33. Structure du groupe des classes d'idéaux.

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)