps de quaternions totalement défini est une algèbre centrale simple  $A$  sur un corps de nombres totalement réel  $k$  telle que pour toute place infinie  $v$  de  $k$ , l'algèbre  $A_v = k_v \otimes_k A$  soit isomorphe au corps des quaternions réels. On note  $k_v$  le complété de  $k$  pour la place  $v$ ,  $v_p$  la valuation ultramétrique associée à un idéal premier  $\mathfrak{p}$  de  $k$ ,  $A_{\mathfrak{p}} = k_{v_p} \otimes_k A$  l'algèbre étendue.

L'algèbre  $A_{\mathfrak{p}}$  est isomorphe à un corps gauche ou à  $M_2(k_{\mathfrak{p}})$ ; dans le premier cas, l'idéal premier  $\mathfrak{p}$  est dit ramifié dans  $A$ . Le nombre d'idéaux premiers ramifiés a même parité que le degré  $n_k$  du corps  $k$  (théorème de Hasse), leur produit  $D_1$  s'appelle le discriminant de  $A$ . On a une réciproque: à tout produit  $D_1$  d'idéaux premiers dont le nombre a même parité que  $n_k$  correspond un unique corps de quaternions totalement défini, ramifié exactement en ces idéaux premiers.

On notera  $\text{Nrd}(\cdot)$  et  $\text{Trd}(\cdot)$  la norme réduite et la trace réduite de  $A$  sur  $k$ . On notera  $N(\cdot)$  la norme absolue de  $k$ ,  $R$  son anneau d'entiers et  $R_{\mathfrak{p}}$  celui de  $k_{\mathfrak{p}}$ . Le groupe des unités d'un anneau  $X$  sera noté  $X^*$ .

Les entiers de  $A$  ne forment pas un anneau; on définit la notion d'ordre et on montre que tout ordre est contenu dans un ordre maximal. Si  $A_{\mathfrak{p}}$  est un corps gauche, les entiers forment un anneau; on a donc un ordre maximal unique. Si  $A_{\mathfrak{p}}$  est isomorphe à  $M_2(k_{\mathfrak{p}})$ , les ordres maximaux sont de la forme  $a M_2(R_{\mathfrak{p}}) a^{-1}$ , où  $a \in M_2(R_{\mathfrak{p}})^*$ .

2. *Ordres d'Eichler* [4], [9], [10]

Soit  $D_1$  un discriminant d'un corps de quaternions  $A$  totalement défini sur un corps de nombres  $k$  et soit  $D_2$  un produit d'idéaux premiers de  $k$  sans facteurs carrés et premier à  $D_1$ . On appelle *ordre d'Eichler sur  $k$  d'invariant  $(D_1, D_2)$*  un ordre de  $A$  localement maximal aux places  $\mathfrak{p}$  ne divisant pas  $D_2$  et sinon isomorphe à l'ensemble des matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R_{\mathfrak{p}})$  avec  $c \in \mathfrak{p} R_{\mathfrak{p}}$ .

Les ordres maximaux de  $A$  sont les ordres d'invariant  $(D_1, 1)$ .

On dit que deux ordres sont du même *genre* lorsqu'ils sont localement isomorphes. Le genre d'un ordre est l'ensemble des ordres qui lui sont localement isomorphes. L'ensemble des ordres d'Eichler d'invariant  $(D_1, D_2)$  donné forme un genre.

Le *discriminant* d'un ordre d'Eichler d'invariant  $(D_1, D_2)$  est égal à  $D_1^2 D_2^2$ .

### 3. Idéaux quasi-normaux [3], [4], [9], [10]

Un idéal *quasi-normal*  $I$  est un idéal de  $A$  localement principal dont l'ordre à gauche  $\mathfrak{O}$  est un ordre d'Eichler. Il existe donc pour tout  $\mathfrak{p}$  un élément  $a_{\mathfrak{p}} \in A_{\mathfrak{p}}^*$  tel que:

$$\mathfrak{I}_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}} a_{\mathfrak{p}}$$

L'ordre à droite de  $\mathfrak{I}_{\mathfrak{p}}$  est  $\mathfrak{O}'_{\mathfrak{p}} = a_{\mathfrak{p}}^{-1} \mathfrak{O}_{\mathfrak{p}} a_{\mathfrak{p}}$  et l'ordre à droite  $\mathfrak{O}'$  de  $\mathfrak{I}$  est donc un ordre d'Eichler appartenant au genre de  $\mathfrak{O}$ .

Un idéal *normal* est un idéal quasi-normal dont les ordres sont maximaux.

Un idéal est *entier* s'il est contenu dans son ordre à gauche. Il est *bilatère* si son ordre à gauche est égal à son ordre à droite.

Les idéaux entiers principaux à gauche de  $\mathfrak{O}_{\mathfrak{p}}$  se mettent de façon unique sous la forme  $\mathfrak{O}_{\mathfrak{p}} a_{\mathfrak{p}}$ , avec:

$$\text{Si } \mathfrak{p} \mid D_1, \quad a_{\mathfrak{p}} = \tilde{\pi}_{\mathfrak{p}}^n$$

où  $\tilde{\pi}$  est une uniformisante de l'ordre maximal  $\mathfrak{O}_{\mathfrak{p}}$ , c'est-à-dire un élément entier de  $A_{\mathfrak{p}}$ , dont la norme réduite est égale à une uniformisante  $\pi_{\mathfrak{p}}$  de  $R_{\mathfrak{p}}$ .

$$\begin{aligned} \text{Si } \mathfrak{p} \mid D_2, \quad a_{\mathfrak{p}} &= \begin{pmatrix} \pi_{\mathfrak{p}}^n & c \\ 0 & \pi_{\mathfrak{p}}^m \end{pmatrix} && \text{ou bien} \\ a_{\mathfrak{p}} &= \begin{pmatrix} 0 & \pi_{\mathfrak{p}}^n \\ \pi_{\mathfrak{p}}^{m+1} & d \end{pmatrix} \end{aligned}$$

où  $n$  et  $m$  sont des entiers positifs ou nuls, où  $c \in R_{\mathfrak{p}}$  est réduit modulo  $\mathfrak{p}^m$  et où  $d \in R_{\mathfrak{p}}$  est réduit modulo  $\mathfrak{p}^{n+1}$ .

$$\text{Si } \mathfrak{p} \nmid D_1 D_2, \quad a_{\mathfrak{p}} = \begin{pmatrix} \pi_{\mathfrak{p}}^n & c \\ 0 & \pi_{\mathfrak{p}}^m \end{pmatrix}$$

où  $n$  et  $m$  sont des entiers positifs et où  $c \in R_{\mathfrak{p}}$  est réduit modulo  $\mathfrak{p}^m$ .

Les idéaux bilatères de  $\mathfrak{O}_{\mathfrak{p}}$  sont les puissances de l'idéal  $\mathfrak{P}_{\mathfrak{p}}$  bilatère de  $\mathfrak{O}_{\mathfrak{p}}$  égal à:

$$\text{Si } \mathfrak{p} \mid D_1, \quad \mathfrak{P}_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}} \tilde{\pi}_{\mathfrak{p}}$$

$$\begin{aligned} \text{Si } \mathfrak{p} \mid D_2, & \quad \mathfrak{P}_p = \mathfrak{D}_p \begin{pmatrix} 0 & 1 \\ \pi_p & 0 \end{pmatrix} \\ \text{Si } \mathfrak{p} \nmid D_1 D_2 & \quad \mathfrak{P}_p = \mathfrak{D}_p \pi_p \end{aligned}$$

#### 4. Idéaux bilatères [4], [6], [9], [10]

Soit  $\mathfrak{D}$  un ordre d'Eichler de  $A$ . Un idéal *premier*  $\mathfrak{P}$  de  $\mathfrak{D}$  est un idéal bilatère de  $\mathfrak{D}$  qui ne se factorise pas de façon non triviale en produit de deux idéaux bilatères de  $\mathfrak{D}$ . L'idéal  $\mathfrak{p} = R \cap \mathfrak{P}$  est un idéal premier de  $k$ . On a deux cas :

$$\begin{aligned} \text{Si } \mathfrak{p} \mid D_1 D_2, & \quad \text{alors } \mathfrak{D}\mathfrak{p} = \mathfrak{P}^2 \quad \text{et} \quad \text{Nrd}(\mathfrak{P}) = \mathfrak{p} \\ \text{Si } \mathfrak{p} \nmid D_1 D_2, & \quad \text{alors } \mathfrak{D}\mathfrak{p} = \mathfrak{P} \quad \text{et} \quad \text{Nrd}(\mathfrak{P}) = \mathfrak{p}^2 \end{aligned}$$

Les idéaux bilatères de  $\mathfrak{D}$  forment un groupe abélien et tout idéal bilatère de  $\mathfrak{D}$  se factorise de façon unique en produit d'idéaux premiers de  $\mathfrak{D}$ . La factorisation de l'idéal  $\mathfrak{D}\mathfrak{p}$  que nous venons de rappeler montre qu'un idéal bilatère de  $\mathfrak{D}$  s'écrit de façon unique sous la forme  $\mathfrak{D}I$  où  $\mathfrak{D}$  est un idéal bilatère de  $\mathfrak{D}$  dont la norme divise  $D_1 D_2$  et où  $I$  est un idéal du centre.

Un idéal bilatère  $\mathfrak{B}$  est déterminé par sa norme et par son ordre. Il est pratique d'utiliser le même symbole  $\mathfrak{B}$  pour tous les idéaux bilatères de norme donnée  $\mathfrak{B}$ . Si  $\mathfrak{S}$  est un idéal quasi normal, on a alors l'égalité

$$\mathfrak{S}\mathfrak{B} = \mathfrak{B}\mathfrak{S} ;$$

dans le membre de gauche,  $\mathfrak{B}$  représente l'idéal bilatère de norme  $B$  de l'ordre à droite de  $\mathfrak{S}$  et dans le membre de droite,  $\mathfrak{B}$  représente l'idéal bilatère de l'ordre à gauche de  $\mathfrak{S}$  de même norme.

L'idéal principal  $\mathfrak{D}a$  est entier et bilatère si et seulement s'il existe deux idéaux  $I$  et  $D$  de  $k$  où  $D \mid D_1 D_2$  tels que :

$$\begin{aligned} & - a \in \mathfrak{D} \\ (1) & - (\text{Nrd}(a)) = D I^2 \\ & - a \pi_p^{-s_p} \in \mathfrak{D}_p \quad \text{si } s_p = v_p(I) \text{ pour tout } \mathfrak{p} \\ & - \text{Trd}(a) \in D I \end{aligned}$$

#### 5. Sous-corps commutatifs maximaux [4], [5], [9]

Soit  $L$  une extension quadratique de  $k$  totalement imaginaire. Soit  $O'$  l'ordre maximal de  $L$  et  $O$  un ordre de  $L$ . Le *conducteur* de  $O$  est le

plus grand idéal de  $O'$  contenu dans  $O$ . Il est engendré par un idéal de  $k$ , noté  $f(O)$ :

$$f(O) = \{a \in k \mid aO' \subseteq O\}$$

A tout idéal entier  $f$  de  $k$  correspond un ordre unique de  $L$  de conducteur  $f$ .

Le nombre de classes des idéaux inversibles de  $O$  est [2]:

$$(2) \quad h(O) = \frac{h_L Nf(O)}{[R_L^* : O^*]} \prod_{p \mid f(O)} \left(1 - \frac{\left(\frac{L}{p}\right)}{Np}\right)$$

où  $h_L$ ,  $R_L^*$ , désignent respectivement le nombre de classes de  $L$ , le groupe des unités de  $L$ , et où  $O^*$  est le groupe des unités de  $O$ . Le symbole  $\left(\frac{L}{p}\right)$  est égal à:

$$(3) \quad \left(\frac{L}{p}\right) = \begin{cases} 0 & \text{si } p \text{ est ramifié dans } L \\ 1 & \text{si } p \text{ est décomposé dans } L \\ -1 & \text{si } p \text{ est inerte dans } L \end{cases}$$

Soit  $W(O)$  le groupe des racines de l'unité contenues dans  $O$ . L'indice des unités de  $O$  c'est-à-dire l'indice [7]:

$$(4) \quad Q(O) = [O^* : W(O)R^*]$$

est égal à 1 ou 2.

On a aussi:

$$Q(O) = [Nrd O^* : R^{*2}]$$

Pour que l'indice des unités  $Q(O)$  soit égal à 2 il faut et il suffit qu'il existe une unité  $\varepsilon \in O^*$  telle que  $\varepsilon \varepsilon'$  ne soit pas un carré dans  $k$  (on note  $\varepsilon'$  le conjugué de  $\varepsilon$  sur  $k$ ). L'indice des unités de  $L$  est l'indice des unités de son ordre maximal.

Les sous corps commutatifs maximaux du corps de quaternions totalement défini  $A$  de discriminant  $D_1$  sont les extensions quadratiques  $L$  de  $k$  totalement imaginaires telles que les idéaux premiers  $p \mid D_1$  ne se décomposent pas dans  $L$ .

Soit  $O$  un ordre de conducteur  $f(O)$  (confondu avec  $f(O)O'$ ) d'une extension quadratique de  $k$  totalement imaginaire. Pour qu'il existe un ordre d'Eichler  $\mathfrak{D}$  sur  $k$  d'invariant  $(D_1, D_2)$  tel que  $O = \mathfrak{D} \cap k(O)$  il faut et il suffit que

Si  $p \mid D_1$ , alors  $p$  ne se décompose pas dans  $k(O)$

$$(5) \quad (f(O), D_1) = 1$$

Si  $p \mid D_2$ , alors  $p \mid f(O)$  ou bien  $p$  ne reste pas inerte dans  $k(O)$ .

On note  $\left\{ \frac{O}{\cdot} \right\}$  le « symbole d'Eichler ». Par définition :

$$(6) \quad \left\{ \frac{O}{p} \right\} = \begin{cases} 1 & \text{si } p|f(O) \\ \left( \frac{k(O)}{p} \right) & \text{sinon} \end{cases}$$

On pose :

$$E_{(D_1, D_2)}(O) = \prod_{p|D_1} \left( 1 - \left\{ \frac{O}{p} \right\} \right) \prod_{p|D_2} \left( 1 + \left\{ \frac{O}{p} \right\} \right)$$

On peut mettre les conditions (5) sous la forme équivalente :

$$(5') \quad E_{(D_1, D_2)}(O) \neq 0$$

Si  $\mathfrak{D}_1$  et  $\mathfrak{D}_2$  sont deux ordres d'Eichler sur  $k$  de même invariant contenant  $O$ , il existe un idéal  $C$  inversible de  $O$  tel que  $\mathfrak{D}_1 C = C \mathfrak{D}_2$ .

## 6. Types d'ordres et classes d'idéaux

On dit que deux ordres  $\mathfrak{D}$  et  $\mathfrak{D}'$  sont du même type lorsqu'ils sont  $R$ -isomorphes. Pour cela, il faut et il suffit qu'il existe  $a \in A^*$  tel que :

$$(7) \quad \mathfrak{D}' = a \mathfrak{D} a^{-1},$$

car tout  $k$ -automorphisme de  $A$  est intérieur.

Le nombre de classes dans un genre est fini. On note  $T_{(D_1, D_2)}$  ou  $T$  s'il n'y a pas d'ambiguïté, le nombre de types des ordres d'invariant  $(D_1, D_2)$ .

On dit que deux idéaux  $I$  et  $I'$  à gauche de  $\mathfrak{D}$  appartiennent à la même classe s'il existe  $a \in A^*$  tel que :

$$(8) \quad \mathfrak{I}' = \mathfrak{I} a.$$

Le nombre de classes dans un genre est fini. On note  $H_{(D_1, D_2)}$  ou  $H$  s'il n'y a pas d'ambiguïté le nombre de classes des idéaux quasi-normaux à gauche d'un ordre d'Eichler d'invariant  $(D_1, D_2)$ . Cette notation est justifiée car le nombre de classes des idéaux quasi-normaux à gauche d'un ordre d'Eichler  $\mathfrak{D}$  est le même pour tous les ordres ayant même invariant. Nous allons le montrer :

Soit  $\mathfrak{D}$  et  $\mathfrak{D}'$  deux ordres d'Eichler de même invariant.

Pour tout idéal premier  $p$  de  $k$  tel que  $\mathfrak{D}'_p \neq \mathfrak{D}_p$  choisissons  $a_p \in A_p^*$  tel que

$$\mathfrak{D}'_p = a_p^{-1} \mathfrak{D}_p a_p.$$

L'idéal quasi-normal  $\mathfrak{I}$  défini par

$$\mathfrak{I}_p = \begin{cases} \mathfrak{D}_p & \text{si } \mathfrak{D}_p = \mathfrak{D}'_p \\ \mathfrak{D}_p a_p & \text{sinon,} \end{cases}$$

est à gauche de  $\mathfrak{D}$  et à droite de  $\mathfrak{D}'$ . La bijection entre les idéaux à gauche de  $\mathfrak{D}'$  et ceux à gauche de  $\mathfrak{D}$ :  $\mathfrak{F} \rightarrow \mathfrak{I} \mathfrak{F}$  définit par passage aux classes une bijection entre les classes à gauche de  $\mathfrak{D}$  et les classes à gauche de  $\mathfrak{D}'$ .

On définit aussi une autre relation d'équivalence sur l'ensemble des idéaux quasi-normaux des ordres d'Eichler sur  $k$  d'invariant  $(D_1, D_2)$  donné, à savoir:

Deux idéaux  $\mathfrak{I}$  et  $\mathfrak{I}'$  sont équivalents si et seulement s'il existe  $a, b \in A^*$  tels que

$$(9) \quad \mathfrak{I}' = a \mathfrak{I} b^{-1}.$$

Le nombre de classes des idéaux quasi-normaux des ordres d'Eichler sur  $k$  d'invariant  $(D_1, D_2)$  pour cette relation d'équivalence est fini et on le note  $H^+_{(D_1, D_2)}$  ou  $H^+$  s'il n'y a pas d'ambiguïté.

### 7. Les nombres $p(n)$

Soit  $N$  un idéal entier de  $k$  et  $\mathfrak{D}$  un ordre d'Eichler sur  $k$  d'invariant  $(D_1, D_2)$ . Nous notons  $\pi^*(N)$  le nombre d'idéaux principaux bilatères entiers de  $\mathfrak{D}$  de norme réduite  $N$ ;  $\pi^*(N)$  est égal à 0 ou à 1, et est toujours nul si  $N$  n'est pas principal ou si  $N \neq D I^2$  où  $D$  et  $I$  sont deux idéaux de  $k$  tels que  $D \mid D_1 D_2$ .

Notons  $(n_1), \dots, (n_t)$  un système de représentants des idéaux principaux de  $k$  de la forme  $D I^2$ , modulo les carrés des idéaux principaux de  $k$ . On a

$$(10) \quad \begin{aligned} \pi^*(N) &= 0 \quad \text{si } N \neq (n_j m^2) \quad \text{avec } m \in k \text{ et } 1 \leq j \leq t \\ \pi^*(n_j m^2) &= \pi^*(n_j). \end{aligned}$$

Nous choisissons un système  $\mathfrak{I}_1 \dots \mathfrak{I}_H$  de représentants des classes des idéaux à gauche de  $\mathfrak{D}$ . Nous notons  $\pi_i^*(n)$  le nombre d'idéaux entiers principaux de norme  $(n)$ , bilatères de l'ordre à droite  $\mathfrak{D}_i$  de l'idéal  $\mathfrak{I}_i$ . Nous posons

$$(11) \quad p(n) = \sum_{i=1}^H \pi_i^*(n)$$

PROPOSITION 1.2. Soit  $(n_1), \dots, (n_t)$  un système de représentants des idéaux  $D I^2$  principaux, avec  $D \mid D_1 D_2$  modulo les carrés des idéaux principaux de  $k$ . Soit  $H, T, H^+$  respectivement:

— le nombre de classes des idéaux  $\mathfrak{S}$  à gauche d'un ordre d'Eichler  $\mathfrak{D}$  d'invariant  $(D_1, D_2)$  pour la relation  $\mathfrak{S}' = \mathfrak{S} a, a \in A^*$ ;

— le nombre de types des ordres d'Eichler d'invariant  $(D_1, D_2)$ ;

— le nombre de classes des idéaux quasi-normaux des ordres d'Eichler d'invariant  $(D_1, D_2)$  pour la relation  $\mathfrak{S}' = a \mathfrak{S} b^{-1}, a, b \in A^*$ .

On a :

$$(12) \quad \begin{aligned} H &= p(1) \\ T &= \frac{1}{h_k 2^s} \sum_{j=1}^t p(n_j) \\ H^+ &= \frac{1}{h_k 2^s} \sum_{j=1}^t p(n_j)^2 \end{aligned}$$

où  $h_k$  est le nombre de classes des idéaux de  $k$  et  $2^s$  le nombre de diviseurs de  $D_1 D_2$ .

*Preuve.* On a  $\pi_i^*(1) = 1$  pour  $1 \leq i \leq H$ , donc  $H = \sum_{i=1}^H \pi_i^*(1) = p(1)$ .

Deux idéaux  $\mathfrak{S}$  et  $\mathfrak{S}'$  vérifiant  $\mathfrak{S}' = \mathfrak{S} a, a \in A^*$  ont leurs ordres à droite du même type, ce qui implique :

$$H = \sum_{i=1}^T H_i$$

où  $H_i$  désigne le nombre de classes des idéaux à gauche de  $\mathfrak{D}$ , dont l'ordre à droite est du type de  $\mathfrak{D}_i$  et  $(\mathfrak{D}_i), 1 \leq i \leq T$  est un système de représentants des types d'ordres.

Fixons un idéal  $\mathfrak{S}$  à gauche de  $\mathfrak{D}$  à droite de  $\mathfrak{D}_i$ . Alors  $H_i$  est le nombre de classes des idéaux  $\mathfrak{S} \mathfrak{B} a$  où  $a \in A^*$  et où  $\mathfrak{B}$  est un idéal bilatère de  $\mathfrak{D}_i$ . Deux idéaux  $\mathfrak{S} \mathfrak{B} a$  et  $\mathfrak{S} \mathfrak{B}' a'$  sont équivalents si et seulement si  $\mathfrak{B}$  est équivalent à  $\mathfrak{B}'$ ; donc  $H_i$  est égal au nombre de classes des idéaux bilatères de  $\mathfrak{D}_i$ .

LEMME 1.2. *Le nombre de classes des idéaux bilatères d'un ordre d'Eichler  $\mathfrak{D}_i$  d'invariant  $(D_1, D_2)$  est égal à*

$$(13) \quad H_i = \frac{h_k 2^s}{\sum_{j=1}^t \pi_i^*(n_j)} .$$

*Preuve.* Un idéal bilatère de  $\mathfrak{D}_i$  s'écrit de façon unique  $\mathfrak{D} I$  où  $\mathfrak{D}$  est un idéal bilatère de  $\mathfrak{D}_i$  dont la norme réduite  $D$  divise  $D_1 D_2$  et où  $I$  est un

idéal de  $k$ . Lorsque  $I_l$ ,  $1 \leq l \leq h_k$  parcourt un système de représentants des classes des idéaux de  $k$ , les classes des idéaux  $\mathfrak{D} I_l^2$  où  $D \mid D_1 D_2$ , modulo les carrés des idéaux principaux sont distinctes. Le nombre  $\sum_{j=1}^t \pi_i^*(n_j)$  est le nombre des idéaux bilatères  $\mathfrak{D} I_l$  qui sont principaux. On note  $2^s$  le nombre d'idéaux  $\mathfrak{D}$ , c'est-à-dire le nombre de diviseurs de  $D_1 D_2$  et on a (13).

Le nombre  $\pi_i^*(n)$  est le même pour tous les ordres du type de  $\mathfrak{D}_i$ , ce qui implique:

$$p(n) = \sum_{i=1}^T H_i \pi_i^*(n)$$

$$\begin{aligned} \text{On a: } \sum_{j=1}^t p(n_j) &= \sum_{j=1}^t \sum_{i=1}^T H_i \pi_i^*(n_j) = \sum_{i=1}^T H_i \sum_{j=1}^t \pi_i^*(n_j) \\ &= \sum_{i=1}^T h_k 2^s = T h_k 2^s \end{aligned}$$

d'où:

$$T = \frac{1}{h_k 2^s} \sum_{j=1}^t p(n_j).$$

Deux idéaux  $\mathfrak{S}'$  et  $\mathfrak{S}$  vérifiant  $\mathfrak{S}' = a \mathfrak{S} b^{-1}$ ,  $a$  et  $b \in A^*$  ont leurs ordres à droite et leurs ordres à gauche du même type, ce qui implique:

$$H^+ = \sum_{\substack{i=1 \dots T \\ j=1 \dots T}} H_{i,j}^+$$

où  $H_{i,j}^+$  désigne le nombre de classes pour la relation (9) des idéaux dont l'ordre à gauche est du type de  $\mathfrak{D}_i$  et l'ordre à droite du type de  $\mathfrak{D}_j$ .

LEMME 1.2. *Le nombre de classes  $H_{i,j}^+$  est égal à :*

$$(14) \quad H_{i,j}^+ = \frac{H_i H_j}{h_k 2^s} \sum_{l=1}^t \pi_i^*(n_l) \pi_j^*(n_l).$$

*Preuve.* On introduit les nombres  $\pi_{i,j}^*(n)$  qui désignent le nombre d'idéaux entiers à gauche de  $\mathfrak{D}_i$  à droite de  $\mathfrak{D}_j$  de norme réduite  $(n)$   $\text{Nrd}(\mathfrak{S})$  et de la forme  $a \mathfrak{S} b^{-1}$  où  $\mathfrak{S}$  est un idéal fixé à gauche de  $\mathfrak{D}_i$  à droite de  $\mathfrak{D}_j$ . On a  $\pi_{i,j}^*(n) = 1$  ou  $0$ . Si  $\pi_{i,j}^*(n) = 1$ , il existe  $a$  et  $b$  tels que les idéaux  $\mathfrak{D}_i a$  et  $\mathfrak{D}_j b$  soient bilatères et  $(n(ab)) = (n)$ . Le symbole «  $\overline{\phantom{x}}$  » signifie l'égalité modulo le carré d'un idéal principal. Si  $(n) \overline{(m)}$  alors  $\pi_i^*(n) = \pi_i^*(m)$  et  $\pi_{i,j}^*(n) = \pi_{i,j}^*(m)$ .

On démontre de façon tout à fait analogue que dans le lemme précédent l'égalité

$$(15) \quad H_{i,j}^+ = \frac{h_k 2^s}{\sum_{l=1}^t \pi_{i,j}^*(n_l)}$$

Le nombre  $\pi_{i,j}^*(n_l)$  n'est pas nul si et seulement s'il existe  $u_o$  et  $v_o$  tels que :

$$(n_l) \equiv_2 (n_{u_o} n_{v_o}), \quad \pi_i^*(n_{u_o}) = \pi_j^*(n_{v_o}) = 1.$$

Dans ce cas :

$$\sum_{(n_u n_v) \equiv_2 (n_l)} \pi_i^*(n_u) \pi_j^*(n_v) = \pi_i^*(n_{u_o}) \pi_j^*(n_{v_o}) \sum_{(n_u n_v) \equiv_2 (n_l)} \pi_i^*(n_u n_{u_o}) \pi_j^*(n_v n_{v_o}).$$

On a

$$(n_u n_v n_{u_o} n_{v_o}) \equiv_2 (n_l^2) \equiv_2 (1) \\ (n_u n_{u_o}) \equiv_2 (n_v n_{v_o})$$

d'où :

$$\sum_{(n_u n_v) \equiv_2 (n_l)} \pi_i^*(n_u) \pi_j^*(n_v) = \sum_{w=1}^t \pi_i^*(n_w) \pi_j^*(n_w).$$

On en déduit que

$$\pi_{i,j}^*(n_l) = \frac{\sum_{(n_u n_v) \equiv_2 (n_l)} \pi_i^*(n_u) \pi_j^*(n_v)}{\sum_{w=1}^t \pi_i^*(n_w) \pi_j^*(n_w)}.$$

En reportant la valeur de  $\pi_{i,j}^*(n_l)$  dans la formule (15), on obtient

$$H_{i,j}^+ = h_k 2^s \frac{\sum_{w=1}^t \pi_i^*(n_w) \pi_j^*(n_w)}{\sum_{l=1}^t \sum_{(n_u n_v) \equiv_2 (n_l)} \pi_i^*(n_u) \pi_j^*(n_v)}.$$

Le dénominateur est le développement du produit

$$\sum_{u=1}^t \pi_i^*(n_u) \cdot \sum_{v=1}^t \pi_j^*(n_v).$$

Nous faisons apparaître les nombres  $H_i$  et  $H_j$

$$H_i = \frac{h_k 2^s}{\sum_{u=1}^t \pi_i^*(n_u)} \quad H_j = \frac{h_k 2^s}{\sum_{v=1}^t \pi_j^*(n_v)}$$

en écrivant  $H_{i,j}^+$  sous la forme

$$H_{i,j}^+ = \frac{1}{h_k 2^s} \sum_{w=1}^t \pi_i^*(n_w) \pi_j^*(n_w) \frac{h_k 2^s}{\sum_{u=1}^t \pi_i^*(n_u)} \cdot \frac{h_k 2^s}{\sum_{v=1}^t \pi_j^*(n_v)}$$

et nous obtenons l'égalité (14).

Nous sommes sur  $i, j$  pour obtenir  $H^+$  :

$$\begin{aligned} H^+ &= \frac{1}{h_k 2^s} \sum_{i,j,w=1 \dots T} H_i H_j \pi_i^*(n_w) \pi_j^*(n_w) \\ H^+ &= \frac{1}{h_k 2^s} \sum_{w=1}^t \sum_{j=1}^T H_j \pi_j^*(n_w) \sum_{i=1}^T H_i \pi_i^*(n_w) \\ H^+ &= \frac{1}{h_k 2^s} \sum_{w=1}^t p(n_w)^2. \end{aligned}$$

### 8. Calcul de $p(n)$

L'objet de ce paragraphe est le calcul des nombres  $p(n)$  qui nous permet avec la proposition 1.2 d'obtenir une formule pour les nombres  $H, T$  et  $H^+$ .

PROPOSITION 1.3. *On a*

$$(16) \quad \begin{aligned} H = p(1) &= \frac{h_k \zeta_k(-1) \Phi_k(D_1, D_2)}{2^{nk-1}} + \sum_O \frac{w(O) - 1}{2 w(O)} E_{D_1, D_2}(O) h(O) \\ p(n) &= \frac{1}{2} \sum_O E_{D_1, D_2}(O) h(O) \quad \text{si } (n) \neq (1) \\ & \hspace{15em} 2 \end{aligned}$$

la somme  $\sum_O$  porte sur les ordres  $O$  des extensions quadratiques de  $k$  totalement imaginaires contenant un élément  $a \notin k$  tel que

- $(Nrd(a)) = D I^2 = (n)$
- $Trd(a) \in D I$
- $a \pi_p^{-s_p} \in O_p$  si  $s_p = v_p(I)$  pour tout  $p$ .

Une conséquence importante de cette proposition est le corollaire suivant :

COROLLAIRE 1.1. *Le nombre de classes du centre  $h_k$  divise  $2H$ .*

*Preuve.* D'après la proposition 1.2., on a :

$$H = p(1)$$

$$T = \frac{1}{h_k 2^s} \sum_{j=1}^t p(n_j) = \frac{1}{h_k 2^s} \left[ p(1) + \sum_{j=2}^t p(n_j) \right]$$

si on suppose que  $(n_1) = (1)$ .

Le nombre de classes du centre  $h_k$  divise  $h(O)$  car  $O$  est un ordre d'une extension quadratique totalement imaginaire de  $k$ , donc  $h_k$  divise  $2p(n_j)$  pour  $2 \leq j \leq t$ .

On a :

$$H = T h_k 2^s - \sum_{j=2}^t p(n_j)$$

donc  $h_k$  divise  $2H$ .

*Remarque.* Si  $n$  est pair, on peut choisir  $(D_1, D_2) = (1, 1)$  alors  $H_{1,1} = h_k T_{1,1}$  et  $H_{1,1}/h_k$  est un entier.

*Démonstration de la proposition 1.3.* On a  $p(n) = 0$  si  $(n) \neq (n_j)$   $1 \leq j \leq t$ . Nous supposons que  $(n) = (n_j)$ . Soit  $(\mathfrak{D}_i)$ ,  $1 \leq i \leq T$ , un système de représentants des ordres d'Eichler de  $A$  d'invariant  $(D_1, D_2)$ . On note  $\mathfrak{D}_i(n)$  l'ensemble des éléments  $\alpha \in \mathfrak{D}_i$  engendrant un idéal bilatère de  $\mathfrak{D}_i$  de norme  $(n)$ . Pour que  $\mathfrak{D}_i(n)$  ne soit pas vide il faut et il suffit que l'idéal bilatère de  $\mathfrak{D}_i$  de norme  $(n)$  soit principal et alors :

$$\mathfrak{D}_i(n) = \mathfrak{D}_i^* \alpha.$$

Comme le corps de quaternions  $A$  est totalement défini, le groupe  $R_k^*$  des unités de  $k$  est d'indice fini  $e_i$  dans le groupe  $\mathfrak{D}_i^*$  des unités de  $\mathfrak{D}_i$  et nous avons alors :

$$1 = \pi_i^*(n) = \frac{|R^* \setminus \mathfrak{D}_i(n)|}{e_i}$$

où on note  $|R^* \setminus \mathfrak{D}_i(n)|$  le nombre de classes d'équivalences définies sur  $\mathfrak{D}_i(n)$  par la relation  $\gamma' = u \gamma$ ,  $u \in R^*$ . On fixe une clôture algébrique  $\hat{k}$  de  $k$ . A tout  $\alpha \in \mathfrak{D}_i(n)$ ,  $\alpha \notin k$  correspond une extension quadratique de  $k$ , contenue dans  $\hat{k}$ , totalement imaginaire et isomorphe à  $k(\alpha)$ . On considère l'ordre  $O$  de cette extension isomorphe à  $k(\alpha) \cap \mathfrak{D}_i$ . On pose

$$O(n) = \{\alpha \notin k / \alpha \in O \cap \mathfrak{D}_i(n)\}$$

c'est-à-dire,  $O(n)$  est égal à l'ensemble des éléments  $\alpha$  de  $O$  vérifiant :

$$(17) \quad \begin{aligned} & - \text{Nrd}(\alpha) = (n) = D I^2 \\ & - \text{Trd}(\alpha) \in D I \\ & - \alpha \pi_p^{-s_p} \in O_p \text{ si } s_p = v_p(I) \text{ pour tout } p \\ & - \alpha \notin k. \end{aligned}$$

On remarque que si  $(n) \neq (1)$  alors  $\mathfrak{D}_i(n) \cap k = \emptyset$  dans ce cas :

$$O(n) = \mathfrak{D}_i(n) \cap O.$$

Si  $(n) \equiv (1)$  alors  $\mathfrak{D}_i(n) \cap k = R^*$  et dans ce cas :

$$O(n) = \mathfrak{D}_i(n) \cap O - R^*.$$

Soit  $g_i(O)$  le nombre d'ordres isomorphes à  $O$  contenus dans  $\mathfrak{D}_i$ . On a

$$\begin{aligned} \pi_i^*(1) &= \frac{1}{e_i} \left[ 1 + \sum_O g_i(O) |R^* \setminus O(n)| \right] \\ \pi_i^*(n) &= \frac{1}{e_i} \sum_O g_i(O) |R^* \setminus O(n)| \quad \text{si } (n) \neq (1). \end{aligned}$$

La somme  $\sum_O$  porte sur les ordres  $O = \mathfrak{D}_i \cap k(\alpha)$  les éléments  $\alpha \in \hat{k}$  étant astreints aux conditions (17).

Ces conditions impliquent que les idéaux premiers  $p \mid D$  sont ramifiés dans  $k(\alpha)$ . L'idéal  $O_\alpha$  est égal à  $\mathfrak{D} I$  où  $\mathfrak{D}$  est l'unique idéal de  $O$  de norme  $D$ . On a :

$$\begin{aligned} O(n) &= O^* \alpha \quad \text{si } (n) \neq (1) \\ O(1) &= O^* - R^*. \end{aligned}$$

On note  $w(O)$  l'indice du groupe  $R_k^*$  des unités de  $k$  dans le groupe  $O^*$  des unités de  $O$  et nous avons

$$\begin{aligned} \pi_i^*(1) &= \frac{1}{e_i} \left[ 1 + \sum_O g_i(O) (w(O) - 1) \right] \\ \pi_i^*(n) &= \frac{1}{e_i} \sum_O g_i(O) w(O) \quad \text{si } (n) \neq (1) \end{aligned}$$

Nous en déduisons pour les nombres  $h(n)$  les formules

$$(18) \quad \begin{aligned} p(1) &= \sum_{i=1}^r H_i \pi_i^*(1) = \sum_{i=1}^r \frac{H_i}{e_i} + \sum_{i=1}^r \sum_O \frac{H_i g_i(O)}{e_i} (w(O) - 1) \\ p(n) &= \sum_{i=1}^r H_i \pi_i^*(n) = \sum_{i=1}^r \sum_O \frac{H_i g_i(O)}{e_i} w(O) \end{aligned}$$

Nous avons la relation [4]:

$$(19) \quad \sum_{i=1}^T \frac{H_i}{e_i} = h_k \zeta_k(-1) \Phi_k(D_1, D_2) 2^{1-n_k}$$

où  $h_k$ ,  $\zeta_k(\cdot)$ ,  $n$  désignent le nombre de classes, la fonction zêta et le degré du corps  $k$  et

$$\Phi_k(D_1, D_2) = \prod_{\mathfrak{p}|D_1} (1 - N\mathfrak{p}) \prod_{\mathfrak{p}|D_2} (1 + N\mathfrak{p}).$$

Nous intervertissons dans les formules (18) la sommation sur les types d'ordres et la sommation sur les ordres quadratiques:

$$(20) \quad \begin{aligned} h(1) &= \frac{h_k \zeta_k(-1) \Phi_k(D_1, D_2)}{2^{n_k-1}} + \sum_{\mathcal{O}} (w(\mathcal{O}) - 1) \sum_{i=1}^T \frac{H_i g_i(\mathcal{O})}{e_i} \\ h(n) &= \sum_{\mathcal{O}} w(\mathcal{O}) \sum_{i=1}^T \frac{H_i g_i(\mathcal{O})}{e_i} \quad \text{si } (n) \neq (1)_2. \end{aligned}$$

LEMME 1.3. *On a*

$$\sum_{i=1}^T \frac{H_i g_i(\mathcal{O})}{e_i} = \frac{h(\mathcal{O})}{2 w(\mathcal{O})} E_{D_1, D_2}(\mathcal{O}).$$

Ce lemme et les relations (20) nous donnent la proposition 1.3.

*Démonstration du lemme 1.3.* On fixe un ordre d'Eichler  $\mathfrak{D}$  d'invariant  $(D_1, D_2)$  tel que  $\mathfrak{D} \cap k(\mathcal{O}) = \mathcal{O}$ . Pour qu'un tel ordre  $\mathfrak{D}$  existe il faut et il suffit que  $E_{D_1, D_2}(\mathcal{O})$  soit non nul (§.4). Un idéal à gauche de  $\mathfrak{D}$  dont l'ordre à droite  $\mathfrak{D}'$  vérifie  $\mathfrak{D}' \cap k(\mathcal{O}) = \mathcal{O}$  s'écrit de façon unique sous la forme  $\mathfrak{D}I$  où  $\mathfrak{D}$  est un idéal bilatère de  $\mathfrak{D}$  dont la norme réduite est un produit d'idéaux premiers non ramifiés dans  $k(\mathcal{O})$  et divisant  $D_1 D_2$  et  $I$  un idéal inversible de  $\mathcal{O}$ . On remarque que  $E_{D_1, D_2}(\mathcal{O})$  s'il n'est pas nul est égal au nombre des idéaux  $\mathfrak{D}$  car

$$E_{D_1, D_2}(\mathcal{O}) = \prod_{\mathfrak{p}|D_1} \left(1 - \left\{\frac{\mathcal{O}}{\mathfrak{p}}\right\}\right) \prod_{\mathfrak{p}|D_2} \left(1 + \left\{\frac{\mathcal{O}}{\mathfrak{p}}\right\}\right).$$

On note  $h_i$  le nombre de classes des idéaux  $I$  inversibles dans  $\mathcal{O}$  engendrant un idéal  $\mathfrak{D}I$  dont l'ordre à droite est du type de  $\mathfrak{D}_i$  et  $I_1 \dots I_{h_i}$  un système de représentants de ces idéaux; on note  $h(\mathcal{O})$  le nombre de classes des idéaux inversibles de  $\mathcal{O}$ . On a:

$$h(\mathcal{O}) = \sum_{i=1}^T h_i.$$

Si  $h_i \neq 0$ , le nombre  $H_i$  qui est égal au nombre de classes des idéaux bilatères de  $\mathfrak{D}_i$ , donc des idéaux à gauche de  $\mathfrak{D}$  dont l'ordre à droite est du type de  $\mathfrak{D}_i$  est aussi égal au nombre de classes des  $h_i E_{D_1, D_2}(O)$  idéaux  $\mathfrak{D}I_j$   $1 \leq j \leq h_i$  pour la relation:

$$\mathfrak{D}'I' = \mathfrak{D}Ia \quad a \in A^* .$$

Pour qu'un idéal  $\mathfrak{D}_i a$  soit de la forme  $\mathfrak{D}I$  il faut et il suffit que  $O a^{-1} \subset \mathfrak{D}_i$ .

On pose

$$O'_i = \{a \in A^* / a O a^{-1} \subset \mathfrak{D}_i\} .$$

pour que:

$$\mathfrak{D}_i a = \mathfrak{D}_i x \quad x \in k(O)$$

il faut et il suffit que  $a \in \mathfrak{D}_i^* k(O)^*$ . Le nombre d'idéaux à gauche de  $\mathfrak{D}_i$  de la forme  $\mathfrak{D}I_j$  (où  $\mathfrak{D}$  représente ici l'idéal bilatère de  $\mathfrak{D}_i$  de norme réduite  $D$ ) qui sont principaux est égal à  $|\mathfrak{D}_i^* k(O)^* \setminus \mathfrak{D}'_i|$ .

On note  $\mathfrak{D}''_i$  le sous-groupe de  $\mathfrak{D}'_i$  formé des  $a \in A^*$  tels que  $a O a^{-1} = O$ . Pour  $a \in \mathfrak{D}''_i$  et  $x \in O$  on a:

$$a x a^{-1} = x \text{ ou } x', \quad x' = \text{le conjugué de } x \text{ sur } k .$$

On choisit  $\alpha \in A$  tel que  $\alpha x \alpha^{-1} = x'$  pour  $x \in k(O)$ . On a:

$$\mathfrak{D}''_i = \{a \in A^* / a \text{ ou } \alpha^{-1} a \text{ commute avec les éléments de } k(O)\}$$

donc

$$\mathfrak{D}''_i = k(O)^* \cup \alpha k(O)^* .$$

On a:

$$|\mathfrak{D}''_i \setminus \mathfrak{D}'_i| = g_i(O)$$

$$|k(O)^* \setminus \mathfrak{D}'_i| = 2 g_i(O)$$

$$|\mathfrak{D}_i^* k(O)^* \setminus \mathfrak{D}'_i| = \frac{|k(O)^* \setminus \mathfrak{D}'_i|}{|O^* \setminus \mathfrak{D}_i^*|} = \frac{2 g_i(O) w(O)}{e_i}$$

Nous obtenons donc pour  $H_i$  lorsque  $h_i \neq 0$

$$H_i = h_i E_{D_1, D_2}(O) \frac{e_i}{2 g_i(O) w(O)}$$

d'où:

$$\sum_{i=1}^T \frac{H_i g_i(O)}{e_i} = \sum_{i=1}^T h_i \frac{E_{D_1, D_2}(O)}{2 w(O)} = \frac{h(O)}{2 w(O)} E_{D_1, D_2}(O) .$$

Nous obtenons donc le lemme 1.3.