

# 44. Cycles d'idéaux semi réduits.

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **7 (1961)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Les idéaux conjugués :

$$(4, \theta+5) = (4, \theta-3), \quad (6, \theta+1) = (6, \theta-5),$$

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

Dans le corps de discriminant pair  $232 = 8 \times 29 = 4 \times 58$  (tableau XXII), la congruence fondamentale, qui a une racine double, mod. 2, est impossible mod. 4. Les normes des idéaux doubles ne peuvent être divisibles par 4 et sont des diviseurs de 58. Les seuls dont le carré est inférieur à 58 sont 1 et 2, qui sont les normes des idéaux réduits doubles  $(1, \theta)$  et  $(2, \theta)$ .

Aux deux décompositions du discriminant :

$$232 = 6^2 + 4 \times 7^2; \quad 232 = 14^2 + 4 \times 3^2;$$

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

$$(7, \theta-3), \quad (3, \theta-7) = (3, \theta-1),$$

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

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

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

#### 44. Cycles d'idéaux semi réduits.

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

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

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

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

$$\text{suisvant de } \mathbf{M} = \text{conjugué de [l'associé de } \mathbf{M}]$$

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

$$\text{précédent de } \mathbf{N}' = \text{associé de [le conjugué de } \mathbf{N}']$$

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

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

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

$$\text{précédent du suisvant de } \mathbf{M} = \text{suisvant du précédent de } \mathbf{M} = \mathbf{M}.$$

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

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

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

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

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

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

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

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

Ces deux constructions et leur détermination prouvent que :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

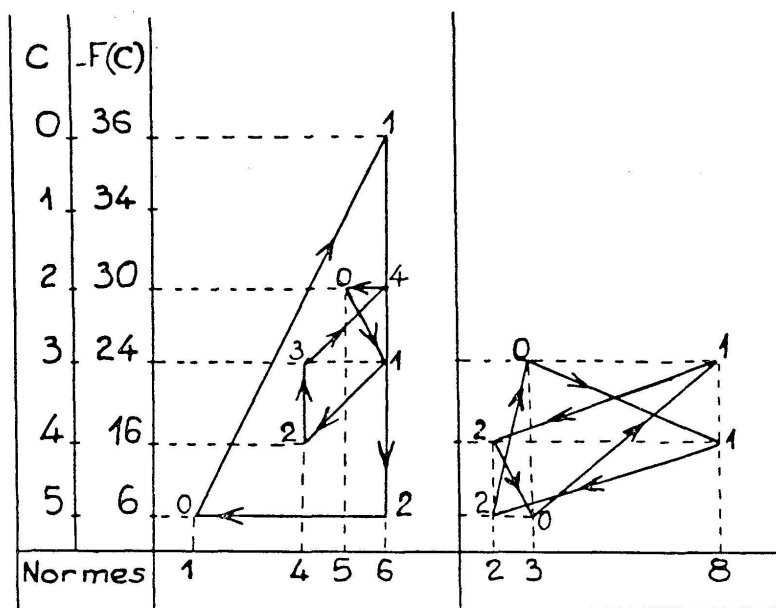
L'égalité des termes extrêmes est celle qui a été indiquée entre un idéal et son suivant, dans un cycle.

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

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

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

TABLEAU XXIV



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

De cette construction, on déduit l'expression des multiplicateurs au moyen de l'un d'entre eux (notamment de  $\rho_0$ ):

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

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