THÉORIE DES NOMBRES

BESANÇON

Année 1983 - 1984

LES NOMBRES CONVENABLES DE LEONHARD EULER

Günther FREI

LES NOMBRES CONVENABLES DE LEONHARD EULER

Günther Frei

Département de mathématiques
Université Laval
Ste-Foy, Québec
Canada G1K 7P4

et

Forschungsinstitut für Mathematik
ETH-Zentrum
CH-8092 Zürich
Suisse

A l'occasion du deux-centenaire de la mort de

Leonhard Euler (4.4.1707 - 18.9.1783)

dédié à mon cher ami Paulo Ribenboim

Préface

Cet article est une version élargie d'une conférence donnée à l'Université de Besançon le 11 juin 1982. J'aimerais remercier vivement mes amis Georges et Marie-Nicole Gras qui m'avaient invité à Besançon et qui m'avaient encouragé à écrire cet article. Je remercie également profondément Monsieur le Professeur Beno Eckmann pour son invitation généreuse à passer l'été 1983 au Forschungsinstitut für Mathematik à l'ETH Zürich et Madame Liselotte Karrer pour des aides pratiques liées à la nature de ce séjour et Madame Hermona Rosinger pour la dactylographie impéccable du manuscrit.

Tarasp, le 21 août 1983

Table des matières

1. Les nombres convenables d'Euler

1. Il est bien connu que les théorèmes de Gauss sur les genres des formes quadratiques équivalent aux théorèmes fondamentaux de la théorie du corps de classes pour les corps quadratiques (voir [Ga] - 1801). Moins connu est le fait que déjà Euler découvrit des propriétés sur les genres et trouva ainsi les premiers résultats reliés à la théorie du corps de classes. C'est Kronecker qui remarqua (voir [Kr], Vol. 2, Nr. 1 - 1875) que le mérite d'avoir trouvé la loi de réciprocité quadratique le premier (avant Legendre et Gauss) revient à Euler (voir [Eu], no. 164 (Ser. 1, Vol. 2, p. 194- 222) - 1751 et no. 552 (Ser. 1, Vol. 3, p. 497-512) - 1783)) et Fueter dans la préface du volume IV de la première série de l'Opera Omnia d' Euler nota en 1941 qu' Euler ne reconnut pas seulement la loi de réciprocité quadratique, mais qu'il observa même que seulement la moitié des genres possibles des formes quadratiques binaires ayant déterminant $-n$ existent (voir [Eu], no. 598 et no. 610 (Ser. 1 Vol. 4, p. 163-220) - 1785 et 1787). On doit à Euler également la notion et la théorie des nombres convenables, théorie que Gauss interpréta en 1801 comme étant une théorie des formes quadratiques binaires ayant une seule classe par genre (voir [Ga], Art. 303).

D'après l'interprétation que donna Takagi en 1920 (voir [Ta]) à la théorie du corps de classes, celle-ci est la théorie des extensions algébriques abéliennes L/K d'un corps de nombres K. Les extensions abéliennes L/K sont précisément les extensions L de K qui se laissent caractériser par des propriétés de congruences dans K, en particulier en ce qui concerne le groupe normique dans K associé à L et les idéaux premiers p dans K complètement scindés dans L et en général la loi de décomposition des premiers p dans K par rapport à L/K. Point de départ du développement conduisant à une théorie du corps de classes est ainsi la théorie des corps abéliens issue de la théorie des corps cyclotomique de Gauss (voir [Ga] - 1801, chapitre V) et la théorie de représentation d'un nombre par une forme, en particulier d'un premier par une forme normique. En ce qui concerne la théorie de représentation l'observation suivante faite par Fermat, Euler et Lagrange est fondamentale:

Les nombres premiers représentés par une forme quadratique binaire donnée se trouvent tous dans les mêmes progressions arithmétiques, et sont donc représentables par des formes linéaires.

2. Une telle première observation se trouve dans une lettre de Fermat adressée à son ami Mersenne le 25 décembre 1640 (voir [Fe]).

Théorème 1.1: Un nombre premier impair p est somme de deux carrés de nombres naturels, $p = x^2 + y^2$, $x,y \in \mathbb{N}$, si et seulement si $p \equiv 1$ modulo 4. De plus, cette représentation est unique et x et y sont premiers entre eux, $(x,y) = 1$.

Nous désignons par $\mathbb{N}$ l'ensemble des nombres naturels, $\mathbb{N} = \{1,2,3,4,...\}$ et par $\mathbb{N}_0$ l'ensemble $\mathbb{N}$ augmenté par 0 , $\mathbb{N}_0 = \{0,1,2,3,4,...\}$. Notons aussi que $(x,y) = 1$ implique $x \neq 0$, $y \neq 0$.

Ce théorème fut complètement démontré par Euler plus d'un siècle plus tard, à savoir en 1750, resp. 1760 et 1758 dans les Nouveaux Commentaires de l'Académie des Sciences à Petersbourg (voir [Eu], no. 134 (Ser. 1, Vol. 2, p. 62-85) - 1750, en particulier Theorema 5, no. 241 (Ser. 1, Vol. 2, p. 328-337) - 1760 et no. 228 (Ser. 1, Vol. 2, p. 295-327) - 1758, en particulier Propositio 7). Mais Euler remarqua et démontra en 1758 aussi l'inverse (voir [Eu], no. 228 (Ser. 1, Vol. 2, p. 295-327) - 1758, en particulier p. 314):

Théorème 1.2: Tout nombre naturel impair $n > 1$ qui n'est représentable que d'une seule manière comme somme de deux carrés de nombres non négatifs, $n = x^2 + y^2$, $x,y \in \mathbb{N}_0$, lesquels nombres sont en plus premiers entre eux, $(x,y) = 1$, est un premier.

Ce critère lui donna un moyen pour examiner le problème des grands nombres premiers posé par Fermat:

Etant donné un "grand" nombre naturel n, décider si n est premier ou non.

D'après le théorème 1.2 il suffit de soustraire à n tous les carrés x^2 inférieurs à $n/2$ et d'examiner s'il ne reste un carré qu'une seule fois. En outre, Euler nota qu'il n'est pas nécessaire d'essayer tous les carrés x^2 inférieurs à $n/2$, car les x doivent satisfaire à certaines conditions de congruence pour un n donné. Il trouva ces conditions moyennant sa théorie des restes quadratiques calculés et rassemblés dans de grandes tables. Par exemple, étant donné $n \equiv 77$ modulo 480, il suffit de vérifier les valeurs $x \equiv \pm 19$, ± 29, ± 61, ± 109 modulo 240 (voir [Eu], no. 369 (Ser. 1, Vol. 3, p. 112-130) - 1769).

Cette méthode ne s'applique qu'aux nombres $n \equiv 1$ modulo 4 puisque d'après le théorème 1.1 uniquement des premiers impairs p de cette forme peuvent être somme de deux carrés. Pour étendre la méthode aussi aux nombres $n \equiv 3$ modulo 4 Euler examina les formes $n = x^2 + 2y^2$ et $n = x^2 + 3y^2$, formes déjà étudiées par Fermat, et plus généralement les formes $n = ax^2 + by^2$ avec $a,b \in \mathbb{N}$. Euler arriva alors au résultat suivant (voir [Eu], no. 256 (Ser. 1, Vol. 2, p. 459-492) - 1761, en particulier Theoremata 4, 10, 11 et 12 et Observatio 8 et no. 449 (Ser. 1, Vol. 3, p. 240-281) - 1774, en particulier art. 85):

Théorème 1.3: 1) Etant donné un premier impair p, l'équation $p = x^2 + 2y^2$ est résoluble et ceci d'une seule manière avec $x,y \in \mathbb{N}$ si et seulement si $p \equiv 1,3$ modulo 8. En plus x et y sont premiers entre eux. 2) Inversement, si $n > 1$ est un nombre naturel impair tel que $n = x^2 + 2y^2$ soit résoluble d'une seule manière avec $x,y \in \mathbb{N}_0$ et qu'en plus x et y soient premiers entre eux, alors n est premier.

Euler publia une démonstration complète de ce théorème à l'exception de la partie qui affirme qu'un premier $p \equiv 3$ module 8 est toujours représentable par $p = x^2 + 2y^2$. Mais Euler dit dans l'article 85 de cette publication (voir [Eu], no. 449, Ser. 1, Vol. 3, p. 275) qu'il sait aussi régler ce cas-ci grâce à une communication d'un ami. C'est cependant Lagrange qui en publia le premier une démonstration en 1775 (voir [La]).

De plus Euler affirme le théorème suivant (voir [Eu], no. 272 Ser. 1, Vol. 2, p. 556-575) - 1763, en particulier Propositio 9):

Théorème 1.4: 1) Etant donné un premier $p \neq 2,3$, l'équation $p = x^2 + 3y^2$ est résoluble et ceci d'une seule manière avec $x,y \in \mathbb{N}$ si et seulement si $p \equiv 1$ modulo 3; x et y sont alors premiers entre eux. 2) Inversement, si $n > 1$ est un nombre naturel impair tel que $n = x^2 + 3y^2$ soit résoluble d'une seule manière avec $x,y \in \mathbb{N}_0$ et qu'en plus x et $3y$ soient premiers entre eux, alors n est premier.

Euler ne publia une démonstration que pour la première partie du théorème. Une démonstration pour la deuxième partie apparut pour la première fois dans l'ouvrage de Lagrange mentionné plus haut (voir [La]).

3. Il n'est pas possible d'obtenir un théorème analogue aux théorèmes 1.2, 1.3 et 1.4 pour la forme $x^2 + 11y^2$, car $15 = 1 \cdot 2^2 + 11 \cdot 1^2$ n'est décomposable que de cette manière en nombres naturels quoique 15 ne soit pas premier. On est donc amené à la question suivante. Pour quels nombres naturels $a,b \in \mathbb{N}$ l'énoncé suivant est-il vrai?

(C) $\left\{\begin{array}{l} \text{Si } n > 1 \text{ est un nombre naturel impair tel que} \\ n = ax^2 + by^2, \text{ avec } a,b \in \mathbb{N} \text{ et } (a,b) = 1 , \\ \text{soit résoluble d'une seule manière avec } x,y \in \mathbb{N}_0 \\ \text{et qu'en plus } ax \text{ et } by \text{ soient premiers entre} \\ \text{eux, } (ax,by) = 1 , \text{ alors } n \text{ est premier.} \end{array}\right.$

Ainsi Euler introduisit la notion suivante (voir [Eu], no. 708 (Ser. 1, Vol. 4, p. 269-289) - 1778, en particulier art. 10) :

Définition 1.5: Une forme $ax^2 + by^2$ avec $a,b \in \mathbb{N}$, $(a,b) = 1$, est appelée une forme congrue ou une forme convenable si tout nombre naturel $n > 1$ qui admet une seule solution

$$n = ax^2 + by^2$$

avec $x,y \in \mathbb{N}_0$ de sorte qu'en plus $(x,y) = 1$, est nécessairement de la forme

$$n = tp \quad \text{ou} \quad n = 2tp \quad \text{ou} \quad n = t2^s ,$$

où t est un diviseur de $a \cdot b$, p est un premier impair et s est un nombre naturel.

Euler dans sa définition ne mentionne pas explicitement la forme $t2^s$ avec $t \neq 1$ qu'il faut cependant ajouter (voir la définition 5.3).

Notons qu'une forme convenable satisfait à la condition (C), car si n est soumis à la condition d'être impair, il faut que $n = tp$, et la condition $(ax,by) = 1$ entraîne $t = 1$; car si q est premier et $q|t$ on a $q|a$ ou $q|b$; comme $q|n$ on en déduit $q|ax$ et $q|by$ et donc $(ax,by) \neq 1$.

Puis Euler démontra (voir [Eu], no. 708, art. 14):

Théorème 1.6: Soit $a,b \in \mathbb{N}$ et $(a,b) = 1$. La forme $ax^2 + by^2$ est convenable si et seulement si la forme $x^2 + aby^2$ est convenable.

La démonstration d' Euler utilise l'hypothèse que a ou b est sans carrés. Une démonstration générale de ce théorème, sans cette hypothèse, fut donnée par Grube en 1874 (voir la section 5 et [Gr], § 8, p. 510). Ceci donne lieu à la (voir [Eu], no. 708, art. 17)

Définition 1.7: Un nombre naturel m est appelé congru ou convenable (idoneus) si la forme $x^2 + my^2$ est convenable.

Un tel nombre m est en effet convenable pour examiner si un nombre donné n est premier ou non et pour découvrir de grands nombres premiers. Euler illustra cette méthode de recherche de nombres premiers, effectuée en 1778, dans [Eu], no. 718 et no. 719 (Ser. 1, Vol. 4 p. 352-394) - 1805.

Dans [Eu], no. 718 Euler détermina tous les nombres premiers p de la forme

$$p = 232x^2 + 1 \qquad \text{avec} \quad 1 \leq x < 300 , \qquad x \in \mathbb{N} ,$$

et dans [Eu], no. 719 Euler examina les nombres

$$n = 10'003 = 1 \cdot 100^2 + 3 \cdot 1^2$$
$$n = 100'003 = 10 \cdot 100^2 + 3 \cdot 1^2$$
$$n = 1'000'003 = 1 \cdot 1000^2 + 3 \cdot 1^2$$

et des nombres n de la forme

$$n = 40x^2 + 13y^2$$

et de la forme

$$n = 1848x^2 + y^2 .$$

En particulier il détermina tous les nombres premiers p de la forme

$$p = 1848x^2 + 197^2 \quad \text{avec} \quad 1 \leq x \leq 100 , \quad x \in \mathbb{N} .$$

Par exemple

$p = 18'518'809 = 1848 \cdot 100^2 + 197^2$ est un nombre premier; en effet, c'est de loin le plus grand nombre premier connu à l'époque sauf pour le premier de Mersenne $p = 2^{31} + 1$ découvert également par Euler.

$n = 100'003$ ainsi que $n = 1'000'003$

sont également premiers, mais $n = 10'003$ ne l'est pas étant donné que

$$n = 10'003 = 1 \cdot 100^2 + 3 \cdot 1^2 = 1 \cdot 16^2 + 3 \cdot 57^2 .$$

En effet, le nombre premier $p = 1429$ est un diviseur de $10'003$:

$$n = 10'003 = 7 \cdot 1429$$

où les facteurs 7 et 1429 sont déterminés par les deux représentations.

Puis Euler nota ce résultat très remarquable (voir [Eu], no. 708, art. 18 ou no. 715 (Ser. 1, Vol. 4, p. 303-328) - 1802, art. 39):

Théorème 1.8: Les 65 nombres suivants sont convenables (numeri idonei):

1	2	3	4	5	6	7	8	9	10
12	13	15	16	18	21	22	24	25	28
30	33	37	40	42	45	48	57	58	60
70	72	78	85	88	93	102	105	112	120
130	133	165	168	177	190	210	232	240	253
273	280	312	330	345	357	385	408	462	520
760	840	1320	1365	1848	.				

Pour calculer cette table "avec assez de facilité" Euler se servit du critère suivant (voir [Eu], no. 715, art. 45 ou no. 498 (Ser. 1, Vol. 3, p. 337-339) - 1776; voir aussi no. 708a (Ser. I, Vol. 3, p. 340-346) - 1778).

Théorème 1.9: Un nombre naturel $m \in \mathbb{N}$ est convenable si et seulement si tout nombre n de la forme

$$n = m + x^2 < 4m \quad \text{avec} \quad x \in \mathbb{N}, \quad (x,m) = 1$$

est de la forme

$$n = p, \quad n = 2p, \quad n = p^2 \quad \text{ou} \quad n = 2^s$$

ou p est un nombre premier impair et s un nombre naturel.

Pour démontrer ce critère il s'appuya sur le théorème suivant (voir [Eu], no. 715, en particulier Theorema 6 et Theorema 7, et encore no. 708, art. 20 ou no. 708a):

Théorème 1.10: Si un nombre composé $r \cdot s$ $(r > 2)$ est représentable par la forme $x^2 + my^2$ d'une seule manière avec $x, y \in \mathbb{N}$ et si $(x,my) = 1$ et $(rs,mxy) = 1$, alors il existe une infinité d'autres

nombres composés ayant la même propriété. En particulier il y a toujours un tel nombre composé $r \cdot s < 4m$.

Euler donna comme exemple pour le théorème 1.9. entre autres les nombres $m = 14, 11, 13$ (voir [Eu], no. 715, art. 38) et $m = 60$ et $m = 15$ (voir [Eu], no. 498):

Pour $m = 13$ il trouva

$$13 + 1^2 = 14 = 2p$$
$$13 + 2^2 = 17 = p$$
$$13 + 3^2 = 22 = 2p$$
$$13 + 4^2 = 29 = p$$
$$13 + 5^2 = 38 = 2p$$
$$13 + 6^2 = 49 = p^2$$

donc $m = 13$ est convenable.

Les calculs pour $m = 60$ et $m = 15$ donnent:

$$60 + 1^2 = 61 = p \qquad 15 + 1^2 = 16 = 2^4$$
$$60 + 7^2 = 109 = p \qquad 15 + 2^2 = 19 = p$$
$$60 + 11^2 = 181 = p \qquad 15 + 4^2 = 31 = p \,.$$
$$60 + 13^2 = 229 = p$$

Ajoutons encore l'exemple du nombre convenable $m = 5$

$$5 + 1^2 = 6 = 2p$$
$$5 + 2^2 = 9 = p^2$$
$$5 + 3^2 = 14 = 2p$$

tandis que $5 + 4^2 = 21 = 3 \cdot 7 > 4 \cdot 5$.

Pour les nombres non-convenables $m = 14$ et $m = 11$ on trouve

$14 + 1^2 = 15 = 3 \cdot 5$ $\qquad$ $11 + 1^2 = 12 = 3 \cdot 4$

$14 + 3^2 = 23 = p$ $\qquad$ $11 + 2^2 = 15 = 3 \cdot 5$

$14 + 5^2 = 39 = 3 \cdot 13$ $\qquad$ $11 + 3^2 = 20 = 4 \cdot 5$

$11 + 4^2 = 27 = 3^3$

$11 + 5^2 = 36 = 2^2 \cdot 3^2$

La démonstration du critère 1.9, par Euler n'est pas du tout satisfaisante comme Grube remarqua en 1874 (voir [Gr], §4). Euler démontra la nécessité seulement pour les nombres de la forme p, $2p$, k^2 ou 2^s où p est premier et k est un nombre entier quelconque, et sa démonstration de la suffisance contient des lacunes sérieuses (voir [Gr], p. 501). C'est Grube qui démontra que le critère est, en fait, nécessaire (voir [Gr], p. 517 et p. 498). Que le critère soit aussi suffisant est resté un problème ouvert quoique Gauss dise dans ses "Disquisitiones arithmeticae" (voir [Ga], art. 303), en 1801, qu'il soit facile à démontrer. En 1874, cependant, Grube réussit à démontrer un critère très semblable au critère 1.9. d' Euler (voir théorème 5.8).

Euler donna encore un autre critère pour des nombres convenables, mais celui-ci n'est pas correct comme Grube remarqua (voir [Gr], §4, p. 503). Le critère dit (voir [Eu], no. 708, art. 21):

Théorème: Un nombre naturel m est un nombre convenable si et seulement si tout nombre n de la forme

$$n = m + x^2 < 4m \quad \text{avec} \quad x \in \mathbb{N}$$

est de la forme

$$n = p\,, \quad n = 2p\,, \quad n = tp\,, \quad n = p^2 \quad \text{ou} \quad n = 2^s$$

ou p est un premier impair, t est un diviseur de m et s est un nombre naturel.

En effet, le critère impliquerait que $m = 33$ et $m = 72$ ne sont pas convenables, parce que

$$33 + 3^2 = 42 = 2 \cdot t \cdot p$$

et $$82 + 3^2 = 81 = t \cdot p^2 ,$$

contrairement au fait que $m = 33$ et $m = 72$ sont convenables (voir théorème 1.8).

Euler fut surpris de voir qu'il ne trouva plus de nombres convenables excédants 1848 malgré qu'il continua ses calculs au delà de 10'000 . Pour comprendre ce phénomène il étudia la distribution des nombres convenables et il en découvrit et démontra les 10 propriétés suivantes (voir [Eu], no. 708, Theoremata 1 à 10):

Théorème 1.11:

(1) Si c est convenable et $c = t^2$, alors $t = 1,2,3,4,5$.

(2) Si c est convenable et $c \equiv 3$ modulo 4 , alors $4c$ est convenable.

(3) Si c est convenable et $c \equiv 4$ modulo 8 , alors $4c$ est convenable.

(4) Si k^2m est convenable, alors m est convenable.

(5) Si c est convenable et $c \equiv 2$ modulo 3 , alors $9c$ est convenable.

(6) Si $c > 1$ est convenable et $c \equiv 1$ modulo 4 , alors $4c$ n'est pas convenable.

(7) Si c est convenable et $c \equiv 2$ modulo 4 , alors $4c$ est convenable.

(8) Si c est convenable et $c \equiv 8$ modulo 16 , alors $4c$ n'est pas convenable.

(9) Si c est convenable et $c \equiv 16$ modulo 32 , alors $4c$ n'est pas convenable.

(10) Si c est convenable et $c + a^2 = p^2 < 4c$ pour un nombre premier p , alors $4c$ n'est pas convenable.

Les propriétés (4), (6), (8), (9) ne furent pas démontrées par Euler avec assez de rigueur et c'est Grube qui les compléta en 1874 (voir [Gr], §10). Grube obtint aussi des résultats plus généraux en ce qui concerne les propriétés (1), (6), (8), (9) et (10) (voir théorème 5.7).

Nous reviendrons aux théorèmes 1.6, 1.9, 1.10 et 1.11 dans la dernière section et au théorème 1.8 dans la section 4. La prochaine section traitera l'interprétation que donna Gauss des nombres convenables en termes de sa théorie des formes quadratiques, et dans la section 3 cette théorie sera traduite suivant Dedekind en langage des corps quadratiques.

2. Théorie des formes quadratiques de Gauss

1. Après les recherches d' Euler sur les formes quadratiques du type $x^2 + by^2$, où $b = 1,2,3,$ et aussi (mais d'une façon moins approfondie) sur les formes $ax^2 + by^2$ (voir [Eu], no. 164, 708 et 708a) c'est Lagrange qui en 1773 et 1775 entreprit une première étude systématique sur les formes quadratiques générales à coefficients entiers $ax^2 + bxy + cy^2$ (voir [La]). Il introduisit par exemple les notions de déterminant, d'équivalence, de classe et de réduction. Un résultat principal de sa théorie est que le nombre de classes des formes quadratiques ayant même déterminant est fini, théorème que Lagrange put déduire en associant à chaque classe une forme réduite.

Pour une théorie systématique il faut cependant attendre Gauss qui la developpa en 1801 dans son oeuvre fondamentale "Disquisitiones arithmeticae" (voir [Ga]). Dans cet ouvrage Gauss, après avoir démontré le premier la loi de réciprocité quadratique d'une façon complète, étudia à fond la théorie des formes quadratiques $ax^2 + 2bxy + cy^2$, c'est-à-

dire les équivalences, les classes, les classes propres, la réduction, et il introdusit les notions fondamentales de genres, d' ordres, de classes ambigues et de composition.

2. Si

$$f = [a,b,c] = ax^2 + 2bxy + cy^2 \quad \text{avec} \quad a,b,c \in \mathbb{Z}$$

est une forme quadratique (binaire et entière) nous associons à f la matrice symétrique

$$M_f = \begin{pmatrix} a & b \\ b & c \end{pmatrix} .$$

Puis nous introduisons les notions suivantes (voir [Ga], art. 154, 226, 157):

Définition 2.1: Soit $f = ax^2 + 2bxy + cy^2$ une forme quadratique.

1) $d = d(f) = -\det M_f = b^2-ac$ est dit le déterminant de f .

2) f est dite primitive, si $(a,b,c) = 1$ et

3) f est dite proprement primitive si $(a, 2b, c) = 1$ où (a,b,c) désigne le plus grand commun diviseur de a,b et c .

4) f est dite improprement primitive si f est primitive mais non proprement primitive, i.e. si $(a,b,c) = 1$ mais $(a, 2b, c) = 2$.

5) $f(\mathbb{Z}^2) = \{ax^2 + 2bx + cy^2 \mid x,y \in \mathbb{Z}\}$ désigne l'ensemble des nombres entiers représentés par f .

Soient f et f' deux formes avec matrices associées M_f et $M_{f'}$.

6) f est équivalente à f', notation: $f \sim f'$, s'il existe une matrice $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$ et avec
$\det T = \alpha\delta - \beta\gamma = \pm 1$, telle que

$$M_{f'} = T^t M_f T \text{ , où } T^t \text{ dénote la transposée de } T .$$

7) f est proprement équivalente à f', notation: $f \equiv f'$, s'il existe une matrice $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$ et avec $\det T = \alpha\delta - \beta\gamma = +1$, telle que

$$M_{f'} = T\,{}^{t}M_{f}T .$$

Comme $ax^2 + 2bxy + cy^2 = X\,{}^{t}M_{f}X$, où $X = \begin{pmatrix} x \\ y \end{pmatrix}$, on déduit immédiatement (voir [Ga], Art. 157, 166, 226, 161) la

Proposition 2.2: Soient f et f' deux formes telles que $f \simeq f'$. Alors

1) $d(f) = d(f')$

2) $f(\mathbb{Z}^2) = f'(\mathbb{Z}^2)$

3) Si f est primitive f' est aussi primitive.

4) Si f est proprement primitive f' est aussi proprement primitive.

5) Si f est improprement primitive f' est aussi improprement primitive.

Point de départ pour la notion des genres est le théorème suivant (voir [Ga], Art. 229):

Théorème 2.3: Soit $f = [a,b,c]$ une forme primitive, $d = d(f) = b^2 - ac$, p un premier $\neq 2$ divisant d, $p|d$, $p \neq 2$ et $f_p(\mathbb{Z}^2) = \{m \in f(\mathbb{Z}^2) \mid (m,p) = 1\}$ les entiers représentés par f et non divisibles par p.

Alors

ou bien $\left(\frac{m}{p}\right) = +1$ pour tous les $m \in f_p(\mathbb{Z}^2)$,

ou bien $\left(\frac{m}{p}\right) = -1$ pour tous les $m \in f_p(\mathbb{Z}^2)$,

où $\left(\frac{-}{p}\right)$ dénote le symbole de Legendre.

Démonstration: Soient $m,m' \in f_p(\mathbb{Z}^2)$, i.e.

$$m = ax^2 + 2bxy + cy^2 \quad \text{et} \quad m' = ax'^2 + 2bx'y' + cy'^2$$

pour certain $x,y,x',y' \in \mathbb{Z}$. Alors

$$mm' = (axx' + b(xy' + yx') + cyy')^2 - d(xy' - yx')^2 .$$

Si $p|d$ on a $\left(\frac{mm'}{p}\right) = +1$ et alors $\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right)$. q.e.d.

En ce qui concerne le premier $p = 2$ on a un théorème analogue (voir [Ga], Art. 229), à savoir le

Théorème 2.4: Soit $f = [a,b,c]$ une forme primitive et $d = b^2 - ac$.

1) Si $4|d$,
alors ou bien $m \equiv 1$ modulo 4 pour tous les $m \in f_2(\mathbb{Z}^2)$
ou bien $m \equiv 3$ modulo 4 pour tous les $m \in f_2(\mathbb{Z}^2)$

2) Si $8|d$,
alors ou bien $m \equiv 1$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$
ou bien $m \equiv 3$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$
ou bien $m \equiv 5$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$
ou bien $m \equiv 7$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$

La démonstration est parfaitement analogue à celle du théorème 2.3.

Les premiers impairs p qui ne divisent pas le déterminant $d(f)$ ne fournissent pas de caractérisation de $f_p(\mathbb{Z}^2)$, mais pour le premier $p = 2$ on a (voir [Ga], Art. 229):

Théorème 2.5: Soit $f = [a,b,c]$ une forme primitive de déterminant $d = b^2 - ac$.

1) Si $d \equiv 3$ modulo 4 ,
alors ou bien $m \equiv 1$ modulo 4 pour tous les $m \in f_2(\mathbb{Z}^2)$
ou bien $m \equiv 3$ modulo 4 pour tous les $m \in f_2(\mathbb{Z}^2)$

2) Si $d \equiv 2$ modulo 8,

alors ou bien $m \equiv 1,7$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$

ou bien $m \equiv 3,5$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$

3) Si $d \equiv 6$ modulo 8,

alors ou bien $m \equiv 1,3$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$

ou bien $m \equiv 5,7$ modulo 8 pour tous les $m \in f_2(\mathbb{Z}^2)$

L'idée de démonstration est toujours la même que celle du théorème 2.3, car si $d \equiv 3$ modulo 4, resp. $d \equiv 2$ modulo 8, resp. $d \equiv 6$ modulo 8, on a $mm' \equiv 1$ modulo 4, resp. $\equiv \pm 1$ modulo 8, resp. $\equiv 1,3$ modulo 8.

D'après le théorème 2.3 les classes ainsi que les classes propres d'équivalence des formes primitives ayant même déterminant d sont caractérisées par t caractères impairs (terminologie introduite par Gauss) $\varepsilon_{p_1}, \ldots, \varepsilon_{p_t}$ qui correspondent aux t diviseurs premiers impairs $p_1, \ldots, p_t$ de d. Avec Dirichlet (voir [Di], XXVII, §3) on peut poser pour une forme primitive f

$$\varepsilon_p(f) = \left(\frac{m}{p}\right) \qquad \text{où} \quad m \in f_p(\mathbb{Z}^2) \tag{2.6}$$

Pour le caractère pair ε_2 on a d'après les théorèmes 2.4 et 2.5

$$\varepsilon_2(f) = \begin{cases} (-1)^{\frac{m-1}{2}}, & \text{si } d \equiv 0,3,4,7 \text{ modulo } 8 \\ (-1)^{\frac{m^2-1}{8}}, & \text{si } d \equiv 0,2 \text{ modulo } 8 \\ (-1)^{\frac{m-1}{2}+\frac{m^2-1}{8}}, & \text{si } d \equiv 6 \text{ modulo } 8 \end{cases} \tag{2.7}$$

où $m \in f_2(\mathbb{Z}^2)$.

Notons que dans le cas où $d \equiv 0$ modulo 8 le caractère ε_2 se décompose en deux caractères indépendants, à savoir

$$\varepsilon_{2_1}(f) = (-1)^{\frac{m-1}{2}}, \qquad \varepsilon_{2_2}(f) = (-1)^{\frac{m^2-1}{8}}.$$

Pour un déterminant négatif on a par analogie avec le théorème 2.3 la

Proposition 2.8: Soit $f = [a,b,c]$ une forme de déterminant $d = b^2 - ac < 0$ et $f_\infty(\mathbb{Z}^2) = \{m \in f(\mathbb{Z}^2) \mid m \neq 0\}$.

Alors ou bien $m > 0$ pour tous les $m \in f_\infty(\mathbb{Z}^2)$

ou bien $m < 0$ pour tous les $m \in f_\infty(\mathbb{Z}^2)$

(voir [Ga], Art. 225).

Si l'on pose pour un entier $m \neq 0$

$$\left(\frac{m}{\infty}\right) = \begin{cases} +1 & \text{si } m > 0 \\ -1 & \text{si } m < 0 \end{cases}$$

on peut associer à une forme f de déterminant négatif $d < 0$ un caractère infini comme suit:

(2.9) $$\varepsilon_\infty(f) = \left(\frac{m}{\infty}\right) \quad \text{où} \quad m \in f_\infty(\mathbb{Z}^2) .$$

Toute forme primitive $f = [a,b,c]$ de déterminant $d = b^2 - ac$ est donc caractérisée par $r = t + s + u$ valeurs de caractères ± 1 où t désigne le nombre de premiers impairs divisant d, $s = 0,1,2$ selon que $d \equiv 1,5$ modulo 8 ou $d \equiv 2,3,4,6,7$ modulo 8 ou $d \equiv 0$ modulo 8 et $u = 0,1$ selon que $d > 0$ ou $d < 0$.

Nous dirons que $2 \mid d$ si $d \not\equiv 1,5$ modulo 8 et que $\infty \mid d$ si $d < 0$. Gauss appelle (voir [Ga], Art. 231)

$$\varepsilon(f) = \{\varepsilon_{p_1}(f), \ldots, \varepsilon_{p_t}(f), \varepsilon_2(f), \varepsilon_\infty(f)\} \subseteq \{\pm 1\}^r$$

le caractère complet de f et il dit que chaque caractère complet définit un genre, plus précisément (voir [Ga], Art. 231):

Définition 2.10: Deux formes proprement primitives f et g ayant le même déterminant d sont dans le même genre, notation: $f \sim g$, si

$$\varepsilon_p(f) = \varepsilon_p(g) \qquad \text{pour tous les } p|d \text{ , i.e.}$$

pour tous les premiers impairs p, tels que $p|d$, pour $p = 2$ si $d \not\equiv 1$ modulo 4 et pour $p = \infty$ si $d < 0$.

La même définition s'applique aux formes improprement primitives, et plus généralement aux formes appartenant au même ordre. Gauss dit que deux formes $f = [a,b,c]$ et $f' = [a',b',c']$ appartiennent au même ordre si $(a,b,c) = (a',b',c')$ et $(a, 2b, c) = (a', 2b', c')$ (voir [Ga] Art. 226). Donc les formes proprement primitives forment un ordre $O(p)$ et les formes improprement primitives forment un autre ordre $O(i)$. Tout ce que nous allons dire sur l'ordre $O(p)$ sera aussi vrai pour l'ordre $O(i)$. Cela s'applique en particulier aux théorèmes 2.11, 2.15, 2.17 et 2.18 (voir [Ga], Art. 252,264,287).

3. Si f est proprement primitive et $f \equiv g$ il s'en suit que $f \simeq g$, et d'après la proposition 2.2 que $f \sim g$. C'est-à-dire les classes propres des formes proprement primitives ayant même déterminant d sont distribuées en genres dont le nombre est tout au plus égal à 2^r.

La forme $f_0 = [1,0, -d]$ de déterminant d est dite forme principale, sa classe propre est dite classe propre principale et son genre est appelé genre principal. Le genre principal est caractérisé par le fait que ses r caractères prennent la valeur $+1$.

Le resultat principal de Gauss sur les genres est le suivant (voir [Ga], Art. 252, 261, 287):

Théorème 2.11: 1) Etant donné un déterminant d, tout genre de déterminant d contient le même nombre de classes propres de formes propre-

ment primitives de déterminant d.

2) Etant donné un déterminant d qui n'est pas un carré, exactement la moitié des 2^r caractères complets possibles correspond aux genres de classes propres de formes proprement primitives de déterminant d.

La deuxième partie du théorème fut démontrée par Gauss en deux étapes. Gauss montra d'abord qu'au plus la moitié des caractères complets peut correspondre à un genre (voir [Ga], Art. 261) et que ce fait équivaut à la loi de réciprocité quadratique (voir [Ga], Art. 262, 263 et voir théorème 3.15 plus bas). Qu'au moins la moitié des caractères complets corresponde à un genre est une proprieté très profonde que Gauss extrait de sa théorie de représentation d'une forme quadratique binaire par une forme quadratique ternaire (voir [Ga], Art. 266 ff et voir théorème 3.15 plus bas). En plus il se sert de sa théorie des classes ambigues (voir [Ga], Art. 163, 224):

Définition 2.12: 1) Une forme $f = [a,b,c]$ est dite ambiguë, si $a|2b$.
2) Une classe propre est dite ambiguë si elle contient une forme ambiguë.

Une forme ambiguë peut aussi être caractérisée ainsi (voir [Ga], Art. 163):

Proposition 2.13: Si f est une forme ambiguë il existe une matrice entière $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\det T = -1$, telle que

$$M_f = T^t M_f T .$$

Donc f est ambiguë si f est improprement équivalente à elle-même, et toutes les formes d'une classe (propre) ambiguë sont proprement et improprement équivalentes entre elles.

Gauss montra alors (voir [Ga], Art. 258):

Théorème 2.14: Le nombre de classes propres ambiguës de formes proprement primitives et de déterminant non-carré d est égal à la moitié du nombre de caractères complets ayant ce même déterminant.

En combinant ce résultat avec le théorème 2.11 on obtient (voir [Ga], Art. 258 I):

Théorème 2.15: Le nombre de genres de classes propres de formes proprement primitives de déterminant d est égal au nombre de classes propres ambiguës de formes proprement primitives de déterminant d.

En plus on a (voir [Ga], Art. 259):

Théorème 2.16: Le nombre de classes propres ambiguës de formes de l'ordre $O(p)$ et de déterminant d est égal au nombre de classes propres ambiguës de formes de l'ordre $O(i)$ et ayant même déterminant d.

Comme application de sa théorie des classes ambiguës Gauss détermina explicitement les solutions $x,y \in \mathbb{Z}$, $x,y > 0$, $(x,y) = 1$ de $p = x^2 + y^2$ pour un nombre premier $p \equiv 1$ modulo 4 (voir [Ga], Art. 265) en se servant du fait qu'il y a une seule classe propre ambiguë de formes proprement primitives de déterminant premier $p \equiv 1$ modulo 4. Car

un tel déterminant $d = p$ ne donne naissance qu'à un seul caractère (impair) ε_p.

Finalement Gauss obtint une caractérisation des nombres convenables de Euler (voir [Ga], Art. 303):

Théorème 2.17: Un nombre naturel $m \in \mathbb{N}$ est convenable si et seulement si tout genre de déterminant $d = -m$ contient précisément une classe propre de formes proprement primitives.

Gauss ne se donna pas la peine de publier une démonstration de ce théorème, un théorème qu'il dit facile à démontrer. Une démonstration complète fut publiée par Grube en 1874 (voir [Gr], §6, §8 et section 5).

En tenant compte du théorème 2.14 on a donc (voir [Ga], Art. 307):

Théorème 2.18: Un nombre $m \in \mathbb{N}$ est convenable si et seulement si toute classe propre de formes proprement primitives de déterminant $d = -m$ est une classe propre ambiguë de formes proprement primitives.

3. Théorie des corps quadratiques de Dedekind

1. Dans le supplément X de la 2-ème édition de "Vorlesungen über Zahlentheorie" de Dirichlet (voir [D-D], §165) Dedekind fait le lien, entre sa théorie sur les idéaux et la théorie de Kummer sur les nombres idéaux d'un côté, et la théorie des formes normiques de Gauss dans le cas des formes quadratiques et de Dirichlet dans le cas des formes de degré général d'un autre côté. C'est déjà Kummer qui fit allusion à cette

correspondance (voir [Ku], p. 208-9) sans donner de détails cependant (voir aussi [Di], Vol. II, V, 27-48).

2. Dans le cas quadratique le lien se fait comme suit. Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique de discriminant d, c'est-à-dire $d \equiv 1$ modulo 4 et sans carré, ou $d = 4d'$ avec $d' \equiv 2,3$ modulo 4 et d' sans carré.

L'ordre principal des entiers algébriques dans K (de discriminant d)

$$o = \{ a + b\,\frac{d+\sqrt{d}}{2} \mid a,b \in \mathbb{Z} \} = \{ u + v\theta \mid u,v \in \mathbb{Z} \} ,$$

$$\theta = \begin{cases} \frac{1+\sqrt{d}}{2} , & \text{si } d \equiv 1 \bmod 4 \\ \frac{\sqrt{d}}{2} , & \text{si } d \equiv 0 \bmod 4 \end{cases}$$

ainsi que tout ordre dans K de conducteur $f \in \mathbb{N}$ et donc de discriminant $D = f^2 d$

$$o_f = \{ a + bf\,\frac{d+\sqrt{d}}{2} \mid a,b \in \mathbb{Z} \} = \{ u + v\theta \mid u,v \in \mathbb{Z} \} ,$$

$$\theta = \begin{cases} \frac{1+\sqrt{D}}{2} , & \text{si } D \equiv 1 \bmod 4 \\ \frac{\sqrt{D}}{2} , & \text{si } D \equiv 0 \bmod 4 \end{cases}$$

est un $\mathbb{Z}$-module libre de rang 2.

Bien entendu, pour $f = 1$ on a $o_1 = o$. En général $f = [o : o_f]$.

Nous appelons tout $\mathbb{Z}$-module libre de rang 2 dans K

$$A = \{\alpha_1 x_1 + \alpha_2 x_2 \mid x_1 , x_2 \in \mathbb{Z}\} = \langle \alpha_1 , \alpha_2 \rangle \quad \text{avec} \quad \alpha_1 , \alpha_2 \in K ,$$

où $\{\alpha_1 , \alpha_2\}$ est une base de K sur $\mathbb{Q}$,

un module complet de K et nous désignons par M l'ensemble des modules complets de K.

Si $A = \langle \alpha_1 , \alpha_2 \rangle \in M$ et $\gamma \in K^x = K - \{0\}$, nous définissons

$$\gamma A = \{\gamma\alpha \mid \alpha \in A\} = \{\gamma\alpha_1 x_1 + \gamma\alpha_2 x_2 \mid x_1 , x_2 \in \mathbb{Z}\} =$$

$$= \langle \gamma\alpha_1 , \gamma\alpha_2 \rangle ,$$

qui est encore un module complet de K.

Etant donné $A \in M$, l'ensemble

$$R = R_A = \{\gamma \in K \mid \alpha \in A \Rightarrow \gamma\alpha \in A\} = \{\gamma \in K \mid \gamma A \subseteq A\}$$

est un sous-anneau de K, dit l'anneau des multiplicateurs de A.

On peut montrer que l'anneau des multiplicateurs R_A d'un module complet A de K est un ordre o_f dans K et que tout ordre o_f de K est l'anneau des multiplicatuers pour un module complet A de K (voir [B-S], chapitre II, §2.2, théorème 3).

Si $\gamma = r+s\sqrt{d}$, avec $r , s \in \mathbb{Q}$, est un nombre algébrique de K, nous désignons par $\bar{\gamma} = r-s\sqrt{d}$ son conjugué et par $N(\gamma) = \gamma\bar{\gamma} = r^2 - s^2 d$ sa norme.

Définition 3.1: Deux modules complets A et B de K sont dits équivalents, notation: $A \simeq B$, s'il existe un $\gamma \in K^x$ tel que $B = \gamma A$. Deux modules complets A et B de K sont dits proprement équivalents, notation: $A \equiv B$, s'il existe un $\gamma \in K^x$ avec $N(\gamma) > 0$ tel que $B = \gamma A$.

Nous avons les propriétés suivantes:

Théorème 3.2:

(1) Si $A,B \in M$ et $A \sim B$, alors $R_A = R_B$.

(2) Pour tout $A \in M$ il existe un $B \in M$ tel que $A \sim B$ et $B \subseteq R_B$.

(3) L'ensemble des modules complets dans K ayant le même ordre o_f comme anneau des multiplicateurs est un groupe commutatif (par rapport à la multiplication de modules). Il sera désigné par M_{o_f}.

(4) Le nombre de classes d'équivalence propre de modules complets ayant le même ordre o_f comme anneau des multiplicateurs est fini. Son nombre sera désigné par h_f.

Pour une démonstration voir [B-S], Chapitre II, §2.2, lemme 1, §7.4, théorème 2 et §6.2, théorème 3.

En vertu de la propriété (3) le nombre de classes d'équivalence de modules complets ayant le même ordre o_f comme anneau des multiplicateurs est également fini. Si h_f^0 désigne ce nombre, alors

$$h_f = h_f^0 \quad \text{ou} \quad h_f = 2\, h_f^0$$

(voir [B-S], Chapitre II, §7.5).

On sait que tout idéal $a \neq (0)$ dans K, entier ou fractionnaire, est un module complet dans K et que son anneau des multiplicateurs R_a est l'ordre principal o dans K, qui est l'ordre maximal dans K. D'autre part tout module complet dans K dont l'anneau des multiplicateurs est o doit être un idéal dans K et M_o devient alors le groupe multiplicatif d'idéaux dans K. Donc les classes ordinaires d'idéaux dans K coïncident avec les classes de modules complets ayant o comme anneau de multiplicateurs et les classes restreintes d'idéaux dans K coïncident avec les classes propres de modules complets ayant o comme anneau de multiplicateurs. Le théorème 3.2 (2) affirme alors qu'il existe pour tout

idéal a un idéal entier b équivalent à a, i.e.

$$b = \gamma a \subseteq o \quad \text{avec un} \quad \gamma \in o \ .$$

On peut maintenant associer à chaque module $A \in M_{o_f}$ une forme quadratique F de déterminant $\frac{df^2}{4}$ de sorte que les classes propres de modules complets dans M_{o_f} correspondent d'une façon biunivoque aux classes propres de formes quadratiques proprement primitives ayant déterminant $\frac{df^2}{4}$.

3. Pour rendre cette correspondance plus souple encore, nous abandonnons la notation de Gauss $ax^2 + 2b'xy + cy^2$, avec $a,b',c \in \mathbb{Z}$ pour la remplacer par la notation $ax^2 + bxy + cy^2$, avec $a,b = 2b'$, $c \in \mathbb{Z}$. Nous appelons la forme $F = [a,b,c]_0 = ax^2 + bxy + cy^2$ <u>primitive</u> si

$$(a,b,c) = 1$$

et nous appelons

$$D = D(F) = b^2 - 4ac = (2b')^2 - 4ac = 4(b'-ac) = 4d(F)$$

le <u>discriminant</u> de F .

Donc une forme de Gauss

$$f = [a,b',c] = ax^2 + 2b'xy + cy^2$$

est proprement primitive si et seulement si la forme correspondante

$$F = [a,b,c]_0 = ax^2 + bxy + cy^2 \ , \quad b = 2b'$$

est primitive.

Par ce changement de notation nous augmenterons l'ensemble des formes

$$\bar{F}_G = \{ax^2 + 2b'xy + cy^2 \mid a,b',c \in \mathbb{Z}\}$$

considéré par Gauss de l'ensemble

$$\bar{F}_N = \{ax^2 + bxy + cy^2 \mid a,b,c \in \mathbb{Z} \text{ et } b \text{ impair}\}$$

pour obtenir l'ensemble des formes

$$\bar{F} = \{ax^2 + bxy + cy^2 \mid a,b,c \in \mathbb{Z}\} .$$

Notons que

$$D(F) \equiv 0 \mod 4 , \text{ si } F \in \bar{F}_G$$

et que

$$D(F) \equiv 1 \mod 4 , \text{ si } F \in \bar{F}_N .$$

La correspondance

$$\varphi : \bar{F}_N \to \bar{F}_G$$

définie par

$$\varphi : F = [a,b,c]_0 \mapsto 2 \cdot F = [2a , 2b , 2c]_0$$

fournit une correspondance biunivoque entre les formes primitives dans $\bar{F}_N$ et les formes improprement primitives dans $\bar{F}_G$.

Les théorèmes 2.11, 2.15, 2.17 et 2.18 de Gauss resteront vrais pour l'ensemble des formes dans $\bar{F}$, étant donné que ces théorèmes restent en-

core vrais pour l'ordre $O(i)$ des formes improprement primitives (voir [Ga] Art. 352, 264 et 287 pour le théorème 2.11 et voir les théorèmes 2.14 et 2.16 pour les théorèmes 2.15, 2.17 et 2.18).

4. Considérons un module complet $A = \langle \alpha_1 , \alpha_2 \rangle$ tel que $A \subseteq R_A = o_f$. D'après le théorème 3.2 un tel module A existe dans chaque classe et aussi dans chaque classe propre.

$$N(A) := [R_A : A] = \text{indice de } A \text{ dans } R_A$$

est dite la norme de A.

Plus généralement, si $\{\alpha_1 , \alpha_2\}$ est une $\mathbb{Z}$-base de A et $\{\beta_1 , \beta_2\}$ est une $\mathbb{Z}$-base de R_A (en général A n'est pas contenu dans R_A), et si T est la transformation linéaire qui applique $\{\beta_1 , \beta_2\}$ sur $\{\alpha_1 , \alpha_2\}$, i.e.

$$T = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \begin{aligned} \alpha_1 &= a_{11}\beta_1 + a_{12}\beta_2 \\ \alpha_2 &= a_{21}\beta_1 + a_{22}\beta_2 \end{aligned}$$

la norme $N(A)$ de A est définie par

$$N(A) := \det T = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

Nous allons utiliser le fait que

$$N(A)^2 = \left| \frac{\Delta A}{\Delta o_f} \right| = \frac{(\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1)^2}{D}$$

où ΔB désigne le discriminant d'un module $B = \langle \beta_1 , \beta_2 \rangle$, i.e.

$$\Delta B = \begin{vmatrix} Tr(\beta_1^2) & Tr(\beta_1\beta_2) \\ Tr(\beta_2\beta_1) & Tr(\beta_2^2) \end{vmatrix} = \begin{vmatrix} \beta_1^2+\bar{\beta}_1^2 & \beta_1\beta_2+\bar{\beta}_1\bar{\beta}_2 \\ \beta_1\beta_2+\bar{\beta}_1\bar{\beta}_2 & \beta_2+\bar{\beta}_2^2 \end{vmatrix} = \begin{vmatrix} \beta_1\beta_2 \\ \bar{\beta}_1\bar{\beta}_2 \end{vmatrix}^2$$

voir [Ri], p. 17 et p. 121.

Nous ordonnons la base $\{\alpha_1 , \alpha_2\}$ de A de sorte que

$$\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1 = N(A)\sqrt{D}$$

soit positif, i.e. dans $\mathbb{N}$, ou positif imaginaire, i.e. dans $i\mathbb{N}$, et nous disons que le module $A = <\alpha_1 , \alpha_2>$ est orienté.

Nous associons alors au module complet orienté $A \subseteq R_A = o_f$ la forme quadratique suivante

$$F_A = F_A(x,y) = \frac{N(\alpha_1 x+\alpha_2 y)}{N(A)} = \frac{\alpha_1\bar{\alpha}_1}{N(A)} x^2 + \frac{\alpha_1\bar{\alpha}_2+\alpha_2\bar{\alpha}_1}{N(A)} xy +$$

$$+ \frac{\alpha_2\bar{\alpha}_2}{N(A)} y^2 = ax^2 + bxy + cy^2 .$$

Si $\alpha \in A$ on a $\alpha o_f \subseteq A \subseteq o_f$ et $N(\alpha o_f) = |N(\alpha)|\, N(o_f) = |N(\alpha)|$ (voir [B-S], Chap. II, §6.1, théorème 2) et donc $N(A)$ divise $N(\alpha)$. En effet $|N(\alpha)| = [o : \alpha o_f]$ et $\frac{|N(\alpha)|}{N(A)} = [A : \alpha o_f]$.

Comme $\alpha = \alpha_1 x + \alpha_2 y$ est dans A pour tout $x,y \in \mathbb{Z}$, alors $F_A(x,y) = ax^2 + bxy + cy^2$ est un entier pour tout $x,y \in \mathbb{Z}$. D'où $a = \frac{N(\alpha_1)}{N(A)} = F_A(1,0)$, $c = \frac{N(\alpha_2)}{N(A)} = F_A(0,1)$ et donc $b = F_A(1,1) - a - c$ sont des entiers.

Le discriminant de F_A est égal au discriminant de l'ordre o_f :

$$D(F_A) = b^2 - 4ac = \frac{(\alpha_1\bar{\alpha}_2+\alpha_2\bar{\alpha}_1)^2 - 4\alpha_1\bar{\alpha}_1\alpha_2\bar{\alpha}_2}{N(A)^2} =$$

$$= \frac{(\alpha_1\bar{\alpha}_2-\alpha_2\bar{\alpha}_1)^2}{N(A)^2} = D = df^2 .$$

F_A est une forme primitive (voir [B-S], Chap. II, §5).

Si $D < 0$, F_A est une forme positive, i.e. $F_A(\mathbb{Z}^2) \geq 0$, car $N(\alpha) = r^2 - s^2 d \geq 0$, pour tout $\alpha = r + s\sqrt{d}$ et donc $a = \frac{N(\alpha_1)}{N(A)} \geq 0$.

Si $D > 0$, F_A est une forme indéfinie, i.e. F_A prend des valeurs positives et négatives.

Etant donné une forme $F = [a,b,c]_0$ de discriminant $D = df^2 = b^2-4ac$, positive si $D < 0$, il existe un module complet orienté A avec une base ordonnée telle que $F_A = F$. En effet, si $D < 0$ ou si $D > 0$ et $a > 0$ nous posons $A = \langle a , \frac{b-\sqrt{D}}{2} \rangle$; si $D > 0$ et $a < 0$ prenons $A = \sqrt{D} < a , \frac{b-\sqrt{D}}{2} >$, où $\sqrt{D}$ est positif ou positif imaginaire (voir [He], p. 214). A est alors un module complet avec $R_A = o_f$ et $F_A = F$.

F_A dépend de la base $\{\alpha_1 , \alpha_2\}$ choisie pour A, mais la classe propre de F_A est indépendante de ce choix.

Plus généralement: Si A et B sont deux modules proprement équivalents, alors aussi les formes correspondantes F_A et F_B, et vice versa (voir [He], Satz 154).

Résumons ces résultats.

Théorème 3.3:

(1) A chaque module complet orienté A avec anneau de multiplicateurs $R_A = o_f$ dans un corps $K = \mathbb{Q}(\sqrt{d})$ de discriminant d correspond une forme quadratique binaire F_A qui est entière et primitive et dont le discriminant $D = f^2d$ égale le discriminant de l'ordre o_f. La forme F_A est positive si $d < 0$ et indéfinie si $d > 0$.

(2) Inversement, à chaque forme $F = [a,b,c]_0$ de discriminant $D = f^2d$, positive si $d < 0$ et indéfinie si $d > 0$, correspond un module complet orienté $A = \langle \alpha_1 , \alpha_2 \rangle$, avec une certaine base ordonnée $\{\alpha_1 , \alpha_2\}$ et d'anneau $R_A = o_f$ dans le corps $K = \mathbb{Q}(\sqrt{d})$, tel que $F = F_A$.

(3) Soit A et B deux modules complets orientés avec même anneau de multiplicateurs o_f. Alors

$$A \equiv B \quad \text{si et seulement si} \quad F_A \equiv F_B .$$

Il y a donc une correspondance bi-univoque β entre le groupe multiplicatif $C_f(d)$ des classes propres de modules complets orientés dans M_{o_f} et les classes propres $D_f(d)$ des formes quadratiques primitives de discriminant $D = df^2$, positives si $d < 0$ et indéfinies si $d > 0$. Donc $C_f(d)$ est fini $|C_f(d)| = |D_f(d)| = h_f$, et $D_f(d)$ peut être muni d'une structure de groupe commutatif, l'opération de groupe dans $D_f(d)$ étant la composition des classes de formes quadratiques introduite par Gauss en 1801 (voir [Ga], Art. 234).

La correspondance β permet de définir la notion de genre pour des modules complets.

Définition 3.4: Soit $A,B \in M_{o_f}$.
A et B sont dans le même genre, en symbole $A \sim B$, si et seulement si $F_A \sim F_B$.

Cette définition est independante des bases choisies pour A et B, car $F_A \equiv F_B$ entraîne $F_A \sim F_B$.

En plus, on peut supposer que $A,B \subseteq o_f$ (à cause du théorème 3.3 (3) et du théorème 3.2.(2)).

5. Les genres dans M_{o_f} peuvent être caractérisés de plusieurs façons. Commençons avec la découverte par Gauss que le genre regroupe les formes représentant les mêmes nombres.

Par la définition de F_A, l'ensemble $F_A(\mathbb{Z}^2)$ des entiers représentés par la forme F_A est donné par

$$F_A(\mathbb{Z}^2) = \left\{ \frac{N(\alpha)}{N(A)} \;\middle|\; \alpha \in A \right\}$$

car $\alpha = \alpha_1 x + \alpha_2 y$ parcourt tout A si x et y parcourent tout $\mathbb{Z}$.

Rappelons que

$$F_A(\mathbb{Z}^2) = F_B(\mathbb{Z}^2) \quad \text{si} \quad A \equiv B$$

(voir la proposition 2.2.(2) et le théorème 3.3.(3)).

D'après la définition 3.4 et la définition 2.10 nous avons

$$(3.5) \qquad A \sim B \iff \varepsilon_p(F_A) = \varepsilon_p(F_B) \quad \text{pour tous les } p|D ,$$

c'est-à-dire

$$(3.6) \qquad A \sim B \iff \left(\frac{N(\alpha)}{N(A)}\right)_p = \left(\frac{N(\beta)}{N(B)}\right)_p \quad \text{pour tous les } p|D$$

où $\alpha \in A$, $\beta \in B$ et $\frac{N(\alpha)}{N(A)} \in (F_A)_p$, $\frac{N(\beta)}{N(B)} \in (F_B)_p$.

Rappelons que D = discriminant de $o_f = D(F_A) = 4d(F_A)$ où $A \in M_{o_f}$ et que

$$D(F_A) \equiv 0 \mod 4 \quad \text{si} \quad F_A \in \bar{F}_G$$

et

$$D(F_A) \equiv 1 \mod 4 \quad \text{si} \quad F_A \in \bar{F}_N .$$

La caractérisation du genre d'un module $A \in M_{o_f}$, moyennant le symbole de Legendre, se limite aux nombres $n = \frac{N(\alpha)}{N(A)}$ représentés par F_A avec $(n,p) = 1$. Pour enlever cette restriction et pour rendre la caractérisation plus générale nous remplaçons le symbole de Legendre $(\frac{n}{p})$ par le <u>symbole de reste normique</u> $(\frac{n,d}{p})$ introduit par Hilbert en 1894 pour un premier p (voir [Hi], Nr. 7, §64, (1897) ou [Hi], Nr. 5, §3, (1894)).

<u>Définition 3.7:</u> Soit $n,d \in \mathbb{Z}$, $n \neq 0$, $d \neq$ carré et p un nombre premier. Alors

$$(\frac{n,d}{p}) = +1 \quad , \quad \text{si} \quad n \equiv N(\gamma_e) \quad \text{modulo} \quad p^e$$

pour un entier algébrique $\gamma_e \in o$ dans le cors $\mathbb{Q}(\sqrt{d})$ et pour toute puissance p^e , $e \in N$,

$$(\frac{n,d}{p}) = -1 \quad \text{autrement.}$$

Si d est un carré on pose

$$(\frac{n,d}{p}) = 1 \ .$$

Le symbole a, entre autres, les propriétés suivantes (voir [Hi], Nr. 7, §64 (1897)):

Proposition 3.8:

(1) $(\frac{n,d}{p}) = 1$, si $p \nmid nd$, $p \neq 2$

(2) $(\frac{n,d}{p}) = (\frac{n}{p})$, si $p \mid d$, $p \nmid n$, $p \neq 2$

(3) $(\frac{n,d}{2}) = (-1)^{\frac{n-1}{2}}$, si $d \equiv 3,7$ modulo 8

$(\frac{n,d}{2}) = (-1)^{\frac{n^2-1}{8}}$, si $d \equiv 2$ modulo 8

$(\frac{n,d}{2}) = (-1)^{\frac{n-1}{2} + \frac{n^2-1}{8}}$, si $d \equiv 6$ modulo 8

(4) $(\frac{nm,d}{p}) = (\frac{n,d}{p})\,(\frac{m,d}{p})$.

Grâce à (4) on peut étendre le symbole aux nombres rationnels $n \in \mathbb{Q}$, $n \neq 0$, et encore aux rationnels $d \in \mathbb{Q}$, $d \neq 0$ à cause de

(5) $(\frac{n,d}{p}) = (\frac{d,n}{p})$.

En plus, on a pour $n,d \in \mathbb{Q}$, $nd \neq 0$

(6) $(\frac{n,d}{p}) = 1 \iff n \equiv N(\gamma_e)$ modulo p^e pour un $\gamma_e \in \mathbb{Q}(\sqrt{d})$

$\gamma_e \neq 0$ et pour toute puissance p^e, $e \in \mathbb{N}$.

En comparant les propriétés (2) et (3) de la proposition 3.8 avec (2.6) et (2.7) nous remarquons que le symbole de Hilbert $(\frac{n,d}{p})$ coïncide avec le caractère de Gauss $\varepsilon_p(f)$ pour une forme de discriminant d qui représente n avec $n \in f_p(\mathbb{Z}^2)$. Rappelons que $d = 4d_0$ où d_0 désigne le déterminant de Gauss de f et que d désigne aussi le discriminant de $\mathbb{Q}(\sqrt{d})$. Notons aussi qu'il y a un seul caractère $(\frac{,d}{2})$ pour le premier $p = 2$ si $4|d$. Nous avons ainsi t caractères non-triviaux $(\frac{,d}{p})$ pour le corps $K = \mathbb{Q}(\sqrt{d})$ de discriminant d si t désigne le nombre des premiers distincts p qui divisent d.

Nous pouvons alors poser pour un module complet $A \subset R_A = o_f$ de discriminant $D = df^2$ dans le corps $\mathbb{Q}(\sqrt{d})$ de discriminant d

$$(3.9) \qquad \varepsilon_p(F_A) = \left(\frac{\frac{N(\alpha)}{N(A)}, D}{p}\right) \text{ pour tout } \alpha \in A \text{ avec } \left(\frac{N(\alpha)}{N(A)}, p\right) = 1 .$$

Un tel $\alpha \in A$ existe, car F_A est une forme primitive. $\varepsilon_p(F_A)$ est ainsi défini pour tous les nombres premiers p, car d'après la propriété (1) de la proposition 3.8 $\varepsilon_p(F_A) = 1$ si p ne divise pas le discriminant D.

Si nous définissons pour $n,d \in \mathbb{Z}$, $n \neq 0$, $d \neq 0$

$$(3.10) \qquad (\frac{n,d}{\infty}) = \begin{cases} +1 & \text{si } n > 0 \text{ ou } d > 0 \\ -1 & \text{si } n < 0 \text{ et } d < 0 \end{cases}$$

la relation (3.9) reste aussi vraie pour $p = \infty$, mais comme nous ne considérons que des formes positives si $d < 0$, le caractère pour $p = \infty$ est trivial, i.e. $\varepsilon_\infty(F_A) = 1$ pour tout module complet A.

Nous avons ainsi obtenu le résultat suivant:

Proposition 3.11: Soit A,B deux modules complets d'anneau de multiplicateurs $R_A = R_B = \mathcal{O}_f$ de discriminant $D = df^2$ et de conducteur f dans le corps quadratique $K = \mathbb{Q}(\sqrt{d})$ de discriminant d. Alors

$$A \sim B \iff \varepsilon_p(F_A) = \varepsilon_p(F_B)$$

pour tous les premiers p (y compris $p = \infty$), où

$$\varepsilon_p(F_A) = \left(\frac{\frac{N(\alpha)}{N(A)}, D}{p}\right) \quad \text{pour tout } \alpha \in A \quad \text{avec} \quad \left(\frac{N(\alpha)}{N(A)}, p\right) = 1 .$$

Remarquons que $(\frac{n,D}{p}) = (\frac{n,d}{p})$, à cause de la propriété (4) de la proposition 3.8, et que $n = \frac{N(\alpha)}{N(A)}$ est un entier représenté par la forme primitive entière F_A. La condition $(n,p) = 1$ pourrait être enlevée. D'après la proposition 3.11 il y a au plus 2^t genres distincts où t désigne le nombre des premiers distincts qui divisent d (2 inclus si $4|d$).

Notons aussi que l'ordre $\mathcal{O}_f$ appartient à la classe propre principale dans $M_{\mathcal{O}_f}$ et donc (selon 2.3, théorème 3.3.(3) et définition 3.4) au genre principal qui est caractérisé par $\varepsilon_p(\ ) = +1$ pour tous les premiers p qui divisent D et donc pour tous les premiers.

Pour en déduire des caractérisations des genres nous allons nous servir du théorème normique de Hilbert (voir [Hi], Nr. 7, Satz 102 (1897) ou [Ha] - 1949, §26.7):

Théorème 3.12: Soit $n,d \in \mathbb{Z}$, $n \neq 0$, $d \neq$ carré. Si

$$(\frac{n,d}{p}) = 1 \quad \text{pour tous les premiers } p$$

alors n est la norme $n = N(\gamma)$ d'un $\gamma \in \mathbb{Q}(\sqrt{d})$

et du théorème sur la réciprocité quadratique auquel Hilbert a donné la forme suivante (voir [Hi], Nr. 7, Hilfssatz 14 ou [Ha] - 1949, §5.6):

Théorème 3.13: Quel que soit $n,d \in \mathbb{Z}$, $n \neq 0$, $d \neq 0$ avec $n > 0$ ou $d > 0$, le produit sur tous les premiers p

$$\prod_p \left(\frac{n,d}{p}\right) \text{ est égal à } 1 .$$

Le lien entre les genres et le symbole de reste normique de Hilbert est alors le suivant:

Théorème 3.14: Soit A et B deux modules complets avec $R_A = R_B = o_f$ dans le corps quadratique $K = \mathbb{Q}(\sqrt{d})$ de discriminant d et $D = df^2$ le discriminant de o_f. Alors:

(1) $\left(\frac{N(\gamma),d}{p}\right) = 1$ pour tout $\gamma \in \mathbb{Q}(\sqrt{d})$, $\gamma \neq 0$.

(2) A est dans le genre principal de M_{o_f} si et seulement si $\left(\frac{N(A),D}{p}\right) = 1$ pour tous les premiers p.

(3) $A \sim B \iff \left(\frac{N(A),D}{p}\right) = \left(\frac{N(B),D}{p}\right)$ pour tous les premiers p.

(4) A est dans le genre principal de M_{o_f} si et seulement s'il existe $\gamma \in \mathbb{Q}(\sqrt{d})$, $\gamma \neq 0$ tel que $N(A) = N(\gamma)$.

(5) Un module $A \in M_{o_f}$ avec $(N(A),D) = 1$ est dans le genre principal si et seulement s'il existe un entier $\gamma \in \mathbb{Q}(\sqrt{d})$ avec $(\gamma,D) = 1$, $N(\gamma) > 0$, tel que $N(A) \equiv N(\gamma) \bmod D$.

(6) Soit $A,B \in M_{o_f}$ et $(N(A),D) = 1$ et $(N(B),D) = 1$. Alors $A \sim B$ si et seulement s'il existe un entier $\gamma \in \mathbb{Q}(\sqrt{d})$, $N(\gamma) > 0$, $(\gamma,D) = 1$, tel que $N(A) \equiv N(\gamma)N(B) \bmod D$.

Démonstration:

(1) est une conséquence immédiate de la proposition 3.8.(6).

(2) est une conséquence de (1) et de la proposition 3.11, car si $\alpha_p \in A$ tel que $\left(\frac{N(\alpha_p)}{p}, p\right) = 1$, alors

$$\left(\frac{N(A),d}{p}\right)\left(\frac{\frac{N(\alpha_p)}{N(A)}, d}{p}\right) = \left(\frac{N(\alpha_p),d}{p}\right) = 1 .$$

A est dans le genre principal si et seulement si

$$\epsilon_p(F_A) = \left(\frac{\frac{N(\alpha_p)}{N(A)}, d}{p}\right) = 1 \quad \text{pour tout premier } p \text{ avec } \alpha_p \in A$$

choisi comme plus-haut; d'où la propriété (2).

(3) est une conséquence immédiate de (2).

(4) Pour (4) nous nous servons du théorème 3.12 et de (1) et (2). Notons que $N(A) > 0$ et donc $N(\gamma) > 0$, et que $N(A) \in \mathbb{Z}$ et donc $\gamma \in o$.

(5) est une conséquence du théorème 3.13, car si $N(A) \equiv N(\gamma) \bmod D$, alors $N(A) \equiv N(\gamma) \bmod p$ pour tout premier p qui divise D. Si $\gamma = \frac{x + y\sqrt{d}}{2}$ avec $x, y \in \mathbb{Z}$ nous obtenons

$$4\,N(A) \equiv x^2 - dy^2 \equiv x^2 \bmod p \text{ , donc}$$

$N(A) \equiv x^2 \bmod p$ est résoluble pour un entier x si $p \neq 2$.
Il est bien connu qu'alors (voir [Se], II, §2, Corollaire 2, p. 29) $N(A) \equiv x^2 \bmod p^e$ est résoluble pour toute puissance p^e de p si $p \neq 2$. Donc

$$\left(\frac{N(A),D}{p}\right) = 1 \quad \text{pour tout premier } p \neq 2 .$$

D'après la loi de réciprocité (théorème 3.13) on a aussi

$$\left(\frac{N(A),D}{2}\right) = 1$$

et donc le critère (5).

(6) est une conséquence immédiate de (5). q.e.d.

La théorie des genres de modules complets dans $M_{\mathcal{O}_f}$ se laisse ramener en quelque sorte à la théorie des genres des modules complets dans $M_{\mathcal{O}}$, c'est-à-dire à la théorie des idéaux dans $\mathbb{Q}(\sqrt{d})$, grâce aux faits suivants:

(1) Tout idéal (ordonné) dans $\mathcal{O}$ est (proprement) équivalent à au moins un module complet dans $M_{\mathcal{O}_f}$ pour un certain ordre $\mathcal{O}_f$ (voir [Co], p. 220).

(2) Les classes dans $M_{\mathcal{O}_f}$ peuvent être obtenues d'après Weber (1897) et Fueter (1903) moyennant une équivalence définie modulo f à l'intérieur de l'ordre pricipal $\mathcal{O}$ (voir [Co], p. 220 et [We] - 1897, §4, §5 ou [We] - 1908, Band 3, Zweites Buch, §96-100).

6. Avant de donner des caractérisations algébriques des genres, déduisons du théorème 3.14 le théorème fondamental de Gauss (1801) sur les genres (voir [Ga], Art. 247, 261/2, 286/7 et comparer avec les théorèmes 2.11, 2.14, 2.15) :

Théorème 3.15: Soit $D = df^2$ le discriminant de l'ordre $\mathcal{O}_f$ du corps quadratique $K = \mathbb{Q}(\sqrt{d})$.

(1) Il y a exactement 2^{t-1} genres distincts, où t désigne le nombre des diviseurs premiers distincts de d.

(2) Le carré d'une classe propre est dans le genre principal.

(3) Toute classe propre dans le genre principal est le carré d'une classe propre.

Démonstration:

(2) est une conséquence de la multiplicativité de la norme et du symbole normique, proposition 3.8.(4), car

$$\left(\frac{N(A^2),D}{p}\right) = \left(\frac{N(A),D}{p}\right)^2 = 1 \quad \text{pour tous les premiers } p.$$

(1) Qu'il y ait au plus 2^{t-1} genres distincts est une conséquence de la réciprocité quadratique qui donne une relation linéaire entre tous les caractères $(\frac{\ ,D}{p})$ (théorème 3.13).

Qu'il y ait au moins 2^{t-1} genres distincts est une propriété très profonde que Gauss obtint via (3) à l'aide de la théorie de représentation d'une forme binaire par une forme ternaire. Elle se laisse essentiellement déduire du théorème (analytique) de Dirichlet qu'une progression arithmétique contient un nombre infini de premiers (voir [B-S], III, §8.3, en particulier théorème 5 et aussi §8.4 théorème 8).

(3) Pour une démonstration complète de (3) voir par exemple [B-S], III, §8.4, théorème 7.

Le théorème fondamental des genres 3.15, démontré par Gauss pour des formes quadratiques de déterminant d_0 peut être interprété comme étant le théorème principal de la théorie du corps de classes pour le corps quadratique $K = \mathbb{Q}(\sqrt{d})$ de discriminant $d = 4d_0$ (voir [B-S], III, §8.2).

4. Théorie des formes quadratiques (suite)

1. Revenons à la théorie des formes quadratiques. En se basant sur des travaux d' Eisenstein , Smith et Minkowski sur les formes quadratiques entières à plusieurs variables, Speiser donna en 1912 une caractérisation algébrique du genre (voir [Sp]):

Théorème 4.1: Deux formes quadratiques primitives (binaires) F et G de discriminant D appartiennent au même genre si et seulement s'il existe une transformation linéaire rationnelle $T = (t_{ij})$, de déterminant $\det T = 1$ et dont les coefficients $t_{ij} \in \mathbb{Q}$ ont des dénominateurs qui sont premiers à D, telle que

$$M_G = T^t M_F T .$$

Ce théorème peut encore se formuler ainsi (voir [Wa], Chapter 5.5 ou [B-S], III, § 8.3 ou [Jo], Chapter V):

Théorème 4.2: Deux formes quadratiques primitives (binaires) F et G de discriminant D appartiennent au même genre si et seulement s'il existe une transformation rationnelle $T = (t_{ij})$, $t_{ij} \in \mathbb{Q}$, telle que

$$M_G = T^t M_F T .$$

En appliquant les nombres p-adiques introduits par K. Hensel en 1897 aux critères de Minkowski (voir [Fr], 1.5) Hasse put donner le critère suivant (voir [Ha] - 1923, Einleitung et [Fr], 1.6 ou [Wa], Chapter 3.7, voir aussi [Hn], Kap. XII, § 8) :

Théorème 4.3: Deux formes quadratiques primitives (binaires) F et G de discriminant D appartiennent au même genre si et seulement si

(1) $M_G = T^t M_F T$ pour une matrice réelle inversible T

(2) $M_G = T_p^t M_F T_p$ pour une matrice p-adique inversible et entière T_p pour chaque premier p .

2. L'importance de la théorie des genres pour la représentation d'un nombre par une forme quadratique (primitive binaire) repose sur le critère 4.4 qui suivra. Si F est une forme quadratique appartenant au genre $\mathcal{G}$ nous désignons les caractères de $\mathcal{G}$ par

$$\varepsilon_p(\mathcal{G}) := \varepsilon_p(F)$$

Cette définition est, bien entendu, indépendente de la forme F choisie dans $\mathcal{G}$. Rappelons que

$$\varepsilon_p(F) = \left(\frac{m,D}{p}\right)$$

où D est le discriminant de F et $m \neq 0$ est un entier représenté par F. Le critère s'énonce alors comme suit:

Théorème 4.4: Un nombre naturel n se laisse représenter par une forme F de genre $\mathcal{G}$ et de discriminant D si et seulement si

$$\left(\frac{n,D}{p}\right) = \varepsilon_p(\mathcal{G}) \quad \text{pour tous les premiers } p.$$

Démonstration: Il est clair que le critère est nécessaire. Pour la suffisance voir [B-S], III, § 8.3, théorème 4.

Le théorème 4.4 se laisse étendre aux entiers $m \in \mathbb{Z}$, $m \neq 0$, si l'on ajoute la condition pour $p = \infty$.

Le théorème 4.4 exprime le fait important que la représentabilité d'un nombre n par une forme F de genre $\mathcal{G}$ et de discriminant D, $(n,D) = 1$, ne dépend que de la classe de congruence de n modulo $|D|$, car $\left(\frac{n,D}{p}\right)$ ne dépend que de n modulo $|D|$, si $p|D$; rappelons que $\left(\frac{n,D}{p}\right) = 1$ si $p \nmid D$.