§4. CLASSES AMBIGES

Définition 5. Une classe C d'idéaux de O_D est *ambige* si elle est égale à sa conjuguée $\bar{C}$, c'est-à-dire si tout idéal I de C est équivalent à son conjugué $\bar{I}$.

PROPOSITION 5. *Les classes ambiges primitives sont les éléments d'ordre 2 du groupe* C_D *des classes primitives d'idéaux de* O_D.

Démonstration. D'après [7] (Proposition 2, Définitions 3 et 4) toute classe C du groupe C_D des classes primitives vérifie $C\bar{C} = 1$, donc $C^2 = 1$ si, et seulement si, $C = \bar{C}$, ce qu'il fallait démontrer.

PROPOSITION 6. *Une classe d'idéaux* C *de* O_D *est ambige si, et seulement si, sa période est formée de couples d'idéaux* $I \equiv \{c, b, a\}$ *et* $\tilde{I} \equiv \{a, b, c\}$.

Démonstration. Soit $I = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ un idéal, $c = \dfrac{D - b^2}{4a}$. On sait ([7], Corollary 2) que $\left[a, \dfrac{b + \sqrt{D}}{2}\right] \sim \left[c, \dfrac{-b + \sqrt{D}}{2}\right]$. Donc la classe de I est ambige si, et seulement si, $\left[a, \dfrac{b + \sqrt{D}}{2}\right] \sim \left[c, \dfrac{b + \sqrt{D}}{2}\right]$. La Proposition 6 s'obtient en considérant les idéaux réduits de C.

PROPOSITION 7. *La classe d'un idéal symétrique est ambige.*

Démonstration. Soit $S = \left[a, \dfrac{b + \sqrt{D}}{2}\right]$ un idéal symétrique où b est choisi de façon que $a = c$. D'après [7], Corollaire 2, on voit que $S \sim \left[a, \dfrac{-b + \sqrt{D}}{2}\right]$, ce qui prouve la Proposition 7.

THÉORÈME 1. *Soit* C *une classe ambige primitive de* O_D *dont la période contient* l *idéaux réduits primitifs.*

Si $N(\varepsilon_D) = -1$ *le nombre* l *est impair et la période de* C *contient* un *idéal ambige et* un *idéal symétrique. La numérotation des idéaux de la période de* C *peut être choisie de façon que ces idéaux soient respectivement* I_0 *(ambige) et* $I_{\frac{l+1}{2}}$ *(symétrique).*

Si $N(\varepsilon_D) = 1$ *le nombre* l *est pair et la période de* C *contient soit* deux *idéaux ambiges, soit* deux *idéaux symétriques. La numérotation des idéaux de la période de* C *peut être choisie de façon que ces deux idéaux soient* I_0 *et* $I_{\frac{l}{2}}$.

Démonstration. Nous considérons une classe ambige dont la période a pour longueur l, contenant les idéaux $I_0 \equiv \{c, b, a\}$ et $I_n \equiv \{a, b, c\}$. Nous distinguons le cas α) où n est impair $(n = 2m + 1)$ et le cas β) où n est pair $(n = 2m)$.

α) On a $I_0 \equiv \{c, b, a\}, I_{2m+1} \equiv \{a, b, c\}$.

Tenant compte de (1.5) et (1.6) on trouve que

$$I_m \equiv \{C, B, A\}, \quad I_{m+1} \equiv \{A, B, C\}$$

ce qui prouve que $A \mid B$ et que $I_m = \left[A, \dfrac{B + \sqrt{D}}{2}\right]$ est un idéal ambige.

D'autre part

$$I_l = I_0 \equiv \{c, b, a\}, \quad I_{2m+1} \equiv \{a, b, c\}.$$

Donc, pour tout $k \geqslant 0$

$$I_{l-k} \equiv \{P, Q, R\}, \quad I_{2m+1+k} \equiv \{R, Q, P\}.$$

Si l *est impair,* l'équation $l - k = 2m + 1 + k$ admet pour solution $k = \dfrac{l-1}{2} - m$, et on voit que l'idéal $I_{l-k} = I_{m + \frac{l+1}{2}} \equiv \{P, Q, P\}$ est symétrique. Changeant la numérotation on voit que I_0 est ambige et $I_{\frac{l+1}{2}}$ symétrique.

Si l *est pair,* l'équation $l - k = 2m + 1 + k + 1$ admet pour solution $k = \dfrac{l}{2} - m - 1$, donc $I_{2m+k+1} = I_{m+\frac{l}{2}}$ est un idéal ambige. Donc, changeant la numérotation, I_0 et $I_{\frac{l}{2}}$ sont des idéaux ambiges.

β) On a

$$I_0 \equiv \{c, b, a\}, \quad I_{2m} \equiv \{a, b, c\}.$$

Tenant compte de (1.5) et (1.6) on voit que I_m est un idéal symétrique.

En outre

$$I_0 = I_l \equiv \{c, b, a\}\ , \qquad I_{2m} \equiv \{a, b, c\}$$

donc, pour tout $k \geqslant 0$,

$$I_{l-k} = \{P, Q, R\}\ , \qquad I_{2m+k} = \{R, Q, P\}\ .$$

Si l *est impair,* l'équation $l - k = 2m + k + 1$ admet pour solution $k = \dfrac{l-1}{2} - m$ ce qui montre que l'idéal $I_{m+\frac{l-1}{2}}$ est ambige.

Changeant la numérotation on voit que I_0 est ambige et $I_{\frac{l+1}{2}}$ symétrique.

Si l *est pair,* l'équation $l - k = 2m + k$ admet pour solution $k = \dfrac{l}{2} - m$, donc l'idéal $I_{m+\frac{l}{2}}$ est symétrique. Donc, changeant la numérotation, on voit que I_0 et $I_{\frac{l}{2}}$ sont symétriques.

En résumé nous voyons que l'on peut choisir la numérotation dans la période pour que:

Si l est impair, I_0 est ambige, $I_{\frac{l+1}{2}}$ symétrique,

Si l est pair, I_0 et $I_{\frac{l}{2}}$ sont ambiges, ou bien symétriques.

Il reste à montrer que la période de C ne contient pas d'autre idéal ambige ou symétrique que ceux que nous venons de trouver.

Si $I_0 \equiv \{c, ka, a\}$ et $I_x \equiv \{C, KA, A\}$ $(0 < x < l)$ sont ambiges, on a $I_{x+1} \equiv \{A, KA, C\}$ et, d'après (1.5) et (1.6), on a $I_0 = I_{2x}$, donc $x = \dfrac{l}{2}$.

Si $I_0 \equiv \{c, ka, a\}$ est ambige et $I_x = \{A, B, A\}$ $(0 < x < l)$ est symétrique, on voit que $I_{x-k} = \tilde{I}_{x+k}$ $(k \geqslant 0)$, donc $I_0 = \tilde{I}_{2x}$, donc $I_1 = \tilde{I}_0 = I_{2x}$ et $I_0 = I_{2x-1}$, donc $x = \dfrac{l+1}{2}$.

Si $I_0 \equiv \{A, B, A\}$ et $I_x \equiv \{C, D, C\}$ sont symétriques $(0 < x < l)$, on voit que $I_0 = I_{2x}$ donc $x = \dfrac{l}{2}$.

Pour achever la démonstration du Théorème 1 il suffit de remarquer que $N(\varepsilon_D) = (-1)^l$.

COROLLAIRE 3. a) *Il existe des classes ambiges ne contenant pas d'idéal ambige si, et seulement si,* $N(\varepsilon_D) = +1$ *et* D *est somme de deux carrés premiers entre eux.*

b) *Le nombre de ces classes est égal à celui des classes ambiges contenant deux idéaux ambiges.*

Démonstration. Le Corollaire 3 est une conséquence immédiate du Théorème 1, de la Proposition 7 et du Lemme 4, c) et d).

Remarque. La méthode que nous avons utilisée pour établir le Théorème 1 est celle que Gauss utilise pour étudier les classes ambiges de formes quadratiques binaires ([1], § 187) et, dans le cas où $D = 4p$, p premier $\equiv 1 \pmod 4$, montrer que la période de la classe principale permet de décomposer p en somme de deux carrés car elle contient les formes symétriques $\pm ax^2 + 2bxy \mp ay^2$ où $p = a^2 + b^2$ avec $a \equiv 1 \pmod 2$ ([1], § 165).

Le Théorème 1 lui-même, exprimé dans le langage des formes quadratiques binaires, se trouve dans [4] (Théorème 1, p. 172).

Dans le cas où D n'a pas de diviseur carré, le Corollaire 3 a) est établi d'une autre manière dans [5] (Corollaire 1), et est équivalent au Satz 107 du Bericht de Hilbert ([2]).

Nous pouvons maintenant comparer modulo 4 la longueur de la période d'une classe ambige non principale avec la longueur de la période de la classe principale, en combinant le Théorème 1 avec les Propositions 2 et 4. Nous commençons par le cas où $N(\varepsilon_D) = -1$.

THÉORÈME 2. *Soit* D *un discriminant tel que* $N(\varepsilon_D) = -1$, l_0 *la longueur de la période la classe principale. Soit* C *une classe ambige primitive non principale d'idéal ambige* I *de norme* D_1 *tel que* $\bar{D} = D_1 D_2$, *et d'idéal symétrique* S *associé à la représentation* (M, N) *de* $\bar{D}$. *Soient* a, b, c, d *les entiers positifs et* S' *l'idéal symétrique définis à partir de* D_1, M *et* N *comme dans la Proposition 4, et soit* l *la longueur de la période de* C.

Alors l'idéal S' est principal, *et*

$$(4.1) \quad \begin{cases} l \equiv l_0 \pmod 4, & si \quad cdD_1 - abD_2 > 0 \\ l \equiv l_0 + 2 \pmod 4, & si \quad cdD_1 - abD_2 < 0 . \end{cases}$$

Démonstration. Comme les idéaux I et S sont équivalents, (3.5) montre que l'idéal S' est principal.

Plus précisément, posant $S = \alpha I$ avec $1 < \alpha \leqslant \varepsilon_D$, on voit que $S' = \left(\dfrac{\gamma}{\alpha D_1}\right)$. D'autre part soit α_0 tel que $S' = (\alpha_0)$ avec $1 < \alpha_0 \leqslant \varepsilon_D$. Le Lemme 3 montre que, en fait,

$$\sqrt{D} - 1 < \alpha_0 \leqslant \varepsilon_D \,.$$

Comme l'idéal ambige I est réduit et non principal on a $1 < D_1 < D_2$ (Proposition 1), ce qui entraîne $\sqrt{D_2} < \sqrt{D} - 1$ si $D \equiv 1 \pmod 4$ et $2\sqrt{D_2} < \sqrt{D} - 1$ si $D \equiv 0 \pmod 4$. Les définitions (3.10) et (3.15) de γ montrent que, comme $D_1 < D_2$, on a

$$\begin{cases} 1 < \dfrac{\gamma}{D_1} < \sqrt{D_2} \,, & \text{si} \quad D \equiv 1 \pmod 4 \,, \\[2ex] 1 < \dfrac{\gamma}{D_1} < 2\sqrt{D_2} \,, & \text{si} \quad D \equiv 0 \pmod 4 \,, \end{cases}$$

ce qui montre, comme $1 < \alpha \leqslant \varepsilon_D$, que

$$\frac{1}{\varepsilon_D} < \frac{\gamma}{\alpha D_1} < \sqrt{D} - 1 < \alpha_0 \leqslant \varepsilon_D \,.$$

Comme $\alpha_0 \equiv \dfrac{\gamma}{\alpha D_1} \pmod{{}^{\times} \varepsilon_D}$ on voit que $\alpha_0 = \dfrac{\gamma \varepsilon_D}{\alpha D_1}$ et, comme $N(\varepsilon_D) = -1$,

$$\operatorname{sgn}(N(\alpha)) = -\operatorname{sgn}(N(\alpha_0))\operatorname{sgn}(N(\gamma))$$

ce qui, tenant compte de (1.7), (3.6) et du Théorème 1, prouve (4.1) et achève la démonstration du Théorème 2.

Nous considérons maintenant le cas où $N(\varepsilon_D) = +1$, et nous commençons par traiter le cas où $D \not\equiv 0 \pmod{32}$.

THÉORÈME 3. *Soit* D *un discriminant tel que* $D \not\equiv 0 \pmod{32}$ *et* $N(\varepsilon_D) = +1$.

a) *Soit* C *une classe ambige non principale primitive contenant deux idéaux ambiges* I_0 *et* I_1 *de normes réduites respectives* D_0 *et* D_1 *et soient* d, d_0 *et* d_1 *les nombres bien déterminés tels que*

$$D_0 = dd_0 \,, \quad D_1 = dd_1 \,, \quad (d_0, d_1) = 1 \,.$$

Alors

$$\text{(4.2)} \qquad \begin{cases} l \equiv l_0 \,(\mathrm{mod}\, 4)\,, & si \quad d_0 d_1 < \sqrt{\bar{D}}\,, \\ l \equiv l_0 + 2\,(\mathrm{mod}\, 4)\,, & si \quad d_0 d_1 > \sqrt{\bar{D}}\,. \end{cases}$$

b) *Soit* I *l'idéal ambige réduit principal et* $\neq (1)$, *de norme* D_1', *et soit* $D_2' = \dfrac{\bar{D}}{D_1'}$. *Soit* C *une classe ambige non principale contenant les deux idéaux symétriques* S *et* S'. *Alors* S' *s'obtient à partir de* S *et* I *par (3.4). De plus*

$$\text{(4.3)} \qquad \begin{cases} l \equiv l_0 \,(\mathrm{mod}\, 4)\,, & si \quad cdD_1' - abD_2' > 0\,, \\ l \equiv l_0 + 2\,(\mathrm{mod}\, 4)\,, & si \quad cdD_1' - abD_2' < 0\,. \end{cases}$$

Démonstration.

a) Nous appliquons la Proposition 2. Comme $I_0 \neq I_1$ et $I_0 \sim I_1$, on voit que l'idéal J est $\neq (1)$ et principal.

Posant $J = (\alpha_0)$ et $I_1 = \alpha I_0$, on trouve l'égalité d'idéaux:

$$(\alpha_0) = \begin{cases} (r\alpha N(I_0))\,, & \text{si} \quad d_0 d_1 < \sqrt{\bar{D}}\,, \\ (r\alpha N(I_0))\sqrt{\bar{D}}\,, & \text{si} \quad d_0 d_1 > \sqrt{\bar{D}}\,, \end{cases}$$

ce qui, compte tenu de ce que $N(\sqrt{\bar{D}}) = -\bar{D}$ et $N(\varepsilon_D) = +1$, prouve (4.2).

b) Posant $I = (\alpha_0)$ et $N(S) = s$, la relation (3.5) implique

$$S' = \frac{\gamma}{D_1' s}\,\alpha_0 \bar{S} = \frac{\gamma}{D_1' s^2}\,\alpha_0 \beta S$$

où, d'après [7] Corollary 2, $\beta = \dfrac{-M + \sqrt{D}}{2}$ ou $\beta = -N + \sqrt{\bar{D}}$ suivant que $D \equiv 1$ ou $D \equiv 0 \,(\mathrm{mod}\, 4)$, et donc $N(\beta) < 0$. Ceci, compte tenu de ce que $N(\varepsilon_D) = +1$ et de (3.6), prouve (4.3) et achève la démonstration du Théorème 3.

Nous pouvons maintenant donner le résultat dont l'observation a été le point de départ de ce travail.

COROLLAIRE 4. *Soit* $D = 8q$, *où* $q = p^s$ *avec* p *premier* $\equiv 1 \,(\mathrm{mod}\, 4)$ *et* $s \geqslant 1$. *Il y a deux classes ambiges, la classe principale* C_0 *et une autre* C, *et les longueurs de leurs périodes vérifient*

$$\text{(4.4)} \qquad l \equiv l_0 + 2\,(\mathrm{mod}\, 4)\,.$$

Démonstration. Les idéaux ambiges primitifs réduits sont (1) et $[2, \sqrt{2q}]$ donc, avec les notations du Théorème 1 si $N(\varepsilon_D) = -1$ et du Théorème 2 si $N(\varepsilon_D) = +1$, on a $D_1 = 2 = 1^2 + 1^2$ et $D_2 = q = c^2 + d^2$ où c et $d > 0$ sont bien définis par $c \equiv 1 \pmod 2$, si bien que ici

$$cdD_1 - abD_2 = 2cd - (c^2 + d^2) = -(c-d)^2 < 0$$

ce qui, tenant compte de (4.1) si $N(\varepsilon_D) = -1$ et de (4.3) si $N(\varepsilon_D) = +1$ prouve (4.4).

Maintenant nous étudions le cas où $D \equiv 0 \pmod{32}$.

THÉORÈME 4. *Soit D un discriminant tel que $D \equiv 0 \pmod{32}$. Soit C une classe ambige non principale primitive contenant deux idéaux ambiges I_0 et I_1 de normes réduites respectives D_0 et D_1 et soient d, d_0 et d_1 les nombres bien déterminés tels que*

$$D_0 = dd_0\,, \quad D_1 = dd_1\,, \quad (d_0, d_1) = 1\,.$$

Alors les classes modulo 4 de l et l_0 vérifient

Types de I_0 et I_1 (Corollaire 2)	$l \equiv l_0 \pmod 4$	$l \equiv l_0 + 2 \pmod 4$
du même type	$d_0 d_1 < \sqrt{\bar{D}}$	$d_0 d_1 > \sqrt{\bar{D}}$
1 *et* 2, 3 *et* 4	$2^t d_0 d_1 < \sqrt{\bar{D}}$	$2^t d_0 d_1 > \sqrt{\bar{D}}$
2 *et* 3, 1 *et* 4	$2^{t-1} d_0 d_1 < \sqrt{\bar{D}}$	$2^{t-1} d_0 d_1 > \sqrt{\bar{D}}$
1 *et* 3, 2 *et* 4	$2 d_0 d_1 < \sqrt{\bar{D}}$	$2 d_0 d_1 > \sqrt{\bar{D}}$

Démonstration. La démonstration du Théorème 4 est semblable à la démonstration du Théorème 3, a).

COROLLAIRE 5. *Soit $D = 2^{t+2}q$ avec $t \geqslant 3, q = p^s, p$ premier impair, $s \geqslant 1$. Il y a deux classes ambiges, la classe principale C_0 et une autre C. On a*

(4.5) $$l \equiv l_0 \pmod 4\,, \quad si \quad q < 2^{t-2} \quad ou\ si \quad q > 2^t\,.$$

(4.6) $$l \equiv l_0 + 2 \pmod 4\,, \quad si \quad 2^{t-2} < q < 2^t\,.$$

Démonstration. Le Corollaire 2 montre qu'il y a trois idéaux ambiges primitifs réduits non principaux.

Si $2^{t-2} < q < 2^t$ le Corollaire 2 montre que ces idéaux sont $[q, \sqrt{\bar{D}}]$, $[4, 2 + \sqrt{\bar{D}}]$ et $[2^t, 2^{t-1} + \sqrt{\bar{D}}]$. Pour toute combinaison de deux de ces idéaux on vérifie facilement que c'est la condition pour que $l \equiv l_0 + 2 \pmod 4$ du Théorème 4 qui est vérifiée, ce qui prouve (4.6). La démonstration de (4.5) est analogue.

Remarque. Si $D = 32q$ $(t = 3)$, (4.5) est vrai pour $q > 8$ et (4.6) pour $q = 3, 5, 7$.

Exemple 1 (Corollaire 4).

$$D = 40 = 8 \times 5\,, \qquad N(\varepsilon_D) = -1\,, \qquad l_0 = 1\,, \qquad l = 3$$

$$D = 136 = 8 \times 17\,, \qquad N(\varepsilon_D) = +1\,, \qquad l_0 = 4\,, \qquad l = 6\,.$$

Pour terminer cette section nous donnons deux exemples numériques, l'un du Théorème 2 où $N(\varepsilon_D) = -1$ et l'autre du Théorème 3 où $N(\varepsilon_D) = +1$.

Exemple 2 (Théorème 2).

$$D = 12325 = 25 \times 17 \times 29\,, \qquad N(\varepsilon_D) = -1\,.$$

Il y a quatre classes ambiges, C_0 (principale), C_1, C_2 et C_3 et nous donnons pour chacune l'idéal ambige réduit, l'idéal symétrique et la longueur, obtenus par réduction ([7], § 5).

$$C_0 : \left[1, \frac{111 + \sqrt{D}}{2}\right] \sim \left[1, \frac{111 + \sqrt{D}}{2}\right]; \qquad l_0 = 1\,.$$

$$C_1 : \left[17, \frac{85 + \sqrt{D}}{2}\right] \sim \left[27, \frac{97 + \sqrt{D}}{2}\right]; \qquad l_1 = 5\,.$$

$$C_2 : \left[25, \frac{75 + \sqrt{D}}{2}\right] \sim \left[53, \frac{33 + \sqrt{D}}{2}\right]; \qquad l_2 = 7\,.$$

$$C_3 : \left[29, \frac{87 + \sqrt{D}}{2}\right] \sim \left[39, \frac{79 + \sqrt{D}}{2}\right]; \qquad l_3 = 5\,.$$

Nous vérifions le Théorème 2 pour la classe C_2.

$$D_1 = 25 = 3^2 + 4^2\,, \qquad D_2 = 17.29 = 13^2 + 18^2 = 3^2 + 22^2\,.$$

On trouve que $33 = 4.18 - 3.13$. Donc $a = 3$, $b = 4$, $c = 13$, $d = 18$. Ensuite, changeant le signe, on trouve $4.18 + 3.13 = 111$, ce qui montre que $S' = \left[1, \frac{111 + \sqrt{D}}{2}\right] \in C_0$. Enfin

$$cdD_1 - abD_2 = 13.18.25 - 3.4.17.29 = -66 < 0$$

donc $l_2 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.

Exemple 3 (Théorème 3):

$$D = 5525 = 25.13.17 \ , \quad N(\varepsilon_D) = +1 \ .$$

Les quatre idéaux ambiges réduits se répartissent dans les deux classes C_0 (principale) et C_1 ainsi

$$C_0 : \left[1, \frac{73+\sqrt{D}}{2}\right] \sim \left[25, \frac{25+\sqrt{D}}{2}\right] ; \quad l_0 = 4 \ .$$

$$C_1 : \left[13, \frac{65+\sqrt{D}}{2}\right] \sim \left[17, \frac{51+\sqrt{D}}{2}\right] ; \quad l_1 = 6 \ .$$

Vérifions le Théorème 3a) pour C_1. On a $D_0 = 13$, $D_1 = 17$, donc $d_0 = 13$, $d_1 = 17$ et $d_0 d_1 > \sqrt{D}$ donc $l_1 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.

Vérifions le Théorème 3b). On a

$$D_1' = 25 = 3^2 + 4^2 \ , \quad D_2' = 13.17 = 11^2 + 10^2 = 5^2 + 14^2 \ ,$$

$$D = 41^2 + 62^2 = 73^2 + 14^2 = 71^2 + 22^2 = 7^2 + 74^2 \ ,$$

et on trouve deux classes ambiges contenant les idéaux symétriques:

$$C_2 : \left[37, \frac{7+\sqrt{D}}{2}\right] \sim \left[7, \frac{73+\sqrt{D}}{2}\right] ; \quad l_2 = 4 \ .$$

$$C_3 : \left[31, \frac{41+\sqrt{D}}{2}\right] \sim \left[11, \frac{71+\sqrt{D}}{2}\right] ; \quad l_3 = 6 \ .$$

On a donc $a = 3$, $b = 4$.

Pour la classe C_2, $7 = 4.10 - 3.11$ et $73 = 4.10 + 3.11$, donc $c = 11$, $d = 10$ et

$$cdD_1' - abD_2' = 11.10.25 - 3.4.13.17 = 98 > 0$$

donc $l_2 \equiv l_0 \pmod 4$, ce qui est vrai.

Pour la classe C_3, $41 = 4.14 - 3.5$, $71 = 4.14 + 3.5$, donc $c = 5$, $d = 14$ et

$$cdD_1' - abD_2' = 5.14.25 - 3.4.13.17 = -902 < 0$$

donc $l_3 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.