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.

Kapitel: CHAPITRE V LES CLASSES D'IDÉAUX DANS LES CORPS IMAGINAIRES — OU DE DISCRIMINANT NÉGATIF —

DOI: https://doi.org/10.5169/seals-37125

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 07.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

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:

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

ETH-BIBLIOTHEK Sto. Bs 74771

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

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

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 $(11,\ \theta-4)$; $[m = (7+15):2,$
$\bar{c} = (15-7):2]$.

Aux décompositions $420 = u \times (4v)$ 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:

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

u, v nombres entiers premiers entre eux.

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

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

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 $\mathbf{M}'$, 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:

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

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 v 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:

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

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

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

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

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

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 $\mathbf{P}$ est différent de $\mathbf{M}$, sa norme p est au plus égale à $m : 2$ et:

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

$\mathbf{P}$ 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 $\mathbf{I}$, est égale à la classe conjuguée, définie par l'idéal conjugué $\mathbf{I}'$ 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 :

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

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:

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

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**:

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

Le cube $\mathbf{I}^3 = (8,\ \theta-2)$ 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 $F(2)$:

$$F(2) = F(-3) = 2^6 \quad \Rightarrow \quad (2,\ \theta-0)^6 \sim (1).$$

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:

$$(3,\ \theta-1),\qquad (7,\ \theta-3),\qquad (8,\ \theta-2).$$

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:

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

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:	
	$\lvert D\rvert \equiv$,	mod.:	$\lvert D\rvert \equiv$,	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:

$$2, \text{ ou } 6, \text{ ou } 7, \text{ ou } 8, \text{ ou } 10; \quad (\text{mod. } 11);$$

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:

$3 + 8\times 2 = \mathbf{19}$; 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:

163, 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.

$$\mathbf{I} = (\mathbf{2},\ \theta-0), \qquad \mathbf{I}^{12} \sim (\mathbf{2},\ \theta+1);$$
$$\mathbf{I}^2 = (\mathbf{4},\ \theta+2), \qquad \mathbf{I}^{11} \sim (\mathbf{4},\ \theta-1);$$
$$\mathbf{I}^3 = (\mathbf{8},\ \theta-2), \qquad \mathbf{I}^{10} \sim (\mathbf{8},\ \theta+3);$$
$$\mathbf{I}^4 = (2^4,\ \theta-10) \sim (11,\ \theta+11) \qquad [F(10)]$$
$$= (11,\ \theta-0) \sim (\mathbf{6},\ \theta+1), \qquad \mathbf{I}^9 \sim (\mathbf{6},\ \theta-0); \qquad [F(0)]$$
$$\mathbf{I}^5 = \mathbf{I}^4 \times \mathbf{I} \sim (\mathbf{6},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (2) \times (\mathbf{3},\ \theta+1), \qquad \mathbf{I}^8 \sim (\mathbf{3},\ \theta-0);$$
$$\mathbf{I}^6 = \mathbf{I}^5 \times \mathbf{I} \sim (\mathbf{3},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (\mathbf{6},\ \theta-2), \qquad \mathbf{I}^7 \sim (\mathbf{6},\ \theta+3);$$

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

$$\mathbf{I} = (\mathbf{2},\ \theta-0), \qquad \mathbf{I}^{14} \sim (\mathbf{2},\ \theta+1);$$
$$\mathbf{I}^2 = (\mathbf{4},\ \theta+2), \qquad \mathbf{I}^{13} \sim (\mathbf{4},\ \theta-1);$$
$$\mathbf{I}^3 = (\mathbf{8},\ \theta+2), \qquad \mathbf{I}^{12} \sim (\mathbf{8},\ \theta-1);$$
$$\mathbf{I}^4 = (2^4,\ \theta+2) \sim (\mathbf{7},\ \theta-1), \qquad \mathbf{I}^{11} \sim (\mathbf{7},\ \theta+2); \qquad [F(-2)]$$
$$\mathbf{I}^5 = (2^5,\ \theta-14) \sim (10,\ \theta+15) = (\mathbf{10},\ \theta+5), \qquad \mathbf{I}^{10} \sim (\mathbf{10},\ \theta-4); \qquad [F(14)]$$
$$\mathbf{I}^6 = (2^6,\ \theta-14) \sim (\mathbf{5},\ \theta+15) = (\mathbf{5},\ \theta-0), \qquad \mathbf{I}^9 \sim (\mathbf{5},\ \theta+1); \qquad [F(14)]$$
$$\mathbf{I}^7 = \mathbf{I}^6 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{2},\ \theta-0) = (\mathbf{10},\ \theta-0), \qquad \mathbf{I}^8 \sim (\mathbf{10},\ \theta+1);$$

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

$$\mathbf{I} = (\mathbf{3},\ \theta-0), \qquad \mathbf{I}^8 \sim (\mathbf{3},\ \theta+1);$$
$$\mathbf{I}^2 = (\mathbf{9},\ \theta-3), \qquad \mathbf{I}^7 \sim (\mathbf{9},\ \theta+4);$$
$$\mathbf{I}^3 = (3^3,\ \theta+6) \sim (\mathbf{5},\ \theta-0), \qquad \mathbf{I}^6 \sim (\mathbf{5},\ \theta+1); \qquad [F(-6)]$$
$$\mathbf{I}^4 = \mathbf{I}^3 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{3},\ \theta-0) = (15,\ \theta-0)$$
$$\sim (\mathbf{7},\ \theta+1), \qquad \mathbf{I}^5 \sim (\mathbf{7},\ \theta-0); \qquad [F(0)]$$

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

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	$\lvert D \rvert$
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 $\mathbf{I}$, montre qu'elle n'est pas non plus congrue à (1). On peut donc prendre comme générateur la classe définie par $\mathbf{I}$, 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	$3\,113 = 11\times 283$ $(\mathbf{1}, \theta-0) = (1)$ $(\mathbf{11}, \theta-0) \sim \mathbf{I}^3\times\mathbf{J}^3$
1	$3\,115 = 5\times 7\times 89$ $(\mathbf{5}, \theta-1) = \mathbf{I}$ $(\mathbf{7}, \theta-1) = \mathbf{J}$ $(\mathbf{35}, \theta-1) = \mathbf{I}\times\mathbf{J}$
2	$3\,119$
3	$3\,125 = 5^5 = 5^3\times\mathbf{25}$ $(\mathbf{25}, \theta-3) \sim \mathbf{I}^3$
4	$3\,133 = 13\times 241$ $(\mathbf{13}, \theta-4) \sim \mathbf{I}^4\times\mathbf{J}^2$
5	$3\,143 = 7\times 449$
6	$3\,155 = 5\times 631$
7	$3\,169$
8	$3\,185 = (5\times 7^2)\times\mathbf{13} = 65\times\mathbf{49}$ $(\mathbf{35}, \theta-8) \sim \mathbf{I}^4\times\mathbf{J}$ $(\mathbf{49}, \theta-8) = \mathbf{J}^2$
9	$3\,203$
10	$3\,223 = 11\times 293$
11	$3\,245 = 5\times 11\times 59 = 59\times\mathbf{55}$ $(\mathbf{55}, \theta-11) \sim \mathbf{I}^4\times\mathbf{J}^3$
12	$3\,269 = 7\times 467$
13	$3\,295 = 5\times 659$
14	$3\,323$
15	$3\,353 = 7\times 479$
16	$3\,385 = 5\times 677$
17	$3\,419 = 13\times 263$
18	$3\,455 = 5\times 691$
19	$3\,493 = 7\times 499$
20	$3\,533$
21	$3\,575 = 5^2\times 11\times 13 = 65\times\mathbf{55}$ $(\mathbf{55}, \theta-21) \sim \mathbf{I}^3\times\mathbf{J}^2$
22	$3\,619 = 7\times 11\times 47 = (7\times 47)\times\mathbf{11}$ $(\mathbf{47}, \theta-22) \sim \mathbf{I}^2\times\mathbf{J}$
23	$3\,665 = 5\times 733$
24	$3\,713 = 47\times 79$
25	$3\,763 = 53\times 71$ $(\mathbf{53}, \theta-25) \sim \mathbf{I}^2\times\mathbf{J}^4$
26	$3\,815 = 5\times 7\times 109$
27	$3\,869 = 53\times 73$
28	$3\,925 = 5^2\times 157$
29	$3\,983 = 7\times 569$
30	$4\,043 = 13\times 311$
31	$4\,105 = 5\times 821$

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

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 $\mathbf{I}$ et $\mathbf{J}$.

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

CALCULS

$$\mathbf{J}^3 = (\mathbf{7}, \theta-1)^3 = (7^3, \theta+139) \sim (65, \theta-138) = (65, \theta-8) \qquad F(-139)$$
$$\sim (\mathbf{49}, \theta+9) = (\mathbf{7}, \theta+2)^2; \qquad F(8)$$
$$\mathbf{I} \times \mathbf{J} = (\mathbf{5}, \theta-1) \times (\mathbf{7}, \theta-1) = (\mathbf{35}, \theta-1);$$
$$\mathbf{I} \times \mathbf{J}^4 \sim (\mathbf{5}, \theta-1) \times (\mathbf{7}, \theta+2) = (\mathbf{35}, \theta+9);$$
$$\mathbf{I} \times \mathbf{J}^2 = (\mathbf{5}, \theta-1) \times (\mathbf{49}, \theta-8) = (5 \times 7^2, \theta-106) \sim (59, \theta+107) \qquad F(106)$$
$$= (59, \theta-11) \sim (\mathbf{55}, \theta+12);$$
$$\mathbf{I} \times \mathbf{J}^3 \sim (\mathbf{5}, \theta-1) \times (\mathbf{49}, \theta+9) = (5 \times 7^2, \theta+9) \sim (13, \theta-8) \qquad F(-9)$$
$$= (\mathbf{13}, \theta+5); \qquad F(11)$$
$$\mathbf{I}^2 \times \mathbf{J} \sim (\mathbf{7}, \theta-1) \times (\mathbf{25}, \theta+4) = (7 \times 5^2, \theta-71) \sim (47, \theta+72) \qquad F(71)$$
$$= (\mathbf{47}, \theta-22);$$
$$\mathbf{I}^2 \times \mathbf{J}^4 \sim (\mathbf{7}, \theta+1) \times (\mathbf{25}, \theta+4) = (7 \times 5^2, \theta+79) \sim (53, \theta-78) \qquad F(-79)$$
$$= (\mathbf{53}, \theta-25);$$
$$\mathbf{I}^2 \times \mathbf{J}^2 \sim (\mathbf{7}, \theta-1) \times (\mathbf{47}, \theta-22) = (7 \times 47, \theta-22) \sim (11, \theta+23) \qquad F(22)$$
$$= (\mathbf{11}, \theta+1);$$
$$\mathbf{I}^3 \times \mathbf{J}^2 \sim (\mathbf{5}, \theta-1) \times (\mathbf{11}, \theta+1) = (\mathbf{55}, \theta-21);$$

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:

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

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

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

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— :

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

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	$75 = 5^2\times\mathbf{3}$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{3},\ \theta-0) \sim \mathbf{I}^6$ $(\mathbf{5},\ \theta-0) = \mathbf{I}$
$+1$	$77 = 7\times 11$ $(\mathbf{7},\ \theta-1) \sim \mathbf{I}^3$
$+2$	$81 = 3^4 = 9^2$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^4$
$+3$	$87 = 3\times 29$
$+4$	$95 = 5\times 19$
$+5$	$107 = 15\times\mathbf{7}$

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

$D = -404 = (-4)\times 101$ $r = 6$; 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 $(\mathbf{1},\ \theta-0) = (1)$
$+1$	$102 = 2\times 3\times 17$ $(\mathbf{2},\ \theta-1) \sim \mathbf{I}^7$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$ $(\mathbf{6},\ \theta-1) \sim \mathbf{I}^8$
$+2$	$105 = (3\times 5)\times\mathbf{7}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^{10}$ $(\mathbf{7},\ \theta-2) \sim \mathbf{I}^5$
$+3$	$110 = 2\times 5\times 11$ $(\mathbf{10},\ \theta-3) \sim \mathbf{I}^{11}$
$+4$	$117 = 3^2\times 13$ $(\mathbf{9},\ \theta-4) = \mathbf{I}^2$
$+5$	$122 = 2\times 61$
$+7$	$150 = 30\times\mathbf{5}$
$+13$	$270 = 27\times\mathbf{10}$

$D = -344 = 8\times(-43)$ $r = 6$; 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	$86 = 2\times 43$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) \sim \mathbf{I}^5$
$+1$	$87 = 3\times 29$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$
$+2$	$90 = (3^2\times 5)\times\mathbf{2}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^7$ $(\mathbf{6},\ \theta-2) \sim \mathbf{I}^4$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^8$
$+3$	$95 = 5\times 19$
$+4$	$102 = 2\times 3\times 17$
$+5$	$111 = 3\times 37$
$+7$	$135 = 27\times\mathbf{5}$

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

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

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	$\lvert D\rvert$ impair		$\lvert D\rvert = 4p$	$\lvert D\rvert = 4\times(2p)$
	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	$\lvert D\rvert$ impair		$\lvert D\rvert$ 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.	»

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

c	$F(c)$	Normes	
0	$240 = 2^4\times3\times5$	**2, 3, 4, 5, 6, 8, 10, 12, 15.**	$(\mathbf{2},\ \theta-0)^4\times(\mathbf{3},\ \theta-0)\times(\mathbf{5},\ \theta-0)\sim(1)$
1	$242 = 2\times11^2$	**11.**	
2	$246 = 2\times3\times41$	**6.**	
3	$252 = 2^2\times3^2\times7$	**7, 9, 12, 14.**	$(\mathbf{2},\ \theta+1)^4\times(\mathbf{3},\ \theta-0)^4\sim(1)$
4	$260 = 2^2\times5\times13$	**10, 13.**	
5	$270 = 2\times3^3\times5$	**15.**	$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^3\times(\mathbf{5},\ \theta+1)\sim(1)$
6	$282 = 2\times3\times47$		
7	$296 = 2^3\times37$		$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^8\sim(1)$
8	$312 = 2^3\times3\times13$		$(\mathbf{3},\ \theta-0)^{36}\sim(1)$
9	$330 = 2\times3\times5\times11$		

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* $-959 = (-7)\times 137$, 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: $8\times3\times5\times7$.