21. Construction des idéaux canoniques.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **6 (1960)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

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.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

LES CORPS QUADRATIQUES

par A. CHÂTELET

(suite)

CHAPITRE III

ALGORITHME DU TABLEAU DE VALEURS

21. Construction des idéaux canoniques.

Dans un corps quadratique, défini (**1**) par son *polynôme fondamental* $F(x)$, pour obtenir tous les idéaux canoniques (**7**), au moins de normes limitées, ainsi que certaines de leurs relations mutuelles de composition et de décomposition (**15** et **16**), on peut utiliser l'algorithme suivant.

On construit la *table des valeurs*, du polynôme $F(x)$, pour les *valeurs entières* c, de la variable x, jusqu'à un certain rang, en principe de part et d'autre de 0. Pour chaque valeur $F(c)$, on forme *les diviseurs* m, entiers positifs; *chacun est la norme d'un idéal canonique*, de racine c, ou défini par la forme canonique $(m,\ \theta—c)$.

Pour construire la table, on peut utiliser les *différences secondes* qui sont constantes et égales à 2, ou les *différences premières*, qui forment une progression arithmétique $—2Sc+S^2$.

Le trinôme $F(x)$ a des valeurs égales pour c et $S—c$, —ou pour des valeurs de x, symétriques par rapport à $S:2$, dont l'une est donc négative— . Par suite la table peut être construite pour les seules valeurs entières de c, croissantes, à partir de 0; il suffit de la compléter par symétrie, s'il y a lieu, explicitement ou implicitement.

La table peut être disposée en colonnes (voir tableaux I et II), dans lesquelles sont inscrits c, $F(c)$ et les diviseurs de $F(c)$.

Il est commode de réserver chaque colonne de diviseurs à un seul idéal **I**, dont la norme m est inscrite devant chacune des racines $c+\lambda m$, qui sont en *progression arithmétique*, ou équidistantes sur le tableau.

Si l'idéal n'est pas double, une colonne contiguë est attribuée à l'idéal conjugué **I'**, de même norme m, inscrite devant les valeurs $c'+\lambda m$, symétrique des précédentes, par rapport à $S:2$.

Dans les deux colonnes d'un couple d'idéaux conjugués différents, on peut, plus spécialement, distinguer les *racines minimum* $\overline{c'}$ négative et $\overline{c}$ symétrique, qui ont été caractérisées (**7. 4**) par les limitations:

$$(S-m):2<\overline{c'}<0\leqslant\overline{c}<(S+m):2; \qquad \overline{c}+\overline{c'}=S.$$

Si l'idéal est *double*, son unique *racine minimum* $\overline{c}$, qui n'est pas négative, est caractérisée par les limitations:

$$0\leqslant\overline{c}\leqslant(S+m):2.$$

Il en résulte qu'on obtient tous les idéaux, de norme au plus égale à m, et, notamment, avec leurs racines minimum, en limitant les valeurs de c, de $(S-m):2$ exclus à $(S+m):2$ inclus, cette limite n'étant atteinte que pour certains idéaux doubles.

Si le tableau n'est pas étendu aux valeurs négatives de c, on peut noter un idéal, dont la racine minimum $\overline{c'}$ est négative, par sa *plus petite racine positive*, qui est $\overline{c'}+m$; les limitations des racines ainsi distinguées sont alors, pour un couple d'idéaux conjugués:

$$0\leqslant\overline{c}\leqslant(S+m):2<\overline{c'}+m<m;$$

Si les idéaux sont égaux (idéal double), $\overline{c}$ est la seule racine minimum et il peut être égal à sa limite supérieure; sinon il ne l'atteint pas.

On obtient alors tous les idéaux de norme au plus égale à m, notamment avec leurs plus petites racines positives, en limitant les valeurs de c, de 0 inclus à m exclu.

On rappelle les propriétés de la *congruence fondamentale* (**5** et **6**) en les interprétant comme des propriétés du tableau et des idéaux canoniques ainsi obtenus.

Un *diviseur* m, *du discriminant* D, sans facteur carré, et notamment le diviseur trivial 1, figure dans *une*, et une seule, *colonne* et définit *un idéal double*. D'après le calcul des zéros doubles (**6**) et les conditions de limitation précédentes, la *racine*

minimum unique et la racine négative immédiatement précédente, sont, suivant les cas:

$m = 1$: $(\overline{c}—1) = —1$; $\overline{c} = 0$;

m diviseur de $D: 4$; $S = 0$: $(\overline{c}—m) = —m$; $\overline{c} = 0$;

m non diviseur de $D: 4$: $(\overline{c}—m) = (S—m): 2$; $\overline{c} = (S+m): 2$.

Si un *nombre premier* p, non diviseur du discriminant est dans le tableau, il y figure dans *un*, et un seul, *couple de colonnes contiguës*, devant deux progressions arithmétiques, symétriques par rapport à $S: 2$, de valeurs de c; il est la norme commune d'*un*, et d'un seul, *couple d'idéaux conjugués*. Il en est alors de même de toute puissance p^h, d'exposant h entier positif.

Si un *nombre composé* m figure dans la table, il en est de même de tous ses facteurs premiers. S'il a $2^{s'}$ *facteurs premiers*, non diviseurs de D, il figure dans $2^{s'-1}$ *couples de colonnes contiguës* et il est la norme d'autant de *couples d'idéaux conjugués*. Le cas de $s' = 0$, ou de m diviseur du discriminant a été étudié ci-dessus.

21. 2. Exemples (1). — Le tableau I donne les valeurs de $F(x) = x^2+x+10$, pour les valeurs entières c, de:

$$(—1 — 15): 2 = —8 \quad \text{à} \quad (—1 + 15): 2 = 7;$$

et leurs diviseurs, au plus égaux à 15, qui sont les normes des idéaux canoniques, limitées par 15.

Les colonnes contiguës, correspondant à un couple d'idéaux conjugués, sont indiquées sans trait de séparation entre les alignements des diviseurs. Les diviseurs qui sont dans les rangées des racines minimum sont en caractères gras. Dans chaque colonne on a indiqué par des traits les limitations extrêmes:

$$—(m+1): 2 \quad (m—1): 2;$$

elles sont comme les racines conjuguées, symétriques par rapport à l'axe également indiqué $x = —1: 2$.

Les diviseurs du discriminant $D = —39$, au plus égaux à 15, sont 1, 3, 13; ils figurent chacun dans une colonne et sont inscrits en caractères gras respectivement dans les rangées de 0, +1, +6. Ils sont les normes des idéaux doubles:

$$(1, \ \theta—0), \quad (3, \ \theta—1), \quad (13, \ \theta—6).$$

TABLEAU I.

$F(x) = x^2 + x + 10$; $D = -39 = -3 \times 13$

c	$F(c)$	Diviseurs ou Normes												
....	...	..	....	..	....	....	....	....	.....	.....	.....	.....	...	.....
−8	66	1	2	3			6				11			
−7	52	1	2		4								13	
−6	40	1	2		4	5		8		10				
−5	30	1	2	3		5	6			**10**				**15**
−4	22	1	2								**11**			
−3	16	1	2		4			**8**						
−2	12	1	2	3	**4**		**6**					**12**		
−1	10	1	**2**			**5**			**10**					
0	10	**1**	**2**			**5**			**10**					
+1	12	1	2	**3**	**4**		**6**					**12**		
+2	16	1	2		4			**8**						
+3	22	1	2								**11**			
+4	30	1	2	3		5	6			**10**				**15**
+5	40	1	2		4	5		8		10				
+6	52	1	2		4								**13**	
+7	66	1	2	3			6				11			
....	...	..	....	..	....	....	....	....	.....	.....	.....	.....	...	.....

Un autre diviseur 39, figurerait dans la table suffisamment étendue, en caractère gras, dans l'alignement de 19 et dans les alignements des $19+39\lambda$, qui sont aussi des racines des trois idéaux précédents.

Il y a des couples d'idéaux conjugués (colonnes contiguës), de normes 2, 4, 8, puissances de 2, de racines minimum respectives:

-1 et 0, -2 et $+1$, -3 et $+2$;

de normes 5 et 11, nombres premiers et de racines minimum respectives:

$$-1 \text{ et } 0; \quad -4 \text{ et } +3;$$

de normes 6, 12, 15, nombres composés avec un seul facteur non diviseur du discriminant, et de racines minimum respectives:

$$-2 \text{ et } +1; \quad -2 \text{ et } +1; \quad -5 \text{ et } +4.$$

Le nombre 10, qui a $s' = 2$ facteurs premiers 2,5 figurant dans la table et non diviseurs de D, figure dans deux couples de colonnes contiguës, sur les alignements des racines minimums respectives:

$$-1 \text{ et } 0; \quad -5 \text{ et } +4.$$

TABLEAU II.

$F(x) = x^2 - 15; \quad D = = + 60 = 4 \times 3 \times 5.$

c	$F(c)$	Diviseurs ou normes													
0	−15	**1**		**3**	**5**						**15**				
1	−14	1	**2**				**7**			**14**					
2	−11	1	—						**11**						
3	−6	1	2	3		**6**									
4	+1	1													
5	10	1	2		5			**10**							
6	21	1		3		—	**7**							**21**	
7	34	1	2									**17**			
8	49	1					7								
9	66	1	2	3		6			**11**						**22**
10	85	1			5			—					**17**		
11	106	1	2						—						
12	129	1		3											
13	154	1	2				7		11		**14**				**22**
14	181	1								—					
15	210	1	2	3	5	6	7	10		14	15			**21**	
16	241	1													
17	274	1	2									—			
18	309	1		3											
19	346	1	2												
20	385	1			5		7		11						
21	426	1	2	3		6								—	
22	469	1					7								—
...	.....	..	..	..	..	..	....	...	.....	.....	...	.....	.....	.....	

Les valeurs $F(c)$, inscrites dans la table montrent encore l'existence d'idéaux canoniques, non inscrits, de racine minimum $\overline{c}$ et de norme m:

$\overline{c}$: —3, +2; —4, +3; —5, +4; —6, +5; —7, +6; —8, +7.
m: 16 22 30 20; 40 26; 52 22; 33; 66.

Le tableau II donne les valeurs de $F(x) = x^2 - 15$, pour les valeurs entières de c, de:

0 à 22

et leurs diviseurs, au plus égaux à 22, qui sont les normes des idéaux canoniques, limités à 22. Le tableau est limité cette fois aux valeurs positives de c pour pouvoir comprendre un nombre plus grand de diviseurs.

Comme pour le premier exemple, les colonnes contiguës, correspondant à un couple d'idéaux conjugués, sont indiquées sans trait de séparation entre les alignements de diviseurs. Les diviseurs qui sont dans les rangées des racines positives minimum sont en caractère gras. Dans chaque colonne, on a indiqué par un trait la limitation extrême m, pour ces racines, sauf quand elle coïncide avec une de ces racines (racine minimum nulle).

Les diviseurs du discriminant, sans facteurs carrés, au plus égaux à 22, sont 1, 2, 3, 5, 6, 10, 15; ils figurent chacun dans une colonne et sont inscrits en caractère gras respectivement dans les rangées 0, 1, 0, 0, 3, 5, 0; ils sont les normes des idéaux doubles:

(1, θ—0), (2, θ—1), (3, θ—0), (5, θ—0), (6, θ—3),
(10, θ—5), (15, θ—0).

Le diviseur 30 figurerait dans la table suffisamment étendue, en caractère gras dans la rangée de 15.

Il y a des couples d'idéaux conjugués (colonnes contiguës), de normes 7, 11, 17, nombres premiers, et de racines positives minimums respectives:

1 et 6, 2 et 9, 7 et 10,

de normes 14, 21, 22 avec un seul facteur non diviseur du discriminant, et de racines positives minimum respectives:

1 et 13, 6 et 15, 9 et 13.

Les valeurs de $F(c)$, inscrites dans la table, montrent encore

l'existence d'idéaux canoniques, non inscrits, de racine positive minimum $\overline{c}$ (ou $\overline{c'}+m$) et de norme m:

$\overline{c}$:	7, 27;	9, 24;	9, 57;	10, 75;	11, 42;	11, 95;
m:	34	33	66	85	53	106 ;
$\overline{c}$:	15, 195;	16, 215;	17, 120;	17, 257;	18, 85;	
m:	210	241	137	274	103	
$\overline{c}$:	18, 291;	19,154;	19,327;	20, 35;	20, 57;	20, 365;
m:	309	173	346	55	77	385
c :	21, 50;	21, 121;	21,192;	21,405;	22, 45;	22, 447.
m:	71	142	213	426	67	469

22. Nombres premiers décomposables dans le corps.

On peut caractériser, à priori, les nombres premiers qui sont des diviseurs des valeurs de la table. En utilisant des propriétés de la Théorie élémentaire des nombres et, plus spécialement la *loi de réciprocité quadratique* [1]), on peut démontrer que:

en plus des diviseurs du discriminant, *les nombres premiers, pour qui la congruence fondamentale est possible*, —ou qui sont *normes de deux idéaux premiers*, du premier degré, conjugués— —ou décomposables en le produit de ces deux idéaux— *sont ceux qui appartiennent à certaines progressions arithmétiques*, dont la raison commune est la valeur absolue $|D|$, du discriminant du corps, et qui sont en nombre $\varphi(|D|)$ |2.

La congruence fondamentale (**1**), caractérisée par le nombre entier d, est *possible ou impossible suivant que*, d et, par suite, *le discriminant* D (égal à d, ou à $4d$) *est congru, ou n'est pas congru*, mod. p, au carré d'un nombre entier.

On peut représenter cette propriété de D, relative au nombre premier p, par le *symbole de* LEGENDRE. Il peut être construit en

---

[1]) Ces propriétés sont notamment exposées dans les ouvrages français: J.-A. SERRET, *Algèbre supérieure*, 3e édition, 1866 et suivantes; section III, ch. 2; E. BOREL et J. DRACH, d'après des leçons de J. TANNERY, *Introduction à la théorie des Nombres et à l'Algèbre supérieure*, 1894, 1re partie, ch. IV; J. TANNERY, *Leçons d'Arithmétique*, 1896, ch. XIV, § 5; E. CAHEN, *Eléments de la Théorie des Nombres*, 1900 — Théorie des Nombres — tome second, 1924, ch. XVI. On trouvera dans ces ouvrages la définition de la fonction — ou indicateur — d'EULER $\varphi(n)$.