Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 7 (1961)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LES CORPS QUADRATIQUES
Autor: Châtelet, A.
DOI: https://doi.org/10.5169/seals-37125

LES CORPS QUADRATIQUES

par A. CHÂTELET

(suite et fin)

CHAPITRE V

LES CLASSES D'IDÉAUX DANS LES CORPS IMAGINAIRES — OU DE DISCRIMINANT NÉGATIF —

La considération des *idéaux réduits* (**25**), qui a permis de montrer que, dans tout corps quadratique, le nombre de classes d'idéaux est fini, permet, plus précisément, dans le cas d'un corps imaginaire (discriminant négatif), de déterminer compètement ces classes et, par suite de construire la « *structure de leur groupe* » (**23**).

30. Idéaux réduits remarquables.

On peut d'abord remarquer que, dans un *corps imaginaire*, dont le polynôme fondamental $F(x)$ ne prend que des valeurs positives:

la racine minimum $\bar{c}$, d'un idéal canonique (**7**), *est aussi celle qui donne à* $F(x)$ *la plus petite valeur.*

Toute autre racine de l'idéal considéré est un terme $\bar{c}+\lambda m$, de la progression arithmétique, dont la raison est la norme m, de l'idéal. Il suffit de former la différence:

$$F(\bar{c}+\lambda m)-F(\bar{c}) = \lambda m \times (2\bar{c}-S+\lambda m).$$

La valeur absolue $|2\bar{c}-S|$ étant au plus égale à m, la valeur entre parenthèses est nulle, ou du signe de l'entier λ; la différence est donc nulle, ou positive.

En dehors du cas trivial $\lambda = 0$, cette différence ne peut être nulle que pour des valeurs $+1$ ou -1, de λ; en outre:

$$|2\bar{c}-S| = m \quad \Leftrightarrow \quad |(S-\bar{c})-\bar{c}| = m;$$

les *zéros conjugués* (**5**) $\bar{c}$ et $\bar{c}' = S - \bar{c}$, définissent le même idéal qui est égal à son conjugué, —ou qui est *double* (**7**)— elles donnent aussi la même valeur (minimum) à $F(x)$.

DÉFINITIONS. — Dans un corps imaginaire, *parmi les idéaux réduits* (**25**), on peut **remarquer**, ou appeler **remarquable**:

1° *un idéal qui est double* (**7**), qui est ainsi **réduit double**; il est égal à son conjugué et représente une *classe double*, égale à sa conjuguée, qui est aussi son inverse, en sorte que le carré de la classe est égal à la classe principale (**23**);

2° *un idéal qui est réfléchi* (**16**), qui est ainsi **réduit réfléchi**; il est équivalent de dire que c'est *un idéal réfléchi relativement à sa racine minimum:*

$$\mathbf{M} \times \mathbf{M} = (\theta - \bar{c}); \qquad F(\bar{c}) = m^2; \qquad |2\bar{c} - S| \leqslant m.$$

L'idéal conjugué $\mathbf{M}'$ est aussi réduit réfléchi (ou réfléchi relativement à sa racine minimum $S - \bar{c}$). Les deux idéaux, qui sont congrus, appartiennent à une même *classe double*.

Il est évident qu'un idéal (canonique) *réfléchi relativement à sa racine minimum* $\bar{c}$ est *réduit*, puisque le carré de sa norme n'est pas supérieur à $|F(c)|$. On peut vérifier que, d'une façon réciproque:

un idéal réduit qui n'est pas réfléchi relativement à sa racine minimum ne peut l'être relativement à tout autre racine.

Car sa norme m est alors inférieure à la norme $F(\bar{c}) : m$, de l'idéal qui lui est associé, relativement à la racine minimum $\bar{c}$, elle l'est, à fortiori, pour tout idéal associé suivant une autre racine c, car, d'après la remarque précédente, $F(\bar{c})$ étant minimum:

$$F(c) \geqslant F(\bar{c}) \quad \Rightarrow \quad n = F(c) : m \geqslant F(\bar{c}) : m > m.$$

On a indiqué la construction d'un *idéal double* (**21**), éventuellement *réduit* (**25**) et celle d'un *idéal réfléchi* (**16**). En les rapprochant pour un idéal réduit, dans le cas d'un corps imaginaire, on obtient une construction générale des *idéaux réduits remarquables.*

THÉORÈME d'existence des idéaux réduits remarquables. Dans un corps quadratique, de discriminant D négatif, *les idéaux*

réduits remarquables sont associés —ou correspondent biunivoquement— *aux décompositions de* $|D|$, s'il est impair, *ou de* $|D|:4$, *en un produit de deux entiers positifs*, dans les conditions suivantes:

Décomposition de $\|D\|$		*Idéal réduit*
$\|D\| = u\times v$; $u \leqslant v$, impairs	$3u \leqslant v$	$m=u$; $\bar{c} = (u+S):2$ (m, θ—$\bar{c}$) *double.*
ou $\|D\|:4 = (u:2)\times(v:2)$ $u:2 \leqslant v:2$, impairs	$3u \geqslant v$	$m = (v+u):4$; $\bar{c} = (v-u-2S):4$ (m, θ—$\bar{c}$) *réfléchi.*
$\|D\| = u\times(4v)$; $u \leqslant v$:		$m=u$; (m, θ—0) *double.*

Tout *idéal double réduit* est obtenu en prenant, pour sa norme m, un diviseur convenable de $|D|$. La limitation de m (**25**) et la valeur de la racine minimum $\bar{c}$ (**21**) sont données, suivant les cas, par:

$S=-1$;	$\|D\| = m\times v$;	m, v impairs;	$\bar{c} = (m-1):2$	$3m^2 \leqslant \|D\|$;
$S=0$;	$\|D\| = 2u\times 2v$;	u, v impairs;	$m = 2u$; $\bar{c} = u$;	$3m^2 \leqslant \|D\|$;
$S=0$;	$\|D\| = m\times 4v$,		$\bar{c} = 0$	$4m^2 \leqslant \|D\|$.

Ce sont bien les circonstances de l'énoncé.

Tout idéal réfléchi, relativement à une racine c, est obtenu (**16**) par une décomposition du discriminant (négatif) en un produit de deux entiers, dont un négatif:

$$D = (-u)+v; \qquad v-(-u) = v+u, \quad \text{multiple de 4.}$$

Ceci exige que $|D|$ soit impair, ou quadruple d'un nombre impair $N = |d|$ [les nombres entiers $|D|$ et N congrus à —1, mod. 4]. Ce sont les deux premiers cas de l'énoncé. La norme m et la racine c sont données par:

$$4m = v+u; \qquad 2\times(2c-S) = v-u.$$

Pour que la racine c soit minimum, ce qui est la condition de réduction, il faut et il suffit que:

$$2\times(v-u) = 4\times(2c-S) \leqslant 4m = (v+u) \quad \Leftrightarrow \quad v \leqslant 3u.$$

La valeur $u = 1$ constitue un cas particulier trivial de la première décomposition; il lui correspond l'idéal unité $(1,\ \theta-0)$. L'idéal est *réduit double*; si

$$1 = u = 3v; \quad [D = (-1)\times 3 = -3; \quad F(x) = x^2+x+1]$$

l'idéal unité est, à la fois, *double et réfléchi.*

Dans le cas de $|D|$ pair, à la décomposition triviale $|D| = 1\times 4v$, correspond encore l'idéal unité, qui est *réduit double.*

Exemple 1. — Dans le corps de discriminant:

$$D = -231 = (-3)\times(-7)\times(-11),$$

dent les calculs sont indiqués dans le tableau IX, aux décompositions:

$$|D| = 1\times 231, \quad 3\times 77, \quad 7\times 33,$$

dont le premier facteur u, est inférieur au tiers du second, correspondent les *idéaux réduits doubles* [norme u, racine minimum $(u-1):2$]:

$$(1,\ \theta-0), \quad (3,\ \theta-1), \quad (7,\ \theta-3).$$

A la décomposition 11×21, correspond l'*idéal réduit réfléchi* [norme $(11+21):4 = 8$; racine minimum $(21-11-2):4 = 2$]:

$$(8,\ \theta-2); \quad F(2) = 8^2; \quad (8,\ \theta-2)^2 = (\theta-2).$$

Exemple: 2. — Dans le corps (tableau XVIII), de discriminant:

$$D = -420 = (-4)\times(-3)\times(+5)\times(-7),$$

aux décompositions de $|D|:4 = 105$, correspondent les idéaux réduits remarquables:

3×35: idéal double $(6,\ \theta-3)$; $[m = 2\times 3, \quad \bar{c} = 3]$
5×21: id. $(10,\ \theta-5)$; $[m = 2\times 5, \quad \bar{c} = 5]$
7×15: idéal réfléchi $(11,\ \theta-4)$; $[m = (7+15):2, \quad \bar{c} = (15-7):2]$.

Aux décompositions $420 = u \times (4\nu)$ correspondent les *idéaux réduits doubles*, de normes 1, 3, 5, 7, et de racine minimum 0.

EXEMPLE 3: Dans le corps de discriminant (tableau XVIII):

$$-440 = (+8) \times (+5) \times (-11),$$

les seules décompositions auxquelles correspondent des idéaux réduits remarquables sont:

$$1 \times (4 \times 110), \quad 2 \times (4 \times 55), \quad 5 \times (4 \times 22), \quad 10 \times (4 \times 11),$$

qui donnent les idéaux doubles, de normes 1, 2, 5, 10, et de racine minimum 0.

31. Détermination des idéaux réduits.

Dans un corps imaginaire les idéaux canoniques réduits représentent les classes, *presque proprement.*

THÉORÈME de la détermination des idéaux réduits — Dans un corps quadratique imaginaire, *une classe d'idéaux contient:* soit *un et un seul idéal* (canonique) *réduit*; soit (exceptionnellement) *deux idéaux réduits conjugués*, qui sont alors *réduits réfléchis.*

On a établi l'existence, dans chaque classe, d'au moins un idéal (canonique) réduit (**25**):

$$\mathbf{M} = (m, \quad \theta - \bar{c}); \qquad |2\bar{c} - S| \leqslant m \leqslant |F(\bar{c})| : m.$$

Il reste à chercher dans quelles conditions un idéal $\mathbf{N} = \mathbf{M} \times (\rho)$, congru à $\mathbf{M}$ —ou dans la même classe— peut être aussi réduit. On peut mettre l'élément ρ, et, par suite l'idéal principal (ρ) sous sa forme canonique (**3** et **11**), d'où:

$$\mathbf{N} = \mathbf{M} \times (u + \nu\theta) \times q = (m, \ \theta - \bar{c}) \times (u + \nu\theta) \times q;$$

u, ν nombres entiers premiers entre eux.

Le produit $\mathbf{M} \times (u + \nu\theta)$ est un idéal entier; en développant et explicitant son expression, on obtient des générateurs d'une base arithmétique libre:

$$(m, \ \theta - \bar{c}) \times (u + \nu\theta) = (mu + m\nu\theta, \quad (-\bar{c}u - \nu N) + [u + \nu(S - \bar{c})]\theta).$$

Le facteur rationnel de cet idéal m_1, est égal au p.g.c.d. des coefficients de θ, dans ces générateurs, il divise leur combinaison:

$$m[u+v(S-\bar{c})]-mv(S-\bar{c}) = mu;$$

divisant mu et mv, il divise m, puisque u,v sont premiers entre eux.

Pour que **N** soit canonique, il faut que le produit $m_1 \times q$ soit égal à 1, et sa norme n est égale à:

$$n = N(\mathbf{N}) = N(\mathbf{M}) \times N(u+v\theta) \times N(q) = m \times N(u+v\theta) \times m_1^{-2}.$$

On peut minorer $N(u+v\theta)$, en supposant v non nul:

$$4N(u+v\theta) = (2u+vS)^2+v^2|D| \geqslant v^2|D|;$$

d'où une minoration de la norme n, de **N**:

$$4n \geqslant m \times v^2 \times |D| \times m_1^{-2} \quad \Rightarrow \quad 4mn \geqslant (m : m_1)^2 \times v^2 \times |D|.$$

Pour que **M** et **N**, qui sont canoniques, soient tous deux réduits, il faut que leurs normes vérifient les limitations:

$$3m^2 \leqslant |D| \quad \text{et} \quad 3n^2 \leqslant |D| \quad \Rightarrow \quad 3mn \leqslant |D|;$$

ce qui entraîne:

$$4|D| \geqslant 12mn \geqslant 3(m : m_1)^2 \times v^2 \times |D| \quad \Rightarrow \quad 4 \geqslant 3(m : m_1)^2 \times v^2.$$

Comme $m : m_1$ et v sont des entiers, ils doivent être tous deux de valeur absolue égale à 1; donc $m = m_1$ et on peut prendre $v = 1$.

La relation entre **N** et **M** devient ainsi:

$$\mathbf{N} \times (m) = \mathbf{M} \times (\theta+u); \quad \text{et} \quad F(-u) = N(\theta+u) = m \times n.$$

On peut mettre l'idéal principal $(\theta+u)$ sous forme canonique et diviser les deux membres par **M** [on a vu (**13**) que $(m) = \mathbf{M} \times \mathbf{M}'$]; on obtient:

$$\mathbf{N} \times \mathbf{M}' = (m \times n, \quad \theta+u) = (m, \quad \theta \times u) \times (n, \quad \theta+u).$$

La racine $-u$, doit être aussi une de racine **M**′, c'est-à-dire est congrue mod. m, au zéro $\bar{c}' = S-\bar{c}$. L'idéal **N** est égal au deuxième facteur (du dernier membre) et $-u$ est congru, mod. n, à sa racine minimum $\bar{c}_1$. Les limitations des racines minimum des idéaux réduits (**25** et remarque de **29**) entraînent les comparaisons:

$$m^2 \leqslant F(\bar{c}') \leqslant F(-u); \quad n^2 \leqslant F(\bar{c}_1) \leqslant F(-u); \quad m \times n \leqslant F(-u).$$

Mais la dernière comparaison est une égalité; il en est donc de même des premières et:

$$m^2 = F(\bar{c}') = F(-u) = F(\bar{c}_1) = n^2 \quad \Rightarrow \quad -u = \bar{c}' = \bar{c}_1.$$

L'idéal **N** est égal au conjugué **M'**, de l'idéal **M**, en sorte que **M** et **M'**, qui sont congrus, sont réfléchis relativement aux racines minimum $\bar{c}$ et $\bar{c}'$. Leur congruence est explicitée (**24**) par:

$$(\theta - \bar{c}) = \mathbf{M}^2 \qquad (\theta - \bar{c}') = \mathbf{M}'^2;$$

ou

$$\mathbf{M}' \times (\theta - \bar{c}) = \mathbf{M} \times (m) \qquad \mathbf{M} \times (\theta - \bar{c}') = \mathbf{M}' \times (m).$$

On trouve bien le cas d'exception signalé et seulement ce cas. Le cas trivial de la congruence de **M** avec lui-même a été écarté en supposant ρ non nul, dans l'expression de ρ.

En conséquence: *pour obtenir les classes d'idéaux*, d'un corps quadratique imaginaire, *il suffit de construire les idéaux canoniqies réduits*, ce qui peut être fait par l'algorithme suivant:

on utilise le *tableau des valeurs* $F(c)$, du polynôme fondamental du corps, pour les valeurs entières de c, croissantes de 0 jusqu'à la limite r, exclue, pour laquelle $3 \times (2c - S)^2$ devient supérieur la valeur absolue $|D|$, du discriminant.

On retient chaque décomposition:

$$F(c) = m \times n; \qquad (2c - S) \leqslant m \leqslant n,$$

en un produit de deux facteurs (entiers) au moins égaux à $2c - S$. *Le premier facteur* (au plus égal au second) *m est la norme de deux idéaux conjugués réduits:*

$$(m, \theta - c), \quad (m, \theta - c'); \qquad c + c' = S.$$

Si m est *diviseur de* $|D|$, ces deux idéaux sont égaux à un *idéal double*, de racine minimum c, qui définit une *classe double.*

Si les deux facteurs sont égaux:

$$m = n \quad \text{et} \quad F(c) = F(c') = m^2,$$

les deux idéaux sont *réfléchis*, ils sont congrus et définissent une seule *classe double.*

TABLEAU IX.

CLASSES d'idéaux et Structure de leur GROUPE.

$F(x) = x+x^2+58$; $D = -231 = (-3)\times(-7)\times(-11)$; $r = 4$.

c	$F(c)$	réduits Idéaux	Classe	Calculs
—4	70	»		$(7, \theta+4) = (\mathbf{7}, \theta-3)$
—3	64	»		$(8, \theta+3) \sim (\mathbf{8}, \theta-2)$
—2	$\mathbf{6}\times 10$ $\mathbf{5}\times 12$ $\mathbf{4}\times 15$	$(\mathbf{6}, \theta+2) = \mathbf{I}\times\mathbf{J}$ $(\mathbf{5}, \theta+2) \sim \mathbf{I}^4\times\mathbf{J}$ $(\mathbf{4}, \theta+2) = \mathbf{I}^2$		$(\mathbf{2}, \theta-0)\times(\mathbf{3}, \theta-1) = (\mathbf{6}, \theta+2)$ $(\mathbf{2}, \theta-0)^2 = (\mathbf{4}, \theta+2)$ $(3, \theta+2) = (\mathbf{3}, \theta-1)$
—1	$\mathbf{2}\times 29$	$(\mathbf{2}, \theta+1) \sim \mathbf{I}^5$		
0	$\mathbf{1}\times 58$ $\mathbf{2}\times 29$	$(\mathbf{1}, \theta-0) = (1)$ $(\mathbf{2}, \theta-0) = \mathbf{I}$		
+1	$\mathbf{3}\times 20$ $\mathbf{4}\times 15$ $\mathbf{5}\times 12$ $\mathbf{6}\times 10$	$(\mathbf{3}, \theta-1) = \mathbf{J}$ $(\mathbf{4}, \theta-1) \sim \mathbf{I}^4$ $(\mathbf{5}, \theta-1) \sim \mathbf{I}^2\times\mathbf{J}$ $(\mathbf{6}, \theta-1) \sim \mathbf{I}^5\times\mathbf{J}$		$(\mathbf{2}, \theta+1)^2 = (\mathbf{4}, \theta-1)$ $(\mathbf{4}, \theta+2)\times(\mathbf{3}, \theta-1) = (12, \theta+2) \sim (\mathbf{5}, \theta-1)$
+2	$\mathbf{8}\times 8$	$(\mathbf{8}, \theta-2) = \mathbf{I}^3$		$(\mathbf{2}, \theta-0)^3 = (\mathbf{8}, \theta-2)$; $(\mathbf{2}, \theta-0)^6 \sim (1)$
+3	$\mathbf{7}\times 10$	$(\mathbf{7}, \theta-3) \sim \mathbf{I}^3\times\mathbf{J}$		$(\mathbf{8}, \theta-2)\times(\mathbf{3}, \theta-1) = (24, \theta-10) \sim (\mathbf{7}, \theta+11) = (\mathbf{7}, \theta-3)$
10	$168 = 7\times 24$			

GROUPE: $\mathbf{I}^x\times\mathbf{J}^y$; x, mod. 6; y, mod. 2; ordre 12.
ou: $(\mathbf{I}^2)^x\times(\mathbf{I}^3)^y\times\mathbf{J}^z$; x, mod. 3; y, z, mod. 2.

Dans tout autre cas, les deux idéaux réduits sont distincts et définissent *deux classes conjuguées.*

Les classes ainsi engendrées sont différentes et *ce sont toutes les classes du corps.*

EXEMPLES. — Le tableau IX indique les calculs pour le corps de discriminant —231; le rang est $r = 4$. Pour c compris entre 0 et 3 inclus, on a inscrit les décompositions $F(c) = m \times n$, en deux facteurs au moins égaux à $2c+1$ et devant chacune l'idéal $(m,\ \theta—c)$, dont la norme est le facteur au plus égal à l'autre. Dans le tableau prolongé en deçà de 0, on a inscrit les idéaux conjugués $(m,\ \theta—c')$.

Il y a cinq idéaux réduits remarquables: trois idéaux doubles, de normes **1**, **3**, **7**, qui définissent des classes doubles; un couple d'idéaux réfléchis, de norme **8**, qui définissent une même classe double. Enfin quatre couples d'idéaux conjugués, de normes 2, 4, 5, 6, définissant des couples de classes conjuguées. En tout:

$$4+2\times4 = 12 \text{ classes.}$$

D'autres tableaux de ce même chapitre donnent encore des exemples de calcul d'idéaux réduits et de classes d'idéaux dans des corps quadratiques imaginaires.

Le tableau XI concerne des corps qui ne contiennent qu'une seule classe et, par suite, sont *principaux.*

Les tableaux XII et XIV concernent des corps dont le discriminant est premier; ils n'ont donc que le seul idéal réduit remarquable (1) et des couples d'idéaux réduits conjugués; en tout un nombre impair de classes.

Les tableaux XV, XVII, XVIII concernent des corps dont le discriminant est composé, pair ou impair.

32. Répartition des idéaux dans les classes.

Les idéaux réduits d'un corps imaginaire et les classes qu'ils définissent étant ainsi calculés, on peut répartir, dans ces classes, les idéaux canoniques donnés par le tableau des valeurs du polynôme fondamental (**21**). Il suffit d'appliquer le calcul de récurrence indiqué ci-dessus (**25**).

Si deux idéaux canoniques conjugués (éventuellement égaux) **M** et **M'** ne sont pas réduits, en considérant l'associé de l'un d'eux suivant sa racine minimum (par exemple celle qui est positive), on peut construire un couple d'idéaux conjugués respectivement congrus à **M'** et **M**, et de norme inférieure. En recommençant éventuellement cette construction, par récurrence descendante, on aboutit à un couple d'idéaux conjugués réduits et, par suite à l'indication des classes auxquelles appartiennent **M** et **M'**.

Exemple. — Le tableau X, donne un exemple de répartition d'idéaux canoniques en classes, pour le corps de discriminant —231, déjà utilisé comme exemple de construction d'idéaux réduits.

Devant chaque valeur $F(c)$, pour c de 0 à 12, on a inscrit les divers couples d'*idéaux associés* (**21** et **24**), donnés par les décompositions:

$$F(c) = m \times n; \qquad (\theta - c) = (m,\ \theta - c) \times (n,\ \theta - c);$$

toutefois les racines indiquées sont les plus petites racines positives, par exemple:

$$F(5) = 88; \qquad (4,\ \theta - 1) \quad (22,\ \theta - 5).$$

Les douze classes ont été désignées par les normes, éventuellement accentuées des idéaux réduits qui les définissent:

classes doubles: **1** — **3** — **7** — **8**;

couples de classes conjuguées: **2**, **2'** — **4**, **4'** — **5**, **5'** — **6**, **6'**.

On a inscrit ces nombres en caractères gras, devant les treize idéaux réduits (la classe **8** contenant deux idéaux congrus, réfléchis), définis par leur plus petite racine positive.

On les a inscrit, en caractères ordinaires, devant les idéaux obtenus pour la première fois, ce nombre étant déterminé par l'idéal réduit congru, obtenu comme il vient d'être dit.

On indique, en exemple, cette construction, pour les idéaux, de norme $10 = 2 \times 5$, qui forment deux couples d'idéaux conjugués; 2 et 5 n'étant pas facteurs du discriminant.

Les idéaux conjugués, inscrits dans la table:

$$(10,\ \theta - 1) \quad \text{et} \quad (10,\ \theta + 2) = (10,\ \theta - 8)$$

Tableau X.

Répartition des idéaux en classes.

$F(x) = x^2+x+58$; $D = -231 = (-3)\times(-7)\times(-11)$

c	$F(c)$				
0	58	(**1**, θ—0)	**1**	(58, θ—0)	1
		(**2**, θ—0)	**2**	(29, θ—0)	2
1	60	(1, θ—0)		(60, θ—1)	1
		(**2**, θ—1)	**2′**	(30, θ—1)	2
		(**3**, θ—1)	3	(20, θ—1)	3
		(**4**, θ—1)	**4**	(15, θ—1)	4′
		(**5**, θ—1)	**5**	(12, θ—1)	5′
		(**6**, θ—1)	**6**	(10, θ—1)	6′
2	64	(1, θ—1)		(64, θ—2)	1
		(2, θ—0)		(32, θ—2)	2′
		(**4**, θ—0)	**4′**	(16, θ—2)	4
		(**8**, θ—2)	**8**		
3	70	(1, θ—0)		(70, θ—3)	1
		(2, θ—1)		(35, θ—3)	2
		(**5**, θ—3)	**5′**	(14, θ—3)	5
		(**7**, θ—3)	**7**	(10, θ—3)	7
4	78	(1, θ—0)		(78, θ—4)	1
		(2, θ—0)		(39, θ—4)	2′
		(3, θ—1)		(26, θ—4)	3
		(**6**, θ—4)	**6′**	(13, θ—4)	6
5	88	(1, θ—0)		(88, θ—5)	1
		(2, θ—1)		(44, θ—5)	2
		(4, θ—1)		(22, θ—5)	4′
		(**8**, θ—5)	**8**	(11, θ—5)	8
6	100	(1, θ—0)		(100, θ—6)	1
		(2, θ—0)		(50, θ—6)	2′
		(4, θ—2)		(25, θ—6)	4
		(5, θ—1)		(20, θ—6)	5′
				(10, θ—6)	7

c	$F(c)$				
7	114	(1, θ—0)		(114, θ—7)	1
		(2, θ—1)		(57, θ—7)	2
		(3, θ—1)		(38, θ—7)	3
		(6, θ—1)		(19, θ—7)	6′
8	130	(1, θ—0)		(130, θ—8)	1
		(2, θ—0)		(65, θ—8)	2′
		(5, θ—3)		(26, θ—8)	5
		(10, θ—8)	6	(13, θ—8)	6′
9	148	(1, θ—0)		(148, θ—9)	1
		(2, θ—1)		(74, θ—9)	2
		(4, θ—1)		(37, θ—9)	4′
10	168	(1, θ—0)		(168, θ—10)	1
		(2, θ—0)		(84, θ—10)	2′
		(3, θ—1)		(56, θ—10)	3
		(4, θ—2)		(42, θ—10)	4
		(6, θ—4)		(28, θ—10)	6
		(7, θ—3)		(24, θ—10)	7
		(8, θ—2)		(21, θ—10)	8
		(12, θ—10)	5	(16, θ—10)	5′
11	190	(1, θ—0)		(190, θ—11)	1
		(2, θ—1)		(95, θ—11)	2
		(5, θ—1)		(38, θ—11)	5′
		(10, θ—1)		(19, θ—11)	6
12	214	(1, θ—0)		(214, θ—12)	1
		(2, θ—0)		(107, θ—12)	2′

12 Classes: **1**, **3**, **7**, **8**, doubles; **2**,**2′**—**4**,**4′**—**5**,**5′**—**6**,**6′**.

ne sont pas réduits. La décomposition:

$$F(1) = F(-2) = 60 = 6\times 10: \quad (\theta-1) = (6,\ \theta-1)\times(10,\ \theta-1);$$

montre que le premier est congru au conjugué de $(6,\ \theta-1)$, qui est réduit; il appartient à la classe désignée par **6′** et son conjugué est dans **6.**

Les autres idéaux, de norme 10:

$$(10,\ \theta-3) \quad \text{et} \quad (10,\ \theta+4) = (10,\ \theta-6),$$

ne sont pas non plus réduits. La décomposition:

$$F(3) = F(-4) = 70 = 7\times 10$$

montre qu'ils sont congrus aux idéaux conjugués, de norme 7; mais ces idéaux sont égaux —ou doubles— . Les deux idéaux appartiennent à la classe désignée par **7** et sont congrus. On remarquera d'ailleurs que le second est réfléchi, relativement à la racine 6 ($F(6) = 100$).

On peut aussi bien rechercher la classe d'un idéal, donné par la décomposition d'une valeur de $F(x)$, extérieure à la table, par exemple $F(103) = 30\times 359$. Les idéaux conjugués, de norme 359, sont

$$\mathbf{M} = (359,\ \theta-103), \quad \mathbf{M}' = (359,\ \theta+104) = (359,\ \theta-255).$$

Cette décomposition montre que **M′** et **M** sont respectivement congrus aux idéaux conjugués:

$$(30,\ \theta-103) = (30,\ \theta-13), \quad (30,\ \theta+104) = (30,\ \theta-16).$$

La décomposition $F(13) = 240 = 8\times 30$, montre que ces idéaux, et par suite **M′** et **M** sont congrus aux idéaux conjugués de norme 8, qui sont congrus entre eux; ils appartiennent donc à la classe double **8.**

33. Structure du groupe des classes d'idéaux.

Pour construire le groupe des classes d'idéaux, d'un corps imaginaire, on peut, évidemment, utiliser les idéaux réduits qui caractérisent —ou déterminent— ces classes. On peut, d'abord, former une table de multiplication du groupe, en déterminant *à quels idéaux réduits sont congrus* —donc à quells classes appar-

tiennent— *les produits d'idéaux réduits*, caractérisant les produits de classes. On peut, notamment, déterminer l'ordre de chacune des classes, en déterminant *un idéal principal égal à une puissance*, d'exposant aussi petit que possible, *de l'idéal* qui caractérise la classe considérée.

On peut limiter cette recherche en appliquant certaines des remarques suivantes:

1. On peut représenter chaque classe —ou l'idéal réduit qui la caractérise— par un produit de *puissance d'idéaux premiers réduits* (dont les normes sont des nombres premiers). Ceci, en raison de la propriété:

> *Tout facteur de la décomposition* en produits d'idéaux premiers (**15. 3**) *d'un idéal réduit est égal à un idéal réduit.*

On considère un idéal canonique réduit $\mathbf{M} = (m,\ \theta - \bar{c})$, de racine minimum $\bar{c}$; tout facteur de sa décomposition est de la forme:

$$\mathbf{P} = (p,\ \theta - \bar{c}); \qquad p \text{ diviseur de } m;$$

sa racine minimum, notée c, est congrue à $\bar{c}$, mod. p. Comme **P** est différent de **M**, sa norme p est au plus égale à $m : 2$ et:

$$p^2 \leqslant (m^2 : 4) \leqslant |D| : 12 \leqslant [4F(c)] : 12 = [F(c)] : 3;$$

P vérifie donc bien les conditions de réduction (**25**).

2. On peut considérer simultanément des *produits* (de puissances d'idéaux premiers) *inverses*, c'est-à-dire formés des mêmes éléments avec des *exposants respectivement opposés*, à certains modules près. Car l'inverse —ou la puissance d'exposant -1— d'une classe, définie par un idéal réduit **I**, est égale à la classe conjuguée, définie par l'idéal conjugué **I'** qui est aussi réduit (**25**).

3. Dans un produit de puissances d'idéaux premiers réduits, dont on cherche la classe, on peut supprimer les facteurs conjugués, dont le produit (partiel) est un idéal principal; le produit ainsi simplifié est congru à l'ancien.

Finalement, on est ramené à des problèmes du type suivant:

Calculer l'idéal réduit qui est congru à un produit de puissances d'idéaux premiers :

$$\mathbf{M} = \Pi\, \mathbf{M}_i; \quad \mathbf{M}_i = \mathbf{P}_i^{h_i}; \quad \mathbf{P}_i = (p_i, \quad \theta - c_i) \quad \text{réduit};$$

les p_i sont des nombres premiers différents (peut-être réduits à un seul); $h_i = 1$, si p_i est diviseur du discriminant.

Les principes de ce calcul ont été déjà exposés pour des idéaux quelconques (**15**, **25**, **32**).

On peut ensuite décomposer le groupe ainsi construit en un *produit direct de groupes cycliques* (**26**), en utilisant une des méthodes générales de décomposition d'un groupe abélien fini.

On peut notamment déterminer le maximum h de l'ordre des différentes classes. On choisit alors un idéal **I** dont la classe est d'ordre h et on construit le groupe cyclique $\mathscr{I}$ engendré par cet idéal —ou par sa classe— .

Si ce premier sous-groupe $\mathscr{I}$ n'est pas identique au groupe de toutes les classes, on peut construire le groupe quotient du groupe des classes par $\mathscr{I}$: on forme, pour chaque classe, l'ensemble des produits de cette classe —ou l'ensemble des produits de l'idéal réduit qui détermine cette classe— par les différents éléments de $\mathscr{I}$ —ou par les puissances de **I**— . On calcule l'ordre de chaque élément de ce groupe quotient —ou on détermine, pour chaque idéal réduit, la puissance d'exposant minimum qui est congrue à une puissance de **I**— . On choisit un idéal $\mathbf{J}_1$ dont la classe a, dans ce groupe quotient, un ordre k aussi grand que possible.

Si $\mathbf{J}_1$ est indépendant de **I** —ou si les groupes cycliques engendrés par **I** et $\mathbf{J}_1$ n'ont en commun que la classe unité $\mathscr{R}$— , on choisit $\mathbf{J} = \mathbf{J}_1$, on forme le groupe cyclique $\mathscr{J}$ engendré par **J** et le produit direct $\mathscr{I} \times \mathscr{J}$.

Si $\mathbf{J}_1$ n'est pas indépendant de **I**, on peut montrer qu'il existe un produit $\mathbf{I}^a\, \mathbf{J}_1^b = \mathbf{J}$, de même ordre k que $\mathbf{J}_1$ dans le groupe quotient, et indépendant de **I**. On forme encore le groupe cyclique $\mathscr{J}$ engendré par **J** et le produit direct $\mathscr{I} \times \mathscr{J}$.

La technique peut être prolongée jusqu'à obtenir un produit direct égal au groupe de toutes les classes $\mathscr{G}/\mathscr{R}$ [1]).

---

[1]) Pour les démonstrations et le détail des opérations, on peut consulter les ouvrages déjà cités dans (**26**).

EXEMPLE. — Le tableau IX, qui concerne le corps de discriminant —231, donne la structure du groupe de ses classes d'idéaux; et le détail des calculs qui permettent de l'établir.

Le groupe qui est d'ordre 12 (**31**) est égal au produit direct de deux groupes cycliques, d'ordres 2 et 6, ce qui est une *décomposition minimum*; on a déjà donné un exemple d'une telle structure et de ses diverses réalisations possibles (**26**).

On a pris ici, pour générateurs de ces sous-groupes, les classes définies par les idéaux réduits:

$$\mathbf{J} = (3,\ \theta\text{—}1), \quad \text{double}; \qquad \mathbf{I} = (2,\ \theta\text{—}0), \quad [\mathbf{I}^6 \sim (1)].$$

Devant chaque idéal réduit, on a inscrit le monôme $\mathbf{I}^x \times \mathbf{J}^y$ auquel il est congru —ou égal— ; x prend les valeurs de 0 (sous-entendu) à 5 et y les valeurs 0 (sous-entendu) et 1.

Ceci résulte notamment des considérations et calculs suivants: le groupe d'ordre 12 contient trois éléments d'ordre 2, définis par les idéaux réduits remarquables, différents de (1) (exemple 1 de **31**); il ne peut donc être cyclique, puisqu'un tel groupe ne contient qu'un élément d'ordre 2 égal à la puissance 6 du générateur.

Les idéaux réduits comprennent les deux premières puissances des idéaux conjugués, de norme 2, dont l'un est appelé **I**:

$$\mathbf{I} = (2,\ \theta\text{—}0), \quad \mathbf{I}^2 = (4,\ \theta+2), \quad \mathbf{I}' = (2,\ \theta\text{—}1), \quad \mathbf{I}'^2 = (4,\ \theta\text{—}1).$$

Le cube $\mathbf{I}^3 = (8,\ \theta\text{—}2)$ est encore réduit, mais comme il est réfléchi, il est congru à son conjugué $\mathbf{I}'^3 = (8,\ \theta+3)$; ils définissent une classe commune qui est double, en sorte que la classe définie par **I**, (comme sa conjuguée, définie par **I**′) est d'ordre 6. Cet ordre est d'ailleurs confirmé par la décomposition de $F(2)$:

$$F(2) = F(\text{—}3) = 2^6 \quad \Rightarrow \quad (2,\ \theta\text{—}0)^6 \sim (1).$$

On a ainsi mis en évidence un sous-groupe cyclique $\mathscr{J}$, d'ordre 6, dont les éléments sont les classes définies par les six puissances de **I**:

$$\mathbf{I}, \quad \mathbf{I}^2, \quad \mathbf{I}^3, \quad \mathbf{I}^4 \sim \mathbf{I}'^2, \quad \mathbf{I}^5 \sim \mathbf{I}', \quad \mathbf{I}^6 \sim (1).$$

D'autre part il y a trois sous-groupes cycliques d'ordre 2, formés respectivement de la classe principale, ou (1), et de l'une des classes doubles, définies par les idéaux réduits remarquables:

$$(3,\ \theta\text{—}1), \qquad (7,\ \theta\text{—}3), \qquad (8,\ \theta\text{—}2).$$

Le troisième est sous-groupe de $\mathcal{J}$, les deux premiers en sont *indépendants* (**26**). On obtient le sous-groupe en formant le produit direct de l'un d'eux avec $\mathcal{J}$.

On a choisi le premier, défini par l'idéal de norme 3, désigné par **J**. Les calculs des produits:

$$\mathbf{I}\times\mathbf{J} = (6,\ \theta-2); \qquad \mathbf{I}^2\times\mathbf{J} = (12,\ \theta+2) \sim (5,\ \theta-1),$$

sont indiqués dans la table; le second utilise la décomposition $F(-2) = 5\times 12$. On en déduit les expressions des classes conjuguées:

$$\mathbf{I}'\times\mathbf{J}' \sim \mathbf{I}^5\times\mathbf{J}, \qquad \mathbf{I}'^2\times\mathbf{J}' \sim \mathbf{I}^4\times\mathbf{J}.$$

Le monôme $\mathbf{I}^3\times\mathbf{J}$, congru à son conjugué, est naturellement congru au seul idéal réduit restant, de norme 7, d'ailleurs remarquable. On en a aussi indiqué un calcul de vérification, qui utilise la décomposition adjointe à la table: $F(10 = 7\times 24$.

34. Corps imaginaires principaux.

On va examiner sommairement quelques-unes des circonstances générales, qui peuvent se présenter dans la structure du groupe des classes des idéaux d'un corps imaginaire.

Pour qu'un corps imaginaire soit *principal* (**19**), ou ne contienne que la seule classe principale (groupe des classes d'ordre 1), il faut et il suffit que *l'idéal unité soit le seul idéal réduit.*

Il est équivalent de dire que, la limite r étant calculée par la condition (**25** et **26**):

$$3\,.\,(2x-S)^2 > |D| \quad \Leftrightarrow \quad x > r;$$

les r premières valeurs $F(c)$, du polynôme fondamental $(0 \leqslant c < r)$ *sont toutes des nombres premiers.*

Pour $|D|$ pair, *les seuls corps principaux sont ceux de discriminants* —4 et —8; il n'y a qu'une valeur $F(c)$ à considérer $(r = 1)$, qui est égale, respectivement à 1 et à 2. Pour tout autre corps, l'idéal de norme 2 et de racine minimum 0 ou 1 est réduit double et n'est pas principal.

Pour $|D|$ *impair*, il est nécessaire que ce soit un nombre premier, si non sa décomposition, non triviale, entraînerait l'existence d'au moins un idéal réduit remarquable, différent de (1)

(double ou réfléchi) (**29**), donc d'une classe double, non principale.

Le tableau XI suivant donne les *sept corps imaginaires principaux*, qui sont connus et, pour chacun d'eux, les r valeurs de leur polynôme fondamental qui sont, comme il vient d'être dit, des nombres premiers. Le polynôme x^2+x+41 a déjà été indiqué comme générateur d'une suite de nombres premiers (**28**); il en est de même des polynômes, de discriminants —43 et —67, qui donnent respectivement des suites de 10 et 16 nombres premiers.

TABLEAU XI.

Corps imaginaires principaux.

Discriminant impair.

$D =$	—3	—7	—11	—19	—43	—67	—163
$r =$	1	1	1	1	2	2	4
$F(0) = N =$	1	2	3	5	11	17	41
$F(1) =$	.....				13	19	43
$F(2) =$	.....						47
$F(3) =$	.....						53

pair.

$D =$	—4	—8
$r =$	1	1
$F(0) = N$	1	2

On peut établir méthodiquement l'existence de ces corps principaux et vérifier qu'il n'y en a pas d'autre, au moins jusqu'à une valeur relativement grande de $|D|$ par les considérations suivantes.

On peut d'abord comparer $|D|$ aux nombres premiers successifs:

$$p_0 = 1,\ p_1 = 2,\ p_2 = 3,\ \ldots\ p_i,\ \ldots$$

Un corps, de discriminant $|D|$, *compris entre:*

$$3p_k^2 \leqslant |D| < 3p_{k+1}^2\ ,$$

est principal, si et seulement si *D n'est pas congru à un carré* —ou n'est pas résidu quadratique— *relativement aux k premiers nombres premiers* (i de 1 à k).

La condition est *nécessaire*: le corps n'ayant pas d'idéal premier réduit, en dehors de (1), donc de norme p_i antérieur à p_{k+1}, la congruence fondamentale doit être impossible pour chacun des nombres premiers p_i.

La condition est *suffisante*: si elle est remplie, il n'y a aucun idéal réduit, différent de (1), car son existence entraînerait celle d'au moins un idéal premier réduit (**32**).

Les valeurs absolues $|D|$. des discriminants qui ne sont pas congrus à un carré, relativement aux nombres premiers successifs, de 2 à p_i, appartiennent à des *progressions arithmétiques*:

de raison: $4P$; $P = 1\times 2\times \ldots \times p_k = \Pi p_i$; ($i$ de 0 à k);

en nombre: $\varphi(4P) : 2^{k+1} = (3-1)\times \ldots \times (p_k-1) : 2^{k-1}$.

Leur détermination peut se faire de proche en proche, en cherchant, pour les valeurs successives de p_i, les valeurs de $|D|$, pour lesquelles D est un discriminant, non congru à un carré; puis en conjuguant les systèmes successifs de relations ainsi formées. On obtient ainsi:

	successivement:		collectivement:	
	$\|D\| \equiv$, mod.:		$\|D\| \equiv$, mod.:	
(1)	3	4		
(2)	3	8	3	8
(3)	1	3	19	$8\times 3 = 24$
(4)	2, ou 3	5	43, ou 67	$24\times 5 = 120$
(5)	3, ou 5, ou 6	7	ou 43, ou 163, ou 403 67, ou 547, ou 667	$120\times 7 = 840$

La condition (1) exprime seulement que D est un discriminant. La condition (6) suivante exprimerait que $|D|$ est congru à:

2, ou 6, ou 7, ou 8, ou 10; (mod. 11);

sa conjonction avec les précédentes conditions exprimerait que $|D|$ est congru, à l'un des trente nombres:

883, 3403, 5083, 5923, 6763; 163, 3523, 6043, 7723, 8563;
2083, 3763, 4603, 5443, 8803; 67, 907, 1747, 5107, 7627;
1387, 2227, 3067, 6427, 8947; 2347, 4027, 4867, 5707, 9067;
(mod. 9240).

En rapprochant la limitation de $|D|$ et son appartenance aux progressions, on obtient les résultats suivants:

$$k = 0; \quad 3 \leqslant |D| < 3\times 2^2 = 12; \quad |D| = 3+4\lambda;$$

les seuls nombres premiers vérifiant ces conditions sont:

$$\mathbf{3}, \quad 3+4 = \mathbf{7}, \quad 3+4\times 2 = \mathbf{11};$$

ce sont les trois premières valeurs du tableau XI.

$$k = 1; \quad 12 \leqslant |D| < 3\times 3^2 = 27; \quad |D| = 3+8\lambda;$$

le seul nombre premier vérifiant ces conditions est:

$$3 + 8\times 2 = \mathbf{19}; \quad \text{quatrième valeur du tableau.}$$

$$k = 2; \quad 27 \leqslant |D| < 3\times 5^2 = 75; \quad |D| = 19+24\lambda;$$

les seuls nombres premiers vérifiant ces conditions sont:

$$19+24 = \mathbf{43}, \quad 19+24\times 2 = \mathbf{67};$$

ce sont les cinquième et sixième valeurs du tableau XI.

$k = 3$; $75 \leqslant |D| < 3\times 7^2 = 147$ $43 + 120\lambda$ ou $67+120\lambda$

aucun nombre premier ne remplit ces conditions.

$$k = 5; \quad 147 \leqslant |D| < 3\times 11^2 = 363;$$

et $|D|$ doit appartenir à une des six progressions indiquées de raison 840. Il n'y a qu'un nombre premier vérifiant ces conditions:

$$\mathbf{163}, \quad \text{dernière valeur du tableau.}$$

$$k = 6; \quad 363 \leqslant |D| < 3\times 13^2 = 507;$$

aucun nombre premier des trois progressions, mod. 9240, ne vérifie cette limitation.

TABLEAU XII.

Corps imaginaires de discriminant premier.

$D = -263$; $r = 5$

c	$F(c)$
−5	$86 = 2\times 43$
−4	$78 = 2\times 3\times 13$
−3	$72 = 2^3\times 3^2$ $(\mathbf{8},\ \theta+3) \sim \mathbf{I}^{10}$ $(\mathbf{6},\ \theta+3) \sim \mathbf{I}^{7}$
−2	$68 = 2^2\times 17$ $(\mathbf{4},\ \theta+2) = \mathbf{I}^{2}$
−1	$66 = 2\times 3\times 11 = 6\times 11$ $(\mathbf{6},\ \theta+1) \sim \mathbf{I}^{4}$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{5}$ $(\mathbf{2},\ \theta+1) \sim \mathbf{I}^{12}$
0	$66 = 2\times 3\times 11 = 11\times \mathbf{6}$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) = \mathbf{I}$ $(\mathbf{3},\ \theta-0) \sim \mathbf{I}^{8}$ $(\mathbf{6},\ \theta-0) \sim \mathbf{I}^{9}$
+1	$68 = 2^2\times 17$ $(\mathbf{4},\ \theta-1) \sim \mathbf{I}^{11}$
+2	$72 = 2^3\times 3^2$ $(\mathbf{6},\ \theta-2) \sim \mathbf{I}^{6}$ $(\mathbf{8},\ \theta-2) = \mathbf{I}^{3}$
+3	$78 = 2\times 3\times 13$
+4	$86 = 2\times 43$
...	
10	$176 = 2^4\times \mathbf{11}$

Ordre 13

$D = -439$; $r = 6$

c	$F(c)$
−6	$140 = 2^2\times 5\times 7$
−5	$130 = 2\times 5\times 13$ $(\mathbf{10},\ \theta+5) \sim \mathbf{I}^{5}$
−4	$122 = 2\times 61$
−3	$116 = 2^2\times 29$
−2	$112 = 2^4\times \mathbf{7}$ $(\mathbf{8},\ \theta+2) = \mathbf{I}^{3}$ $(\mathbf{7},\ \theta+2) \sim \mathbf{I}^{11}$ $(\mathbf{4},\ \theta+2) = \mathbf{I}^{2}$
−1	$110 = 2\times 5\times 11$ $(\mathbf{10},\ \theta+1) \sim \mathbf{I}^{8}$ $(\mathbf{5},\ \theta+1) \sim \mathbf{I}^{9}$ $(\mathbf{2},\ \theta+1) \sim \mathbf{I}^{14}$
0	$110 = 2\times 5\times 11$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) = \mathbf{I}$ $(\mathbf{5},\ \theta-0) \sim \mathbf{I}^{6}$ $(\mathbf{10},\ \theta-0) \sim \mathbf{I}^{7}$
+1	$112 = 2^4\times 7$ $(\mathbf{4},\ \theta-1) \sim \mathbf{I}^{13}$ $(\mathbf{7},\ \theta-1) \sim \mathbf{I}^{4}$ $(\mathbf{8},\ \theta-1) \sim \mathbf{I}^{12}$
+2	$116 = 2^2\times 29$
+3	$122 = 2\times 61$
+4	$130 = 2\times 5\times 13$ $(\mathbf{10},\ \theta-4) \sim \mathbf{I}^{10}$
+5	$140 = 2^2\times 5\times 7$
...	
14	$320 = 2^6\times \mathbf{5} = 2^5\times \mathbf{10}$

Ordre 15

$D = -419$; $r = 6$

c	$F(c)$
−6	$135 = 3^3\times \mathbf{5}$
−5	$125 = 5^3$
−4	$117 = 3^2\times 13$ $(\mathbf{9},\ \theta+4) \sim \mathbf{I}^{7}$
−3	$111 = 3\times 37$
−2	107
−1	$105 = 3\times 5\times 7$ $(\mathbf{7},\ \theta+1) \sim \mathbf{I}^{4}$ $(\mathbf{5},\ \theta+1) \sim \mathbf{I}^{6}$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{8}$
0	$105 = 3\times 5\times 7 = 15\times \mathbf{7}$ $(\mathbf{1},\ \theta-0 = (1)$ $(\mathbf{3},\ \theta-0) = \mathbf{I}$ $(\mathbf{5},\ \theta-0) \sim \mathbf{I}^{3}$ $(\mathbf{7},\ \theta-0) \sim \mathbf{I}^{5}$
+1	107
+2	$111 = 3\times 37$
+3	$117 = 3^2\times 13$ $(\mathbf{9},\ \theta-3) = \mathbf{I}^{2}$
+4	$125 = 5^3$
+5	$135 = 3^3\times 5$

Ordre 9

Calcul des idéaux réduits

congrus aux puissances de l'idéal générateur.

$D = -263$; 13 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{2},\ \theta-0)$, $\mathbf{I}^{12} \sim (\mathbf{2},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{4},\ \theta+2)$, $\mathbf{I}^{11} \sim (\mathbf{4},\ \theta-1)$;

$\mathbf{I}^3 = (\mathbf{8},\ \theta-2)$, $\mathbf{I}^{10} \sim (\mathbf{8},\ \theta+3)$;

$\mathbf{I}^4 = (2^4,\ \theta-10) \sim (11, \theta+11)$ [$F(10)$]

$= (11,\ \theta-0) \sim (\mathbf{6},\ \theta+1)$, $\mathbf{I}^9 \sim (\mathbf{6},\ \theta-0)$; [$F(0)$]

$\mathbf{I}^5 = \mathbf{I}^4 \times \mathbf{I} \sim (\mathbf{6},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (2) \times (\mathbf{3},\ \theta+1)$, $\mathbf{I}^8 \sim (\mathbf{3},\ \theta-0)$;

$\mathbf{I}^6 = \mathbf{I}^5 \times \mathbf{I} \sim (\mathbf{3},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (\mathbf{6},\ \theta-2)$, $\mathbf{I}^7 \sim (\mathbf{6},\ \theta+3)$;

$D = -439$; 15 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{2},\ \theta-0)$, $\mathbf{I}^{14} \sim (\mathbf{2},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{4},\ \theta+2)$, $\mathbf{I}^{13} \sim (\mathbf{4},\ \theta-1)$;

$\mathbf{I}^3 = (\mathbf{8},\ \theta+2)$, $\mathbf{I}^{12} \sim (\mathbf{8},\ \theta-1)$;

$\mathbf{I}^4 = (2^4,\ \theta+2) \sim (\mathbf{7},\ \theta-1)$, $\mathbf{I}^{11} \sim (\mathbf{7},\ \theta+2)$; [$F(-2)$]

$\mathbf{I}^5 = (2^5,\ \theta-14) \sim (10,\ \theta+15) = (\mathbf{10},\ \theta+5)$, $\mathbf{I}^{10} \sim (\mathbf{10},\ \theta-4)$; [$F(14)$]

$\mathbf{I}^6 = (2^6,\ \theta-14) \sim (\mathbf{5},\ \theta+15) = (\mathbf{5},\ \theta-0)$, $\mathbf{I}^9 \sim (\mathbf{5},\ \theta+1)$; [$F(14)$]

$\mathbf{I}^7 = \mathbf{I}^6 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{2},\ \theta-0) = (\mathbf{10},\ \theta-0)$, $\mathbf{I}^8 \sim (\mathbf{10},\ \theta+1)$;

$D = -419$; 9 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{3},\ \theta-0)$, $\mathbf{I}^8 \sim (\mathbf{3},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{9},\ \theta-3)$, $\mathbf{I}^7 \sim (\mathbf{9},\ \theta+4)$;

$\mathbf{I}^3 = (3^3,\ \theta+6) \sim (\mathbf{5},\ \theta-0)$, $\mathbf{I}^6 \sim (\mathbf{5},\ \theta+1)$; [$F(-6)$]

$\mathbf{I}^4 = \mathbf{I}^3 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{3},\ \theta-0) = (15, \theta-0)$

$\sim (\mathbf{7},\ \theta+1)$, $\mathbf{I}^5 \sim (\mathbf{7}, \theta-0)$; [$F(0)$]

$$k = 7; \quad 507 \leqslant |D| < 3 \times 17^2 = 867;$$

cette limitation n'est vérifiée par aucun nombre des trente progressions donc, à fortiori par aucun des $30 \times 6 = 180$ progressions construites en adjoignant une condition, mod. 13.

Au lieu de continuer ce raisonnement, on peut étudier directement les nombres premiers contenus dans les trente progressions, limités, par exemple à 100.000. Un calcul de congruences permet d'éliminer ceux qui sont congrus à un carré, mod. 13 ou mod. 17. Pour ceux qui restent, la construction directe des corps qui les admettent comme discriminants, montre qu'ils ne sont pas principaux.

35. Corps imaginaires, de discriminant premier.

On a signalé ci-dessus (**34**) que les corps, de discriminant (négatif) premier, sont les seuls, pour lesquels *l'idéal unité est l'unique idéal réduit* remarquable. Les classes contiennent donc, en plus de la classe principale, des couples de classes conjuguées; *l'ordre g du groupe des classes est un nombre impair*; il est égal à 1 pour les sept corps principaux indiqués.

Ce groupe des classes peut être *cyclique*; il en est toujours ainsi si son ordre g est *premier*, ou *produit de nombres premiers différents* —ou sans facteur carré— .

Dans les trois exemples du *tableau XII*, le groupe des classes est *cyclique*. Pour chacun d'eux, on a dressé les valeurs de $F(c)$ pour c inférieur au rang r; pour des raisons de clarté, on a prolongé le tableau en deçà de 0, de façon à indiquer les idéaux réduits devant leur racine minimum.

On a choisi un idéal réduit (convenable) désigné par **I**; définissant une classe génératrice du groupe. Devant chaque idéal réduit, on a indiqué à quelle puissance de **I**, il est congru, ou éventuellement égal. Les calculs sont détaillés en face; on a indiqué simultanément les idéaux réduits congrus aux classes inverses, —ou d'exposants opposés— .

Dans le *premier exemple*, le nombre de classes est premier, le groupe est cyclique et on peut choisir arbitrairement un générateur. On a utilisé l'idéal de norme 2, dont le tableau donne immédiatement

Tableau XIII.

Répartition des *corps quadratiques imaginaires* de discriminant D premier (négatif, congru à $+1$, mod. 4)

d'après le nombre de leurs *classes d'ideaux* (ordre du groupe).

Ordre	$\|D\|$
1	3, 7, 11, 19, 43, 67, 163. (Corps principaux.)
3	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 883, 907.
5	47, 79, 103, 127, 131, 179, 227, 347, 443, 523, 571, 619, 643, 683, 691, 739, 787, 947.
7	71, 151, 223, 251, 463, 467, 487, 587, 811, 827, 859.
9	199, 367, 419, 491, 563, 823.
11	167, 271, 659, 967.
13	191, 263, 607, 631, 727.
15	239, 439, 751, 971.
17	383, 991.
19	311, 359, 919.
21	431, 503, 743, 863.
23	647.
25	479, 599.
27	983.
29	887.
31	719, 911.
33	839.

les idéaux réduits égaux aux trois premières puissances de cet idéal et de son conjugué.

Dans le *deuxième exemple*, le nombre de classes est $15 = 3 \times 5$, nombre composé sans facteur carré. Le groupe est cyclique, mais on ne peut choisir arbitrairement le générateur. Le tableau donne immédiatement le cube de $\mathbf{I} = (\mathbf{2}, \theta - 0)$, qui n'est pas congru à 1. La décomposition de $F(14)$, formé pour étudier la puissance d'exposant 5 de **I**, montre qu'elle n'est pas non plus congrue à (1). On peut donc prendre comme générateur la classe définie par **I**, qui, n'étant pas d'ordre 3 ou 5, est d'ordre 15.

Dans le *troisième exemple*, il y a neuf classes et le groupe pourrait être un produit direct de deux groupes cycliques d'ordre 3. Mais la décomposition de $F(-6)$ montre que le cube de l'idéal $\mathbf{I} = (\mathbf{3}, \theta - 0)$ n'est pas congru à (1); il définit une classe qui, n'étant pas d'ordre 3, est d'ordre 9 et peut être prise comme générateur.

On constate que, pour tous les corps quadratiques imaginaires, dont *le discriminant est un nombre premier, inférieur à* 1000, le groupe des classes d'idéaux est *cyclique.* On donne ci-dessous le tableau XIII de leur répartition, d'après l'ordre du groupe.

On remarquera que, pour les groupes dont l'ordre est un carré (six groupes d'ordre 9 et deux groupes d'ordre 25), il convient de vérifier qu'ils sont bien cycliques, alors que pour les autres, cette qualité résulte de la seule nature arithmétique de leur ordre (nombre premier, ou produit de nombres premiers différents). Cette vérification a été explicitement indiquée dans le troisième exemple du tableau XII, concernant le corps de discriminant —419, qui comprend neuf classes d'idéaux.

La complexité de la structure paraît bien augmenter avec la grandeur du discriminant: il semble que ce soit seulement pour des valeurs relativement grandes (de sa valeur absolue) qu'il existe des groupes de classes non cycliques. Un exemple en est donné dans le tableau XIV, qui concerne le corps de discriminant premier —12 451.

L'exemple comprend, comme pour les précédents, une table des valeurs du polynôme fondamental $F(x)$, limitée toutefois aux valeurs

TABLEAU XIV.

Structure d'un groupe de classes d'idéaux.

$F(x) = x^5+x+3\,113$; $D = -12\,451$; $r = 32$.

0	$3\,113 = 11\times283$ $(\mathbf{1}, \theta-0) = (1)$ $(\mathbf{11}, \theta-0) \sim \mathbf{I}^3\times\mathbf{J}^3$
1	$3\,115 = 5\times7\times89$ $(\mathbf{5}, \theta-1) = \mathbf{I}$ $(\mathbf{7}, \theta-1) = \mathbf{J}$ $(\mathbf{35}, \theta-1) = \mathbf{I}\times\mathbf{J}$
2	$3\,119$
3	$3\,125 = 5^5 = 5^3\times\mathbf{25}$ $(\mathbf{25}, \theta-3) \sim \mathbf{I}^3$
4	$3\,133 = 13\times241$ $(\mathbf{13}, \theta-4) \sim \mathbf{I}^4\times\mathbf{J}^2$
5	$3\,143 = 7\times449$
6	$3\,155 = 5\times631$
7	$3\,169$
8	$3\,185 = (5\times7^2)\times\mathbf{13} = 65\times\mathbf{49}$ $(\mathbf{35}, \theta-8) \sim \mathbf{I}^4\times\mathbf{J}$ $(\mathbf{49}, \theta-8) = \mathbf{J}^2$
9	$3\,203$
10	$3\,223 = 11\times293$
11	$3\,245 = 5\times11\times59 = 59\times\mathbf{55}$ $(\mathbf{55}, \theta-11) \sim \mathbf{I}^4\times\mathbf{J}^3$
12	$3\,269 = 7\times467$
13	$3\,295 = 5\times659$
14	$3\,323$
15	$3\,353 = 7\times479$
16	$3\,385 = 5\times677$
17	$3\,419 = 13\times263$
18	$3\,455 = 5\times691$
19	$3\,493 = 7\times499$
20	$3\,533$
21	$3\,575 = 5^2\times11\times13 = 65\times\mathbf{55}$ $(\mathbf{55}, \theta-21) \sim \mathbf{I}^3\times\mathbf{J}^2$
22	$3\,619 = 7\times11\times47 = (7\times47)\times\mathbf{11}$ $(\mathbf{47}, \theta-22) \sim \mathbf{I}^2\times\mathbf{J}$
23	$3\,665 = 5\times733$
24	$3\,713 = 47\times79$
25	$3\,763 = 53\times71$ $(\mathbf{53}, \theta-25) \sim \mathbf{I}^2\times\mathbf{J}^4$
26	$3\,815 = 5\times7\times109$
27	$3\,869 = 53\times73$
28	$3\,925 = 5^2\times157$
29	$3\,983 = 7\times569$
30	$4\,043 = 13\times311$
31	$4\,105 = 5\times821$

$F(71) = 7\,225 = (5^2\times7)\times\mathbf{47}$
$F(-79) = F(78) = 9\,275 = (5^2\times7)\times\mathbf{55}$
$F(106) = 14\,455 = (5\times7^2)\times\mathbf{59}$
$F(-139) = F(138) = 22\,295 = 7^3\times\mathbf{65}$

entières de x, entre 0 et la limite r. Elle est complétée sur la page, de face, par une *table de Pythagore, de la multiplication des classes*, caractérisées par les idéaux réduits, et par un *détail des calculs* de sa construction.

Dans ce détail, les couples d'idéaux réduits conjugués, écrits avec leurs racines minimum (de somme —1), ont leurs normes en caractères gras, pour les distinguer des idéaux servant d'intermédiaires. Par contre, dans la table de multiplication cette distinction d'écriture a été conservée aux seuls idéaux réduits, de racine minimum non négative et ce sont les seuls qui ont été inscrits dans la table des valeurs, en face de leur racine.

Les monômes $\mathbf{I}^x \times \mathbf{J}^y$ (x,y prenant les valeurs de 0, sous-entendu à 4), inscrits dans la table des valeurs et dans celle de multiplication, montrent que le groupe des classes est un *produit direct* (**26**) *de deux sous-groupes cycliques*, d'ordre 5, pour lesquels on peut prendre pour générateurs respectifs, les classes définies par les idéaux réduits de normes 5 et 7, notés **I** et **J**.

Pour les calculs l'ordre adopté est le suivant: la décomposition $F(3) = F(-4) = 5^5$, montre que les idéaux réduits, conjugués, de norme 5 ont leur puissance, d'exposant 5, congrue à (1). Les classes définies par les quatre idéaux réduits de normes 5 et 25, avec la classe (1) constituent par suite un *sous-groupe cyclique, d'ordre 5.*

Le calcul du cube $\mathbf{J}^3$, de l'idéal $\mathbf{J} = (7,\ \theta-1)$ montre qu'il est congru au carré $\mathbf{J}^{12}$, de son idéal conjugué $\mathbf{J}' = (7, \theta+2)$. Il en résulte que les puissances d'exposant 5, de **J** et $\mathbf{J}'$ (ainsi que de leurs carrés) sont aussi congrues à (1). Les quatre idéaux, de forme 7 et 49, définissent des classes, qui avec la classe (1) forment *un sous-groupe cyclique, d'ordre* 5, *indépendant du précédent* [sans élément commun, sauf (1)]. Le *produit direct de ces deux sous-groupes cyliques*, qui a vingt-cinq éléments, *est donc égal au groupe*, dont il est une décomposition minimum (**26**).

On a calculé ensuite les produits $\mathbf{I} \times \mathbf{J}$ et $\mathbf{I} \times \mathbf{J}^4$ (en remplaçant $\mathbf{J}^4$ par l'idéal réduit congru $\mathbf{J}'$, conjugué de **J**). Leurs expressions obtenues par un calcul de congruences arithmétiques sont directement dans la table des valeurs.

Pour les autres produits, on passe par des idéaux intermédiaires dont les décompositions de valeurs de $F(x)$, permettent comme il a été dit, de trouver des idéaux congrus, de norme inférieure. En fait,

TABLE DE PYTHAGORE

DE MULTIPLICATION DES CLASSES D'IDÉAUX

(Produit direct de 2 sous-groupes cycliques d'ordre 5).

	$\mathbf{J}^5 \sim (1)$	$\mathbf{J}$	$\mathbf{J}^2$	$\mathbf{J}^3$	$\mathbf{J}^4$
$\mathbf{I}^5 \sim (1)$	(1)	(**7**, θ—1)	(**49**, θ—8)	(49, θ+9)	(7, θ+2)
$\mathbf{I}$	(**5**, θ—1)	(**35**, θ—1)	(55, θ+12)	(13, θ+5)	(35, θ+9)
$\mathbf{I}^2$	(25, θ+4)	(**47**, θ—22)	(11, θ+1)	(55, θ+22)	(**53**, θ—25)
$\mathbf{I}^3$	(**25**, θ—3)	(53, θ+26)	(**55**, θ—21)	(**11**, θ—0)	(47, θ+23)
$\mathbf{I}^4$	(5, θ+2)	(**35**, θ—8)	(**13**, θ—4)	(**55**, θ—11)	(35, θ+2)

CALCULS

$\mathbf{J}^3 = (\mathbf{7},\ \theta—1)^3 = (7^3,\ \theta+139) \sim (65,\ \theta—138) = (65,\ \theta—8)$ $F(—139)$

$\sim (\mathbf{49},\ \theta+9) = (\mathbf{7},\ \theta+2)^2;$ $F(8)$

$\mathbf{I} \times \mathbf{J} = (\mathbf{5},\ \theta—1) \times (\mathbf{7},\ \theta—1) = (\mathbf{35},\ \theta—1);$

$\mathbf{I} \times \mathbf{J}^4 \sim (\mathbf{5},\ \theta—1) \times (\mathbf{7},\ \theta+2) = (\mathbf{35},\ \theta+9);$

$\mathbf{I} \times \mathbf{J}^2 = (\mathbf{5},\ \theta—1) \times (\mathbf{49},\ \theta—8) = (5 \times 7^2,\ \theta—106) \sim (59,\ \theta+107)$ $F(106)$

$= (59,\ \theta—11) \sim (\mathbf{55},\ \theta+12);$

$\mathbf{I} \times \mathbf{J}^3 \sim (\mathbf{5},\ \theta—1) \times (\mathbf{49},\ \theta+9) = (5 \times 7^2,\ \theta+9) \sim (13,\ \theta—8)$ $F(—9)$

$= (\mathbf{13},\ \theta+5);$ $F(11)$

$\mathbf{I}^2 \times \mathbf{J} \sim (\mathbf{7},\ \theta—1) \times (\mathbf{25},\ \theta+4) = (7 \times 5^2,\ \theta—71) \sim (47,\ \theta+72)$ $F(71)$

$= (\mathbf{47},\ \theta—22);$

$\mathbf{I}^2 \times \mathbf{J}^4 \sim (\mathbf{7},\ \theta+1) \times (\mathbf{25},\ \theta+4) = (7 \times 5^2,\ \theta+79) \sim (53,\ \theta—78)$ $F(—79)$

$= (\mathbf{53},\ \theta—25);$

$\mathbf{I}^2 \times \mathbf{J}^2 \sim (\mathbf{7},\ \theta—1) \times (\mathbf{47},\ \theta—22) = (7 \times 47,\ \theta—22) \sim (11,\ \theta+23)$ $F(22)$

$= (\mathbf{11},\ \theta+1);$

$\mathbf{I}^3 \times \mathbf{J}^2 \sim (\mathbf{5},\ \theta—1) \times (\mathbf{11},\ \theta+1) = (\mathbf{55},\ \theta—21);$

au cours des déterminations successives, on a remplacé certains produits par des idéaux congrus, déjà calculés:

$$\mathbf{I}\times\mathbf{J}^3 \text{ par } \mathbf{I}\times\mathbf{J}'^2;\quad \mathbf{J}^4 \text{ par } \mathbf{J}';\quad \mathbf{I}^2\times\mathbf{J}^2 \text{ par } \mathbf{J}\times(\mathbf{I}^2\times\mathbf{J});$$
$$\mathbf{I}^3\times\mathbf{J}^2 \text{ par } \mathbf{I}\times(\mathbf{I}^2\times\mathbf{J}^2).$$

On aurait aussi bien pu faire des calculs, en apparence plus directs. Par exemple un calcul de congruences arithmétiques donne:

$$\mathbf{I}^2\times\mathbf{J}^2 = (25,\ \theta+4)\times(49,\ \theta-8) = (25\times 49,\ \theta-596).$$

La décomposition de $F(596)$ donne la congruence:

$$F(596) = 358\,925 = (25\times 49)\times 293 \Rightarrow \mathbf{I}^2\times\mathbf{J}^2 \sim (293,\ \theta-597).$$

Dans ce dernier idéal la racine minimum est -11; la décomposition de $F(-11) = F(10)$ donne alors la congruence:

$$F(-11) = 3\,223 = 293\times 11 \Rightarrow \mathbf{I}^2\times\mathbf{J}^2 \sim (11,\ \theta-10) = (11,\ \theta+1).$$

36. Corps imaginaires dont le discriminant a deux facteurs premiers.

Dans un corps quadratique imaginaire, *le groupe*, des classes d'idéaux, *ne contient qu'un seul élément d'ordre* 2, qui est une classe double, définie par un idéal réduit remarquable, si et seulement si *le discriminant n'a que deux facteurs premiers différents*, dont l'un peut être 2, à l'exposant 2 ou 3.

S'il en est ainsi *l'ordre du groupe* —ou le nombre des classes— *est pair.*

Si cet ordre n'a pas de facteur carré impair —ou est de la forme:

$2^h\times P;\quad h \geqslant 0;$

P produit de nombres premiers impairs différents—

le groupe est cyclique.

La première propriété résulte du théorème d'existence des idéaux réduits remarquables (**30**). L'élément double unique est la classe définie, suivant les cas, par un idéal: double, ou réfléchi, de norme impaire (si $|D|$ est impair); double, de norme 2, si $|D|$ est pair.

En plus des deux classes, unité et double, il peut y avoir éventuellement des couples de classes conjuguées inégales, donc en tout un nombre pair.

Si un groupe, dont l'ordre est de la forme indiquée, n'est pas cyclique, il a une décomposition minimum en un produit de deux groupes cycliques, de générateurs **I** et **J**, dont les ordres, l'un étant diviseur de l'autre sont nécessairement:

$$m = 2^u, \quad n = 2^v \times P; \quad 0 < u \leqslant v;$$

il contiendrait alors au moins deux éléments d'ordre 2:

$$\mathbf{I}^{m:2} \quad \mathbf{J}^{n:2};$$

ce ne peut donc être un groupe de classes de l'un des corps envisagés.

Le tableau XV, disposé comme le tableau XII, donne trois exemples de corps, dont le discriminant a deux facteurs premiers et dont le groupe de classes d'idéaux est cyclique. Pour chacun d'eux on a précisé la structure du groupe, en indiquant, pour chaque idéal réduit, sa congruence avec la puissance de l'un d'entre eux **I**, choisi (convenablement) pour définir une classe génératrice du groupe cyclique. On a limité à cette indication le prolongement de la table des valeurs en deça de O. On a aussi transcrit un sommaire des calculs qui établissent cette structure.

Pour le *premier exemple*, la décomposition du discriminant (impair) $-299 = 13 \times (-23)$ entraîne l'existence d'un *idéal réduit réfléchi*, —congru à son conjugué— :

$$F(2) = 9^2 \quad (\mathbf{9}, \quad \theta - 2) \sim (9, \theta + 3).$$

Il y a, d'autre part trois couples d'idéaux réduits conjugués, donc *huit classes*; leur groupe est cyclique, en raison de la remarque générale précédente (l'ordre n'a pas de facteur carré impair).

La table donne immédiatement des valeurs des idéaux conjugués **I** et **I'**, de *norme 5* (de racines minimum 0 et —1), qui sont réduits et de leurs carrés, de *norme 25* et de mêmes racines, qui ne sont pas réduits. La décomposition de $F(0) = 3^4 \times \mathbf{3}$ montre que ces carrés sont congrus aux idéaux réduits, de *norme 3*, de racines —1 et 0.

Tableau XV.

Exemples de corps imaginaires dont le discriminant a deux facteurs premiers.

$D = -299 = 13\times(-23)$ $r = 5$; ordre **8**	
-2	$(\mathbf{7},\ \theta+2) \sim \mathbf{I}^5$
-1	$(\mathbf{5},\ \theta+1) \sim \mathbf{I}^7$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^2$
0	$75 = 5^2\times\mathbf{3}$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{3},\ \theta-0) \sim \mathbf{I}^6$ $(\mathbf{5},\ \theta-0) = \mathbf{I}$
$+1$	$77 = 7\times11$ $(\mathbf{7},\ \theta-1) \sim \mathbf{I}^3$
$+2$	$81 = 3^4 = 9^2$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^4$
$+3$	$87 = 3\times29$
$+4$	$95 = 5\times19$
$+5$	$107 = 15\times\mathbf{7}$

$\mathbf{I}^2 = (5^2,\ \theta-0) \sim (\mathbf{3},\ \theta+1);\ [F(0)]$
$\mathbf{I}^8 \sim (\mathbf{3},\ \theta+1)^4 \sim (1);\ [F(2)]$
$\mathbf{I}^2\times\mathbf{I} \sim (15,\ \theta-5) \sim (\mathbf{7},\ \theta-1),\ [F(5)]$

$D = -404 = (-4)\times101$ $r = 6$; ordre **14**	
-4	$(\mathbf{9},\ \theta+4) \sim \mathbf{I}^{12}$
-3	$(\mathbf{10},\ \theta+3) \sim \mathbf{I}^3$
-2	$(\mathbf{7},\ \theta+2) \sim \mathbf{I}^9$ $(\mathbf{5},\ \theta+2) \sim \mathbf{I}^4$
-1	$(\mathbf{6},\ \theta+1) \sim \mathbf{I}^6$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{13}$
0	101 $(\mathbf{1},\ \theta-0) = (1)$
$+1$	$102 = 2\times3\times17$ $(\mathbf{2},\ \theta-1) \sim \mathbf{I}^7$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$ $(\mathbf{6},\ \theta-1) \sim \mathbf{I}^8$
$+2$	$105 = (3\times5)\times\mathbf{7}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^{10}$ $(\mathbf{7},\ \theta-2) \sim \mathbf{I}^5$
$+3$	$110 = 2\times5\times11$ $(\mathbf{10},\ \theta-3) \sim \mathbf{I}^{11}$
$+4$	$117 = 3^2\times13$ $(\mathbf{9},\ \theta-4) = \mathbf{I}^2$
$+5$	$122 = 2\times61$
$+7$	$150 = 30\times\mathbf{5}$
$+13$	$270 = 27\times\mathbf{10}$

$D = -344 = 8\times(-43)$ $r = 6$; ordre **10**	
-2	$(\mathbf{9},\ \theta+2) = \mathbf{I}^2$ $(\mathbf{6},\ \theta+2) \sim \mathbf{I}^6$ $(\mathbf{5},\ \theta+2) \sim \mathbf{I}^3$
-1	$(\mathbf{3},\ \theta+1) \sim \mathbf{I}^9$
0	$86 = 2\times43$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) \sim \mathbf{I}^5$
$+1$	$87 = 3\times29$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$
$+2$	$90 = (3^2\times5)\times\mathbf{2}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^7$ $(\mathbf{6},\ \theta-2) \sim \mathbf{I}^4$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^8$
$+3$	$95 = 5\times19$
$+4$	$102 = 2\times3\times17$
$+5$	$111 = 3\times37$
$+7$	$135 = 27\times\mathbf{5}$

$\mathbf{I}^3 = (3^3,\ \theta-7) \sim (\mathbf{5},\ \theta+2);\ [F(7)]$
$\mathbf{I}^3\times\mathbf{I}^2 \sim (45,\ \theta+2) \sim (\mathbf{2},\ \theta-0)\ [F(2)]$

$\mathbf{I}^3 = (3^3,\ \theta-13) \sim (\mathbf{10},\ \theta+3);\ [F(13)]$
$\mathbf{I}^3\times\mathbf{I} \sim (30,\ \theta-7) \sim (\mathbf{5},\ \theta+2);\ [F(7)]$
$\mathbf{I}^3\times\mathbf{I}^2 \sim (\mathbf{2},\ \theta-0)$

La décomposition de $F(2) = 3^4$ montre que ces idéaux ont leur puissance d'exposant 4, congrue à (1). Il en résulte que les classes définies par **I**, ou **I**′ sont d'*ordre 8* et peuvent (chacune) servir de générateur au groupe cyclique, qui a le même ordre. Ces considérations donnent les puissances de **I** qui sont congrues aux idéaux, de *normes 5, 3, 9* (idéal réfléchi). Les produits des idéaux, de normes 3 et 5 (congrus à $\mathbf{I}^2$ et **I**, et à leurs conjugués respectifs) donnent des idéaux de *norme 15* et de racines 5 et —6. La décomposition $F(5) = 15 \times \mathbf{7}$, adjointe à la table montre qu'ils sont congrus aux idéaux réduits de *norme 7*.

Dans le *deuxième exemple*, l'idéal de norme 2 est *réduit double* et il y a six couples d'idéaux réduits conjugués; en tout *quatorze classes*; leur groupe est cyclique, pour la même raison.

La table des valeurs donne immédiatement les couples d'idéaux conjugués réduits **I** et **I**′, de *norme 3* et de racines (minimum) 1 et —1 ainsi que leurs carrés, de *norme 9* et de racines 4 et —4. Un calcul de congruence arithmétique (**15**) donne la forme canonique de leurs cubes, de *norme 27* et de racines 13 et —13. La décomposition de $F(13) = 27 \times \mathbf{10}$, dont la valeur est adjointe à la table, montre que ces cubes sont congrus aux idéaux de *norme 10* et de racines —3 et 3.

En multipliant ces idéaux par ceux de norme 3, on obtient des idéaux congrus à $\mathbf{I}^4$ et $\mathbf{I}'^4$, qui sont de *norme 30* et de racines 7 et —7; la décomposition de $F(7) = 30 \times \mathbf{5}$, aussi adjointe à la table, montre qu'ils sont congrus aux idéaux réduits, de *norme 5*.

En multipliant les idéaux réduits, ainsi obtenus congrus à $\mathbf{I}^4$ et $\mathbf{I}^3$

$$(\mathbf{10},\ \theta+3)\times(\mathbf{5},\ \theta+2)$$

$$(\mathbf{2},\ \theta+1)\times(\mathbf{5},\ \theta-2)\times(\mathbf{5},\ \theta+2) \sim (\mathbf{2},\ \theta+1)$$

on constate que $\mathbf{I}^7$ est congru à l'idéal double (d'ordre 2). Les classes définies par **I** et **I**′ sont donc d'*ordre 14* et chacune d'elles est générateur du groupe.

On a obtenu, en même temps les puissances de **I** congrues aux idéaux réduits, de *normes 3, 9, 10, 5, et 2* (double). Un calcul de multiplication, immédiat, donne les idéaux de *norme 6* et la décomposition de $F(2)$ donne ceux de *norme 7*.

Dans le *troisième exemple*, l'idéal de norme 2 est double et il y a quatre couples d'idéaux conjugués réduits, en tout *dix classes*; leur groupe est cyclique.

TABLEAU XVI.

Répartition, d'après l'ordre du groupe des classes des Corps quadratiques imaginaires, dont le discriminant D à deux facteurs premiers.

Ordre	$\|D\|$ impair		$\|D\| = 4p$	$\|D\| = 4\times(2p)$
	Idéal réduit réfléchi	Idéal réduit double	p premier impair	
2	3×5; 5×7; 7×13; 11×17; 13×31;	3×17; 5×23; 3×41; 5×47; 3×89; 7×61;	4×5; 4×13; 4×37;	8×3; 8×5; 8×11; 8×29;
4	5×11; 17×19; 23×29;	3×13; 5×31; 7×29; 3×73; 7×37; 3×97; 5×71; 3×241; 7×109; 5×191;	4×17; 4×73; 4×97; 4×193;	8×7; 8×17; 8×23; 8×41; 8×71;
6	13×19;	3×29; 3×113; 3×137; 11×41; 5×103; 7×101; 3×257; 5×167; 3×281;	4×29; 4×53; 4×61; 4×109; 4×157;	8×13; 8×19; 8×53; 8×59; 8×101; 8×107;
8	13×23;	5×19; 3×37; 3×61; 5×59; 7×53; 5×79; 3×193; 11×53; 3×313; 11×89; 5×199;	4×41; 4×113; 4×137;	8×31; 8×47; 8×79; 8×89; 8×113;
10	7×17; 11×13; 11×29; 19×41; 23×37;	3×53; 3×101; 5×83; 13×47; 5×127; 3×233; 11×73; 13×71;	4×181; 4×197; 4×229;	8×37; 8×43; 8×61; 8×83; 8×109;
12	17×43;	3×109; 3×181; 5×131; 3×229; 5×151;	4×89; 4×233; 4×241;	»
14	17×23; 19×37; 29×31;	5×43; 7×41; 3×149; 7×73; 5×107; 3×269;	4×101; 4×149; 4×173;	8×67;
16	17×47; 23×41;	11×37; 3×157; 13×43; 5×179;	»	8×73
18	17×31;	5×67; 3×173; 7×97;	»	»
20	»	»	»	8×97; 8×103;

Ordre	$\|D\|$ impair		$\|D\|$ pair
	Idéal réduit réfléchi	Idéal réduit double	
22	»	3×197; 7×89; 13×59; 13×67; 3×293;	»
24	»	5×139;	»
26	19×29;	3×317;	»
28	»	3×277;	»
30	»	11×61; 5×163;	»
32	»	7×113;	»
34	»	»	»
36	»	7×137.	»

$$F(x) = x^2+x+240; \quad D = -959 = (-7)\times137; \quad r = 9.$$

c	$F(c)$	Normes
0	$240 = 2^4\times3\times5$	**2**, **3**, **4**, **5**, **6**, **8**, **10**, **12**, **15**.
1	$242 = 2\times11^2$	**11**.
2	$246 = 2\times3\times41$	**6**.
3	$252 = 2^2\times3^2\times7$	**7**, **9**, **12**, **14**.
4	$260 = 2^2\times5\times13$	**10**, **13**.
5	$270 = 2\times3^3\times5$	**15**.
6	$282 = 2\times3\times47$	
7	$296 = 2^3\times37$	
8	$312 = 2^3\times3\times13$	
9	$330 = 2\times3\times5\times11$	

$(\mathbf{2},\ \theta-0)^4\times(\mathbf{3},\ \theta-0)\times(\mathbf{5},\ \theta-0) \sim (1)$

$(\mathbf{2},\ \theta+1)^4\times(\mathbf{3},\ \theta-0)^4 \sim (1)$

$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^3\times(\mathbf{5},\ \theta+1) \sim (1)$

$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^8 \sim (1)$

$(\mathbf{3},\ \theta-0)^{36} \sim (1)$

La table des valeurs donne immédiatement les couples d'idéaux conjugués **I** et **I'**, réduits, de *norme 3* et de racines (minimum) 1 et —1, ainsi que leurs carrés, de *norme 9* et de racines —2 et 2. On calcule encore leurs cubes, qui sont de *normes 27* et de racines 7 et —7. La décomposition $F(7) = 27 \times \mathbf{5}$, adjointe à la table, montre qu'ils sont congrus aux idéaux, de *norme 5* et de racines —2 et 2.

Les produits des idéaux de norme 9 et 5, donnent des idéaux congrus à $\mathbf{I}^5$ et $\mathbf{I}'^5$; ils sont de *norme 45* et de racines +2 et —2; la décomposition de $F(2) = 45 \times \mathbf{2}$ montrent qu'ils sont congrus à l'*idéal double* (d'ordre 2). Les idéaux **I** et **I'** définissent donc des classes d'ordre 10, qui peuvent servir chacune de générateur au groupe cyclique.

On a obtenu, en même temps les puissances de **I**, qui sont congrues aux idéaux, de *normes 3, 9, 5, 2* (double); pour les idéaux de *norme 6*, elles s'obtiennent par un calcul immédiat de multiplication.

Comme dans ces exemples, on constate que, pour tous les corps, dont le discriminant est de valeur absolue inférieure à 1 000 et a seulement deux facteurs premiers différents, le groupe des classes d'idéaux est cyclique, son ordre étant un des nombres pairs de 2 à 36 [à l'exception des corps de discriminant —4 et —8, qui sont principaux; (**34**)]. Le tableau XVI en donne une répartition, d'après l'ordre de leur groupe, en distinguant, pour les discriminants pairs, ceux qui ont un *facteur* 4, ou 8 et, pour les discriminants impairs la nature de l'idéal (unique) réduit remarquable: *réfléchi*, ou *double* (**29**).

On peut affirmer à priori que les groupes de ces différents corps sont cycliques, par la seule considération de leur ordre qui n'a pas de facteur impair carré. Il y a exception pour les quatre corps dont le groupe est d'ordre 18 et pour celui dont cet ordre est 36; il convient alors de faire une vérification.

On peut à cet effet chercher les idéaux réduits qui sont congrus aux puissances de l'un d'entre eux, convenablement choisi; ou former deux sous-groupes cycliques *indépendants*, dont le produit des ordres est égal à celui du groupe; si ces ordres sont premiers entre eux, le groupe est cyclique (**26**).

C'est ainsi que dans le corps de polynôme fondamental:

$$F(x) = x^2+x+170, \qquad D = -679 = (-7)\times 97,$$

l'idéal réduit (**2**, θ—0) engendre un sous-groupe cyclique, d'ordre 9, qui ne contient pas la classe double définie par l'idéal réduit de norme 7, diviseur de *D*. Le groupe qui a dix-huit classes est égal au produit direct du sous-groupe cyclique d'ordre 9 et de celui d'ordre 2, engendré par la classe double. Il est donc cyclique d'ordre 18.

On peut dans certains cas faire une vérification plus rapide, qui n'exige pas le calcul complet de la structure. Un exemple en est donné pour le corps de *discriminant* —959 = (—7)×137, dont le groupe est d'ordre 36: (suite du *tableau XVI*).

On a seulement indiqué, dans le tableau de valeurs, les normes des idéaux réduits; il y en a six qui sont des nombres premiers 2, 3, 5, 7 (idéal double), 11, 13. On s'occupe d'abord des relations entre les idéaux correspondants. Les décompositions de:

$$F(0) = F(-1), \qquad F(3) = F(-4), \qquad F(5) = F(-6)$$

donnent des relations entre les idéaux, des quatre premières normes, sous formes de monômes congrus à (1). On peut remplacer chaque monôme par celui des idéaux conjugués; c'est ce qui a été fait en utilisant la décomposition de $F(-6)$ au lieu de $F(5)$. Le monôme qui résulte de la décomposition de $F(3)$ contient l'idéal double, de norme 7, dont le carré est congru à (1), le carré de ce monôme qui est toujours congru à (1), est alors congru à un monôme des seuls idéaux, de normes 2 et 3.

On a ainsi formé trois monômes, des idéaux de normes 2, 3, 5, respectivement congrus à (1). En les multipliant convenablement, on peut obtenir des relations plus simples (le produit de deux idéaux conjugués est congru à (1) et peut être supprimé dans un monôme). On obtient notamment en formant le produit des trois monômes [l'idéal (3, θ—0) étant désigné par **I**]:

$$(2,\ \theta-0)\times\mathbf{I}^8 \sim (1) \quad \Leftrightarrow \quad (2,\ \theta+1) \sim \mathbf{I}^8;$$

puis par combinaison avec la deuxième relation:

$$\mathbf{I}^{36} \sim (1); \qquad (3,\ \theta+1) \sim \mathbf{I}^{35}; \qquad (2,\ \theta-0) \sim \mathbf{I}^{28}.$$

Les décompositions résultant de la table, permettent alors de former les puissances de **I**, auxquelles sont congrus les idéaux réduits de normes: 5 [$F(0)$]; 13 [$F(8)$]; 11 [$F(9)$ adjoint à la table]; 7 [$F(3)$]; pour ce dernier dont l'ordre est 2, on peut affirmer à priori, qu'il est

congru à $\mathbf{I}^{18}$. Les expressions des autres idéaux réduits dont les normes sont composées avec ces nombres premiers s'obtiennent par multiplication.

Comme dans le cas d'un discriminant premier, il semble que ce soit seulement pour des valeurs relativement grandes de $|D|$ qu'il soit possible d'obtenir des groupes de classes non cycliques. Un exemple en est donné dans le tableau XVII, disposé comme le tableau XIV, qui concerne le corps de discriminant $-19\,451 = (-43)\times 437$.

Il a dix-huit classes d'idéaux, dont une classe double représentée par l'idéal réduit double de norme 43. Leur groupe n'est pas cyclique: il a une *décomposition minimum* en un produit direct de sous-groupes cycliques d'ordres 3 et 6 et ses éléments peuvent être représentés par les monômes (indiqués dans le tableau):

$$\mathbf{I}^x\times\mathbf{J}^y;\quad x,\ \text{mod. } 3;\quad y,\ \text{mod. } 6.$$

La vérification peut être faite comme suit: la décomposition de $F(0) = 17^3$ montre que les idéaux de norme 17, forment avec (1), un *sous-groupe cyclique*, d'ordre 3. La décomposition de $F(21) = 5^3\times 43$ montre que les idéaux, de normes 5 et 25 ont leur troisième puissance congru à l'idéal double, de norme 7; ils définissent, par suite, avec cet idéal et (1), un *sous-groupe de six classes*, *cyclique*, indépendant du précédent (dont il ne contient pas d'élément, sauf (1)). Le groupe est donc égal au produit direct de ces deux sous-groupes; il n'a aucun élément d'ordre 18 et il n'est pas cyclique.

On peut préciser sa structure en calculant les idéaux réduits congrus aux divers monômes en $\mathbf{I}$ et $\mathbf{J}$; c'est ce qui a été indiqué dans le tableau; la première congruence résulte d'un calcul de multiplication d'idéaux canoniques, de normes premières entre elles, obtenus successivement:

$$\mathbf{I}\times\mathbf{J};\quad \mathbf{I}\times(\mathbf{I}\times\mathbf{J});\quad \mathbf{I}\times(\mathbf{I}\times\mathbf{J}^2);\quad \mathbf{I}\times(\mathbf{I}\times\mathbf{J}^3);\quad \mathbf{I}\times\mathbf{J}'.$$

37. Corps imaginaires, dont le discriminant a plus de deux facteurs premiers.

Le discriminant est alors décomposable, au moins de deux façons, en un produit de deux facteurs. Il en résulte l'existence

TABLEAU XVII.

$F(x) = x^2+x+4\,913$; $D = -19\,651 = (-43)\times 437$; $r = 40$.
(Groupe d'ordre 3 × Groupe d'ordre 6).

0	$4\,913 = 17^3$ $(\mathbf{1},\ \theta-0) \sim \mathbf{I}^3 \sim \mathbf{J}^6$ $(\mathbf{17},\ \theta-0) \sim \mathbf{I}$
1	$4\,915 = 5\times 983$ $(\mathbf{5},\ \theta-1) = \mathbf{J}$
2	4 919
3	$4\,925 = 5^2\times 197$ $(\mathbf{25},\ \theta-3) \sim \mathbf{J}^4$
4	4 933
5	4 943
6	$4\,955 = 5\times 991$
7	4 969
8	$4\,985 = 5\times 997$
9	5 003
10	5 023
11	$5\,045 = 5\times 1\,009$
12	$5\,069 = 37\times 137$ $(\mathbf{37},\ \theta-12) \sim \mathbf{I}\times\mathbf{J}^3$
13	$5\,095 = 5\times 1\,019$
14	$5\,123 = 47\times 109$ $(\mathbf{47},\ \theta-14) \sim \mathbf{I}\times\mathbf{J}^2$
15	5 153
16	$5\,185 = (5\times 17)\times\mathbf{61}$ $(\mathbf{61},\ \theta-16) \sim \mathbf{I}\times\mathbf{J}^5$
17	$5\,219 = 17\times 307$
18	$5\,255 = 5\times 1\,051$
19	$5\,293 = 67\times 79$ $(\mathbf{67},\ \theta-19) \sim \mathbf{I}^2\times\mathbf{J}^2$
20	5 333
21	$5\,375 = 5^3\times\mathbf{43}$ $(\mathbf{43},\ \theta-21) \sim \mathbf{J}^3$
22	5 419
23	$5\,465 = 5\times 1\,093$
24	$5\,513 = 37\times 149$
25	5 563
26	$5\,615 = 5\times 1\,123$
27	5 669
28	$5\,725 = 5^2\times 229$
29	5 783
30	5 843
31	$5\,905 = 5\times 1\,181$
32	$5\,969 = 67\times 127$
33	$6\,035 = (5\times 17)\times\mathbf{71}$ $(\mathbf{71},\ \theta-33) \sim \mathbf{I}\times\mathbf{J}$
34	$6\,103 = 17\times 359$
35	6 173
36	$6\,245 = 5\times 1\,249$
37	$6\,319 = 71\times 89$
38	$6\,395 = 5\times 1\,279$
39	6 473

$F(61) = 8\,695 = (5\times 47)\times\mathbf{37}$
$F(86) = 12\,395 = (5\times 37)\times\mathbf{67}$
$F(108) = 16\,685 = (5\times 71)\times\mathbf{47}$

$\mathbf{I}\times\mathbf{J} \sim (5\times 17,\ \theta+34) \sim (\mathbf{71},\ \theta-33)$
$\mathbf{I}\times\mathbf{J}^2 \sim (5\times 71,\ \theta-108) \sim (\mathbf{47},\ \theta-14)$
$\mathbf{I}\times\mathbf{J}^3 \sim (5\times 47,\ \theta-61) \sim (\mathbf{37},\ \theta-12)$
$\mathbf{I}\times\mathbf{J}^4 \sim (5\times 37,\ \theta-86) \sim (\mathbf{67},\ \theta+20)$
$\mathbf{I}\times\mathbf{J}^5 \sim (5\times 17,\ \theta+17) \sim (\mathbf{61},\ \theta-16)$

d'au moins deux idéaux réduits remarquables, en plus de l'idéal unité. Le groupe des classes, qui contient au moins deux éléments d'ordre 2, n'est pas cyclique.

Le tableau XVIII, disposé comme les tableaux XII et XV, donne trois exemples de tels corps. Pour le *premier*, de discriminant $-420 = -4\times3\times5\times7$, il y a six idéaux réduits doubles, de normes 2, 3, 5, 7, 10 et un idéal réduit réfléchi, de norme 11 (résultant de la décomposition $420 = 20\times21$). Il y a en tout sept classes, chacune d'ordre 2 dans le groupe, qui, avec la classe principale, constituent un groupe d'ordre 8, produit direct de trois groupes cycliques d'ordre 2.

Pour le *deuxième exemple*, de discriminant $-435 = -3\times5\times29$, il y a deux idéaux réduits doubles, de normes 3 et 5 et un idéal réduit réfléchi, de norme 11 (résultant de la décomposition $435 = 15\times29$). Il y a en tout trois classes, chacune d'ordre 2, qui, avec la classe principale, constituent un groupe, d'ordre 4, produit direct de deux groupes cycliques d'ordre 2 (groupe de Klein).

Pour le *troisième exemple*, de discriminant $-440 = -8\times5\times11$, il n'y a pas d'idéal réduit réfléchi, mais seulement trois idéaux réduits doubles, de normes 2, 5, 10, et, en outre quatre couples d'idéaux réduits conjugués, de normes 3, 6, 7, 9. Il y a en tout, $3+2\times4 = 11$ classes, qui, avec la classe principale, constituent un groupe, d'ordre 12, produit direct de deux groupes cycliques, d'ordre 6 et 2.

Le tableau XIX donne encore la répartition des corps imaginaires dont le discriminant est de valeur absolue inférieure à 1000, et contient au moins trois facteurs premiers, d'après la structure du groupe de leurs classes d'idéaux. On a distingué les discriminants impairs et les discriminants qui ont un facteur 4 ou 8.

Le discriminant de trois seulement de ces corps contient quatre facteurs: le groupe des classes d'idéaux de chacun de ces corps est le produit direct de deux groupes cycliques d'ordre 2. Pour tous les autres corps, le groupe des classes d'idéaux est le produit direct de deux groupes cycliques.

En généralisant la construction des exemples précédents, on peut aisément vérifier que, pour un corps imaginaire, dont *le discriminant a n facteurs premiers*, différents, le groupe des

TABLEAU XVIII.

Exemples de corps imaginaires dont le discriminant a au moins 3 facteurs premiers.

$D = -420$; $r = 6$	
c	
0	$105 = 3\times5\times7$ $(\mathbf{1}, \theta-0) = (1)$ $(\mathbf{3}, \theta-0) = \mathbf{J}$ $(\mathbf{5}, \theta-0) \sim \mathbf{I}\times\mathbf{K}$ $(\mathbf{7}, \theta-0) = \mathbf{K}$
1	$106 = 2\times53$ $(\mathbf{2}, \theta-1) = \mathbf{I}$
2	109
3	$114 = 2\times3\times19$ $(\mathbf{6}, \theta-3) \sim \mathbf{I}\times\mathbf{J}$
4	$121 = 11^2$ $(\mathbf{11}, \theta-4) \sim \mathbf{I}\times\mathbf{K}$
5	$130 = 2\times5\times13$ $(\mathbf{10}, \theta-5) \sim \mathbf{I}\times\mathbf{J}\times\mathbf{K}$
7	$154 = 2\times7\times11$

$(\mathbf{3}, \theta)\times(\mathbf{5}, \theta)\times(\mathbf{7}, \theta) \sim (1)$ $[F(0)]$

$(\mathbf{2}, \theta-1)\times(\mathbf{7}, \theta)\times(\mathbf{11}, \theta+4) \sim (1)$ $[F(7)]$

3 groupes cycliques d'ordre 2

$\mathbf{I}^x\times\mathbf{J}^y\times\mathbf{K}^z$

x, y, z, mod. 2

$D = -435$; $r = 6$	
c	
0	109 $(\mathbf{1}, \theta-0) = (1)$
1	$111 = 3\times37$ $(\mathbf{3}, \theta-1) = \mathbf{I}$
2	$115 = 5\times23$ $(\mathbf{5}, \theta-2) = \mathbf{J}$
3	$121 = 11^2$ $(\mathbf{11}, \theta-3) \sim \mathbf{I}\times\mathbf{J}$
4	$129 = 3\times43$
5	139
7	$165 = 3\times5\times11$

$(\mathbf{3}, \theta-1)\times(\mathbf{5}, \theta-2)\times(\mathbf{11}, \theta-7) \sim (1)$ $[F(7)]$

2 groupes cycliques d'ordre 2

$\mathbf{I}^y\times\mathbf{J}^z$

x, y, mod. 2

$D = -440$; $r = 7$	
c	
-4	$(\mathbf{9}, \theta+4) \sim \mathbf{I}^4$
-3	$(\mathbf{7}, \theta+3) \sim \mathbf{I}^4\times\mathbf{J}$
-2	$(\mathbf{6}, \theta+2) \sim \mathbf{I}\times\mathbf{J}$
-1	$(\mathbf{3}, \theta+1) \sim \mathbf{I}^5$
0	$110 = 2\times5\times11$ $(\mathbf{1}, \theta-0) = (1)$ $(\mathbf{2}, \theta-0) = \mathbf{J}$ $(\mathbf{5}, \theta-0) \sim \mathbf{I}^3$ $(\mathbf{10}, \theta-0) \sim \mathbf{I}^3\times\mathbf{J}$
1	$111 = 3\times37$ $(\mathbf{3}, \theta-1) = \mathbf{I}$
2	$114 = 2\times3\times19$ $(\mathbf{6}, \theta-2) \sim \mathbf{I}^5\times\mathbf{J}$
3	$119 = 7\times17$ $(\mathbf{7}, \theta-3) \sim \mathbf{I}^2\times\mathbf{J}$
4	$126 = 2\times3^2\times7$ $(\mathbf{9}, \theta-4) \sim \mathbf{I}^2$
5	$135 = 3^3\times5$
6	$146 = 2\times7^3$

2 groupes cycliques d'ordres 6 et 2

$\mathbf{I}^x\times\mathbf{J}^y$

x, mod. 6; y, mod. 2

classes d'idéaux est le *produit direct d'au moins n—1 groupes cycliques.*

C'est ainsi que, pour le corps de discriminant:

$$-5\,450 = -4\times3\times5\times7\times13,$$

il y a quinze classes, chacune d'ordre 2 dans le groupe, qui est le produit direct de quatre groupes cycliques, d'ordre 2.

Tableau XIX.

Répartition, d'après la structure du groupe des classes, des corps quadratiques imaginaires dont le dicriminant a au moins 3 facteurs premiers.

Produit de deux groupes cycliques d'ordre 2 (groupe de Klein):

$|D|$ impair: $3\times5\times13$; $3\times5\times29$; $3\times7\times23$; $3\times5\times37$; $5\times7\times17$; $3\times11\times19$; $5\times11\times13$; $3\times5\times13$;

$|D|$ multiple de 4: $4\times3\times7$; $4\times3\times11$; $4\times3\times19$; $4\times5\times17$; $4\times3\times31$; $4\times7\times19$; $4\times3\times59$;

$|D|$ multiple de 8: $8\times3\times5$; $8\times3\times7$; $8\times5\times7$; $8\times3\times13$; $8\times3\times17$ $8\times5\times13$; $8\times5\times19$;

Produit direct de deux groupes cycliques d'ordres 2 et 4:

$|D|$ impair: $3\times7\times31$; $3\times5\times61$; $3\times7\times47$;

$|D|$ multiple de 4: $4\times5\times13$; $4\times3\times23$; $4\times7\times11$; $4\times3\times47$; $4\times5\times29$; $4\times5\times41$; $4\times3\times71$; $4\times7\times31$;

$|D|$ multiple de 8: $8\times3\times11$; $8\times3\times19$; $8\times3\times23$; $8\times7\times11$; $8\times5\times19$;

Produit direct de deux groupes cycliques d'ordres 2 et 6:

$|D|$ impair: $3\times7\times11$; $3\times5\times17$;

$|D|$ multiple de 4: $4\times3\times43$; $4\times3\times67$; $4\times3\times79$; $4\times3\times83$;

$|D|$ multiple de 8: $8\times5\times11$; $8\times5\times17$; $8\times3\times29$; $8\times3\times31$; $8\times3\times37$; $8\times3\times41$;

Produit direct de deux groupes cycliques d'ordres 2 et 8:

$|D|$ impair: $3\times7\times19$; $3\times13\times17$; $3\times7\times43$;

$|D|$ multiple de 4: $4\times7\times23$; $4\times5\times37$; $4\times13\times17$;

Produit direct de deux groupes cycliques d'ordres 2 et 10:

$|D|$ impair: $5\times7\times13$; $3\times5\times41$;

$|D|$ multiple de 4: $4\times11\times19$;

$|D|$ multiple de 8: $8\times5\times23$;

Produit direct de deux groupes cycliques d'ordres 2 et 12:

$|D|$ impair: $3\times11\times23$;

Produit direct de deux groupes cycliques d'ordres 2 et 14:

$|D|$ impair: $5\times11\times17$;

Produit direct de trois groupes cycliques d'ordre 2:

$|D|$ multiple de 4: $4\times3\times5\times7$; $4\times3\times5\times11$;

$|D|$ multiple de 8: $8\times3\times5\times7$.

CHAPITRE VI

LES CLASSES D'IDÉAUX ET LES DIVISEURS DE L'UNITÉ DANS LES CORPS RÉELS

Dans un corps réel, ou de discriminant positif, la considération des idéaux réduits (**25**) suffit pour montrer que le nombre de classes d'idéaux est fini. Mais elle ne permet plus de déterminer toujours, avec certitude, la structure de leur groupe (ou la table de PYTHAGORE de leur multiplication). On définit alors une catégorie plus étendue d'idéaux, qui sont appelés *semi réduits*. Chaque classe d'idéaux est caractérisée par un système, ou, plus précisément, par un *cycle* (système ordonné) d'*un nombre fini d'idéaux semi réduits*. Ces cycles permettent, en même temps, de réaliser la construction, au moins théorique, des *diviseurs de l'unité*, dans le corps réel considéré.

Avant d'exposer cette notion nouvelle, on montre d'abord comment dans certains cas, notamment pour des discriminants peu élevés, le calcul des seuls idéaux réduits permet encore d'aboutir à une affirmation.

38. Corps réels principaux triviaux.

Dans un corps réel, la valeur $F(c)$, du polynôme fondamental est négative, pour un nombre fini de valeurs entières, comprises entre les deux zéros (irrationnels) du polynôme, qui sont de signes contraires. La considération de ces valeurs fournit un criterium, moins strict, pour la détermination des idéaux réduits.

On peut d'abord modifier une remarque faite pour les idéaux des corps imaginaires (**29**): pour un idéal canonique d'un *corps réel, s'il existe des racines c qui rendent* $F(x)$ *négatif, la racine minimum* $\bar{c}$ *est celle, d'entre elles, qui donne à* $F(x)$ *la plus grande valeur absolue.*

Il suffit encore de considérer la différence:

$$F(\bar{c}+\lambda m)-F(\bar{c}) = \lambda m \times (2\bar{c}-S+\lambda m); \quad \lambda \text{ entier rationnel;}$$

si $\bar{c}$ est racine minimum, $|2\bar{c}-S|$ est au plus égal à m, $(2\bar{c}-S+\lambda m)$ est nul, ou du signe de λ, supposé non nul; la différence est positive ou nulle. S'il existe des racines $x = \bar{c}+\lambda m$ qui rendent $F(x)$ négative il en est de même de $\bar{c}$, puisque $F(\bar{c})$ est au plus égal à $F(\bar{c}+\lambda m)$ et il en résulte la comparaison des valeurs absolues:

$$F(\bar{c}) \leqslant F(\bar{c}+\lambda m) \quad \Rightarrow \quad |F(\bar{c})| \geqslant |F(\bar{c}+\lambda m)|.$$

Théorème caractéristique d'un idéal réduit. — *Dans un corps réel*, ou de discriminant positif, *pour qu'un idéal*, et, par suite, son idéal conjugué, soit réduit, *il faut et il suffit qu'il ait au moins une racine c, telle que* $F(c)$ *soit négative* et que le carré de sa norme soit au plus égal à la valeur absolue $|F(c)|$:

$$m \text{ diviseur de } |F(c)|; \quad F(c) < 0; \quad m^2 \leqslant |F(c)|.$$

La condition est *nécessaire*, car pour un idéal réduit, ces conditions sont vérifiées en prenant pour c la racine minimum $\bar{c}$ (**25**).

La condition est *suffisante*, la racine minimum de l'idéal est alors l'entier $\bar{c}$, de plus petite valeur absolue, congru à c, mod. m. Il donne encore une valeur négative à $F(x)$, au plus égale à $F(c)$ en sorte que:

$$m^2 \leqslant |F(c)| \leqslant |F(\bar{c})|;$$

ce qui vérifie la condition de réduction.

On peut encore vérifier que la définition d'un *idéal double* et sa propriété caractéristique (**7**) sont valables: sa norme est diviseur du discriminant. Mais la condition de *réduction* donnée pour les corps imaginaires (**29**) devient (coefficient 3 remplacé par 5):

$$\begin{array}{ll} 5m^2 \leqslant D, & \left\{ \begin{array}{l} \text{si } D \text{ est impair;} \\ \text{si } D = 4d; \quad d \text{ impair}; \quad m = 2u', \quad u' \text{ diviseur de } d; \end{array} \right. \\ 4m^2 \leqslant D, & \text{si } D = 4d, \quad m \text{ diviseur de } d. \end{array}$$

Les idéaux réduits ne représentent plus proprement les classes d'idéaux; dans chacune d'elles, il peut exister plusieurs

idéaux réduits, toutefois en nombre fini. Pour rechercher leur table de multiplication, comme il a été fait pour les corps imaginaires, il faudrait, au moins en principe, avoir préalablement réparti en classes les idéaux réduits eux-mêmes.

On peut cependant affirmer directement le résultat lorsque les calculs de multiplication des idéaux et les relations résultant des décompositions de valeurs du tableau permettent de constater que tous les idéaux réduits sont principaux, c'est-à-dire que *le corps est principal.*

TABLEAU XX.

Corps réels où le seul idéal réduit est (1).

$D =$	5	13	$21 = 3\times7$	29	53	$77 = 7\times11$	173	293	$437 = 19\times23$		8	12
$r =$	1	1	1	1	2	2	3	4	5		1	1
$-F(0)$	1	3	5	7	13	19	43	73	109		2	3
$-F(1)$	−1	1	3	5	11	17	41	71	107		1	2
$-F(2)$					7	13	37	67	103			
$-F(3)$							31	61	97			
$-F(4)$								53	89			
$-F(5)$									79			

Une première circonstance, presque *triviale*, pour laquelle cette affirmation est possible est réalisée lorsque l'idéal unité est le seul qui soit réduit:

pour qu'un corps réel soit principal, il suffit que les r *premières valeurs du polynôme fondamental* $F(c)$*:*

$$0 \leqslant c < r; \quad x \geqslant r \quad \Leftrightarrow \quad |F(x)| < (2x-S)^2$$

qui sont négatives, *soient toutes des nombres premiers.*

Dans le cas des corps imaginaires, cette condition est aussi suffisante, mais elle est également nécessaire (**34**).

Pour les *discriminants pairs*, elle n'est vérifiée que pour les valeurs 8 et 12 (polynômes fondamentaux x^2-2 et x^2-3); pour tous les autres, l'idéal, de norme 2 et de racine 0 ou 1 est réduit.

Elle est, d'autre part, vérifiée pour 9 corps, de *discriminants impairs* (et aucun autre inférieur à 1000), qui sont donnés dans le tableau XX. On remarquera que dans ceux de discriminants 21 et 77, il y a un idéal double, non réduit.

39. Exemples de vérification de corps principaux.

Dans certains cas, la considération des idéaux réduits suffit encore à constater que le corps est principal. Quelques exemples de calcul en sont donnés dans le tableau XXI, qui est disposé de la même façon que les tableaux X, XII, XVI, donnés en exemples de corps imaginaires. On a toutefois inscrits, en caractères gras, les normes des idéaux réduits.

Une première circonstance est l'*existence d'un seul couple d'idéaux réduits conjugués* (en plus de l'idéal unité), éventuellement égaux, *dont la décomposition d'une valeur ultérieure du tableau montre qu'ils sont principaux.*

Dans le corps, de discriminant 317 (première colonne du tableau XXI) les 3 seuls idéaux réduits sont l'idéal (1) et le couple d'idéaux conjugués (inégaux), de norme 7. La valeur $F(8) = -7$, montre qu'ils sont principaux $(\theta-8) = (7, \theta-8)$. La valeur antérieure $F(5) = -49$ montre aussi qu'ils sont congrus (idéal réfléchi, non réduit).

Pour le corps de discriminant pair $152 = 8\times19$ (deuxième colonne du même tableau), les 2 seuls idéaux réduits sont (1) et l'idéal double de norme 2. La valeur $F(6) = -2$ montre que cet idéal est principal.

De telles vérifications peuvent se faire pour un assez grand nombre de corps de discriminants inférieurs à 1000, notamment:

impairs: 17, 33, 37, 41, 61, 69, 93, 101, 133, 149, 157, 197, 213, 237, 269, 317, 341, 413, 453, 461, 557, 677, 717, 773, 941;

pairs: 24, 28, 44, 56, 92, 152, 188, 248, 332, 668, 908.

Tableau XXI.

Exemples de corps réels principaux.

(Calculs avec les idéaux réduits.)

	$D = 317$ $r = 4$	$D = 152 = 8\times19$ $r = 3$	$D = 193$ $r = 3$	$D = 184 = 8\times23$ $r = 4$
$-F(0)$	79 $(\mathbf{1}, \theta)$	$38 = 2\times29$ $(\mathbf{1}, \theta)$ $(\mathbf{2}, \theta) = (\mathbf{2}, \theta')$	$48 = 2^4\times3$ $(\mathbf{1}, \theta)$ $(\mathbf{2}, \theta)$ | $(\mathbf{2}, \theta')$ $(\mathbf{3}, \theta)$ | $(\mathbf{3}, \theta')$ $(\mathbf{4}, \theta)$ | $(\mathbf{4}, \theta')$ $(\mathbf{6}, \theta)$ | $(\mathbf{6}, \theta')$	$46 = 2\times23$ $(\mathbf{1}, \theta)$ $(\mathbf{2}, \theta) = (\mathbf{2}, \theta')$
$-F(1)$	$77 = 7\times11$ $(\mathbf{7}, \theta-1)$ $(\mathbf{7}, \theta'-1)$	37	$46 = 2\times23$	$45 = 3^2\times5$ $(\mathbf{3}, \theta-1)$ | $(\mathbf{3}, \theta'-1)$ $(\mathbf{5}, \theta-1)$ | $(\mathbf{5}, \theta'-1)$
$-F(2)$	73	$34 = 2\times17$	$42 = 2\times3\times7$ $(\mathbf{6}, \theta-2)$ | $(\mathbf{6}, \theta'-2)$	$42 = 2\times3\times7$ $(\mathbf{6}, \theta-2)$ | $(\mathbf{6}, \theta'-2)$
$-F(3)$	67	29	36	37
$-F(4)$	59			30
$-F(5)$	$49 = 7\times7$		$18 = 6\times3$	
$-F(6)$		2	$6 = 2\times3$	$10 = 2\times5$
$-F(7)$				-3
$-F(8)$	7			
	$F(8)$: $(7, \theta-1) \sim (1)$	$F(6)$: $(2, \theta) \sim (1)$	$F(6)$: $(6, \theta) \sim (1)$ $F(5)$: $(6, \theta')\times(3, \theta') \sim (1)$ $F(6)$: $(2, \theta)\times(3, \theta) \sim (1)$	$F(7)$: $(3, \theta-1) \sim (1)$ $F(1)$: $(3, \theta-1)^2\times(5, \theta-1) \sim (1)$ $F(6)$: $(2, \theta)\times(5, \theta-1) \sim (1)$

Une circonstance, moins évidente lorsqu'il existe plusieurs couples d'idéaux conjugués, est *l'existence de valeurs du tableau, dont les décompositions montrent successivement que certains des idéaux réduits sont principaux*, et qu'il en est, par suite de même de leurs produits mutuels, qui peuvent constituer tous les autres.

Dans le corps, de discriminant 193 (troisième colonne du tableau XVIII), il y a 11 idéaux réduits dont (1) et 5 couples d'idéaux conjugués différents. Les décompositions de $-F(6) = 1\times 6$, $-F(5) = 6\times 3$, et, à nouveau $-F(6) = 2\times 3$ montrent successivement que: un des couples d'idéaux, de norme 6, puis le couple de norme 3, puis celui de norme 2 sont principaux. Il en résulte la même propriété pour le couple de norme 4 et l'autre couple de norme 6.

Dans le corps de discriminant 184 (quatrième colonne du même tableau), il y a 8 idéaux réduits, dont (1) et l'idéal double, de norme 2. Les décompositions de $-F(7) = 3\times 1$, $-F(1) = 3^2\times 5$, et $-F(6) = 2\times 5$ montrent successivement que les idéaux, de norme 3, donc ceux de norme 3^2 (non réduits), puis ceux de norme 5, puis l'idéal double, de norme 2 sont principaux. Il en résulte la même propriété pour les deux autres idéaux réduits, de norme 6.

De telles vérifications peuvent se faire pour *presque tous les corps principaux*, de discriminant inférieur à 500 et pour un très grand nombre de ceux dont le discriminant est compris entre 500 et 1000. Les calculs sont, d'ailleurs, en général plus simples que dans le cas des corps imaginaires. Cette simplification tient, pour une part, au petit nombre de diviseurs des valeurs $F(c)$, pour c voisin des zéros (irrationnels) de ce polynôme.

On est ainsi conduit, pour « *distinguer* » des idéaux (ou des couples d'idéaux conjugués), à utiliser, *au lieu des racines minimums* (les plus proches de 0), les racines les plus proches des zéros (irrationnels) du polynôme, et comprises entre ces zéros (ou rendant $F(x)$ négatif) c'est-à-dire encore *les racines qui donnent à* $-F(x)$ *les plus petites* valeurs positives. C'est ce qui va être fait dans les considérations et les définitions suivantes.

40. Idéaux semi réduits.

Pour « étendre » la définition des idéaux réduits, on peut d'abord déduire de la propriété caractéristique, établie ci-dessus (**38**), une remarque complémentaire.

Dans un corps réel, *un idéal réduit* $\mathbf{M} = (m, \theta - \bar{c})$ *a, au moins, deux racines distinctes, qui donnent à* $F(x)$ *des valeurs négatives.*

Pour l'idéal réduit **M**, de racine minimum $\bar{c}$, la somme:

$$F(\bar{c}+m)+F(\bar{c}-m) = 2[F(\bar{c})+m^2]$$

n'est pas positive, puisque $F(\bar{c})$ est négative et m^2 au plus égal à $|F(\bar{c})|$. Il en résulte que l'une au moins des valeurs $F(\bar{c}+m)$, et $F(\bar{c}-m)$, qui ne peuvent être nulles, est négative, en même temps que $F(\bar{c})$. Comme $\bar{c}+m$ et $\bar{c}-m$ sont différents de $\bar{c}$, la propriété est établie.

Ceci suggère la définition suivante: Définition. — Dans un corps quadratique réel, *un idéal canonique est* **semi réduit**, *lorsqu'il a*, au moins, *deux racines distinctes, qui donnent des valeurs négatives à* $F(x)$*:*

$$\mathbf{M} = (m,\ \theta - c_1) = (m,\ \theta - c_2); \quad c_1 - c_2 \equiv 0, \pmod{m};$$
$$c_1 \neq c_2; \quad F(c_1) < 0, \quad F(c_2) < 0.$$

En particulier, un idéal réduit est, a fortiori, semi réduit. *L'idéal* **M'**, *conjugué, d'un idéal* **M** *semi réduit, est aussi semi réduit*, car les racines $S - c_1$ et $S - c_2$, de l'idéal **M'**, donnent à $F(x)$, les mêmes valeurs négatives, que les racines c_1 et c_2, de **M**.

Pour un idéal semi réduit, il y a ainsi plusieurs (2 ou plus) termes successifs de la progression arithmétique des racines qui donnent une valeur négative à $F(x)$; ils comprennent la racine minimum $\bar{c}$; ils sont en nombre fini [contenus entre les zéros irrationnels, négatif et positif, de $F(x)$]; et ils ont deux termes extrêmes. Ceci suggère la définition générale suivante.

Définition. — Dans un corps quadratique réel, *on appelle* **racine initiale** et **racine finale**, d'un idéal canonique **M**, *la plus*

petite (ou la première) *et la plus grande* (ou la dernière) *des racines*, s'il en existe, *qui donnent une valeur négative au polynôme fondamental* $F(x)$.

Elles sont caractérisées par l'équivalence de conditions:

$$F(c) < 0 \quad \Leftrightarrow \quad \{c_i \text{ initiale} \leqslant c \leqslant c_f \text{ finale}\};$$

ce qui est équivalent à la proposition contraposée ($F(c)$ ne pouvant être nul):

$$F(c) > 0 \quad \Leftrightarrow \quad \{c < c_i \text{ initiale, } ou\ c > c_f \text{ finale}\}$$

Les racines initiale et finale de l'idéal **M'**, conjugué d'un idéal **M**, sont respectivement les racines conjuguées:

$$c_i' = S - c_f, \qquad c_f' = S - c_i,$$

des racines finale et initiale de **M**.

Pour un idéal semi réduit, les racines initiale et finale existent et sont distinctes. En outre le nombre entier $(2c - S)$ est

positif, pour la racine finale: $2c_f - S > 0$;

négatif, pour la racine initiale: $2c_i - S < 0$;

(il n'est pas nul).

La différence $c_f - c_i$ est positive et multiple de m, en sorte que $c_f - m \geqslant c_i$ et $c_i + m \leqslant c_f$ donnent des valeurs négatives à $F(x)$. Il en est de même des racines conjuguées:

$$F(S - [c_f - m]) = F(c_f - m) < 0; \qquad F(S - [c_i + m]) = F(c_i + m) < 0.$$

Donc $S - c_f + m$ et $S - c_i - m$ sont, tous deux, inférieurs à $c_f + m$ et supérieurs à $c_i - m$ (qui donnent des valeurs positives à $F(x)$). Il en résulte:

$$S - c_f + m < c_f + m \quad \Leftrightarrow \quad 2c_f - S > 0;$$
$$S - c_i - m > c_i + m \quad \Leftrightarrow \quad 2c_i - S < 0.$$

41. Couple d'idéaux associés semi réduits.

Les idéaux semi réduits se présentent par couples d'idéaux associés relativement à une racine (**26**), aussi bien initiale que finale. Pour les idéaux d'un tel couple on peut en effet donner

des conditions de semi réduction, qui sont: nécessaires séparément et suffisantes simultanément.

THÉORÈME caractéristique de semi réduction. — *Deux idéaux canoniques* **M** *et* **N**, *étant associés*, relativement à une racine c qui donne à $F(x)$ une valeur négative:

$$F(c) = -m \times n; \quad \mathbf{M} = (m, \ \theta - c), \quad \mathbf{N} = (n, \ \theta - c);$$
$$m, \ n \text{ entiers positifs;}$$

pour que l'un d'eux soit semi réduit, et admette c comme racine soit initiale, soit finale, *il est nécessaire que leurs normes vérifient l'une des conditions*, qui sont équivalentes:

$$|m-n| < |2c-S| \quad \text{ou} \quad (m+n)^2 < D.$$

Cette *condition est suffisante* pour que les deux idéaux soient simultanément semi réduits.

Pour chaque idéal, la racine est finale ou initiale, suivant que $2c-S$, qui ne peut être nul, est positif ou négatif.

L'équivalence des deux comparaisons résulte du calcul immédiat:

$$(m-n)^2 < (2c-S)^2 \Leftrightarrow (m+n)^2 < (2c-S)^2 + 4m \times n$$
$$= (2c-S)^2 - 4F(c) = D.$$

Pour établir leur nécessité, on calcule les valeurs de $F(x)$, pour les racines de **M**, précédant et suivant immédiatement la racine c. On obtient aisément les expressions, qui ne peuvent être nulles:

$$F(c-m) = m \times [(m-n)-(2c-S)];$$
$$F(c+m) = m \times [(m-n)+(2c-S)].$$

Pour que **M** soit semi réduit et que c en soit racine finale, ou initiale, il faut et il suffit que, suivant le cas:

c finale: $2c-S > 0$; $F(c-m) < 0$; $F(c) < 0$; $F(c+m) > 0$;

c initiale: $2c-S < 0$; $F(c-m) > 0$; $F(c) < 0$; $F(c+m) < 0$.

Il est équivalent de dire que les crochets, qui ne peuvent être nuls, doivent avoir les mêmes signes que leurs seconds termes. Pour cela, il est nécessaire et suffisant que la valeur absolue $|2c-S|$ de ces termes soit supérieure à la valeur absolue $|m-n|$, des premiers termes.

Réciproquement si cette condition est remplie, elle l'est à la fois pour **M** et **N**, puisque $m—n$ n'intervient que par sa valeur absolue. Elle suffit donc pour que **M** et **N**, associés relativement à la racine c, soient semi réduits et admettent c comme racine, finale ou initiale suivant le signe de $2c—S$.

La simultanéité des conditions suffisantes peut encore être exprimée sous la forme de l'existence d'idéaux (en général différents) associés à un même idéal semi réduit:

si un idéal **M** *est semi réduit, les idéaux* $\mathbf{N}_i$ *et* $\mathbf{N}_f$, *associés à* **M**, relativement à ses racines c_i initiale et c_f finale:

$$\mathbf{M}\begin{cases} = (m,\ \theta—c_i); & F(c_i) = —m\times n_i; & \mathbf{N}_i = (n_i,\ \theta—c_i); \\ = (m,\ \theta—c_f); & F(c_f) = —m\times n_f; & \mathbf{N}_f = (n_f,\ \theta—c_f); \end{cases}$$

sont semi réduits et c_i, c_f en sont, respectivement, les racines initiale pour $\mathbf{N}_i$, finale pour $\mathbf{N}_f$.

Sauf précision contraire, on utilisera, de préférence, les couples d'*idéaux associés, relativement à leur racine finale* (en sous entendant l'indication de cette racine), donc pour une valeur positive de $2c—S$, et, par suite pour une valeur non négative de c.

Tout idéal réduit est, ainsi qu'il a été dit (**40**), a fortiori semi réduit. La réciproque n'est pas vraie, on peut seulement affirmer que

dans tout couple d'idéaux semi réduits, associés, relativement à une racine c (finale ou initiale):

$$\mathbf{M} = (m,\ \theta—c),\quad \mathbf{N} = (n,\ \theta—c);\qquad m \leqslant n;$$

le premier, au moins, **M** (de norme au plus égale à celle du second) *est réduit.*

La norme m, de l'idéal considéré a un carré au plus égal à $|F(c)| = m\times n$. On détermine la racine minimum $\bar{c}$, de cet idéal **M**; la valeur $F(\bar{c})$ est aussi négative et de valeur absolue maximum (**38**). Donc:

$$m^2 \leqslant |F(c)| \leqslant |F(\bar{c})|;$$

M vérifie bien la condition de réduction (**35**).

42. Construction des idéaux semi réduits.

Pour obtenir tous les idéaux semi réduits d'un corps, *il suffit de construire les couples*, ou les produits, *d'idéaux associés relativement à leur racine finale.*

On utilise le tableau des valeurs négatives de $F(c)$, pour les valeurs entières de c, à partir de 0. Pour chaque valeur $|F(c)|$, on cherche celles de ses décompositions en produit $m \times n$, de deux entiers positifs, vérifiant la condition caractéristique, $|m—n|$ inférieur à $(2c—S)$; (ou la condition équivalente $(m+n)^2$ inférieur à D).

Chaque décomposition donne un des produits cherchés:

$$(m,\ \theta—c) \times (n,\ \theta—c) = (\theta—c).$$

Les idéaux ne sont ainsi obtenus qu'une fois, puisque c en est une racine déterminée (finale). Dans leurs expressions, on peut évidemment remplacer c par une racine congrue relativement à la norme.

Pour chaque produit ainsi obtenu, les idéaux respectivement conjugués, de mêmes normes m, n, sont semi réduits, associés relativement à la racine conjuguée $c' = S—c$, qui est leur racine initiale commune:

$$\mathbf{M}' = (m,\ \theta'—c) = (m,\ \theta—c'); \quad \mathbf{N}' = (n,\ \theta'—c) = (n,\ \theta—c')$$

$$\mathbf{M}' \times \mathbf{N}' = (\theta'—c) = (\theta—c'); \quad |F(c')| = |F(c)| = m \times n.$$

Ces idéaux conjugués sont les mêmes que les précédents; mais ils sont exprimés avec leurs racines initiales et leur répartition en produits, ou en couples, est différente de la répartition précédente.

Exemples. — Le tableau XXII donne des exemples de calcul, à la fois de *couples d'idéaux conjugués réduits*, et de produits d'*idéaux semi réduits associés à leur racine finale.* Pour faciliter les comparaisons, les idéaux ont été exprimés avec leur plus petite racine non négative.

Dans le corps, de discriminant 145, la majorante des racines minima des idéaux réduits est $r = 3$: le carré de $(2c—S)$ devient,

Tableau XXII.

Exemples de construction d'idéaux réduits et d'idéaux semi réduits.

$F(x) = x^2+x-36$; $D = +145 = 5\times 29$, $r = 3$

c	$2c-S$	Idéaux réduits conjugués	Idéaux semi réduits
0	1	$-36 = -2^2\times 3^2$	
		$(\mathbf{1}, \theta)$	
		$(\mathbf{2}, \theta)$ | $(\mathbf{2}, \theta-1)$	
		$(\mathbf{3}, \theta)$ | $(\mathbf{3}, \theta-2)$	
		$(\mathbf{4}, \theta)$ | $(\mathbf{4}, \theta-3)$	
		$(\mathbf{6}, \theta)$ | $(\mathbf{6}, \theta-5)$	$(\mathbf{6}, \theta)\times(\mathbf{6}, \theta)$
1	3	$-34 = -2\times 17$	
2	5	$-30 = -2\times 3\times 5$	
		$(\mathbf{5}, \theta-2) = (\mathbf{5}, \theta-2)$	$(\mathbf{5}, \theta-2)\times(6, \theta-2)$
3	7	$-24 = -2^3\times 3$	
			$(\mathbf{3}, \theta)\times(8, \theta-3)$
			$(\mathbf{4}, \theta-3)\times(6, \theta-3)$
4	9	$-16 = -2^4$	
			$(\mathbf{2}, \theta)\times(8, \theta-4)$
			$(\mathbf{4}, \theta)\times(\mathbf{4}, \theta)$
5	11	$-6 = -2\times 3$	
			$(\mathbf{1}, \theta)\times(\mathbf{6}, \theta-5)$
			$(\mathbf{2}, \theta-1)\times(\mathbf{3}, \theta-2)$
6		$+6$	

$(\mathbf{1}, \theta-5) \to (\mathbf{6}, \theta)$ $(\mathbf{3}, \theta-3) \to (8, \theta-4)$
$\uparrow\!\!\downarrow$ $(\mathbf{6}, \theta-5)$ $\uparrow\!\!\downarrow$ $(\mathbf{2}, \theta-5)$
$(\mathbf{5}, \theta-2) \to (6, \theta-3) \to (\mathbf{4}, \theta-4)$
$\uparrow\!\!\downarrow$ $(6, \theta-2) \leftarrow (\mathbf{4}, \theta-3)$
$(\mathbf{3}, \theta-5) \to (\mathbf{2}, \theta-4)$
$\uparrow\!\!\downarrow$ $(8, \theta-3)$

$F(x) = x^2-58$; $D = +232 = 8\times 29$, $r = 4$

c	$2c-S$	Idéaux réduits conjugués	Idéaux semi réduits
0	0	$-58 = -2\times 29$	
		$(\mathbf{1}, \theta)$	
		$(\mathbf{2}, \theta) = (\mathbf{2}, \theta)$	
1	2	$-57 = -3\times 19$	
		$(\mathbf{3}, \theta-1)$ | $(\mathbf{3}, \theta-2)$	
2	4	$-54 = -2\times 3^3$	
		$(\mathbf{6}, \theta-2)$ | $(\mathbf{6}, \theta-4)$	$(\mathbf{6}, \theta-2)\times(9, \theta-2)$
3	6	$-49 = -7^2$	
		$(\mathbf{7}, \theta-3) \sim (\mathbf{7}, \theta-4)$	$(\mathbf{7}, \theta-3)\times(\mathbf{7}, \theta-3)$
4	8	$-42 = -2\times 3\times 7$	
			$(\mathbf{6}, \theta-4)\times(\mathbf{7}, \theta-4)$
5	10	$-33 = -3\times 11$	
			$(\mathbf{3}, \theta-2)\times(11, \theta-5)$
6	12	$-22 = -2\times 11$	
			$(\mathbf{2}, \theta)\times(11, \theta-6)$
7	14	$-9 = -3^2$	
			$(\mathbf{1}, \theta)\times(9, \theta-7)$
			$(\mathbf{3}, \theta-1)\times(\mathbf{3}, \theta-1)$
8		$+6$	

$(\mathbf{1}, \theta-7) \to (9, \theta-2) \to (\mathbf{6}, \theta-4) \to (\mathbf{7}, \theta-3)$
$\uparrow\!\!\downarrow$ $(9, \theta-7) \leftarrow (\mathbf{6}, \theta-2) \leftarrow (\mathbf{7}, \theta-4)$
$(\mathbf{2}, \theta-6) \to (\mathbf{11}, \theta-5) \to (\mathbf{3}, \theta-7)$
$\uparrow\!\!\downarrow$ $(11, \theta-6) \leftarrow (\mathbf{3}, \theta-5)$

pour cette valeur, supérieur à $|F(c)|$. Il y a 6 couples d'idéaux réduits conjugués, mais ceux de normes 1 et 5 sont doubles, d'où seulement 10 idéaux réduits .En outre les idéaux du couple, de racine minimum 0 et de norme 6 sont réfléchis, donc congrus; il y a au plus 9 classes. Ces couples sont inscrits devant la racine minimum (non négative) de l'un de leurs termes, mais ils sont indiqués avec leur plus petite racine non négative.

Le tableau a été prolongé, jusqu'à la première valeur positive de $F(c)$; devant chacune de ses valeurs, on a inscrit d'autre part les produits d'idéaux semi réduits, calculés par les relations:

$$|F(c)| = m \times n;\ |m—n| < 2c—S;\ (m,\ \theta—c_1) \times (n,\ \theta—c_2)$$

c_1 et c_2 sont les plus petites valeurs, non négatives, congrues à c, relativement aux modules respectifs m et n. Il y a, ainsi, 8 produits d'idéaux semi réduits, mais pour deux d'entre eux, de racines finales 0 et 4, leurs termes sont égaux, et de normes 6 et 4. Il n'y a donc que 14 idéaux semi réduits différents, qui comprennent les 10 idéaux réduits précédents, dont les normes sont en caractères gras, et en outre 2 couples d'idéaux conjugués, de normes 6 et 8.

Dans le corps, de discriminant pair 232, la majorante des racines minima des idéaux réduits est $r = 4$. Il y a 5 couples d'idéaux réduits conjugués, dont deux idéaux doubles, de normes 1 et 2, en tout 8 idéaux réduits différents, dont 2 réfléchis, de norme 7 (au plus 7 classes).

Il y a d'autre part 7 produits d'idéaux associés semi réduits, dont 2 à termes égaux, de racines finales 3 et 7 et de normes 7 et 3. Il n'y a donc que 12 idéaux semi réduits différents, qui comprennent les 8 idéaux réduits précédents (dont les normes sont en caractères gras) et deux couples d'idéaux conjugués, de normes 9 et 11.

Le tableau XXIII donne, pour les mêmes exemples, la correspondance entre les produits d'idéaux semi réduits associés à leur racine finale c (non négative) et les produits conjugués associés à leur racine initiale $S—c$ (négative). Chacun de ses idéaux est encore désigné par sa plus petite racine non négative.

On peut résumer comme suit la définition, et la construction, au moyen du tableau de valeurs, de tout idéal semi réduit, de son associé (relativement à la racine finale) et de son conjugué.

Tableau XXIII.

Correspondance des produits conjugués d'idéaux semi réduits associes à leurs racines finale et initiale.

$F(x) = x^2+x-36$; $D = 145 = 5\times29$			
c_f finale	$(\theta-c_f)$	c_i initiale	$(\theta-c_i)$
0	$(\mathbf{6},\ \theta)\times(\mathbf{6},\ \theta)$	—1	$(\mathbf{6},\ \theta-5)\times(\mathbf{6},\ \theta-5)$
2	$(\mathbf{5},\ \theta-2)\times(6,\ \theta-2)$	—3	$(\mathbf{5},\ \theta-2)\times(6,\ \theta-3)$
3	$(\mathbf{3},\ \theta)\times(8,\ \theta-3)$ $(\mathbf{4},\ \theta-3)\times(6,\ \theta-3)$	—4	$(\mathbf{3},\ \theta-2)\times(8,\ \theta-4)$ $(\mathbf{4},\ \theta)\times(6,\ \theta-2)$
4	$(\mathbf{2},\ \theta)\times(8,\ \theta-4)$ $(\mathbf{4},\ \theta)\times(\mathbf{4},\ \theta)$	—5	$(\mathbf{2},\ \theta-1)\times(8,\ \theta-3)$ $(\mathbf{4},\ \theta-3)\times(\mathbf{4},\ \theta-3)$
5	$(\mathbf{1},\ \theta)\times(\mathbf{6},\ \theta-5)$ $(\mathbf{2},\ \theta-1)\times(\mathbf{3},\ \theta-2)$	—6	$(\mathbf{1},\ \theta)\times(\mathbf{6},\ \theta)$ $(\mathbf{2},\ \theta)\times(\mathbf{3},\ \theta)$

$F(x) = x^2-58$; $D = 232 = 8\times29$			
c_f finale	$(\theta-c_f)$	c_i initiale	$(\theta-c_i)$
0	»	0	»
1	»	—1	»
2	$(\mathbf{6},\ \theta-2)\times(9,\ \theta-2)$	—2	$(\mathbf{6},\ \theta-4)\times(9,\ \theta-7)$
3	$(\mathbf{7},\ \theta-3)\times(\mathbf{7},\ \theta-3)$	—3	$(\mathbf{7},\ \theta-4)\times(\mathbf{7},\ \theta-4)$
4	$(\mathbf{6},\ \theta-4)\times(\mathbf{7},\ \theta-4)$	—4	$(\mathbf{6},\ \theta-2)\times(\mathbf{7},\ \theta-3)$
5	$(\mathbf{3},\ \theta-2)\times(11,\ \theta-5)$	—5	$(\mathbf{3},\ \theta-1)\times(11,\ \theta-6)$
6	$(\mathbf{2},\ \theta)\times(11,\ \theta-6)$	—6	$(\mathbf{2},\ \theta-2)\times(11,\ \theta-5)$
7	$(\mathbf{1},\ \theta)\times(9,\ \theta-7)$ $(\mathbf{3},\ \theta-1)\times(\mathbf{3},\ \theta-1)$	—7	$(\mathbf{1},\ \theta)\times(9,\ \theta-2)$ $(\mathbf{3},\ \theta-2)\times(\mathbf{3},\ \theta-2)$

Un **idéal** (canonique) **semi réduit M**, de racine finale c, est caractérisé par:

$$\mathbf{M} = (m,\ \theta - c) = (m,\ \theta - c_1);\quad c_1 \equiv c,\ (\text{mod. } m);$$
$$0 < 2c - S;\quad F(c) = -m \times n;\quad |m - n| < 2c - S [\text{ou } (m+n)^2 < D]$$

Son **idéal associé N** (relativement à sa racine finale c), qui est aussi semi réduit, est:

$$\mathbf{N} = (n,\ \theta - c) = (n,\ \theta - c_2);\quad c_2 \equiv c,\ (\text{mod. } n).$$

Son **idéal conjugué M'**, qui est aussi semi réduit, de même norme et de racine finale c', est:

$$\mathbf{M}' = (m,\ \theta - c');\quad c' \equiv S - c,\ (\text{mod. } m);$$
$$F(c') < 0 < F(c'+m);$$

on peut évidemment remplacer la racine finale c' par tout entier c'_1, congru à c' (ou à $S-c$), mod. m.

43. Idéaux semi réduits remarquables.

Par analogie avec la notion des idéaux réduits remarquables dans un corps imaginaire (**29**), on peut donner les définitions suivantes.

DÉFINITIONS. — Dans un corps quadratique réel, *parmi les idéaux semi réduits* (**42**), on peut **remarquer**, ou appeler **remarquables**:

1. un idéal qui est double (7) et qui est ainsi **semi réduit double**; il est égal à son conjugué.

2. un idéal qui est réfléchi, ou égal à son associé relativement à sa racine finale et qui est ainsi **semi réduit réfléchi** (puisque la différence des normes des idéaux associés qui est nulle est inférieure à $2c-S$, qui ne l'est pas).

THÉORÈME d'existence d'un idéal semi réduit double. — Pour qu'un idéal soit *semi réduit double*, il faut et il suffit que *sa norme m soit un diviseur du discriminant D et vérifie les comparaisons*:

1. Si D *est impair*, ou si $D = 4d$, d *impair et* m *pair*: $m^2 < D$.

2. Si $D = 4d$ et m *diviseur de* d: $m^2 < d = D:4$.

Comme D ne peut avoir d'autre facteur carré que 4 (éventuellement), m^2 ne peut être égal, ni à D, ni à $d = D:4$ (il n'y a pas de corps réel, de discriminant égal à 4).

Pour qu'un idéal canonique soit double (**7**), il faut et il suffit que sa norme divise le discriminant; c'est la conséquence de l'étude de la congruence fondamentale (**6**). La condition supplémentaire de semi réduction résulte de l'examen des deux cas.

Dans le *premier cas*, m ne divisant pas $D:4$, on utilise l'expression du polynôme:

$$4F(x) = (2x—S)^2—D;$$

on obtient des zéros conjugués, mod. m:

$$c = (S+m):2 \quad c' = S—c = (S—m):2; \qquad (c' = c—m);$$

qui sont des *racines consécutives* de l'idéal, de norme m, pour lesquelles les valeurs du polynôme sont égales:

$$4F(c) = 4F(c') = m^2—D.$$

Si $m^2 < D$, ces deux valeurs sont négatives, c'est la propriété caractéristique de semi réduction (**40**) de l'idéal, de norme m et de racines c ou c'.

Si $m^2 > D$, les deux racines c et c' et tous les autres termes de la progression:

$$c'—\lambda m;\ c+\lambda m;\ \lambda \text{ entier positif}$$

donnent à $F(x)$ des valeurs positives; l'idéal ne peut être réduit.

Dans le *deuxième cas*, on utilise l'expression du polynome:

$$F(x) = x^2—d; \qquad D = 4d.$$

m étant un diviseur de d, les entiers $—m$, 0, $+m$ sont des racines consécutives de l'idéal double, de norme m.

Si $m^2 < d$, les valeurs:

$$F(—m) = F(+m) = m^2—d,$$

sont négatives, de même que $F(0) = —d$; l'idéal est semi réduit.

Si $m^2 > d$, la valeur $F(0) = -d$ est encore négative, mais toutes les autres valeurs $F(\lambda m)$, pour tout entier λ non nul, sont positives, il n'existe pas de racines consécutives de l'idéal qui donnent à $F(x)$ des valeurs négatives; l'idéal n'est pas semi réduit.

THÉORÈME d'existence d'un idéal semi réduit réfléchi. — Pour qu'un idéal, de norme m, soit *semi réduit réfléchi, il faut et il suffit que le discriminant D soit égal à la somme des carrés de deux nombres entiers*, dont un égal à $2m$:

$$D = a^2+4m^2 \begin{cases} a \text{ impair, si } D \text{ est impair;} \\ a \text{ pair, si } D \text{ est multiple de 8.} \end{cases}$$

Il n'y a pas d'idéal semi réduit réfléchi, dans un corps dont le discriminant est quadruple d'un nombre impair ($D = 4d$; d impair).

Ainsi qu'il a été déjà vérifié (**16**), la condition de décomposition est manifestement nécessaire et suffisante pour que l'idéal:

$$\mathbf{M} = (m,\ \theta - c); \qquad 2c - S = a;$$

soit réfléchi, relativement à la racine c, qui donne à $F(x)$ la valeur négative $-m^2$.

Il n'y a pas de condition de comparaison: les deux facteurs de la décomposition de $-F(c)$ étant égaux, leur différence est nulle, donc inférieure à $2c - S = a$, qui ne peut être nul.

EXEMPLES. — Dans le corps de discriminant impair $145 = 5 \times 29$ (tableau XXII), les facteurs du discriminant D, de carré au plus égal à D sont 1 et 5, qui sont les normes des deux idéaux semi réduits doubles:

$$(\mathbf{1},\ \theta) \qquad (\mathbf{5},\ \theta - 2).$$

Aux deux décompositions du discriminant:

$$145 = 9^2+4\times 4^2, \qquad 145 = 1^2+4\times 6^2,$$

correspondent les idéaux semi réduits réfléchis:

$$(\mathbf{4},\ \theta - 4) = (\mathbf{4},\ \theta); \qquad (\mathbf{6},\ \theta),$$

de racines finales respectives 4 et 0.

Les idéaux conjugués:

$$(\mathbf{4},\ \theta+5) = (\mathbf{4},\ \theta-3), \qquad (\mathbf{6},\ \theta+1) = (\mathbf{6},\ \theta-5),$$

également semi réduits, sont réfléchis, mais relativement à leurs racines *initiales* —5 et —1 (tableau XXIII).

Dans le corps de discriminant pair $232 = 8\times29 = 4\times58$ (tableau XXII), la congruence fondamentale, qui a une racine double, mod. 2, est impossible mod. 4. Les normes des idéaux doubles ne peuvent être divisibles par 4 et sont des diviseurs de 58. Les seuls dont le carré est inférieur à 58 sont 1 et 2, qui sont les normes des idéaux réduits doubles $(\mathbf{1},\ \theta)$ et $(\mathbf{2},\ \theta)$.

Aux deux décompositions du discriminant:

$$232 = 6^2+4\times7^2; \qquad 232 = 14^2+4\times3^2;$$

(qui sont composées des mêmes termes, mais où le quadruple du carré mis en évidence n'est pas le même) correspondent les idéaux semi réduits réfléchis:

$$(\mathbf{7},\ \theta-3), \qquad (\mathbf{3},\ \theta-7) = (\mathbf{3},\ \theta-1),$$

de racines finales respectives 3 et 7. Les idéaux conjugués sont encore en évidence dans le tableau XXIII.

L'*idéal unité* est, dans tous les cas *un idéal semi réduit double*, sa norme 1 est diviseur de D comme de $D:4$ et son carré est inférieur à cette valeur. Sa racine finale est le plus grand entier c, qui donne à $F(x)$ une valeur négative; son idéal associé est l'idéal principal $(-F(c),\ \theta-c) = (\theta-c)$.

Si cet entier c donne à $F(x)$ la valeur —1, l'idéal associé est égal à l'idéal unité, qui est alors, à la fois, semi réduit double et réfléchi.

44. Cycles d'idéaux semi réduits.

On va établir que, dans un corps quadratique réel, les idéaux semi réduits peuvent être *répartis en* (un ou plusieurs) *cycles*, d'idéaux congrus entre eux. Par cycle, on entend un système de termes, en nombre fini, *ordonnés circulairement.*

A cet effet on définit et on justifie la relation d'ordre, puis la répartition qui en résulte; on vérifie la congruence, ou l'appartenance à une même classe des idéaux d'un cycle.

Dans une deuxième étape, moins évidente (**45** à **47**), on établit que *chaque classe d'idéaux d'un corps contient un et un seul cycle*, en sorte que, pour la détermination et le calcul des classes, les cycles jouent, dans un corps réel, le rôle rempli par les idéaux réduits dans un corps imaginaire (**30** et **31**).

DÉFINITIONS. — On appelle **suivant**, d'un idéal semi réduit **M**, l'idéal **N'**, égal au conjugué de l'idéal **N**, associé à **M** (relativement à sa racine finale):

suivant de **M** = conjugué de [l'associé de **M**]

On appelle **précédent**, d'un idéal semi réduit **N'**, l'idéal **M**, égal à l'associé (relativement à la racine finale) de l'idéal **N**, conjugué de **N'**:

précédent de **N'** = associé de [le conjugué de **N'**]

Le conjugué et l'associé d'un idéal semi réduit étant aussi semi réduits, il en est de même des idéaux précédent et suivant. En outre leurs constructions sont manifestement déterminées et réciproques; c'est ce qu'exprime le théorème suivant.

THÉORÈME de la réciprocité de la succession. — Tout idéal semi réduit est *le suivant d'un et un seul idéal semi réduit, qui est l'idéal précédent*;

il est le précédent d'un et un seul idéal semi réduit qui est l'idéal suivant:

précédent du suivant de **M** = suivant du précédent de **M** = **M**.

Le suivant et le précédent sont déterminés comme le sont le conjugué et l'associé; leurs constructions sont d'ailleurs évidentes sur le tableau des valeurs négatives de $F(c)$; pour c entier croissant à partir de 0.

Un idéal semi réduit **M** étant donné par sa norme m et sa racine finale c, on calcule la norme n, *puis* la racine finale c', de l'idéal suivant **N'** par les formules:

$$n = -F(c):m; \qquad c' = S-c+\lambda n;$$

λ étant choisi par la condition que c' soit le dernier terme de la progression arithmétique, qui figure dans le tableau, c'est-à-dire qui

donne à $F(x)$ une valeur négative. Ce choix est possible, puisque $\mathbf{N}'$ étant semi réduit, il existe dans le tableau, au moins un terme de la progression (de ses racines).

Inversément un idéal semi réduit $\mathbf{N}'$ étant donné par sa norme n et sa racine finale c', on calcule la racine finale c, *puis* la norme m, de l'idéal précédent $\mathbf{M}$ par les formules:

$$c = S - c' + \lambda n; \qquad m = -F(c) : n;$$

λ étant choisi par la condition que c soit le dernier terme de la progression arithmétique qui figure dans le tableau. Ce choix est aussi possible, puisque l'idéal $\mathbf{M}$ est semi réduit.

Ces deux constructions et leur détermination prouvent que:

$$\mathbf{N}' = \text{suivant de } \mathbf{M} \iff \mathbf{M} = \text{précédent de } \mathbf{N}'.$$

Théorème de répartition en cycles. — Dans un corps quadratique réel, *les idéaux semi réduits peuvent être* **répartis** *en* (un ou plusieurs) **cycles** (ou systèmes d'un nombre fini d'idéaux), *tels que*:

un cycle contient le précédent et le suivant de chacun de ses idéaux.

Par « *répartition* », on entend que chaque idéal semi réduit appartient à un et un seul cycle, de sorte que deux cycles différents n'ont pas d'élément commun et que la réunion des cycles est égale au système des idéaux semi réduits.

D'autre part, un cycle ayant un nombre fini h, de termes, l'appartenance du précédent et du suivant peut être exprimée par la possibilité d'affecter, à chaque idéal du cycle, un indice i, entier défini mod. h, tel que:

$$\text{suivant de } \mathbf{M}_i = \mathbf{M}_{i+1}; \qquad \text{précédent de } \mathbf{M}_i = \mathbf{M}_{i-1}.$$

Construction d'un cycle. — Un idéal semi réduit étant choisi arbitrairement et affecté de l'indice 0, on construit les suivants successifs, affectés des indices i, a priori entiers positifs successifs

$$\mathbf{M}_1 = \text{suivant de } \mathbf{M}_0; \quad \ldots \quad \mathbf{M}_{i+1} = \text{suivant de } \mathbf{M}_i; \quad \ldots$$

Ils ne peuvent être indéfiniment différents, puisque les idéaux semi réduits sont en nombre fini. On désigne par $\mathbf{M}_h$ le premier idéal ainsi construit, qui soit égal à un idéal déjà obtenu $\mathbf{M}_i$, donc d'indice i, au plus égal à h. Ce ne peut être que $\mathbf{M}_0$; si non $\mathbf{M}_i$ aurait un précé-

dent $\mathbf{M}_{i-1}$, à qui serait égal le précédent $\mathbf{M}_{h-1}$, de $\mathbf{M}_h$, ce qui serait contraire à la détermination de h.

Les h idéaux, ainsi construits de $\mathbf{M}_0$ à $\mathbf{M}_{h-1}$ sont différents et:

$\mathbf{M}_i$ = suivant de $\mathbf{M}_{i-1}$ $(0 < i < h)$; et $\mathbf{M}_0$ suivant de $\mathbf{M}_{h-1}$.

En affectant chaque idéal de l'indice $i+\lambda h$, (ou i, défini mod. h) ces deux relations sont équivalentes à la relation unique:

$$\mathbf{M}_i = \text{suivant de } \mathbf{M}_{i-1}; \quad i,\ i-1, \text{ définis mod. } h.$$

La réciprocité de la succession entraîne $\mathbf{M}_i$ = précédent de $\mathbf{M}_{i+1}$.

On a ainsi établi l'appartenance de tout idéal semi réduit à un cycle et l'ordonnance des idéaux d'un cycle.

Répartition. — La même construction faite en partant d'un idéal quelconque $\mathbf{M}_a$ du cycle, désigné par $\mathbf{P}_0$ redonne évidemment les mêmes idéaux, dans la même ordonnance circulaire, ou, plus précisément avec la correspondance

$$\mathbf{P}_i = \mathbf{M}_{a+i}; \ (i,\ a,\ a+i, \text{ définis mod. } h).$$

La propriété est évidente par récurrence sur i: $\mathbf{P}_{i+1}$ et $\mathbf{M}_{a+i+1}$ étant respectivement les suivants de $\mathbf{P}_i$ et $\mathbf{M}_{a+i}$. Cette remarque montre que deux cycles qui ont un élément commun sont égaux (propriété de répartition).

Il peut se faire qu'un cycle ne contienne qu'un seul idéal, ou que $h = 1$. Pour cela il faut et il suffit que l'idéal $\mathbf{M}_0$ choisi pour l'engendrer soit égal à son suivant et à son précédent, c'est-à-dire encore au conjugué de son associé et à l'associé de son conjugué. Sa norme m_0 et sa racine finale c_0 doivent vérifier:

$$F(c_0) = -m_0^2; \quad 2c_0 \equiv S, \pmod{m_0}.$$

L'idéal est, à la fois semi réduit double et associé. Les égalités vérifiées par un idéal réfléchi:

$$D = (2c_0+1)^2+4m_0^2, \quad \text{ou} \quad D:4 = c_0^2+m_0^2; \ (c_0,\ m_0 \text{ impairs})$$

jointes à celles de l'idéal double, montrent que m_0^2 doit diviser D ou $D:4$. Ceci n'est possible que pour $m_0 = 1$, c'est-à-dire pour le seul idéal unité, et dans un corps dont le discriminant a une valeur de la forme:

$$(2c+1)^2+4, \quad \text{ou} \quad 4.(c^2+1), \ c \text{ entier impair.}$$

C'est le cas déjà signalé ci-dessus (**43**); alors:

$$F(c) = -1 \quad \text{et} \quad \mathbf{M} = (1,\ \theta - c).$$

Exemples. — $D = 13$; $F(x) = x^2 + x - 3$; $\mathbf{M} = (1,\ \theta - 1)$.

$D = 173$; $F(x) = x^2 + x - 43$; $\mathbf{M} = (1,\ \theta - 6)$.

$D = 104$; $F(x) = x^2 - 26$; $\mathbf{M} = (1,\ \theta - 5)$.

Théorème de congruence. — *Tous les idéaux* (semi réduits) *d'un cycle sont congrus entre eux.* La congruence d'un idéal $\mathbf{M}_i$ et de son suivant $\mathbf{M}_{i+1}$, définis respectivement par leurs normes m_i, m_{i+1} et leurs racines finales c_i, c_{i+1}, peut être explicitée par l'égalité:

$$(m_{i+1}) \times \mathbf{M}_i = (\theta - c_i) \times \mathbf{M}_{i+1}; \text{ ou } \mathbf{M}_i = ([\theta - c_i] : m_{i+1}) \times \mathbf{M}_{i+1}.$$

On peut considérer que les parenthèses représentent soit des éléments du corps, soit les idéaux principaux qui ont ces éléments pour bases respectives.

On a indiqué que deux idéaux associés, **M**, **N**, relativement à une racine c, appartiennent à des classes inverses, ou conjuguées (**24**), puisque leur produit $\mathbf{M} \times \mathbf{N}$ est égal à un idéal principal $(\theta - c)$. Le conjugué $\mathbf{N}'$, de l'un d'eux **N**, appartient donc à la classe définie par l'autre **M**, ou lui est congru. On peut d'ailleurs le vérifier directement par la suite d'égalités (où n est la norme de **N**):

$$(n) \times \mathbf{M} = (\mathbf{N}' \times \mathbf{N}) \times \mathbf{M} = (\mathbf{M} \times \mathbf{N}) \times \mathbf{N}' = (\theta - c) \times \mathbf{N}'.$$

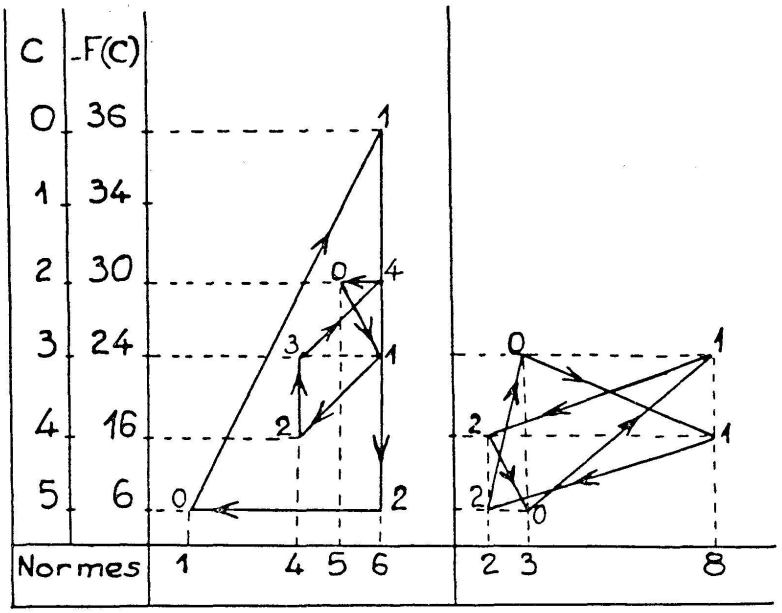
L'égalité des termes extrêmes est celle qui a été indiquée entre un idéal et son suivant, dans un cycle.

Exemples. — On a complété le tableau XXII en indiquant la répartition en cycles, des idéaux semi réduits, désignés par leurs racines finales et séparés par des flèches qui indiquent le passage d'un idéal à son suivant.

Dans le corps de discriminant 145, il y a 4 *cycles*, l'un contient l'idéal unité (de racine finale 5) et deux autres idéaux (conjugués) de norme 6 qui, étant congrus à (1), sont aussi principaux [c'est d'ailleurs ce que montre la décomposition de $F(c) = -1 \times 6$]. Un autre cycle de 5 idéaux comprend un idéal double, de norme 5 et un

idéal réfléchi, de norme 4; les idéaux de ce cycle appartiennent par suite à une même *classe double*. Enfin deux autres cycles, de chacun 3 idéaux ne comprennent pas d'idéaux remarquables, leurs idéaux sont respectivement conjugués (de normes 3, 8, 2) dans chaque cycle, mais dans un ordre différent. Ces cycles appartiennent par suite à deux classes conjuguées, ou inverses, ou dont le produit est égal à la classe principale.

TABLEAU XXIV



Dans le corps de discriminant 232, il y a deux cycles. L'un contient l'idéal unité (de racine finale 7) et 6 autres idéaux (deux à deux conjugués) qui sont par suite principaux. Cette qualité est d'ailleurs mise en évidence par les décompositions successives des valeurs:

$$F(7) = -1\times 9 \Rightarrow (9,\ \theta-7) \sim (1) \quad \text{et} \quad (9,\ \theta-2) \sim 1;$$
$$F(2) = -9\times 6 \Rightarrow (6,\ \theta-2) \sim (1) \quad \text{et} \quad (6,\ \theta-4) \sim 1;$$
$$F(4) = -6\times 7 \Rightarrow (7,\ \theta-4) \sim (1) \quad \text{et} \quad (7,\ \theta-3) \sim 1.$$

L'autre cycle de 5 idéaux contient un idéal double, de norme 2, un idéal réfléchi, de norme 3, son conjugué et deux idéaux conjugués de norme 11. Les idéaux de ce cycle appartiennent donc à une classe double.

Le schéma XXIV illustre la construction des cycles; ils sont représentés par des lignes polygonales fermées: à un idéal correspond un sommet, dont l'abscisse est la norme et dont l'ordonnée est la

racine finale. Les côtés orientés de la ligne indiquent les passages d'un idéal à son suivant. (Pour la clarté des figures, on a consacré deux graphiques, chacun à deux cycles.)

Un *idéal double*, qui est le suivant d'un idéal, de même racine finale, est représenté par l'extrémité d'un côté, parallèle à l'axe des normes. Un *idéal réfléchi*, qui a la même norme que son suivant, est représenté par l'origine d'un côté, parallèle à l'axe des racines. On peut encore remarquer que les idéaux suivant et précédent d'un idéal double ont des normes égales; les sommets voisins (précédent et suivant) du sommet représentatif sont sur une même parallèle à l'axe des racines.

45. Multiplicateurs d'un cycle d'idéaux semi réduits.

On peut exprimer les relations de congruence entre les idéaux d'un cycle, en utilisant une suite d'éléments du corps, dont les termes se reproduisent en progressions géométriques.

DÉFINITION. — Relativement à un cycle d'idéaux semi réduits:

$$\mathbf{M}_i = (m_i, \theta - c_i); \qquad i, \quad \text{mod. } h;$$

on appelle **multiplicateurs** *une suite*, doublement illimitée, *d'éléments* ρ_i *du corps, vérifiant la relation de récurrence:*

$$(\theta - c_i) \times \rho_i = m_{i+1} \times \rho_{i+1}; \qquad i \text{ entier quelconque};$$

dont les coefficients sont, avec une transposition, ceux de la relation de récurrence entre les idéaux du cycle.

On convient, en outre, de prendre $\rho_0 = 1$, ce qui revient à distinguer, plus spécialement l'idéal $\mathbf{M}_0$, affecté de l'indice nul, dans le cycle.

De cette construction, on déduit l'expression des multiplicateurs au moyen de l'un d'entre eux (notamment de ρ_0):

$$\left.\begin{aligned} \rho_{r+\lambda} &= \rho_r \times [\Pi(\theta - c_{i-1})] : [\Pi m_i]; \quad i \text{ de } r+1 \text{ à } r+\lambda; \\ \rho_{r-\lambda} &= \rho_r \times [\Pi m_{i+1}] : [\Pi(\theta - c_i)]; \quad i \text{ de } r-\lambda \text{ à } r-1; \end{aligned}\right\} \lambda \text{ entier positif.}$$

En particulier, on obtient ρ_λ et $\rho_{-\lambda}$, en prenant r nul et $\rho_0 = 1$. On aurait pu, plus généralement, choisir arbitrairement la valeur d'un des multiplicateurs ρ_r, toutefois égale à un élément du corps.

La périodicité des coefficients $\theta - c_i$ et m_i (i défini mod. h) entraîne une répartition en h progressions géométriques des multiplicateurs ρ_i; (ou une périodicité de multiplication):

THÉORÈME de la périodicité de multiplication. — *Pour des indices en progression arithmétique, de raison h* (nombre d'éléments du cycle), *les multiplicateurs forment une progression géométrique*, dont la raison est un élément ω, du corps:

$$\rho_{r+\mu h} = \rho_r \times \omega^{\mu}; \quad \omega = [\Pi(\theta - c_j)] : [\Pi m_j]; \quad j \text{ de } 0 \text{ à } h-1;$$

μ entier quelconque.

En remplaçant λ par h, dans l'expression des multiplicateurs, au moyen de ρ_r, on obtient:

$$\rho_{r+h} = \rho_r \times \omega; \quad \omega = [\Pi(\theta - c_{i-1})] : [\Pi m_i]; \quad i \text{ de } r+1 \text{ à } r+h.$$

Mais, en raison de la périodicité de c_i et de m_i, les deux produits $\Pi(\theta - c_j)$, et Πm_j ont des valeurs déterminées, quand j prend h valeurs entières successives quelconques, ce qui est le cas pour les deux termes du quotient précédent; sa valeur ω est donc indépendante de r et notamment est égale à l'expression de l'énoncé du théorème.

L'expression de $\rho_{r+\mu h}$ s'en déduit immédiatement, par récurrence sur μ (positif ou négatif).

La relation entre multiplicateurs et idéaux du cycle est alors exprimée par l'égalité:

le produit $\rho_i \times \mathbf{M}_i$, ou $(\rho_i) \times \mathbf{M}_i$, de chaque idéal $\mathbf{M}_i$, du cycle par le multiplicateur ρ_i, de même indice (défini, mod. h), ou par l'idéal principal (ρ_i) qui a ce multiplicateur pour base, *est égal à l'idéal* $\mathbf{M}_0$ *d'indice nul* (on a convenu $\rho_0 = 1$):

$$\rho_i \times \mathbf{M}_i \quad \text{ou} \quad (\rho_i) \times \mathbf{M}_i = \mathbf{M}_0.$$

Il est équivalent de dire que l'idéal $(\rho_i) \times \mathbf{M}_i$ est un idéal invariant dont une expression est notamment $(1) \times \mathbf{M}_0$. On peut vérifier d'abord cette invariance lorsque i est remplacé par $i+1$. Elle résulte du rapprochement des deux relations de récurrence, entre les idéaux et entre

les multiplicateurs, qu'on peut remplacer par les idéaux principaux qui les ont pour bases:

$$(m_{i+1})\times\mathbf{M}_i = (\theta—c_i)\times\mathbf{M}_{i+1}; \quad (\rho_i)\times(\theta—c_i) = (\rho_{i+1})\times(m_{i+1});$$

en les multipliant membre à membre, puis en divisant par le produit des idéaux principaux $(m_{i+1})\times(\theta—c_i)$, qui n'est pas nul, on obtient:

$$(\rho_i)\times\mathbf{M}_i = (\rho_{i+1})\times\mathbf{M}_{i+1}.$$

La relation s'étend au remplacement de i par $i+\lambda$, par récurrence sur λ entier quelconque.

Si ρ_r (au lieu de ρ_0) était choisi égal à un élément γ du corps, la valeur commune des idéaux $(\rho_i)\times\mathbf{M}_i$ serait $(\gamma)\times\mathbf{M}_r$.

On déduit encore de cette propriété que les produits d'un idéal $\mathbf{M}_i$ par tous les multiplicateurs, d'indice $i+\lambda h$, sont égaux; notamment:

$$\mathbf{M}_0 = (\rho_{\lambda h})\times\mathbf{M}_0 = (\omega^\lambda)\times\mathbf{M}_0$$

Théorème des diviseurs de l'unité (I). — *Les puissances et leurs opposés*, $\pm\omega^\lambda$, de l'élément ω construit au moyen des idéaux $(m_j,\ \theta—c_j)$, semi réduits d'un cycle:

$$\omega = [\Pi(\theta—c_j)]:[\Pi m_j]; \quad j \text{ de } 0 \text{ à } h—1; \quad \lambda \text{ entier};$$

sont des diviseurs de l'unité du corps (**3**).

L'égalité de $\mathbf{M}_0$ et de son produit par l'idéal principal (ω^λ), exige que cet idéal soit égal à l'idéal unité (**14**) et par suite que sa base ω^λ, et l'opposé $—\omega^\lambda$ soient des diviseurs de l'unité du corps (**11**).

On montre ci-dessous que, réciproquement, tous les diviseurs de l'unité du corps sont obtenus ainsi; il en résulte notamment que les valeurs de $\pm\omega$, sont les mêmes pour chacun des cycles d'idéaux semi réduits, (**48**).

Exemples. — Dans le corps de discriminant 145 (tableau XXII), les idéaux semi réduits, du cycle engendré par l'idéal unité peuvent être affectés des indices (i, mod. 3):

$$\mathbf{M}_0 = (1,\ \theta—5); \quad \mathbf{M}_1 = (6,\ \theta); \quad \mathbf{M}_2 = (6,\ \theta—5);$$

les racines étant, bien entendu finales. Les multiplicateurs sont:

$$\rho_0 = 1;\ \rho_1 = (\theta—5):6;\ \rho_2 = \rho_1\times(\theta:6) = (\theta—5)\times\theta:36 = (—\theta+6):6$$

Les autres multiplicateurs sont des produits de ceux là par des puissances de $\omega = \rho_3$, qui est égal à:

$$\omega = \rho_3 = \rho_2 \times (\theta - 5) : 1 = (-\theta + 6) \times (\theta - 5) : 6 = 2\theta - 11.$$

On vérifie aisément que ω et, par suite ses puissances et leurs opposées sont des diviseurs de l'unité; il suffit de calculer la norme de ω:

$$N(\omega) = \omega \times \omega' = (2\theta - 11) \times (2\theta' - 11) = -4 \times 36 + 22 + 121 = -1.$$

Pour le cycle de 5 idéaux:

$$\mathbf{M}_0 = (5,\ \theta - 2),\quad \mathbf{M}_1 = (6,\ \theta - 3),\quad \mathbf{M}_2 = (4,\ \theta - 4),$$
$$\mathbf{M}_3 = (4,\ \theta - 3),\quad \mathbf{M}_4 = (6,\ \theta - 2);$$

les multiplicateurs sont:

$$\rho_0 = 1,\quad \rho_1 = (\theta - 2) : 6,\quad \rho_2 = (-\theta + 7) : 4,\quad \rho_3 = (3\theta - 16) : 4,$$
$$\rho_4 = (-7\theta + 39) : 6;\ \omega = \rho_5 = 2\theta - 11.$$

On retrouve la valeur précédente.

Dans le cas d'un cycle d'un seul idéal $(1,\ \theta - c)$, les multiplicateurs sont les puissances de:

$$\omega = \rho_1 = (\theta - c);$$

cet élément est d'ailleurs manifestement un diviseur de l'unité:

$$(\theta - c) \times (\theta' - c) = F(c) = -1.$$

46. Suite de bases d'un idéal semi réduit.

A un cycle d'idéaux semi réduits $\mathbf{M}_i$ auquel est associé une suite de multiplicateurs ρ_i, on peut aussi associer une suite de bases, arithmétiques libres de l'idéal $\mathbf{M}_0$ (qui peut être choisi arbitrairement dans le cycle, ou même être remplacé par un idéal $(\gamma) \times \mathbf{M}_r$).

Théorème de la suite des bases. — *Dans l'idéal* $\mathbf{M}_0$, d'un cycle d'idéaux semi réduits $\mathbf{M}_i = (m_i,\ \theta - c_i)$, *on peut construire une suite*, doublement illimitée, d'*éléments* α_i (entiers de $\mathbf{M}_0$), par les relations:

$$\alpha_i = m_i \times \rho_i = (\theta - c_{i-1}) \times \rho_{i-1};$$
$$\alpha_{i+1} = m_{i+1} \times \rho_{i+1} = (\theta - c_i) \times \rho_i;$$

Tout couple d'éléments successifs α_i, α_{i+1} *constitue une base arithmétique libre de* $\mathbf{M}_0$.

Les ρ_i sont les multiplicateurs définis ci-dessus par la relation de récurrence, de coefficients m_i, $\theta - c_i$; il en résulte l'égalité des deux expressions données pour chaque élément.

D'autre part le couple d'éléments m_i, $\theta - c_i$ est la base canonique, donc arithmétique libre, de l'idéal $\mathbf{M}_i$; son produit par ρ_i est donc encore une base arithmétique libre de l'idéal congru $(\rho_i)\times\mathbf{M}_i$, qui est précisément $\mathbf{M}_0$ (**24**). Notamment pour $i = 0$, on trouve la base canonique de $\mathbf{M}_0$: m_0 et $\theta - c_0$.

On peut calculer directement les α_i par la relation de récurrence, déduite de leur définition:

$$\alpha_0 = m_0; \qquad m_i \times \alpha_{i+1} = (\theta - c_i) \times \alpha_i.$$

Ils ont la même périodicité de multiplication que les multiplicateurs ρ_i; l'expression de ω résulte immédiatement de leur récurrence:

$$\alpha_{r+\mu h} = \alpha_r \times \omega^{\mu}; \qquad \omega = [\Pi(\theta - c_i)] : [\Pi m_i]; \quad i \text{ de } 0 \text{ à } h-1.$$

On vérifie ci-dessous (**48**) par un calcul direct, que les α_i sont bien des entiers de l'idéal et on indique une loi de récurrence linéaire.

Exemples. — Corps de discriminant 145 (tableau XXII) et cycle engendré par l'idéal unité $\mathbf{M}_0 = (1, \theta - 5)$:

i	c_i	m_i	
..	..	..	
-1	5	6	$\alpha_{-1} = 1:[(\theta-5):6] = -\theta'+5 = \theta+6;$
0	**5**	**1**	$\alpha_0 = 1$
1	**0**	**6**	$\alpha_1 = 1\times[(\theta-5):1] = \theta-5;$
2	**5**	**6**	$\alpha_2 = \alpha_1\times[\theta:6] = [(\theta-5)\theta]:6 = -\theta+6$
3	5	1	$\alpha_3 = \alpha_2\times[(\theta-5):6] = (-\theta+6)\times(\theta-5):6 = 2\theta-11 = \omega.$
..	..	..	... ...

Dans le cas d'un cycle d'un seul idéal $(1,\ \theta—c)$, les multiplicateurs ρ_i et les termes des bases α_i sont les puissances de $\theta—c$:

$$\ldots\ (\theta—c)^{-1} = —\theta'+c,\quad 1,\quad \theta—c,\quad (\theta—c)^2,\ \ldots$$

On peut caractériser les bases ainsi construites par des comparaisons de grandeurs entre leurs éléments et, éventuellement, avec les éléments de l'idéal, considérés comme des *nombres réels*. Pour ce faire il convient de distinguer les deux zéros (irrationnels, mais réels) de $F(x)$; on convient de désigner par θ (lettre non accentuée) celui qui est positif. On peut alors énoncer une autre condition de semi réduction.

THÉORÈME caractéristique de semi réduction. — *Pour qu'un idéal* $\mathbf{M} = (m,\ \theta—c)$ *soit semi réduit*, et admette c comme racine finale, *il faut et il suffit que*: les nombres qui constituent sa base vérifient les conditions de comparaison:

$$0 < (\theta—c):m < 1;\qquad (\theta'—c):m < —1.$$

Les conditions de semi réduction peuvent être exprimées par le signe des valeurs de $F(x)$ pour les trois racines successives, encadrant la racine finale c:

$$F(c—m) < 0;\quad F(c) < 0;\quad F(c+m) > 0.$$

Il est équivalent de dire que $c—m$ et c sont compris entre les zéros θ' et θ et que $c+m$ est supérieur à θ (sans égalités possibles, $F(x)$ n'ayant pas de zéro rationnel). Cette condition peut être exprimée par:

$$\theta' < c—m < c < \theta < c+m \quad\Leftrightarrow\quad (\theta'—c) < —m < 0 < (\theta—c) < m$$
$$\Leftrightarrow\quad (\theta'—c):m < —1 \quad \textit{et} \quad 0 < (\theta—c):m < +1.$$

De cette condition, on déduit les propriétés suivantes des multiplicateurs ρ_i et de la suite des termes α_i des bases de $\mathbf{M}_0$.

Les multiplicateurs ρ_i sont positifs et tendent vers 0, lorsque i tend vers $+\infty$ et vers $+\infty$ lorsque i tend vers $—\infty$.

Les éléments α_i de la suite des bases réduites sont positifs décroissants, de $+\infty$ à 0 (pour i de $—\infty$ à $+\infty$).

Les conjugués α_i' de ces éléments sont alternativement positifs et négatifs; leurs valeurs absolues sont croissantes, de 0 à $+\infty$ (pour i de $—\infty$ à $+\infty$).

Les limites pour i infini des multiplicateurs ρ_i et des éléments α_i résultent de leur appartenance à des progressions géométriques. La raison ω, de ces progressions est le produit de quotients $(\theta—c_i):m_i$ (i de 0 à $h—1$) positifs et inférieurs à 1; elle est donc inférieure à 1, d'où les limites des termes des progressions.

La croissance des éléments α_i et de leurs conjugués α_i', et la comparaison (des signes) des éléments consécutifs, résulte de leur construction au moyen des bases de $\mathbf{M}_i$, qui sont semi réduits:

$$\alpha_{i+1}:\alpha_i = [\rho_i\times(\theta—c_i)]:[\rho_i\times m_i] = (\theta—c_i):m_i < 1,$$
$$\alpha_{i+1}':\alpha_i' = [\rho_i'\times(\theta'—c_i)]:[\rho_i'\times m_i] = (\theta'—c_i):m_i < —1.$$

47. Détermination des cycles.

La considération de la suite des bases de $\mathbf{M}_0$ permet d'établir que les cycles d'idéaux semi réduits représentent les classes *proprement.*

Théorème de la détermination des cycles. — Dans un corps réel, *chaque classe d'idéaux contient un et un seul cycle d'idéaux semi réduits.*

En définissant les idéaux (canoniques) réduits (**20**), pour un corps quadratique quelconque (réel ou imaginaire), il a été établi que toute classe d'idéaux contient au moins un idéal $\mathbf{M}_0$ réduit, qui, pour un corps réel, est, a fortiori, semi réduit (**40**). La classe renferme, par suite, le cycle des idéaux réduits $\mathbf{M}_i$, obtenus en formant les suivants successifs de $\mathbf{M}_0$, puisque ces idéaux sont congrus à $\mathbf{M}_0$.

Pour établir que le cycle ainsi construit est unique, on peut d'abord démontrer que:

dans un idéal $\mathbf{M}_0$ semi réduit, *pour qu'une base arithmétique libre*, de deux éléments positifs $\gamma_j > \gamma_{j+1}$, *appartienne à la suite des bases*, $\alpha_i\,\alpha_{i+1}$, associée au cycle d'idéaux semi réduits engendré par $\mathbf{M}_0$, *il faut et il suffit que*: ces termes et leurs conjugués vérifient les comparaisons:

$$\gamma_{j+1}:\gamma_j < 1; \quad \gamma_{j+1}':\gamma_j' < —1;$$

la première résulte de l'ordre adopté pour numéroter les deux termes.

La condition est *nécessaire* puisqu'elle a été vérifiée ci-dessus pour la suite des bases α_i.

Pour démontrer qu'elle est *suffisante*, il peut être commode d'établir d'abord que pour un idéal qui a une base vérifiant ces conditions (même s'il n'est pas semi réduit):

tout élément non nul ξ, de cet idéal, dont la valeur absolue n'est égale ni à γ_j, ni à γ_{j+1}, *vérifie l'une*, au moins, des *comparaisons*:

$$|\xi| > \gamma_j > \gamma_{j+1}; \quad \text{ou} \quad |\xi'| > |\gamma'_{j+1}| > |\gamma'_j|.$$

Cet élément ξ peut être construit par additions et soustractions au moyen des termes de la base considérée, de sorte que:

$$\xi = x\gamma_j + y\gamma_{j+1}; \quad \xi' = x\gamma'_j + y\gamma'_{j+1}; \quad x, y \text{ nombres entiers.}$$

Il suffit alors d'examiner les divers cas, dépendant des signes et de la nullité des entiers x, y:

$xy > 0$: $|\xi| = |x\gamma_j + y\gamma_{j+1}| = |x\gamma_j| + |y\gamma_{j+1}| > \gamma_j$;

$xy < 0$: $|\xi'| = |x\gamma'_j + y\gamma'_{j+1}| = |x\gamma'_j| + |y\gamma'_{j+1}| > |\gamma'_{j+1}|$;

$y = 0$ et $|x| \neq 1$: $|\xi| = |x\gamma_j| > \gamma_j$;

$x = 0$ et $|y| \neq 1$: $|\xi'| = |y\gamma'_{j+1}| > |\gamma'_{j+1}|$.

On peut mettre la disjonction ainsi vérifiée sous la forme d'implications:

$$|\xi| < \gamma_j \Rightarrow |\xi'| \geqslant |\gamma'_{j+1}|;$$
$$|\xi'| < |\gamma'_{j+1}| \Rightarrow |\xi| \geqslant \gamma_j.$$

Ceci acquis, on compare, dans $\mathbf{M}_0$, à la suite des bases $\alpha_i\ \alpha_{i+1}$, une base $\gamma_j\ \gamma_{j+1}$ vérifiant la condition indiquée. La suite des α_i décroissant de $+\infty$ à 0, γ_j est situé dans l'un des intervalles, il existe i, tel que:

$$\alpha_i \geqslant \gamma_j > \alpha_{i+1}.$$

Il y a égalité, si non d'après la propriété précédente, appliquée à γ_j comparée à la base des α, puis à α_{i+1}, comparée à la base des γ:

$$\gamma_j < \alpha_i \Rightarrow |\gamma'_j| > |\alpha'_{i+1}| \Rightarrow \alpha_{i+1} > \gamma_j;$$

ce qui est contradictoire avec le choix de α_i.

On peut alors comparer α_{i+1} à la base $\gamma_j = \alpha_i$, γ_{j+1}; il en résulte:

$$\alpha_{i+1} < \alpha_i = \gamma_j \Rightarrow |\alpha'_{i+1}| \geqslant |\gamma'_{j+1}|.$$

La dernière comparaison est une égalité, si non la comparaison de γ_{j+1} à la base des α entrainerait:

$$|\gamma'_{j+1}| < |\alpha'_{i+1}| \quad \Rightarrow \quad \gamma_{j+1} > \alpha_i = \gamma_j,$$

ce qui est contradictoire avec la définition de la base des γ.

L'égalité des valeurs absolues $|\gamma'_{j+1}| = |\alpha'_{i+1}|$ entraîne celle des conjugués $\gamma_{j+1} = \alpha_{i+1}$, puisqu'ils sont positifs.

Le théorème résulte aisément de cette propriété préalable: si un idéal $\mathbf{M} = (m,\ \theta—c)$, semi réduit, de racine finale c, est congru aux idéaux $\mathbf{M}_i$ d'un cycle et notamment à $\mathbf{M}_0$, dans lequel est construit une suite de bases $\alpha_i\,\alpha_{i+1}$, il existe un élément ρ, qui peut être choisi positif, tel que $(\rho)\times\mathbf{M}$ soit égal à $\mathbf{M}_0$. Le couple d'éléments:

$$\gamma_j = \rho\times m \quad \gamma_{j+1} = \rho\times(\theta—c)$$

est une base arithmétique libre de $\mathbf{M}_0$, qui vérifie les conditions précédentes et qui par suite est égale à une des bases de la suite:

$$\rho\times m = \alpha_i = \rho_i\times m_i \quad \rho\times(\theta—c) = \alpha_{i+1} = \rho_i(\times\theta—c_i).$$

Dans la dernière égalité, la comparaison des coefficients de θ montre que:

$$\rho = \rho_i, \quad m = m_i, \quad c = c_i, \quad \mathbf{M} = \mathbf{M}_i.$$

Tout idéal **M**, *semi réduit, congru aux idéaux d'un cycle d'idéaux semi réduits est égal à un idéal de ce cycle.*

48. Diviseurs de l'unité.

Théorème des diviseurs de l'unité (II). — Dans un corps réel, pour chacun des cycles d'idéaux semi réduits, désignés par leurs racines finales:

$$\mathbf{M}_i = (m_i,\ \theta—c_i); \qquad i \text{ de } 0 \text{ à } h—1;$$

les diviseurs de l'unité sont égaux aux produits par $+1$ *et* $—1$ *des puissances* ω^λ, (d'exposants λ entiers quelconques) *de:*

$$\omega = [\Pi(\theta—c_i)]:[\Pi m_i]; \qquad i \text{ de } 0 \text{ à } h—1.$$

Cette expression a la même valeur pour tous les cycles du corps.

On a déjà indiqué (Théorème I des diviseurs de l'unité, **45**) que les éléments $+\omega^\lambda$ et $-\omega^\lambda$ sont des diviseurs de l'unité. Réciproquement, les opposés de diviseurs de l'unité étant encore des diviseurs de l'unité, on peut se borner à chercher ceux qui sont positifs.

On considère un cycle, engendré par un idéal semi réduit $\mathbf{M}_0 = (m_0,\ \theta - c_0)$, dans lequel on a construit une suite de bases de termes positifs α_i. Le produit $\eta \times \mathbf{M}_0$, de cet idéal par un diviseur positif η, de l'unité, lui reste égal et les éléments positifs $\eta \times m_0$ et $\eta \times (\theta - c_0)$ en constituent une base arithmétique libre. Comme cette base vérifie les relations:

$$[\eta \times (\theta - c_0)] : (\eta \times m_0) = (\theta - c_0) : m_0 < 1;$$
$$[\eta' \times (\theta' - c_0)] : (\eta' \times m_0) = (\theta' - c_0) : m_0 < -1;$$

elle est égale à l'une des bases de la suite, de sorte que:

$$\eta \times (\theta - c_0) = \alpha_{i+1} = \rho_i \times (\theta - c_i);$$

ce qui entraîne:

$$\eta = \rho_i, \quad c_0 = c_i \quad \Rightarrow \quad i = \lambda h; \quad \eta = \omega^\lambda; \quad \lambda \text{ entier.}$$

La démonstration montre notamment que *la valeur de l'expression qui donne* ω *est indépendante du cycle utilisé.* On peut obtenir cette valeur par un calcul de multiplication, dans le corps quadratique (en utilisant la relation $\theta^2 = -S\theta + N$), notamment en cherchant de proche en proche les valeurs $\alpha_{i+1} = \alpha_i \times (\theta - c_i) : m_i$.

On peut aussi utiliser une relation linéaire qui existe entre trois termes successifs de la suite des α_i:

$$\alpha_{i+1} = \alpha_{i-1} - q_i \times \alpha_i; \qquad q_i = (c_i + c_{i-1} - S) : m_i.$$

Cette égalité résulte de la construction des idéaux successifs du cycle: l'idéal $\mathbf{M}_i = (m_i,\ \theta - c_i)$ est le conjugué de l'associé de son précédent $\mathbf{M}_{i-1}$, de sorte que:

$$c_i + c_{i-1} \equiv S, \text{ (mod. } m_i); \qquad \text{ou} \qquad c_i = S - c_{i-1} + q_i \times m_i;$$

q_i étant le nombre entier positif, indiqué plus haut.

En transportant cette valeur dans la relation de récurrence multiplicative des α_i, on obtient:

$$\alpha_{i+1} = [(\theta - c_i) : m_i] \times \alpha_i = [(\theta - S + c_{i-1}) : m_i] \times \alpha_i - q_i \times \alpha_i.$$

Mais le premier terme du second membre est égal à α_{i-1}, on le vérifie en exprimant α_i, par la relation de récurrence; le terme devient:

$$[(-\theta'+c_{i-1}):m_i]\times[(\theta-c_{i-1}):m_{i-1}]\times\alpha_{i-1}$$

et le facteur de α_{i-1} est égal à:

$$-[(\theta'-c_{i-1})\times(\theta-c_{i-1})]:(m_i\times m_{i-1}) = [-F(c_{i-1})]:(m_i\times m_{i-1}) = 1$$

la dernière égalité résulte de l'association de $\mathbf{M}_{i-1}$ et du conjugué de $\mathbf{M}_i$.

La relation de récurrence linéaire peut être mise sous forme matricielle. Les bases, disposées en colonnes (comme il a été fait ci-dessus; **9**), vérifient l'égalité:

$$\left\|\begin{matrix}\alpha_{i+1}\\ \alpha_i\end{matrix}\right\| = \left\|\begin{matrix}-q_i & 1\\ 1 & 0\end{matrix}\right\| \times \left\|\begin{matrix}\alpha_i\\ \alpha_{i-1}\end{matrix}\right\|; \qquad q_i = (c_{i-1}+c_i-S):m_i.$$

Ceci appliqué à h bases consécutives (par exemple aux h premières) donne une propriété de ω:

$$\left\|\begin{matrix}\omega\times\alpha_1\\ \omega\times\alpha_0\end{matrix}\right\| = \left\|\begin{matrix}\alpha_{h+1}\\ \alpha_h\end{matrix}\right\| = \Pi\left(\left\|\begin{matrix}-q_i & 1\\ 1 & 0\end{matrix}\right\|\right) \times \left\|\begin{matrix}\alpha_1\\ \alpha_0\end{matrix}\right\|;$$

les matrices sont prises de $i = 1$ à $i = h$, mais disposées de *droite à gauche.* Toutes les matrices multipliées ayant un déterminant égal à —1, la matrice produit a un déterminant égal à —1 ou à +1, suivant que h, nombre d'idéaux du cycle, est impair, ou pair. Ce produit est donc de la forme:

$$\Pi\left(\left\|\begin{matrix}-q_i & 1\\ 1 & 0\end{matrix}\right\|\right) = \left\|\begin{matrix}U & V\\ V' & U'\end{matrix}\right\|; \quad U\times U'-V\times V' = \varepsilon(+1 \text{ ou } -1).$$

La relation obtenue entraîne:

$$\left\|\begin{matrix}\omega\times\alpha_1\\ \omega\times\alpha_0\end{matrix}\right\| = \left\|\begin{matrix}U & V\\ V' & U'\end{matrix}\right\| \times \left\|\begin{matrix}\alpha_1\\ \alpha_0\end{matrix}\right\| \Rightarrow \text{déterminant} \left|\begin{matrix}U-\omega & V\\ V' & U'-\omega\end{matrix}\right| = 0$$

Il en résulte que le diviseur de l'unité ω vérifie l'équation du second degré:

$$\omega^2 - (U+U') \times \omega + \varepsilon = 0;$$

et la norme $\omega \times \omega'$ est égale à ε; sa valeur absolue est 1 et son signe est — ou +, suivant que h est impair ou pair.

Il en résulte que *tous les cycles*, d'un même corps quadratique, *ont la même parité du nombre de leurs idéaux.*

Les matrices multipliées étant symétriques (égales respectivement à leurs transposées), la transposée de leur produit est égale à leur produit, mais disposé dans l'ordre inverse:

$$\Pi \begin{Vmatrix} -q_i & 1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} U & V' \\ V & U' \end{Vmatrix} ; \; i \text{ de } 1 \text{ à } h.$$

(On obtiendrait d'ailleurs ces produits en disposant les termes des bases en lignes.) L'équation en ω reste la même.

Exemples. — On a indiqué ci-dessus (**46**) le calcul de ω dans le corps de discriminant 145, en utilisant la relation de récurrence (multiplicative) entre deux α_i successifs. L'emploi de la récurrence linéaire conduit aux calculs suivants (pour le même cycle):

$\mathbf{M}_0 = (1, \theta - 5)$	$\mathbf{M}_1 = (6, \theta - 0)$	$\mathbf{M}_2 = (6, \theta - 5)$	$\mathbf{M}_0 = (1, \theta - 5)$
$q_i = \ldots\ldots\ldots$	$(5+0+1):6 = 1$	$(0+5+1):6 = 1$	$(5+5+1):1 = 11$
$\alpha_0 = 1$	$\alpha_1 = \theta - 5$	$\alpha_2 = \alpha_0 - 1 \times \alpha_1$	$\alpha_3 = \alpha_1 - 1 \times \alpha_2$
		$-\theta + 6$	$2\theta - 11 = \omega$

Le produit des matrices (i de 1 à 3, de gauche à droite) est:

$$\begin{Vmatrix} -1 & 1 \\ 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} -1 & 1 \\ 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} -11 & 1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} -23 & 2 \\ 12 & -1 \end{Vmatrix} ;$$

l'équation vérifiée par ω est:

$$\omega^2 + 24\omega - 1 = 0;$$

ce qu'on peut constater directement.

Le tableau XXV donne encore un exemple de calculs des idéaux semi réduits dans le corps de discriminant 377. Il y a 2 cycles de 4 et

de 6 idéaux. Il indique, pour le premier de ces cycles, le calcul des α_i et du diviseur de l'unité ω, par récurrence multiplicative et par récurrence linéaire, ainsi que le produit des substitutions linéaires (ou des matrices unimodulaires).

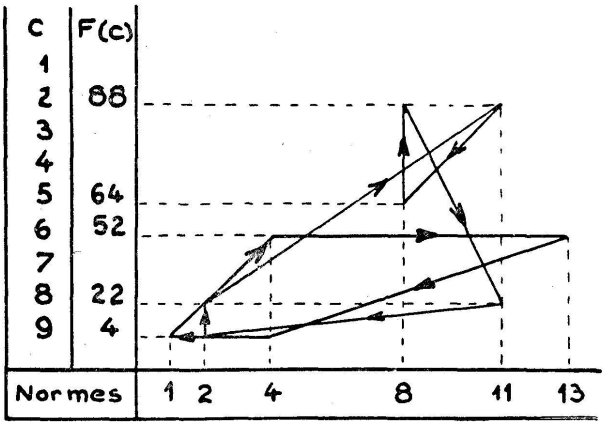
La norme de ω est $+1$, puisque les nombres d'idéaux de chaque cycle sont pairs.

TABLEAU XXV.

Exemples de calculs de cycles et de diviseurs de l'unité.

$F(x) = x^2+x-94$; $\quad D = 377 = 13\times 29$

c	$\frac{2c}{-S}$	$-F(c)$	Idéaux semi réduits
0	1	$94 = 2\times 47$	
1	3	$92 = 2^2\times 23$	
2	5	$88 = 2^3\times 11$	$(8,\ \theta-2)\times(11,\ \theta-2)$
3	7	$82 = 2\times 41$	
4	9	$74 = 2\times 37$	
5	11	$64 = 2^6$	$(\mathbf{8},\ \theta-5)\times(\mathbf{8},\ \theta-5)$
6	13	$52 = 2^2\times 13$	$(4,\ \theta-6)\times(\mathbf{13},\ \theta-6)$
7	15	$38 = 2\times 19$	
8	17	$22 = 2\times 11$	$(2,\ \theta-8)\times(11,\ \theta-8)$
			$(\mathbf{2},\ \theta-9)\times(\mathbf{2},\ \theta-9)$
9	19	$4 = 2^2$	
			$(\mathbf{1},\ \theta-9)\times(4,\ \theta-9)$



$$(1,\ \theta-9) \to (4,\ \theta-6) \qquad (2,\ \theta-8) \to (11,\ \theta-2) \to (8,\ \theta-5)$$
$$(4,\ \theta-9) \leftarrow (13,\ \theta-6) \qquad (2,\ \theta-9) \leftarrow (11,\ \theta-8) \leftarrow (8,\ \theta-2)$$

Calcul des diviseurs de l'unité.

$\mathbf{M}_0 = (1, \theta-9)$	$\mathbf{M}_1 = (4, \theta-6)$	$\mathbf{M}_2 = (13, \theta-6)$	$\mathbf{M}_3 = (4, \theta-9)$	$\mathbf{M}_0 = (1, \theta-9)$
$q_i = \ldots\ldots\ldots$	$(9+6+1):4 = 4$	$(6+5+1):13 = 1$	$(6+9+1):4 = 4$	$(9+9+1):1 = 19$
$\alpha_0 = 1$	$\alpha_1 = (\theta-9)$	$\alpha_1\times(\theta-6):4$	$\alpha_2\times(\theta-6):13$	$\alpha_3\times(\theta-9):4$
		$\alpha_2 = \alpha_0-4\alpha_1$	$\alpha_3 = \alpha_1-1\times\alpha_2$	$\alpha_3 = \alpha_2-4\times\alpha_3$
		$-4\theta+37$	$5\theta-46$	$-24\theta+221$

$$\begin{Vmatrix} -4 & 1 \\ 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} -1 & 1 \\ 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} -4 & 1 \\ 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} -19 & 1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 461 & -24 \\ -96 & 5 \end{Vmatrix}$$

$$\omega^2-466\omega+1 = 0.$$

49. Les quatre types de cycles.

Le numérotage (par indice i, mod. h) des termes d'un cycle d'idéaux semi réduits permet d'établir aisément qu'il existe seulement 4 types de cycles. On indique d'abord leurs caractéristiques en les illustrant par des exemples déjà cités; la justification en est explicitée au numéro suivant.

1. *Le cycle contient un idéal semi réduit double et un idéal semi réduit réfléchi.* Il a alors un *nombre impair de termes* et contient leurs conjugués et leurs associés (relativement à la racine finale).

Pour le corps de discriminant 145 (tableaux XXII et XXIV), dans le cycle de trois idéaux:

$$(1,\ \theta\text{—}5) \rightarrow (6,\ \theta) \rightarrow (6,\ \theta\text{—}5);$$

le premier est double, le second est réfléchi ($F(0) = -6^2$).

De même dans le cycle de cinq idéaux:

$$(5,\ \theta\text{—}2) \rightarrow (6,\ \theta\text{—}3) \rightarrow (4,\ \theta\text{—}4) \rightarrow (4,\ \theta\text{—}3) \rightarrow (6,\ \theta\text{—}2)$$

le premier idéal est double (5 diviseur du discriminant), le troisième est réfléchi ($F(4) = -4^2$).

Dans le corps de discriminant $D = 232$ (mêmes tableaux), un cycle de 7 termes comprend un idéal double (1, θ—7) et un idéal réfléchi (7, θ—3). Un autre cycle de 5 termes comprend un idéal double (2, θ—6) et un idéal réfléchi (3, θ—7).

Dans ce type de cycles rentrent les *cycles d'un seul terme*, constitués par l'idéal unité, lorsqu'il est, à la fois double et réfléchi, ce qui se présente dans les cas signalés ci-dessus (**43** et **44**). Si le corps ne contient que ce seul cycle, il est principal et il présente le caractère trivial signalé ci-dessus (**38**); c'est le cas de 7 des corps du tableau XX; de discriminants:

5, 13, 29, 53, 173, 293 et 8.

2. *Le cycle contient deux idéaux semi réduits doubles.* Il a alors *un nombre pair de termes* et contient aussi leurs conjugués et leurs associés (relativement à la racine finale).

Dans le corps de discriminant 377 (tableau XXV), le cycle de quatre termes contient deux idéaux doubles, de normes 1 et 13, diviseurs du discriminant. Dans le graphique représentatif, ce sont les extrémités de côtés parallèles à l'axe des normes.

Un *cycle de deux termes* est nécessairement de ce type 2, les deux idéaux qui le constituent sont doubles.

En effet, les deux idéaux doivent être donnés par des décompositions:

$$(\theta - c) = (m,\ \theta - c) \times (n,\ \theta - c), \quad (\theta - c') = (m,\ \theta - c') \times (n,\ \theta - c')$$

et c, c' doivent être conjugués relativement à m et n et congrus suivant ces mêmes nombres qui sont par suite des normes d'idéaux doubles (donc diviseurs du discriminant).

Un tel cycle peut notamment contenir l'*idéal unité* (ce qui est une condition nécessaire pour qu'il n'y ait pas d'autre cycle et que le corps soit principal). Il est alors obtenu par la décomposition de la dernière valeur négative de $F(c) = 1 \times m$, lorsque m est diviseur du discriminant.

Cette circonstance se présente notamment dans les corps de discriminants:

$$21 = 3 \times 7, \quad 77 = 7 \times 11, \quad 437 = 19 \times 23,$$

signalés ci-dessus (tableau XX) comme corps principaux triviaux et pour lesquels les décompositions des dernières valeurs négatives de $F(x)$ sont, respectivement:

$$F(1) = -3, \quad F(3) = -7, \quad F(9) = -19.$$

Cette circonstance se produit encore pour les corps dont le discriminant est de la forme $D = 4 \times (c^2+2)$; ils contiennent un cycle de deux idéaux de normes 1 et 2, parmi les premiers desquels ceux de discriminants:

$$12 = 4.(1+2), \quad 24 = 4.(4+2), \quad 44 = 4.(9+2), \quad 152 = 4.(36+2),$$
$$332 = 4.(81+2), \quad 908 = 4.(225+2)$$

n'ont pas d'autres cycles, donc sont principaux. Il n'y a pas de corps de discriminants 72, 108, 684, 792, donnés par les valeurs de c: 4, 5,

13, 14. Les corps de discriminants 204, 264, 408, 492, 584; donnés par les valeurs de c: 7, 8, 10, 11, 12 contiennent d'autres cycles et ne sont pas principaux.

3. *Le cycle contient deux idéaux semi réduits réfléchis.* Il a *un nombre pair de termes* et contient leurs conjugués et leurs associés (relativement à la racine finale).

Dans le corps de discriminant 377 (tableau XXV), le cycle de six termes contient deux idéaux réduits réfléchis, donnés par les décompositions

$$(\theta\text{—}9) = (2,\ \theta\text{—}9)\times(2,\ \theta\text{—}9);\quad (\theta\text{—}5) = (8,\ \theta\text{—}5)\times(8,\ \theta\text{—}5);$$

dans le graphique représentatif, ce sont les origines des côtés parallèles à l'axe des racines.

Un cycle de ce type doit contenir au moins *quatre éléments et ne peut contenir d'idéal unité.* Il ne peut en exister dans un corps principal.

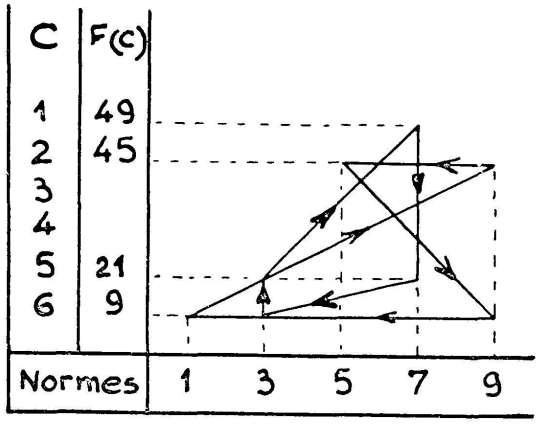
Le tableau XXVI donne un exemple de corps, de discriminant 205, qui contient deux cycles de quatre termes; l'un de type 2, l'autre de type 3.

TABLEAU XXVI.

Exemple de calculs de cycles.

$F(x) = x^2+x-51;\qquad D = 205 = 5\times 41.$

c	$\frac{2c}{-S}$	$-F(c)$	Idéaux semi réduits
0	1	$51 = 3\times 17$	
1	3	$49 = 7^2$	$(\mathbf{7},\ \theta\text{—}1)\times(\mathbf{7},\ \theta\text{—}1)$
2	5	$45 = 3^2\times 5$	$(\mathbf{5},\ \theta\text{—}2)\times(9,\ \theta\text{—}2)$
3	7	$39 = 3\times 13$	
4	9	31	
5	11	$21 = 3\times 7$	$(3,\ \theta\text{—}5)\times(7,\ \theta\text{—}5)$
			$(\mathbf{3},\ \theta\text{—}6)\times(\mathbf{3},\ \theta\text{—}6)$
6	13	$9 = 3^2$	
			$(\mathbf{1},\ \theta\text{—}6)\times(9,\ \theta\text{—}6)$



$$(\mathbf{1},\ \theta\text{—}6) \to (9,\ \theta\text{—}2) \qquad (\mathbf{3},\ \theta\text{—}6) \to (3,\ \theta\text{—}5)$$
$$\uparrow \qquad\qquad \downarrow \qquad\qquad \uparrow \qquad\qquad \downarrow$$
$$(9,\ \theta\text{—}6) \leftarrow (\mathbf{5},\ \theta\text{—}2) \qquad (7,\ \theta\text{—}5) \leftarrow (\mathbf{7},\ \theta\text{—}1)$$

Les normes des idéaux remarquables sont en caractères gras.

4. *Le cycle ne contient pas d'idéaux remarquables*, notamment pas d'idéal unité. Les conjugués de ses idéaux forment un cycle différent, dont les idéaux sont respectivement associés à ceux du précédent. Les deux cycles peuvent être qualifiés *conjugués et associés;* ils définissent deux classes d'idéaux différentes conjuguées et inverses.

Les cycles des trois premiers types (précédents) sont conjugués et associés à eux-mêmes; ils définissent des classes doubles.

Le corps de discriminant 145 (tableaux XXII et XXIV) contient, en plus de deux cycles de type 1, deux cycles conjugués (et associés), de chacun trois idéaux:

$(3, \theta\text{—}3) \to (8, \theta\text{—}4) \to (2, \theta\text{—}5)$; $(3, \theta\text{—}5) \to (2, \theta\text{—}4) \to (8, \theta\text{—}3)$.

Les conjugués des idéaux, d'indices 0, 1, 2, du premier cycle sont respectivement les idéaux d'indices 0, 2, 1, du second cycle (somme des indices congrue à 0, mod. 3); leurs associés sont respectivement les idéaux d'indices 2, 1, 0 (somme des indices congrue à —1, mod. 3). Les sens de circulation sur les deux schémas sont opposés.

50. Justification des types.

Pour établir que les quatres types de cycles sont les seuls possibles, on va étudier, comme il a été dit, le numérotage des éléments des cycles; en comparant deux cycles, non nécessairement différents, dont chacun contient les associés et par suite aussi les conjugués (dans un ordre différent) des termes de l'autre.

Théorème de la correspondance des indices. — Dans un corps réel, *pour que deux cycles* (éventuellement égaux), d'idéaux semi réduits, $\mathbf{M}_i$ et $\mathbf{N}_j$, *contiennent chacun les idéaux associés*, et, par suite aussi, conjugués, *des idéaux de l'autre, il suffit* (et il faut évidemment) :

qu'*il existe un terme* $\mathbf{M}_p$, de l'un, *et un terme* $\mathbf{N}_q$, de l'autre, *qui soient conjugués;*

ou qu'*il existe un terme* $\mathbf{M}_p$ *et un terme* $\mathbf{N}_{q-1}$, *qui soient associés*, relativement à leur racine finale, commune.

Chacune des deux conditions entraîne l'autre; les deux cycles ont alors le même nombre h de termes et les indices des idéaux qui se correspondent par conjugaison, ou par association, ont une somme constante, mod. h:

$$\mathbf{M}_i \text{ et } \mathbf{N}_j \text{ conjugués} \Leftrightarrow i+j \equiv p+q, \quad (\text{mod. } h),$$
$$\mathbf{M}_{i'} \text{ et } \mathbf{N}_{j'} \text{ associés} \Leftrightarrow i'+j' \equiv p+q-1, \quad (\text{mod. } h).$$

Pour la première condition, on vérifie que:

$$\mathbf{M}_p \text{ et } \mathbf{N}_q \text{ conjugués} \Rightarrow \mathbf{M}_{p+1} \text{ et } \mathbf{N}_{q-1} \text{ conjugués},$$

ce qui résulte des égalités de définition de la succession dans les cycles considérés (**44**), qui peuvent être mis sous les formes suivantes, en tenant compte de la réciprocité de la conjugaison et de l'association

$$(\text{associé de } \mathbf{N}_{q-1}) = (\text{conjugué de } \mathbf{N}_q) = \mathbf{M}_p$$
$$\Rightarrow \mathbf{N}_{q-1} = (\text{associé de } \mathbf{M}_p) = (\text{conjugué de } \mathbf{M}_{p+1}).$$

On en déduit, par récurrence sur les indices, λ étant a priori, indéfini,

$$\mathbf{M}_{p+\lambda} \text{ et } \mathbf{N}_{q-\lambda} \text{ conjugués}; \quad [(p+\lambda)+(q-\lambda) = p+q].$$

En outre si h est le nombre d'idéaux $\mathbf{M}_i$, leur périodicité entraîne:

$$\mathbf{M}_{p+h} = \mathbf{M}_p \Rightarrow \mathbf{N}_{q-h} = \mathbf{N}_q.$$

Le nombre d'idéaux $\mathbf{N}_j$ est aussi h et l'égalité des sommes d'indices est une congruence, mod. h.

D'autre part l'égalité de succession entraîne:

$$\text{associé de } \mathbf{N}_{q-\lambda-1} = (\text{conjugué de } \mathbf{N}_{q-\lambda}) = \mathbf{M}_{p+\lambda};$$

de sorte que la relation entre les indices i' et j' d'idéaux respectivement associés est bien:

$$i'+j' \equiv (p+\lambda)+(q-\lambda-1) \equiv p+q-1, \quad (\text{mod. } h).$$

La démonstration est corrélative et la propriété reste valable pour la deuxième condition (existence d'un couple d'idéaux associés).

Cette propriété acquise, on obtient les trois premiers types de cycles, en considérant *un cycle* (ou deux cycles égaux) *qui renferme les conjugués. et par suite les associés de chacun de ses termes. Il suffit*, pour cela, de constater *qu'il renferme:*

le conjugué d'un de ses idéaux (éventuellement double);
ou *l'associé d'un de ses idéaux* (éventuellement réfléchi).

1. Si un tel cycle a un *nombre impair d'idéaux*, il contient *un* (et un seul) *idéal double et un* (et un seul) *idéal réfléchi;* il est du *type* 1.

Les idéaux conjugués et associés étant respectivement définis par les congruences:

$$i+j \equiv a; \quad i'+j' \equiv a-1, \quad (\text{mod. } h);$$

l'indice x, d'un idéal double et l'indice x' d'un idéal réfléchi sont déterminés par les équations congruentielles:

$$2x \equiv a; \quad 2x' \equiv a-1, \quad \text{mod. } h.$$

Comme h est impair (premier avec 2) chacune a une et une seule solution.

2 et 3. Si un tel cycle a un *nombre pair d'idéaux*, il contient, *ou bien deux idéaux doubles*, ou *bien deux idéaux réfléchis;* il est soit du *type* 2, soit du *type* 3.

Comme h est pair, une seule des équations congruentielles précédentes est possible; celle dont le second membre, a ou $a-1$ est un entier pair. Elle a alors deux solutions de différence $h:2$ (mod. h).

Pour $h = 2$, le type 2 est le seul possible (ainsi qu'il a déjà été dit), car si deux idéaux successifs $\mathbf{M}_0$ et $\mathbf{M}_1$ du cycle étaient associés, ils seraient aussi conjugués, puisque:

$$\mathbf{M}_1 = \text{associé de } \mathbf{M}_0 = \text{conjugué de } \mathbf{M}_1.$$

Les deux idéaux auraient des normes égales et des racines égales, donc seraient égaux; le cycle n'aurait qu'un seul terme, l'idéal unité.

4. Par contraposition des propriétés précédentes, *un cycle qui ne contient pas d'idéal semi réduit remarquable*, ne peut contenir de couples, ni d'idéaux conjugués, ni d'idéaux associés; *il n'est pas égal à son cycle conjugué*, qui lui est aussi associé, il est du *type* 4.

Dans la notation indicielle, de deux cycles conjugués, de type 4, d'ordre h, les indices d'idéaux conjugués ont une somme constante, qui peut être choisie arbitrairement (notamment 0, mod. h); les

indices des idéaux associés ont alors pour somme constante a—1 (notamment —1, mod. h). Ce sont ces constantes 0 et —1 qui ont été adoptées dans l'exemple des tableaux XXII et XXIV.

La constante de la somme des indices d'idéaux correspondants, dont, par ailleurs les points correspondants ont même abscisse, ou même ordonnée, explique la différence des sens de parcours sur les schémas. On peut aussi remarquer que les conjugués d'un idéal et de son suivant sont un idéal et son précédent.

51. Structure du groupe des classes d'idéaux.

Dans un corps réel, pour établir la table de PYTHAGORE (de la multiplication) des classes d'idéaux, il suffit d'établir celle des cycles qui les caractérisent, ou les représentent proprement.

Pour multiplier deux cycles, on en choisit des représentants, qui figurent dans des décompositions (convenables) de valeurs de la table (éventuellement prolongée). Comme, dans le cas d'un corps imaginaire, on cherche, au besoin par récurrence, un idéal semi réduit qui soit congru à ce produit; le cycle auquel appartient cet idéal est le produit des cycles considérés; ou, plus exactement, détermine la classe qui est le produit des classes représentées par les cycles multipliés.

Dans un corps qui n'a qu'un petit nombre de cycles (ce qui est le cas pour des discriminants relativement petits), la détermination de la structure du groupe des classes (ou des cycles) est, en général aisée; elle peut être facilitée par la considération du nombre de cycles, qui est l'ordre du groupe. Si cet ordre est un nombre premier le groupe est cyclique et chacun de ses termes, différent de l'unité (ou de la classe principale) en est un générateur. Si l'ordre est un produit de nombres premiers différents, le groupe est encore cyclique, mais il y a lieu de chercher ses générateurs; ce sont les termes dont l'ordre est égal à celui du groupe. Dans le cas général, la comparaison de l'ordre de certains termes à l'ordre du groupe peut permettre d'affirmer que le groupe est, ou n'est pas cyclique.

Le tableau XXVII donne un exemple de recherche de la structure du groupe des classes, pour un corps de discriminant assez élevé; 62 501; dont le polynôme fondamental est $F(x) = x^2+x$—15 625.

Tableau XXVII.

$F(x) = x^2+x-15\,625$; $D = 62\,501$; $r = 56$.

c	$-F(c)$		
0	$15\,625 = 5\times 25\times 125$	$\mathbf{125^2}$;	$\mathbf{U_1^2}$
1	$623 = 17\times 919$		
2	619		
3	$613 = 13\times 1201$		
4	$605 = 5\times 3121$		
5	$15\,595 = 5\times 3119$		
6	583		
7	569		
8	$553 = 103\times 151$		
9	$535 = 5\times 13\times 239$		
10	$15\,515 = 5\times 29\times 107$		
11	493		
12	$469 = 31\times 499$		
13	443		
14	$415 = 5\times 3083$		
15	$15\,385 = 5\times 17\times 181$		
16	$353 = 13\times 1181$		
17	319		
18	$283 = 17\times 29\times 31$		
19	$245 = 5\times 3049$		
20	$15\,205 = 5\times 3041$		
21	$163 = 59\times 257$		
22	$119 = 13\times 1163$		
23	073		
24	$025 = 5^2\times 601$		
25	$14\,975 = 5^2\times 599$		
26	923		
27	869		
28	813		
29	$755 = 5\times 13\times 227$		
30	$14\,695 = 5\times 2939$		
31	633		
32	$569 = 17\times 857$		
33	503		
34	$435 = 5\times 2885$		
35	$14\,365 = 5\times 17\times 13^2$		
36	293		
37	$219 = 59\times 241$		
38	143		
39	$065 = 5\times 29\times 97$	$\mathbf{97\times 145}$;	$\mathbf{K_5\times K_3^1}$
40	$13\,985 = 5\times 2797$		
41	903		
42	$819 = 13\times 1063$		
43	$733 = 31\times 443$		
44	$645 = 5\times 2729$		
45	$13\,555 = 5\times 2711$		
46	463		
47	$369 = 29\times 461$		
48	$273 = 13\times 1021$		
49	$175 = 5^2\times 17\times 31$	$\mathbf{85\times 155}$;	$\mathbf{L_1\times L_3'}$
50	$13\,075 = 5^2\times 523$		
51	12 973		
52	$869 = 17\times 757$		
53	763		
54	$655 = 5\times 2531$		
55	$12\,545 = 5\times 13\times 593$		
	. . . . .		
56	433		
57	$319 = 97\times 127$	$\mathbf{127\times 97}$;	$\mathbf{K_4\times K_2'}$
58	203		
59	$085 = 5\times 2437$		
60	$11\,965 = 5\times 2393$		
61	$843 = 13\times 911$		
62	719		
63	593		
64	$465 = 5\times 2293$		
65	$11\,335 = 5\times 2287$		
66	$203 = 17\times 659$		
67	069		
68	$10\,933 = 13\times 29^2$		
69	$795 = 5\times 17\times 127$	$\mathbf{85\times 127}$;	$\mathbf{K_3\times K_3'}$

c	$-F(c)$		
70	$10\,655 = 5\times 2131$		
71	513		
72	369		
73	223		
74	$075 = 5^2\times 13\times 31$	$\mathbf{155\times 65}$;	$\mathbf{J}_4\times\mathbf{J}_0'$
75	$9\,925 = 5^2\times 397$		
76	$773 = 29\times 337$		
77	619		
78	463		
79	$305 = 5\times 1861$		
80	$9\,145 = 5\times 31\times 59$	$\mathbf{59\times 155}$;	$\mathbf{J}_3\times\mathbf{J}_1'$
81	$8\,983 = 13\times 691$		
82	819		
83	$653 = 17\times 509$		
84	$485 = 5\times 1697$		
85	$8\,315 = 5\times 1663$		
86	$143 = 17\times 479$		
87	$7\,969 = 13\times 613$		
88	793		
89	$615 = 5\times 1523$		
90	$7\,435 = 5\times 1487$		
91	253		
92	069		
93	6 883		
94	$695 = 5\times 13\times 103$	$\mathbf{103\times 65}$;	$\mathbf{K}_1\times\mathbf{K}_5'$
95	$6\,505 = 5\times 1301$		
96	$313 = 59\times 107$	$\mathbf{107\times 59}$;	$\mathbf{J}_2\times\mathbf{J}_2'$
97	$119 = 29\times 211$	$\mathbf{29\times 211}$;	$\mathbf{L}_3\times\mathbf{L}_1'$
98	5 923		
99	$725 = 5^2\times 229$		
100	$5\,525 = 5^2\times 13\times 17$	$\mathbf{25\times 221}$;	$\mathbf{I}_1\times\mathbf{I}_1'$
		$\mathbf{65\times 85}$;	$\mathbf{K}_2\times\mathbf{K}_4'$
101	323		
102	119		
103	$4\,913 = 17^3$		
104	$705 = 5\times 941$		

c	$-F(c)$		
105	$4\,495 = 5\times 29\times 31$	$\mathbf{155\times 29}$;	$\mathbf{L}_2\times\mathbf{L}_2'$
		$\mathbf{145\times 31}$;	$\mathbf{K}_6\times\mathbf{K}_0'$
106	283		
107	$069 = 13\times 313$		
108	3 853		
109	$635 = 5\times 727$		
110	$3\,415 = 5\times 683$		
111	$193 = 31\times 103$	$\mathbf{31\times 103}$;	$\mathbf{K}_0\times\mathbf{K}_0'$
112	2969		
113	$743 = 13\times 211$	$\mathbf{211\times 13}$;	$\mathbf{L}_4\times\mathbf{L}_0'$
114	$515 = 5\times 503$		
115	$2\,285 = 5\times 457$		
116	053		
117	$1\,819 = 17\times 107$	$\mathbf{17\times 107}$;	$\mathbf{J}_1\times\mathbf{J}_3'$
118	583		
119	$345 = 5\times 269$		
120	$1\,105 = 5\times 13\times 17$	$\mathbf{65\times 17}$;	$\mathbf{J}_0\times\mathbf{J}_4'$
		$\mathbf{13\times 85}$;	$\mathbf{L}_0\times\mathbf{L}_4'$
		$\mathbf{221\times 5}$;	$\mathbf{I}_2\times\mathbf{I}_0'$
121	0 863		
122	619		
123	373		
124	$125 = 5^3$	$\mathbf{1\times 125}$;	$\mathbf{U}_0\times\mathbf{U}_2$
	. . . . .	$\mathbf{5\times 25}$;	$\mathbf{I}_0\times\mathbf{I}_2'$
125	-125		

$(\theta\text{—}124) = \mathbf{I}_0^3 \sim 1$;

$(\theta\text{—}103) = \mathbf{J}_1^3 \sim 1$;

$(\theta\text{—}49) = \mathbf{I}_2'\times\mathbf{J}_1\times\mathbf{K}_0 \sim 1$;

$(\theta\text{—}120) = \mathbf{I}_0'\times\mathbf{L}_0\times\mathbf{J}_4' \sim 1$.

Devant chaque valeur $-F(c)$, est inscrite sa décomposition en facteurs premiers et une sous ligne indique ceux de ces facteurs, ou produits de facteurs qui sont des normes d'idéaux réduits (**38**); la majorante de leurs racines est $r = 56$.

D'autre part, devant certaines valeurs (positives de $-F(c)$), l'indication d'un produit égal, de deux *nombres* (en caractères gras), est celle de normes d'un couple d'idéaux semi réduits associés, de racine finale c. Le produit suivant de deux *lettres*, est une représentation de ces idéaux: la lettre (**U**, **I**, **J**, **K**, **L**) désigne le cycle; l'indice désigne la succession dans ce cycle. On peut vérifier que chacun de ces couples renferme au moins un des idéaux réduits, signalés par ailleurs.

Il y a neuf cycles; l'un d'eux de trois termes, désignés par la lettre **U** est du type 1; il contient un idéal double $(1,\ \theta-124)$ et un idéal réfléchi $(125,\ \theta)$; ses idéaux sont principaux, c'est le cycle principal.

Les autres cycles se répartissent en quatre couples de cycles conjugués; désignés respectivement par la même lettre, avec et sans accent, dont les nombres de termes sont: trois pour **I** et **I'**; cinq pour **J** et **J'**; sept pour **K** et **K'**; cinq pour **L** et **L'**; ces nombres sont impairs, comme celui des idéaux du cycle **U**. La somme des indices des idéaux conjugués est congrue à 0, celle des idéaux associés est congrue à -1 (**49**).

Dans le groupe chacun des huit termes, différents de l'unité **U**, est d'ordre 3. Le groupe est *produit direct de deux groupes cycliques d'ordre* 3, engendrés respectivement par les puissances de deux cycles, non conjugués, par exemple **I** et **J**.

Cette structure résulte immédiatement des décompositions de certaines des valeurs de la table. Celles de:

$$F(124) = 5^3 \quad \Rightarrow \quad (\theta-124) = (5,\ \theta-124)^3 = \mathbf{I}_0^3;$$

$$F(103) = 17^3 \quad \Rightarrow \quad (\theta-103) = (17,\ \theta-103)^3 = (17,\ \theta-117)^3 = \mathbf{J}_1^3$$

montrent que les cycles **I** et **J**, ainsi que leurs conjuguées **I'** et **J'** sont des termes d'ordre 3 du groupe. Par suite ce groupe qui est d'ordre 9, ne peut être cyclique (si non il ne contiendrait que deux termes d'ordre 3, puissances 3 et 6 d'une base). Il est donc produit de deux groupes cycliques, d'ordre 3. Ses termes peuvent notamment être exprimés par:

$$\mathbf{I}^x \times \mathbf{J}^y; \quad x, y \text{ entiers, mod. } 3.$$

On peut compléter cette indication en cherchant les expressions de **K** et de **L**. Elles résultent notamment des décompositions:

$$F(49) = 25\times17\times31 \Rightarrow (25,\ \theta\text{—}49)\times(17,\ \theta\text{—}49)\times(31,\ \theta\text{—}49)$$
$$= (25,\ \theta\text{—}124)\times(17,\ \theta\text{—}117)\times(31,\ \theta\text{—}111) \sim 1$$
$$F(120) = 5\times13\times17 \Rightarrow (5, \theta\text{—}120)\times(13, \theta\text{—}120)\times(17, \theta\text{—}120) \sim 1.$$

Elles entraînent:

$$\mathbf{K} = \mathbf{I}\times\mathbf{J}^2; \quad \mathbf{L} = \mathbf{I}\times\mathbf{J}.$$

Les cycles conjugués sont aussi inverses, l'un de l'autre, de sorte que chacun d'eux est égal au carré de l'autre (exposant 2, mod. 3).

52. Corps de discriminant premier.

On va examiner quelques unes des circonstances qui peuvent se présenter dans la structure du groupe des classes des idéaux semi réduits, ou des cycles.

Dans un corps réel, dont *le discriminant est un nombre premier*, nécessairement congru à $+1$, mod. 4, il n'y a qu'*une seule classe double*, caractérisée par *un cycle, du type* 1, *d'un nombre impair d'idéaux.* Il peut exister en outre *des couples de cycles conjugués*, et associés, du type 4, qui ont aussi un nombre impair d'idéaux.

Si le cycle principal existe seul, *le corps est principal.* Dans le cas contraire l'*ordre du groupe des classes est impair* et supérieur à 1; si cet ordre est un nombre premier, ou un produit de nombres premiers différents, le groupe est cyclique, mais cette condition suffisante n'est pas nécessaire.

Un corps, de discriminant premier ne contient qu'un idéal double de norme 1, qui engendre un cycle de type 1, évidemment principal. Ce cycle doit donc contenir un idéal semi réduit réfléchi, ce qui entraîne l'existence d'une décomposition du discriminant en une somme de carrés de deux nombres entiers.

C'est là une nouvelle preuve de la propriété déjà établie par la considération du corps $\mathbf{R}(i)$: *un nombre premier, congru à* $+1$, mod. 4; *est égal à une somme de carrés de deux nombres entiers* (**20**).

Cette démonstration établissait aussi la détermination de ces deux carrés; il est possible de le vérifier également par des considéra-

tions simples de congruences, dont le module est le nombre premier considéré. Cette précision montre qu'il ne peut y avoir d'autre idéal remarquable dans le corps, donc aucun autre cycle de type 1, 2, ou 3.

Le tableau XXI donne deux exemples de corps, de discriminants premiers, 317 et 193, dont la considération des idéaux réduits permet d'affirmer qu'ils sont principaux. Le tableau XXVIII indique comment ceci peut être établi par la considération des idéaux semi réduits; la disposition est la même que dans le tableau XXVII; mais dans chaque corps il n'y a qu'un seul cycle, dont les idéaux sont désignés par la lettre **I**: ils sont de trois termes dans le premier corps, de quinze termes dans le second.

Pour les discriminants peu élevés, on constate que, pour une très grande proportion d'entre eux, il n'y a pas de cycles de type 4, et que, par suite, le corps est principal. On indique ci-dessous la répartition des corps principaux de discriminant premier inférieur à 1000, suivant le nombre d'idéaux dans le cycle unique (les corps sont désignés par leurs discriminants):

1 idéal dans le cycle: 5, 13, 29, 53, 173, 293;
3 idéaux: 17, 37, 61, 101, 197, 317, 461, 557, 677, 773;
5 idéaux: 41, 149, 157, 181, 269, 397, 941;
7 idéaux: 89, 109, 113, 137, 373, 389, 509, 653, 797, 853, 997;
9 idéaux: 73, 97, 233, 277, 349, 353, 613, 821, 877;
11 idéaux: 541, 593, 661, 701, 857;
13 idéaux: 421, 757;
15 idéaux: 193, 281;
17 idéaux: 521, 617, 709;
19 idéaux: 241, 313, 449, 829, 953;
21 idéaux: 337, 569, 977;
23 idéaux: 433, 457, 641, 881;
25 idéaux: 929;
27 idéaux: 409;
29 idéaux: 673, 809;
31 idéaux: 937;
33 idéaux: 601;
35 idéaux: 769.

Les six corps, dont le cycle principal n'a qu'un seul idéal, sont indiqués dans le tableau XX (avec cinq autres, de discriminant non premier).

Les seuls corps, de discriminant premier, inférieur à 1000, qui ne sont pas principaux sont ceux de discriminants:

229, 257, 733, 761, qui comprennent chacun trois *cycles* (ou classes) formant par suite *un groupe cyclique d'ordre* 3;

401, qui comprend cinq *cycles*, formant *un groupe cyclique d'ordre* 5 ;

577, qui comprend sept *cycles*, formant *un groupe cyclique d'ordre* 7.

Le tableau XXVIII donne aussi les calculs des cycles pour trois de ces corps, de discriminants:

577: cycle **U** de trois idéaux; trois couples de cycles conjugués; **I**, **I'** et **J**, **J'** de chacun trois idéaux; **K**, **K'** de chacun cinq idéaux;

401: cycle **U** de trois idéaux; deux couples de cycles conjugués; **I**, **I'** de chacun trois idéaux; **J**, **J'** de chacun cinq idéaux;

761: cycle **U** de cinq idéaux; deux cycles conjugués, **I**, **I'** de chacun sept idéaux.

Pour des discriminants relativement élevés, le groupe de cycles (ou de classes) peut n'être pas cyclique. L'exemple de calcul de structure du tableau XXVII concerne un corps dont le discriminant, 62 501, est premier, et dont le groupe des cycles, d'ordre 9 est produit direct de deux groupes cycliques d'ordre 3.

53. Corps à une seule classe double.

Le corps, de caractère exceptionnel, défini par le polynôme fondamental:

$$F(x) = x^2 - 2; \qquad D = 8;$$

a un seul idéal semi réduit, à la fois double et réfléchi, qui est l'idéal unité. Il n'y a donc qu'un seul cycle, d'un seul terme, et le corps, comme ce cycle, est principal.

A l'exception de ce corps, et en plus de ceux dont le discriminant est un nombre premier, il existe des corps qui n'ont qu'une seule classe double (conjuguée d'elle-même); ce sont ceux dont le discriminant a au plus deux facteurs premiers impairs, congrus à —1, mod. 4. En tenant compte des conditions de construction d'un corps réel (**1**), on obtient l'énoncé suivant:

Un corps réel, dont le discriminant D est:

Tableau XXVIII.

Exemples de corps de discriminant premier (corps principaux).

c	$-(x^2+x-79)$
0	79
1	77
2	73
3	67
4	59
5	$49 = 7\times 7$; $\mathbf{I}_2\times\mathbf{I}_2$
6	37
7	23
8	$7 = 1\times 7$; $\mathbf{I}_0\times\mathbf{I}_1$

$-(x^2+x-48)$	
48	
46	
$42 = 7\times 6$	$\mathbf{I}_6\times\mathbf{I}_8$
$36 = 9\times 4 = 6\times 6$;	$\mathbf{I}_4\times\mathbf{I}_{10}$; $\mathbf{I}_7\times\mathbf{I}_7$
$28 = 4\times 7$;	$\mathbf{I}_5\times\mathbf{I}_9$
$18 = 6\times 3 = 2\times 9$;	$\mathbf{I}_1\times\mathbf{I}_{13}$; $\mathbf{I}_3\times\mathbf{I}_{11}$
$6 = 1\times 6 = 3\times 2$;	$\mathbf{I}_0\times\mathbf{I}_{14}$; $\mathbf{I}_2\times\mathbf{I}_{12}$
.....	

(Corps non principaux.)

c	$-(x^2+x-144)$
0	$144 = 12\times 12$; $\mathbf{U}_1\times\mathbf{U}_1$
1	142
2	138
3	$132 = 11\times 12$; $\mathbf{K}_3\times\mathbf{K}_1'$
4	124
5	114
6	$102 = 6\times 17$; $\mathbf{J}_1\times\mathbf{J}_1'$
7	$88 = 8\times 11$; $\mathbf{K}_2\times\mathbf{K}_2'$
8	$72 = 4\times 18$; $\mathbf{I}_1\times\mathbf{I}_1'$
	$= 12\times 6$; $\mathbf{K}_4\times\mathbf{K}_0'$
	$= 9\times 8$; $\mathbf{K}_1\times\mathbf{K}_3'$
9	$54 = 18\times 3$; $\mathbf{I}_2\times\mathbf{I}_0'$
	$= 6\times 9$; $\mathbf{K}_0\times\mathbf{K}_0'$
10	$34 = 17\times 2$; $\mathbf{J}_2\times\mathbf{J}_0'$
11	$12 = 1\times 12$; $\mathbf{U}_0\times\mathbf{U}_2$
	$= 2\times 6$; $\mathbf{J}_0\times\mathbf{J}_2'$
	$= 3\times 4$; $\mathbf{I}_0\times\mathbf{I}_2'$
12	. . . . .
13	

$-(x^2+x-100)$	
$100 = 10^2$	$\mathbf{U}_1\times\mathbf{U}_1$
98	
94	
$88 = 8\times 11$;	$\mathbf{J}_3\times\mathbf{J}_1'$
$80 = 10\times 8$;	$\mathbf{J}_2\times\mathbf{J}_2'$
$70 = 5\times 14$;	$\mathbf{I}_1\times\mathbf{I}_1'$
$= 7\times 10$;	$\mathbf{J}_1\times\mathbf{J}_3'$
58	
$44 = 11\times 4$;	$\mathbf{J}_4\times\mathbf{J}_0'$
$28 = 14\times 2$;	$\mathbf{I}_2\times\mathbf{I}_0'$
$= 4\times 7$;	$\mathbf{J}_0\times\mathbf{J}_4'$
$10 = 1\times 10$;	$\mathbf{U}_0\times\mathbf{U}_2$
$= 2\times 5$;	$\mathbf{I}_0\times\mathbf{I}_2'$
. . . . .	

$-(x^2+x-190)$		c
190		0
188		1
184		2
178		3
$170 = 10\times 17$;	$\mathbf{I}_5\times\mathbf{I}_1'$	4
$160 = 16\times 10$;	$\mathbf{I}_4\times\mathbf{I}_2'$	5
148		6
134		7
118		8
$100 = 20\times 5$;	$\mathbf{I}_2\times\mathbf{I}_4'$	9
$= 10\times 10$;	$\mathbf{U}_2\times\mathbf{U}_2$	
$80 = 4\times 20$;	$\mathbf{I}_1\times\mathbf{I}_5'$	10
$= 5\times 16$;	$\mathbf{I}_3\times\mathbf{I}_3'$	
$= 8\times 10$;	$\mathbf{U}_1\times\mathbf{U}_3$	
58		11
$34 = 17\times 2$;	$\mathbf{I}_6\times\mathbf{I}_0'$	12
$8 = 1\times 8$;	$\mathbf{U}_0\times\mathbf{U}_4$	13
$= 2\times 4$;	$\mathbf{I}_0\times\mathbf{I}_6'$	

1. impair, nécessairement congru à $+1$, mod. 4, *produit* $u \times v$, *de deux nombres premiers impairs, dont l'un*, et par suite l'autre, *est congru à* -1, mod. 4;

2. *produit par* 4 *d'un nombre premier* d, impair, nécessairement *congru à* -1, mod. 4;

3. *produit par* 4 *du double* $d = 2d'$, *d'un nombre premier* d', nécessairement impair, mais *congru à* -1, mod. 4;

ne contient qu'une seule classe double d'idéaux, nécessairement principale, caractérisée par un cycle du type 2, d'un nombre pair de termes. Il peut y exister, en outre, des *cycles du type* 4, répartis par couples de cycles conjugués, chacun ayant aussi un nombre pair d'idéaux.

Dans les trois cas, le discriminant D, considéré dans le corps $\mathbf{R}(i)$, est le produit de deux idéaux (principaux), dont l'un au moins est premier rationnel (u et v; ou d; ou d'; puisque congru à -1, mod. 4). Il n'est donc pas égal à une somme de carrés de deux nombres entiers (**20**) et le corps ne contient pas d'idéal semi réduit réfléchi (deuxième théorème d'existence de **43**).

Par contre il existe deux, et seulement deux idéaux semi réduits doubles, car D a seulement deux diviseurs dont le carré lui soit inférieur et qui sont, suivant les cas:

$$1 \text{ et } u \text{ ou } v; \qquad 1 \text{ et } 2$$

ceci puisque, dans le second cas, d étant au moins égal à 3:

$$2^2 < D = 4d; \qquad \text{et} \qquad d^2 > D:4 = d;$$

et que, dans le troisième cas, d' étant au moins égal à 3 ($D = 8$ étant excepté):

$$2^2 < D:4 = 2d'; \qquad \text{et} \qquad d'^2 > D:4 = 2d'.$$

Il n'y a donc qu'un seul cycle, du type 2, qui contient deux idéaux semi réduits doubles.

Les autres cycles, s'il en existe, ne peuvent contenir d'idéaux semi réduits remarquables et ne peuvent être que du type 4.

Comme pour un discriminant premier, si le cycle principal existe seul, *le corps est principal.*

Dans le cas contraire, l'*ordre du groupe des classes est impair* (un cycle principal et des couples de cycles). Si cet ordre est un nombre premier ou un produit de nombres premiers différents, *le groupe est cyclique*, mais cette condition suffisante n'est pas nécessaire.

Pour les discriminants peu élevés, on constate aussi que, pour une très grande proportion d'entre eux, il n'existe pas de cycles de type 4, et que, par suite, le corps est principal. On indique ci-dessous la répartition de ces corps principaux, de discriminant inférieur à 1000, suivant le nombre d'idéaux dans le cycle unique. Les corps sont indiqués par les décompositions de leurs discriminants et dans l'ordre des trois cas:

2 idéaux dans le cycle: 3×7, 7×11, 3×31, 3×79, 19×23, 3×151; 4×3, 4×11, 4×23, 4×83, 4×227; 8×3, 8×19;
4 idéaux: 3×11, 3×23, 7×19, 3×47, 3×71, 7×59, 3×191, 3×239; 4×7, 4×47, 4×167; 8×7, 8×31;
6 idéaux: 3×19, 11×23, 3×103, 11×31, 3×127, 7×107, 3×271, 19×47; 4×19, 4×59, 4×107, 4×131; 8×11;
8 idéaux: 3×167, 7×83, 3×263, 11×79, 7×131, 23×43; 4×31, 4×71; 8×79, 8×103;
10 idéaux: 3×43, 7×23, 7×43, 11×47, 3×199, 3×223; 4×43, 4×67, 8×43, 8×59;
12 idéaux: 3×59, 11×19, 3×311, 7×139; 4×103, 4×127, 4×239; 8×23;
14 idéaux: 3×67, 7×71, 23×31; 4×179; 8×67;
16 idéaux: 7×31, 3×83, 7×47, 3×131, 3×179, 19×31; 4×191; 8×47;
18 idéaux: 3×139, 3×211, 11×67, 11×71; 4×139, 4×163;
20 idéaux: 4×151, 4×199; 22 idéaux: 3×163; 8×83;
24 idéaux: 3×251; 26 idéaux: 7×79; 4×211; 8×107;
32 idéaux: 3×227, 11×83; 34 idéaux: 11×59, 3×283, 3×307;
36 idéaux: 7×103; 42 idéaux: 7×127.

Les seuls corps, de discriminant inférieur à 1000, vérifiant les conditions précédentes et qui ne sont pas principaux, sont ceux de discriminant:

$321 = 3\times107$, $469 = 7\times67$, $473 = 11\times43$, $993 = 3\times331$;
$316 = 4\times79$, $892 = 4\times223$; $568 = 8\times71$;

qui comprennent chacun un cycle principal et un couple de cycles conjugués formant par suite un *groupe d'ordre* 3, *cyclique*,

et le corps de discriminant $817 = 19\times43$, qui comprend, en plus du cycle principal, deux couples de cycles conjugués, formant *un groupe d'ordre* 5, *cyclique.*

54. Corps à deux classes doubles.

Par un raisonnement analogue aux précédents (**52** et **53**), on peut caractériser les corps qui ont deux et seulement deux classes doubles d'idéaux.

Condition suffisante. — Un corps réel a deux, et seulement deux, classes doubles d'idéaux lorsque son discriminant a l'une des formes suivantes:

1. il est impair, nécessairement congru à $+1$, mod. 4, *égal à un produit* $u\times v$, *de deux nombres premiers, congrus chacun à* $+1$, mod. 4;

2. il est pair, *égal au produit par* 4, *du double* $2d'$, *d'un nombre premier* d', *congru à* $+1$, mod. 4;

[Dans ces deux cas les classes doubles sont caractérisées par *deux cycles*, soit du *type* 1 (d'un nombre impair de termes), soit *l'un du type* 2 *et l'autre du type* 3 (tous deux d'un nombre pair d'éléments).]

3. il est impair, *égal à un produit* $u\times v\times w$, *de trois nombres premiers, dont un est congru à* $+1$ *et chacun des deux autres à* -1, mod. 4;

4. il est pair, *égal au produit par* 4, *d'un produit* $d = u\times v$, ou du double $d = 2d'$, d'un produit $d' = u'\times v'$, *de deux nombres premiers, dont l'un est congru à* $+1$ *et l'autre à* -1, mod. 4;

5. il est pair, égal *au produit par* 4 *du double* $d = 2d'$, *d'un produit* $d' = u' \times v'$, *de deux nombres premiers, congrus chacun à* —1, mod. 4.

[Dans ces trois cas, les classes doubles sont caractérisées par deux cycles du type 2 (d'un nombre pair de termes).]

L'un des cycles contenant nécessairement l'idéal unité est principal; il peut exister, en outre, des cycles du type 4, répartis par couples de cycles conjugués, chacun ayant un nombre de termes de même parité que celui des termes du cycle principal.

Dans les cas 1 et 2, D ou $d = 2d'$, considéré dans le corps $\mathbf{R}(i)$, est la norme d'un produit de deux idéaux premiers du premier degré (non rationnels); il est donc décomposable de deux façons en une somme de deux carrés et le corps contient deux idéaux semi réduits réfléchis.

D'autre part, dans chaque cas il existe deux (et seulement deux) idéaux doubles, dont les normes sont les diviseurs du discriminant: 1 et le plus petit des entiers u et v, pour le premier cas; 1 et 2 pour le second cas (d'après le raisonnement déjà fait ci-dessus lorsque d' est congru à —1; **53**).

Il y a donc quatre (et seulement quatre) idéaux semi réduits remarquables donc deux cycles contenant chacun deux d'entre eux. Ils sont du type 1 si chacun contient un idéal double et un idéal réfléchi; ils sont l'un du type 2, l'autre du type 3, dans le cas contraire.

Dans les cas 3 à 5, D ou d, qui contient au moins un facteur premier, congru à —1, mod. 4, n'est pas égal à une somme de deux carrés; le corps ne contient pas d'idéal semi réduit réfléchi.

Par contre il y a quatre (et seulement quatre) idéaux semi réduits doubles dont les normes sont, suivant le cas:

3 — 1, u ou $v \times w$, v ou $w \times u$, w ou $u \times v$;
4 — 1, 2, u ou v, $2u$ ou $2v$;
5 — 1, 2, u' ou $2v'$, v' ou $2u'$.

Il y a donc encore quatre idéaux semi réduits remarquables, donc deux cycles, mais chacun d'eux est du type 2.

Dans chacun des 5 cas, le corps a donc deux classes doubles. Si ces classes (ou ces cycles) existent seules, elles constituent *un groupe, d'ordre* 2, *cyclique.*

Dans le cas contraire, l'*ordre du groupe des classes est pair* (deux classes doubles et des couples de classes conjuguées). Si cet ordre est le double d'un produit de nombres premiers impairs différents, le groupe est cyclique. Il l'est encore si ces nombres premiers comprennent un facteur 2 (notamment si l'ordre est égal à 4); car un produit direct d'un groupe d'ordre pair par un

TABLEAU XXIX.

Exemples de corps à deux classes doubles.

c	$D = 685 = 5\times137$ $-(x^2+x-171)$	c
0	171	0
1	$169 = 13\times13$; $\mathbf{V}_2\times\mathbf{V}_2$	1
2	$165 = 15\times11$; $\mathbf{U}_1\times\mathbf{U}_5$	2
3	159	3
4	151	4
5	141	5
6	129	6
7	115	7
8	$99 = 11\times9$; $\mathbf{U}_2\times\mathbf{U}_4$	8
9	$81 = 9\times9$; $\mathbf{U}_3\times\mathbf{U}_3$	9
10	61	10
11	$39 = 3\times13$; $\mathbf{V}_1\times\mathbf{V}_3$	11
12	$15 = 1\times15$; $\mathbf{U}_0\times\mathbf{U}_6$ $= 5\times3$; $\mathbf{V}_0\times\mathbf{V}_4$	12
13		13
14		14
15		15

Ordre 2

$(\theta-1) = \mathbf{V}_2\times\mathbf{V}_2$

$\mathbf{V}^2 \sim 1$

$D = 689 = 13\times53$ $-(x^2+x-172)$
172
170
166
$160 = 16\times10$; $\mathbf{U}_1\times\mathbf{U}_4$
152
142
$130 = 10\times13$; $\mathbf{U}_2\times\mathbf{U}_3$
116
$100 = 5\times20$; $\mathbf{I}_2\times\mathbf{I}_2'$ $= 10\times10$; $\mathbf{V}_2\times\mathbf{V}_2$
82
62
$40 = 20\times2$; $\mathbf{I}_3\times\mathbf{I}_0'$ $= 4\times10$; $\mathbf{V}_1\times\mathbf{V}_3$ $= 8\times5$; $\mathbf{I}_1\times\mathbf{I}_2'$
$16 = 1\times16$; $\mathbf{U}_0\times\mathbf{U}_5$ $= 2\times8$; $\mathbf{I}_0\times\mathbf{I}_3'$ $= 4\times4$; $\mathbf{V}_0\times\mathbf{V}_0$
. . . . .

Ordre 4

$(\theta-12) = \mathbf{I}_0^4$

$\mathbf{I}^4 \sim 1$

$D = 904 = 8\times113$ $-(x^2-226)$	c
226	0
$225 = 15\times15$; $\mathbf{V}_1\times\mathbf{V}_1$	1
222	2
217	3
$210 = 15\times14$; $\mathbf{K}_1\times\mathbf{K}_3'$	4
201	5
$190 = 10\times19$; $\mathbf{J}_1\times\mathbf{J}_1'$	6
177	7
$162 = 9\times18$; $\mathbf{K}_3\times\mathbf{K}_1'$	8
145	9
$126 = 6\times21$; $\mathbf{I}_1\times\mathbf{I}_1'$ $= 18\times7$; $\mathbf{K}_4\times\mathbf{K}_0'$ $= 14\times9$; $\mathbf{K}_2\times\mathbf{K}_2'$	10
$105 = 21\times5$; $\mathbf{I}_2\times\mathbf{I}_0'$ $= 7\times15$; $\mathbf{K}_0\times\mathbf{K}_4'$	11
82	12
$57 = 19\times3$; $\mathbf{J}_2\times\mathbf{J}_0'$	13
$30 = 2\times15$; $\mathbf{V}_0\times\mathbf{V}_2$ $= 3\times10$; $\mathbf{J}_0\times\mathbf{J}_2'$ $= 5\times6$; $\mathbf{I}_0\times\mathbf{I}_2'$	14
$1 = 1\times1$; $\mathbf{U}_0\times\mathbf{U}_0$	15

Ordre 8

$(\theta-8) = \mathbf{J}_0^4\times\mathbf{V}_0$

$\mathbf{J}^8 \sim \mathbf{V}^2 \sim 1$

groupe d'ordre 2 contient au moins deux termes d'ordre 2; or la classe double non principale est le seul terme d'ordre 2, du groupe des classes.

Pour des discriminants peu élevés, on constate encore que, pour une assez grande proportion d'entre eux, il n'y a pas de cycles de type 4, et que, par suite leur groupe est d'ordre 2 et cyclique. Pour les discriminants inférieurs à 1000, il y a ainsi 91 corps qui n'ont que deux classes d'idéaux [la classe principale et une classe égale à sa conjuguée et de carré égal à la classe principale]. Ils se répartissent suivant les cinq conditions précédentes en:

21 (condition 1); 12 (2°); 20 (3°); 32 (4°); 6 (5°).

Les seuls corps qui, en vérifiant les conditions précédentes ont un groupe d'ordre supérieur à 2 (ou contiennent des cycles de type 4) sont: ceux de discriminants:

$145 = 5\times29$, $445 = 5\times89$, $505 = 5\times101$, $689 = 13\times53$,

$793 = 13\times61$, $901 = 17\times53$, $905 = 5\times181$; $328 = 8\times41$;

$777 = 3\times7\times37$; $897 = 3\times13\times23$; $876 = 4\times3\times73$;

qui ont un *groupe, d'ordre* 4, *cyclique;*

ceux de discriminants:

$785 = 5\times157$, $985 = 5\times197$; $940 = 4\times235$;

qui ont un *groupe d'ordre* 6, *cyclique*;

et celui de discriminant $904 = 8\times113$, qui a un *groupe d'ordre* 8, et qui est *cyclique*, car il ne contient qu'un seul terme d'ordre 2.

Le tableau XIX donne des exemples de calcul des idéaux semi réduits et de vérification de la structure des groupes pour trois corps, [deux classes doubles] dont les discriminants sont:

$685 = 5\times137$ (premier cas de la condition) qui a deux cycles d'un nombre impair d'idéaux (7 et 5), du type 1;

$689 = 13 \times 53$ (même cas) qui a deux cycles de type 2 et 3, d'un nombre pair d'idéaux (6 et 4) et un couple de cycles conjugués de type 4, de chacun quatre idéaux. Son groupe est d'ordre 4, cyclique;

$904 = 8 \times 113$ (deuxième cas), qui a deux cycles de type 1 contenant un et trois idéaux et trois couples de cycles conjugués de type 4, contenant respectivement trois, trois et cinq idéaux. Son groupe est d'ordre $2+2\times 3 = 8$, cyclique.

55. Corps à plus de deux classes doubles.

Les conditions, énoncées ci-dessus, *suffisantes* pour qu'un corps contienne seulement une ou deux classes doubles d'idéaux, sont aussi *nécessaires:* si elles ne sont pas vérifiées par le discriminant, le corps a au moins trois classes doubles. Cette propriété peut être explicitée sous forme d'une condition suffisante analogue aux précédentes.

Un corps réel a *au moins trois classes doubles* d'idéaux lorsque son discriminant D a l'une des formes suivantes:

1. il est impair, nécessairement congru à $+1$, mod. 4, *égal à un produit* $u \times v \times w$, de trois nombres premiers, *congrus chacun à* $+1$, mod. 4;

2. il est pair, égal au *produit par* 4, *du double* $2d'$ d'un produit $d' = u' \times v'$, de deux nombres premiers, *congrus chacun à* $+1$, mod. 4;

3. Il est impair, nécessairement congru à $+1$, mod. 4, égal à un *produit de plus de trois nombres premiers impairs.*

4. Il est pair, produit par 4 d'un nombre impair d, congru à -1, mod. 4, ou du double $2d'$ d'un nombre impair d', *produit d'au moins trois nombres premiers impairs.*

Il est équivalent de dire que D vérifie ces conditions, ou ne vérifie pas les conditions précédentes; c'est ce qui résulte du tableau des diverses conditions:

	D impair $\equiv +1$	D pair $= 4d$	
		d impair $\equiv -1$	$d = 2d'$, d' impair
1 seule classe double	D premier — — — — — — — — — $D = u \times v$ u, v premiers $\equiv -1$	d premier	d' premier $\equiv -1$
2 classes doubles	$D = u \times v$ u, v premiers $\equiv +1$ — — — — — — — — — $D = u \times v \times w$ u, v, w premiers u et $v \equiv -1$	$d = u \times v$ u, v premiers $u \equiv -1$	d' premier $\equiv +1$ — — — — — — — — — $d' = u' \times v'$ u', v' premiers; $u' \equiv -1$; v' impair
3 classes doubles au moins	$D = u \times v \times w$ u, v, w premiers $\equiv +1$ 4 facteurs premiers, au moins	3 facteurs premiers impairs au moins	$d' = u' \times v'$ u', v' premiers $\equiv +1$ — — — — — — — — —

Dans les cas 1 et 2, D est décomposable de quatre façons en somme de deux carrés; le corps contient donc quatre idéaux semi réduits réfléchis.

D'autre part, il existe quatre idéaux doubles, dont les normes sont 1, u ou vw, v ou uw, uv ou w dans le premier cas, et 1, 2, u' ou $D{:}8u'$, $2u'$ ou $D{:}4u'$ dans le second cas.

Il y a donc *huit* idéaux semi réduits remarquables, donc quatre cycles, contenant chacun deux de ces idéaux et définissant chacun une classe double.

Dans les cas 3 et 4, il y a huit idéaux semi réduits doubles, au moins, dont les normes sont suivant les cas:

3 — 1, u ou $D{:}u$, v ou $D{:}v$, uv ou $D{:}uv$, w ou $D{:}w$, uw ou $D{:}uw$, vw ou $D{:}vw$, uvw ou $D{:}uvw$,

4 — 1, 2, u ou $D{:}u$, $2u$ ou $D{:}2u$, v ou $D{:}v$, $2v$ ou $D{:}2v$, uv ou $D{:}uv$, $2uv$ ou $D{:}2uv$;

si u, v, w sont des facteurs premiers impairs de D.

Il y a au moins huit idéaux semi réduits remarquables, donc au moins quatre cycles, définissant chacun une classe double.

Dans chacun de ces cas, le groupe des classes d'idéaux contient au moins deux éléments d'ordre 2, donc contient un sous-groupe, produit direct de deux groupes cycliques d'ordre 2.

TABLEAU XXX.

Exemples de corps à plus de deux classes doubles.

c	$D = 1\,105 = 5\times13\times17$ $-(x^2+x-276)$	
0	276	
1	274	
2	$270 = 15\times18;$	$I_9\times I_2$
3	264	
4	$256 = 16\times16;$	$U_3\times U_3$
5	246	
6	$234 = 13\times18;$	$I_6\times I_5$
7	$220 = 11\times20;$	$J_2\times J_9$
	$= 10\times22;$	$K_2\times K_9$
8	$204 = 12\times17;$	$K_5\times K_6$
9	186	
10	166	
11	$144 = 12\times12;$	$K_0\times K_0$
	$= 8\times18;$	$I_4\times I_7$
	$= 9\times16;$	$U_2\times U_4$
	$= 6\times24;$	$J_4\times J_7$
12	$120 = 10\times12;$	$K_{10}\times K_1$
	$= 8\times15;$	$I_8\times I_3$
	$= 6\times20;$	$J_8\times J_3$
	$= 5\times24;$	$J_6\times J_5$
13	94	
14	$66 = 6\times11;$	$J_1\times J_{10}$
	$= 3\times22;$	$K_8\times K_3$
15	$36 = 6\times6;$	$J_0\times J_0$
	$= 4\times9;$	$U_1\times U_5$
	$= 3\times12;$	$K_4\times K_7$
	$= 2\times18;$	$I_1\times I_{10}$
16	$4 = 2\times2;$	$I_0\times I_0$
	$= 1\times4;$	$U_0\times U_6$
....	.....	

produit direct de 2 groupes cycliques d'ordre 2

$I\times J\sim K$

c	$D = 1\,365 = 3\times5\times7\times13$ $-(x^2+x-341)$	
0	341	
1	339	
2	335	
3	329	
4	321	
5	311	
6	$299 = 13\times23;$	$J_2\times J_1$
7	$285 = 15\times19;$	$K_3\times K_2$
8	269	
9	251	
10	$231 = 11\times21;$	$K_5\times K_0$
11	$209 = 11\times19;$	$K_1\times K_4$
12	185	
13	159	
14	131	
15	101	
16	$69 = 3\times23;$	$J_0\times J_3$
17	$35 = 5\times7;$	$I_0\times I_1$
	$= 1\times35;$	$U_0\times U_1$
....	.....	

produit direct de 2 groupes cycliques d'ordre 2

$I\times J\sim K$

Les seuls corps, à plus de deux classes doubles, dont le discriminant D est inférieur à 1000, sont les cinq corps dont les discriminants sont:

$$D = 520 = 8\times5\times13$$
$$D = 680 = 8\times5\times17$$
$$D = 840 = 8\times3\times5\times7$$
$$D = 780 = 4\times3\times5\times13$$
$$D = 924 = 4\times4\times7\times11$$

Le groupe des classes d'idéaux de chacun de ces corps est le produit direct de deux groupes cycliques d'ordre 2.

Le tableau XXX donne deux exemples de calcul des idéaux semi réduits et de vérification de la structure des groupes pour les corps dont les discriminants sont:

1 105 $= 5\times13\times17$, qui a un cycle de sept idéaux (U) et trois cycles de onze idéaux;

1 365 $= 3\times5\times7\times13$, qui a deux cycles de deux idéaux, un cycle de quatre idéaux et un cycle de six idéaux.

On peut encore généraliser la construction des exemples précédents, pour obtenir des corps contenant exactement n classes doubles d'idéaux.

NOTE I

La théorie des corps de nombres algébriques, et plus précisément l'étude des propriétés arithmétiques de leurs entiers, a pour origine des travaux de K. F. Gauss (1777-1855). Gauss a introduit la notion d'entier algébrique et établit les propriétés de divisibilité des entiers de quelques corps particuliers. Mais c'est seulement E. E. Kummer (1810-1893) qui a introduit la notion essentielle d'idéal, dans un anneau d'entiers algébriques, permettant d'obtenir des propriétés arithmétiques dans tout corps de nombres algébriques de degré fini. Cette notion a été précisée et développée, dans le cours du XIX^{o} siècle, surtout par l'école allemande: R. Dedekind (1831-1916), L. Kronecker

(1823-1891), H. MINKOWSKI (1864-1909). On peut également citer le Suisse A. HURWITZ (1859-1919) et le Français C. HERMITE (1822-1901).

En 1897, D. HILBERT (1862-1943) publiait, à la demande de la Deutsche Mathematiker Vereinigung, un rapport sur la théorie des corps de nombres algébriques. On pouvait alors estimer que les propriétés arithmétiques essentielles d'un corps de nombres algébrique de degré fini étaient obtenues. Mais HILBERT, utilisant largement ses propres travaux, ouvrait une nouvelle série de recherches en comparant l'arithmétique d'un corps de nombres algébriques à celle d'une de ses extensions abéliennes. Cette nouvelle étude, qui est habituellement appelée « théorie du corps des classes », a été poursuivie, pendant tout le XX^e^ siècle par de nombreux arithméticiens: P. FURTWANGLER, T. TAKAGI, C. CHEVALLEY, A. WEIL...

L'étude des corps quadratiques a tenu une place importante dans le développement de ces théories, autant comme exemple d'application des résultats généraux, que comme source de résultats particuliers suggérant de nouvelles recherches. C'est cette étude, et celle des corps circulaires, qui a le plus influencé les travaux de GAUSS, comme ceux d'HILBERT.

Le rapport d'HILBERT (*Jahresb. der Deutsche Mat. Ver.*, 1897; traduction française de A. LÉVY et Th. GOT, *Annales de la Fac. Sc. Toulouse*, 1913) consacre un chapitre (sur cinq) à la théorie des corps quadratiques. Le fascicule du *Mémorial des Sciences Mathématiques* de H. HERBRAND (« Le développement moderne de la théorie des corps algébriques », Paris, 1936) consacre également un chapitre à cette théorie.

Ces deux rapports sont très condensés et de lecture difficile. Mais il existe aussi des ouvrages plus élémentaires, contenant des expositions plus ou moins détaillées de l'arithmétique des corps quadratiques. La première partie du livre de J. SOMMER (*Introduction à la théorie des nombres algébriques*, traduction française de A. LÉVY, Paris, 1911) traite en détail de cette théorie, comme introduction à des études plus générales. Le livre de H. HECKE (*Algebraische Zahlen*, Leipzig, 1923) contient un chapitre où l'étude des corps quadratiques est présentée comme application et illustration de propriétés établies dans les

chapitres précédents. Le livre récent de H. HASSE (*Zahlentheorie*, Berlin, 1959) contient un chapitre conçu dans le même esprit. Le livre plus élémentaire du même auteur (*Vorlesungen über Zahlentheorie*, Berlin, 1950) expose la théorie des corps quadratiques de façon plus détaillée et plus indépendante. D'autres traités (R. FUETER, *Synthetische Zahlentheorie*, Lepizig, 1919) utilisent plutôt les corps circulaires comme exemple de corps de nombres algébriques. Enfin certains (H. WEYL, *Algebraic theory of numbers*, Princeton, 1940; H. POLLARD, *The theory of algebraic numbers*, New York, 1950) ne consacrent que quelques lignes aux exemples particuliers de ces corps.

Une conférence d'Albert CHATELET (« L'arithmétique des idéaux », Conférences du Palais de la Découverte, Paris, 1950) étudie de façon détaillée et élémentaire deux exemples de corps quadratiques et compare l'arithmétique de leurs entiers et de leurs idéaux à celle des entiers rationnels.

Il faut enfin signaler que les exposés sur la théorie des formes quadratiques binaires sont essentiellement équivalents à un exposé sur l'arithmétique des corps quadratiques.

Le présent exposé précise et complète une méthode qui avait été esquissée par A. LÉVY au Congrès international de mathématiques réuni à Toronto (*Proc. Congress Toronto*, 1924, Tome 1, pp. 229-244). Cette méthode permet une construction effective du groupe des classes d'idéaux d'un corps quadratique, par des calculs élémentaires.

F. C.

NOTE II

La méthode utilisée ici, pour définir et construire un corps quadratique, a été choisie de telle sorte que les entiers (algébriques) du corps (**3**) puissent être engendrés de façon aussi simple que possible. C'est pour cette raison que l'entier caractéristique d est supposé dépourvu de facteurs carrés et que le polynome fondamental (**1**) se présente sous deux formes différentes, suivant que $d-1$ est ou n'est pas divisible par 4. Ce qui simplifie sensiblement l'exposé et les calculs ultérieurs.

Mais on peut se demander quelle est l'origine de la notion d'entier (d'un corps quadratique, ou plus généralement d'un corps de nombres algébriques de degré fini); ou encore se demander pourquoi les entiers ainsi définis ont une telle importance en arithmétique. On trouvera dans plusieurs ouvrages ou mémoires (notamment, dans l'article de R. DEDEKIND: « Sur la théorie des entiers algébriques », traduction française dans le *Bul. des Sc. math.*, 1876 et 1877) des explications sur l'origine et l'intérêt de la notion d'idéal dans l'anneau des entiers d'un corps algébrique. Mais, depuis GAUSS, la notion d'entier algébrique est rarement discutée.

On peut invoquer la propriété classique: tout élément d'une extension finie de l'anneau des entiers rationnels est entier algébrique (c'est-à-dire est zéro d'au moins un polynome d'une variable dont les coefficients sont des entiers rationnels et dont le coefficient de la puissance la plus élevée est 1). On trouvera la démonstration de cette propriété notamment dans le traité d'Albert CHATELET: *Arithmétique et Algèbre modernes*, Tome III (en préparation). La notion d'entier algébrique est essentiellement destinée à obtenir, entre ces entiers, des propriétés de divisibilité aussi analogues que possible à celle des entiers rationnels et comprenant ces dernières propriétés. Il est donc nécessaire que l'ensemble de ces nouveaux entiers contienne les entiers rationnels et les produits de nouveaux entiers par les entiers rationnels. Il est aussi souhaitable que l'ensemble des nouveaux entiers contienne la somme et la différence de 2 de ces éléments, comme l'ensemble des entiers rationnels contient une telle somme et une telle différence. Enfin, il est naturel de choisir, pour un corps de nombres algébriques donné, un ensemble de nombres du corps qui puissent être engendré, au moyen des opérations précédentes, à partir d'un ensemble restreint, si possible fini, de nouveaux entiers; et, s'il existe plusieurs ensembles vérifiant ces conditions, de choisir l'ensemble le plus étendu possible. Le résultat rappelé montre qu'il faut choisir l'ensemble de tous les entiers algébriques contenu dans le corps.

On peut aussi donner des explications moins axiomatiques et plus constructives, en discutant simultanément la notion d'entier et celle d'idéal. Lorsque GAUSS a introduit les extensions

du corps des nombres rationnels et de l'anneau des entiers rationnels par adjonction de l'imaginaire principale (corps de GAUSS et entiers de GAUSS), il cherchait à utiliser certains nombres algébriques pour résoudre des problèmes sur les entiers rationnels, et plus précisément des problèmes diophantiens. C'était une sorte de généralisation de la méthode de Jérôme CARDAN, qui avait utilisé des nombres imaginaires pour calculer les racines réelles d'une équation du troisième degré.

Ainsi, la recherche des systèmes d'entiers rationnels x, y, z qui vérifient la relation:

$$x^2 - ay^2 = bz^2, \tag{1}$$

où a, b, c sont des entiers donnés, peut être remplacée par la recherche des nombres algébriques conjugués, $\alpha = x + \sqrt{a}y$, $\alpha = x - \sqrt{a}y$, x, y entiers, qui vérifient la relation:

$$\alpha\bar{\alpha} = bz^2 \tag{2}$$

On peut chercher des propriétés de divisibilité entre les nombres algébriques, α, $\bar{\alpha}$, afin d'utiliser une méthode analoque à la méthode élémentaire de résolution d'une équation:

$$uv = bz^2.$$

Mais on peut aussi utiliser les propriétés des congruences entre entiers (développées précisément par GAUSS) au lieu des propriétés de divisibilité. Un calcul classique montre que, si l'entier b n'a aucun facteur carré, il est nécessaire, pour que l'équation (1) ait des solutions en entiers x, y, z non tous nuls, que la congruence:

$$x^2 - ay^2 \equiv 0, \pmod{b}, \tag{3}$$

admette des solutions en entiers x, y telles que y soit premier avec b. Ces dernières solutions peuvent d'ailleurs se déduire des solutions c_i, si elles existent, de la congruence:

$$t^2 - a \equiv 0, \pmod{b} \tag{4}$$

au moyen des formules:

$$x = c_i\lambda_1 + b\lambda_2, \qquad y = \lambda_1.$$

On reconnaît que l'ensemble des nombres algébriques:

$$x+\theta y = (\theta+c_i)\lambda_1+m\lambda_2 \qquad (\theta^2—a)$$

forme un idéal canonique, de norme a, de racine c_i, du corps quadratique engendré par $\theta = \sqrt{a}$, si toutefois a n'est pas congru à $+1$, (mod. 4) (définition constructive des idéaux canoniques (**7**, **1**)).

Limitons-nous provisoirement aux entiers a, sans facteurs carrés, et non congrus à $+1$, (mod. 4). Il est classique de comparer les solutions d'une congruence suivant un entier composé aux solutions de la même congruence suivant les facteurs de cet entier. Cette comparaison, faite pour la congruence (3), conduit aux règles de multiplication des idéaux canoniques (**15**) et à la décomposition de ses idéaux en produits d'idéaux correspondant aux seuls modules premiers (**15**, **3**).

Si on essaie d'appliquer la même méthode aux entiers a, sans facteurs carrés, congrus à $+1$, (mod. 4), on découvre une anomalie. Les deux congruences:

$$t^2—a \equiv 0, \ (\text{mod.}2),$$
$$t^2—a \equiv 0, \ (\text{mod. } 4),$$

ont les mêmes solutions (les entiers t impairs); la congruence:

$$t^2—a \equiv 0, \ (\text{mod. } 8),$$

a ou n'a pas de solutions suivant que a est congru à $+1$ ou à 3, (mod. 8). Les solutions des congruences (3) suivant les modules impairs conduisent encore aux mêmes règles de multiplication et de décomposition des idéaux canoniques que dans le cas précédent. Mais l'étude de cette congruence suivant les modules pairs ne conduit aux mêmes règles que si on fait jouer au module 8 le rôle joué précédemment par le module premier 2.

Mais, si on remplace les congruences (3) et (4) par les congruences:

$$x^2+xy—Ny^2 \equiv 0, \ (\text{mod. } b),$$
$$t^2+t—N \equiv 0, \ (\text{mod. } b),$$

avec $N = (1—a):4$, l'anomalie précédente disparaît; les règles

de multiplication et de décomposition des idéaux canoniques sont les mêmes pour tous les modules composés.

Ce changement de congruences revient encore à remplacer les nombres $\alpha = x+ay$, x, y entiers, par les nombres $\alpha = x+\theta y$, x, y entiers, où θ est une des racines de l'équation:

$$x^2+x-N = 0.$$

Ces derniers nombres sont bien les entiers du corps considéré.

On découvre une anomalie analogue en essayant d'appliquer la méthode à un entier a possédant des facteurs carrés. Si p est un nombre premier dont le carré divise a, les deux congruences

$$t^2-a \equiv 0, \ (\text{mod. } p),$$
$$t^2-a \equiv 0, \ (\text{mod. } p^2),$$

ont les mêmes solutions (les entiers divisibles par p); la congruence:

$$t^2-a \equiv 0, \ (\text{mod. } p^2),$$

peut n'admettre aucune solution. On peut encore faire disparaître l'anomalie en supprimant les facteurs carrés de a.

On est ainsi conduit à la construction utilisée du corps quadratique, et à la définition classique des entiers du corps.

F. C.

ERRATA

Au chapitre I, paragraphe 2 (tome VI, fascicule 2), page 87:

ligne 9 en commençant par le bas:
lire $r^2+Srs+Ns^2$ au lieu de $r^2-Srs+Ns^2$;

ligne 7 en commençant par le bas:
lire $(r^2+Srs+Ns^2)$ au lieu de $(r^2-Ss+Ns^2)$.