Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 6 (1960)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LES CORPS QUADRATIQUES
Autor: Châtelet, A.
Kapitel: CHAPITRE III ALGORITHME DU TABLEAU DE VALEURS
DOI: https://doi.org/10.5169/seals-36342

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 $\varphi(n)$.

utilisant l'indice de D, défini par une racine primitive g, mod. p:

$$g^{\text{ind. } D} \equiv D, \quad (\text{mod. } p) \quad \Rightarrow \quad \left(\frac{D}{p}\right) = (-1)^{\text{ind. } D}.$$

Ce symbole est égal à $+1$, *ou à* -1, suivant que l'exposant ind. D, (défini mod. $p-1$) est pair ou impair —ou que D est congru ou n'est pas congru à un carré— donc *suivant que la congruence fondamentale est possible ou impossible.*

L'expression du symbole met en évidence son caractère multiplicatif: il est égal au produit des symboles des facteurs (entiers positifs ou négatifs) d'une décomposition de D en produit:

$$D = \Pi\delta_i \quad \Rightarrow \quad (-1)^{\text{ind. } D} = (-1)^{\Sigma(\text{ind. } \delta_i)} = \Pi\left(\frac{\delta_i}{p}\right).$$

Il est commode de décomposer D en un produit de facteurs δ_i, comprenant éventuellement un facteur, noté δ_1, égal à -4, ou $+8$, ou -8, et des facteurs premiers impairs, différents, chacun étant affecté d'un signe convenable, de façon qu'il soit congru à $+1$, mod. 4. [Exemples: -3, $+5$, -7, -11, $+13$, ...]

L'examen des divers cas montre que ceci est possible:

1. *d impair*, positif ou négatif, *congru à* $+1$, mod. 4. Alors D est égal à d; sa valeur absolue est égale à un produit de facteurs premiers impairs différents. Le nombre de ceux qui sont congrus à -1, mod. 4, est pair ou impair, suivant que d est positif ou négatif; on peut donc les affecter du signe —. Exemples:

$d = -3;\ +5;\ +21;\ -15;\ +65;\ \ldots$
$D = -3;\ +5;\ (-3)\times(-7);\ (-3)\times(+5);\ (+5)\times(+13);\ \ldots$

2. *d impair*, positif ou négatif, congru à -1, mod. 4. Alors D est égal à $4d$; on conserve le signe de D, en affectant 4 du signe —. Exemples:

$d = -1;\ +3;\ -5;\ -21;\ \ldots$
$D = -4;\ (-4)\times(-3);\ (-4)\times(+5);\ (-4)\times(-3)\times(-7);\ \ldots$

3. *d pair*, positif ou négatif. Alors $D = 4d$ a un facteur 8 qu'on affecte du signe $+$ ou —, suivant les signes affectés éventuellement aux autres facteurs. Exemples:

$d = +2;\ -2;\ +6;\ -6;\ +10;\ \ldots$
$D = +8;\ -8;\ (-8)\times(-3);\ (+8)\times(-3);\ (+8)\times(+5);\ \ldots$

Pour calculer les divers symboles, ainsi considérés, on peut utiliser la *loi de réciprocité*, bornée au cas d'un facteur δ, impair et congru à $+1$, mod. 4, ou égal à -4, $+8$, ou -8. Elle est alors exprimée par les égalités:

δ impair premier, congru à $+1$, mod. 4: $\left(\frac{\delta}{p}\right) = \left(\frac{p}{|\delta|}\right)$;

$\left(\frac{-4}{p}\right) = +1$ ou -1, suivant que $p \equiv +1$ ou -1, (mod. 4);

$\left(\frac{+8}{p}\right) = +1$ ou -1, suivant que $\begin{cases} p \equiv +1 \text{ ou } -1, \\ \text{ou} \\ p \equiv +3 \text{ ou } -3, \end{cases}$ (mod. 8);

$\left(\frac{-8}{p}\right) = +1$ ou -1, suivant que $\begin{cases} p \equiv +1 \text{ ou } +3, \\ \text{ou} \\ p \equiv -1 \text{ ou } -3, \end{cases}$ (mod. 8).

Il en résulte que, pour chaque facteur δ, considéré (y compris -4, $+8$, et -8), le symbole a la même valeur pour des nombres premiers p, congrus entre eux, mod. $|\delta|$ et, pour le calculer, on peut remplacer p par tout nombre congru, mod. $|\delta|$; notamment par le reste de sa division par $|\delta|$ (compris entre 1 et $|\delta|$ et premier avec $|\delta|$).

Les facteurs $|\delta_i|$ étant premiers entre eux, deux à deux, pour que des nombres soient simultanément congrus, suivant chacun d'eux, il faut et il suffit qu'ils soient congrus suivant leur produit $|D|$.

Les valeurs simultanées des symboles des facteurs δ_i et par suite celle de leur produit sont donc les mêmes pour tous les nombres premiers appartenant à une même progression arithmétique, de raison $|D|$; —donc congrus, mod. $|D|$— .

Dans les $\varphi(|\delta_i|)$ valeurs, incongrues, mod. $|\delta_i|$:

$|\delta_i|$ impair, $\varphi(|\delta_i|) = |\delta_i| - 1$; $\varphi(4) = 2$; $\varphi(8) = 4$;

la moitié ont un *symbole de* LEGENDRE positif. Un raisonnement simple de récurrence montre qu'il en est de même pour les

$\varphi(|D|) = \Pi\varphi(|\delta_i|)$ valeurs incongrues, mod. $|D| = \Pi|\delta_i|$.

Il y a $\varphi(|D|) : 2$ progressions pour lesquelles le symbole de

LEGENDRE est positif; les nombres premiers qui leur appartiennent sont ceux qui sont normes d'idéaux premiers conjugués distincts —ou diviseurs des valeurs du tableau, non diviseurs de $|D|$.

Le tableau III donne un exemple de calcul de ces progressions pour le corps de discriminant —39 (tableau I). On a calculé directement, sans utiliser les indices, les classes, mod. 3 et mod. 13, qui sont congrues à des carrés.

On obtient ainsi 12 progressions arithmétiques, on donne les premiers nombres premiers (inférieurs à 500) qui leur appartiennent;

TABLEAU III.

Corps de discriminant $D = -39 = (-3)\times(+13)$; $\varphi(39) = 24$.

Classes mod. 3: $1^2 \equiv 2^2 \equiv 1$,

Mod. 13: $\begin{cases} 1^2 \equiv 12^2 \equiv 1; & 2^2 \equiv 11^2 \equiv 4; & 3^2 \equiv 10^2 \equiv 9 \\ 4^2 \equiv 9^2 \equiv 3; & 5^2 \equiv 8^2 \equiv 12; & 6^2 \equiv 7^2 \equiv 10. \end{cases}$

$p \equiv a$ mod. 39	mod. 3	mod. 13	$\left(\frac{-3}{p}\right) = \left(\frac{a}{3}\right)$	$\left(\frac{13}{p}\right) = \left(\frac{a}{13}\right)$	$\left(\frac{-39}{p}\right)$
1	1	1	+1	+1	+1
2	2	2	—1	—1	+1
4	1	4	+1	+1	+1
5	2	5	—1	—1	+1
7	1	7	+1	—1	—1
8	2	8	—1	—1	+1
10	1	10	+1	+1	+1
11	2	11	—1	—1	+1
14	2	1	—1	+1	—1
16	1	3	+1	+1	+1
17	2	4	—1	+1	—1
19	1	6	+1	—1	—1
20	2	7	—1	—1	+1
22	1	9	+1	+1	+1
23	2	10	—1	+1	—1
25	1	12	+1	+1	+1
28	1	2	+1	—1	—1
29	2	3	—1	+1	—1
31	1	5	+1	—1	—1
32	2	6	—1	—1	+1
34	1	8	+1	—1	—1
35	2	9	—1	+1	—1
37	1	11	+1	—1	—1
38	2	12	—1	+1	—1

chacun d'eux est la norme de deux idéaux canoniques conjugués; dont l'un a une racine minimum positive c, indiquée entre parenthèses; la racine minimum de l'autre est $-1-c$ (ainsi qu'il est indiqué dans le tableau I, pour les premiers de ces idéaux, de normes 2 et 5):

$1+39\lambda$: 79 (17); 157 (39); 313 (141);
$2+39\lambda$: 2 (0); 41 (8); 197 (71); 353 (145); 431 (192);
$4+39\lambda$: 43 (20); 199 (44); 277 (66); 433 (41);
$5+39\lambda$: 5 (0); 83 (12); 239 (102); 317 (43);
$8+39\lambda$: 47 (16); 281 (23); 359 (53);
$10+39\lambda$: 127 (35); 283 (33); 439 (209);
$11+39\lambda$: 11 (3); 89 (26); 167 (31); 401 (89); 479 (169);
$16+39\lambda$: 211 (79); 367 (60);
$20+39\lambda$: 59 (21); 137 (28); 293 (113); 449 (189);
$22+39\lambda$: 61 (24); 139 (64); 373 (38);
$25+39\lambda$: 103 (47); 181 (46); 337 (100);
$32+39\lambda$: 71 (11); 149 (54); 227 (42); 383 (27); 461 (52).

Le tableau IV donne de même un exemple de calcul des progressions pour le corps de discriminant $+60$ (tableau II).

TABLEAU IV.

$F(x) = x^2-15$; $D = +60 = (-4)\times(-3)\times(+5)$; $\varphi(60) = 16$.

mod. 60	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
mod. 4	1	3	3	1	1	3	3	1	3	1	1	3	3	1	1	3
$\left(\frac{-4}{p}\right)$	+	−	−	+	+	−	−	+	−	+	+	−	−	+	+	−
mod. 3	1	1	2	1	2	1	2	2	1	1	2	1	2	1	2	2
$\left(\frac{-3}{p}\right)$	+	+	−	+	−	+	−	−	+	+	−	+	−	+	−	−
mod. 5	1	2	1	3	2	4	3	4	1	2	1	3	2	4	3	4
$\left(\frac{5}{p}\right)$	+	−	+	−	−	+	−	+	+	−	+	−	−	+	−	+
$\left(\frac{60}{p}\right)$	+	+	+	−	+	−	−	−	−	−	−	+	−	+	+	+

On obtient 8 progressions arithmétiques, dont on donne encore les premiers nombres premiers (inférieurs à 500), ainsi que la norme minimum positive de l'un des idéaux dont ils sont la norme:

$1+15\lambda$: 61 (25); 181 (14); 241 (16); 421 (65);
$7+15\lambda$: 7 (1); 67 (22); 127 (53); 307 (130); 367 (105); 487 (224);
$11+15\lambda$: 11 (2); 71 (21); 131 (43); 191 (46); 251 (39); 311 (126); 431 (51); 491 (83);
$17+15\lambda$: 17 (7); 137 (17); 197 (58); 257 (23); 317 (40);
$43+15\lambda$: 43 (12); 103 (18); 163 (34); 223 (98); 283 (79); 463 (101);
$49+15\lambda$: 109 (48); 229 (106); 349 (109); 409 (158);
$53+15\lambda$: 53 (11); 113 (44); 173 (19); 233 (99); 293 (111); 353 (108);
$59+15\lambda$: 59 (29); 179 (33); 239 (60); 359 (71); 419 (68); 479 (203).

Il y a une infinité de nombres premiers vérifiant les conditions précédentes, donc d'*idéaux premiers du premier degré*, dans tout corps quadratique.

On peut le démontrer en s'inspirant du raisonnement arithmétique qui est utilisé couramment pour démontrer l'existence d'une infinité de nombres premiers. On forme le produit C, des m premiers nombres premiers p_i, à l'exception des diviseurs du discriminant D. Le nombre entier C^2-D admet un diviseur premier p, supérieur à tous les p_i, et qui vérifie la condition imposée [1]).

23. Congruence et classes d'idéaux.

De même qu'on a construit le groupe quotient $\mathcal{G}|\mathfrak{L}$, des classes du groupe $\mathcal{G}(\theta)$, relativement au sous-groupe $\mathfrak{L}$, des

[1]) Cette propriété résulte aussi du *théorème de la progression arithmétique*, qui affirme l'existence d'une infinité de nombres premiers dans chacune des progressions arithmétiques, construites comme il a été dit, de raison $|D|$ et dont les premiers termes sont premiers avec $|D|$. Ceci montre aussi bien l'existence d'une infinité d'idéaux premiers du second degré —ou de nombres premiers ne vérifiant pas la condition imposée—. On pourrait aussi en donner une démonstration directe, mais sans distinguer l'appartenance des normes aux différentes progressions.

idéaux principaux rationnels (**14 bis**), on peut construire le groupe quotient $\mathcal{G}|\mathcal{R}$, relativement au sous-groupe $\mathcal{R}$, des idéaux principaux (ρ). Il peut être utile de donner une construction directe de cette répartition, en définissant d'abord une *congruence* —ou un mode d'égalité— .

DÉFINITION. — *Deux idéaux*, non nuls, d'un corps $\mathbf{R}(\theta)$, *sont* **congrus** [sous entendu, mod. $\mathcal{R}$] *lorsque leur quotient est égal à un idéal principal.*

Cette relation est désignée par le signe $\sim$, séparant les idéaux congrus; elle a les qualités d'une égalité. Elle est *réflexive* ($\mathbf{I} \sim \mathbf{I}$) le quotient d'un idéal par lui-même est l'idéal unité qui est principal. Elle est *symétrique*, l'ordre du quotient est indifférent: si $\mathbf{I}\times\mathbf{J}^{-1}$ est principal, il en est de même de $\mathbf{J}\times\mathbf{I}^{-1}$, qui est l'idéal inverse. Elle est *transitive*:

$$\{\mathbf{I} \sim \mathbf{J} \quad \text{et} \quad \mathbf{J} \sim \mathbf{K}\} \quad \Rightarrow \quad \mathbf{I} \sim \mathbf{K};$$

car si les quotients $\mathbf{I}\times\mathbf{J}^{-1}$ et $\mathbf{J}\times\mathbf{K}^{-1}$ sont des idéaux principaux, il en est de même de $\mathbf{I}\times\mathbf{K}^{-1}$, qui est égal à leur produit.

Il est équivalent de dire que deux idéaux sont congrus, si l'un d'eux, et, par suite, chacun d'eux, est égal au produit de l'autre par un idéal principal (ρ) non nul, ou par la base ρ de cet idéal:

$$\mathbf{I} \sim \mathbf{J} \quad \Leftrightarrow \quad \text{Existe } \rho \neq 0 \quad \text{et} \quad \mathbf{I} = (\rho)\times\mathbf{J} \quad \text{ou} \quad \rho\times\mathbf{J}.$$

La multiplication et la division conservent —ou sont compatibles avec— la congruence: des produits et des quotients d'idéaux respectivement congrus, sont des idéaux congrus.

En effet si $\mathbf{I}\times\mathbf{I}_1^{-1}$ et $\mathbf{J}\times\mathbf{J}_1^{-1}$ sont des idéaux principaux, il en est de même des idéaux:

$$(\mathbf{I}\times\mathbf{J})\times(\mathbf{I}_1\times\mathbf{J}_1)^{-1} = (\mathbf{I}\times\mathbf{I}_1^{-1})\times(\mathbf{J}\times\mathbf{J}_1^{-1});$$

$$(\mathbf{I}\times\mathbf{J}^{-1})\times(\mathbf{I}_1\times\mathbf{J}_1^{-1})^{-1} = (\mathbf{I}\times\mathbf{I}_1^{-1})\times(\mathbf{J}\times\mathbf{J}_1^{-1})^{-1};$$

qui en sont un produit et un quotient.

La conjugaison conserve —ou est compatible avec— la congruence: les idéaux conjugués de deux idéaux congrus sont congrus: si $\mathbf{I}\times\mathbf{J}^{-1}$ est principal, il en est de même de $\mathbf{I}'\times(\mathbf{J}')^{-1}$, qui est son conjugué.

DÉFINITION. — Dans un corps quadratique, on appelle **classe d'idéaux** (sous-entendu mod. $\mathcal{R}$) toute famille d'idéaux formée par *ceux qui sont congrus à un idéal non nul.*

En raison de la transitivité de la congruence, les idéaux d'une classe sont congrus entre eux, deux à deux; la classe peut être définie —ou engendrée— par un de ses idéaux, choisi arbitrairement.

Les classes d'idéaux, dans un corps constituent une *répartition* de l'ensemble —ou du groupe $\mathcal{G}$— des idéaux non nuls: tout idéal appartient à une classe (celle qu'il engendre); deux classes qui ont un idéal commun sont égales.

On peut **multiplier** les classes d'idéaux d'un corps: l'ensemble des produits de tout idéal **A**, d'une classe $\mathcal{A}$, par tout idéal **B**, d'une classe $\mathcal{B}$ (éventuellement égale à $\mathcal{A}$) est une classe, qui est appelée le **produit** (de la multiplication) des classes et qui est désignée par $\mathcal{A}\times\mathcal{B}$.

Les produits $\mathbf{A}\times\mathbf{B}$ sont congrus entre eux, en raison de la conservation de la congruence dans la multiplication. En outre tout idéal **I** congru à un produit $\mathbf{A}\times\mathbf{B}$ est lui-même égal à un produit, puisque:

$$\mathbf{I} = (\mathbf{A}\times\mathbf{B})\times\rho = \mathbf{A}\times(\mathbf{B}\times\rho);$$

et $\mathbf{B}\times\rho$ appartient à $\mathcal{B}$.

La multiplication des classes ainsi définie, s'étend à plusieurs facteurs; elle est manifestement *associative* et *commutative*, comme celle des idéaux (**12**), qui sert à la définir. Elle permet de définir les puissances (d'exposants entiers positifs) d'une classe.

La **classe principale** est la famille —ou le groupe— $\mathcal{R}$, de tous les idéaux principaux (ρ), non nuls, qui sont manifestement tous ceux qui sont congrus à l'un quelconque d'entre eux.

Cette classe est un *élément neutre* —ou *unité*— pour la multiplication (des classes): toute classe est égale à son produit par $\mathcal{R}$:

$$\mathcal{A}\times\mathcal{R} = \mathcal{A}; \quad \text{notamment} \quad \mathcal{R}^2 = \mathcal{R}\times\mathcal{R} = \mathcal{R}.$$

Deux classes $\mathcal{A}$ et $\mathcal{A}'$ (notées par une même lettre avec et sans accent) *sont* **conjuguées**, *lorsque l'une*, et, par suite, chacune d'elles, *est constituée par les idéaux conjugués de tous les idéaux de l'autre.*

Les conjugués des idéaux d'une classe sont en effet congrus entre eux, en raison de la conservation de la congruence dans la conjugaison, et la relation est réciproque. Pour que deux classes soient conjuguées, il suffit que l'une contienne le conjugué d'*un* idéal de l'autre.

Deux classes sont **inverses** (au sens général de ce qualificatif) —ou chacune d'elles est l'inverse de l'autre— *lorsque leur produit est égal à la classe principale* —ou classe unité— .

Deux classes conjuguées sont inverses et réciproquement:

$$\mathcal{A}\times\mathcal{A}' = \mathcal{R} \quad \text{et} \quad \mathcal{A}\times\mathcal{A}^{-1} = \mathcal{R} \quad \Rightarrow \quad \mathcal{A}^{-1} = \mathcal{A}'.$$

D'une part, le produit $\mathcal{A}\times\mathcal{A}'$ de deux classes conjuguées contient le produit $\mathbf{A}\times\mathbf{A}'$ de deux idéaux conjugués, qui est égal à l'idéal principal (rationnel), $(N(\mathbf{A}))$, dont la base est la norme (commune) des idéaux conjugués (**13**); c'est donc la classe $\mathcal{R}$, des idéaux principaux. Inversement si deux idéaux sont inverses, l'associativité de la multiplication montre qu'ils sont conjugués:

$$\mathcal{A}\times\mathcal{A}^{-1} = \mathcal{R} \quad \Rightarrow \quad (\mathcal{A}'\times\mathcal{A})\times\mathcal{A}^{-1} = \mathcal{A}'\times\mathcal{R} \quad \Rightarrow \quad \mathcal{A}^{-1} = \mathcal{A}'.$$

Deux classes conjuguées sont donc, chacune constituée par les inverses des idéaux de l'autre. C'est aussi bien une conséquence de la construction de l'inverse (**14**); l'idéal $\mathbf{A}'\times(N(\mathbf{A}))^{-1}$ est à la fois inverse de $\mathbf{A}$ et congru à son conjugué $\mathbf{A}'$.

Un raisonnement général (déjà utilisé ci-dessus pour la division des idéaux; **14**) permet de déduire de l'*existence* d'une classe inverse, *la possibilité et la détermination de la division* des classes.

Etant données une classe dividende $\mathcal{D}$ et une classe diviseur $\mathcal{A}$, *il existe une et une seule classe* $\mathcal{B}$, appelée **quotient** de $\mathcal{D}$ par $\mathcal{A}$, *dont le produit* (de la multiplication) *par* $\mathcal{A}$ *est égal à* $\mathcal{D}$.

Ce quotient est égal au *produit de la classe dividende par l'inverse* —ou la conjuguée— *de la classe diviseur.*

C'est une conséquence de l'associativité de la multiplication:

$$\mathcal{A}\times\mathcal{B} = \mathcal{D} \quad \Leftrightarrow \quad (\mathcal{A}'\times\mathcal{A})\times\mathcal{B} = \mathcal{A}'\times\mathcal{D} \quad \Leftrightarrow \quad \mathcal{B} = \mathcal{A}'\times\mathcal{D}.$$

Cette règle comprend, comme cas particulier, la construction, déjà faite, du quotient de la classe principale —ou unité— $\mathcal{R}$, par une classe $\mathcal{A}$, qui est égal à la classe conjuguée —ou inverse— $\mathcal{A}'$.

Une classe est **double**, *lorsqu'elle est égale à sa conjuguée*, qui est aussi son inverse, son carré est égal à $\mathcal{R}$.

Pour qu'une classe soit double, il suffit qu'elle contienne deux idéaux conjugués; notamment un idéal double.

Les qualités de la multiplication et de la division des classes peuvent encore être exprimées (partiellement) par la constitution d'un *groupe* (ainsi qu'il a déjà été dit, dans un corps $\mathbf{R}(\theta)$, pour ses éléments non nuls (**1**); pour ses idéaux non nuls (groupe $\mathcal{G}$) et pour ses idéaux principaux rationnels (groupe $\mathfrak{Q}$) [**14** et **14** *bis*].

Dans un corps quadratique, *les classes d'idéaux* (mod. $\mathcal{R}$) *forment un groupe multiplicatif abélien*, dont l'élément unité est la classe principale $\mathcal{R}$, qui peut être aussi désignée par (1).

Ce groupe contient les *puissances* $\mathcal{A}^x$, d'exposant x, entier quelconque (**14**), d'une classe $\mathcal{A}$, et les *monômes* —ou produits— de puissances de classes $\mathcal{A}^x \times \mathcal{B}^y \times \ldots$ Toutes les puissances de $\mathcal{R}$ sont égales à elle-même.

On aurait pu construire ce groupe des classes en utilisant des *propriétés générales des groupes abéliens.*

Dans le groupe multiplicatif $\mathcal{G}(\theta)$, des idéaux non nuls (**14 bis**), les idéaux principaux (ρ) constituent évidemment un sous-groupe $\mathcal{R}$, (contenant lui-même le sous-groupe $\mathfrak{Q}$ des idéaux principaux rationnels). Deux idéaux de $\mathcal{G}$ sont *congrus* lorsque leur quotient est dans $\mathcal{R}$, ce qui est une propriété réciproque en raison de la commutativité de la multiplication.

Les *classes d'idéaux* sont les *classes de répartition* des éléments du groupe $\mathcal{G}$, relativement au sous-groupe $\mathcal{R}$; on vérifie d'une façon générale qu'elles se multiplient et se divisent et constituent par suite un groupe multiplicatif abélien, qui est appelé (généralement) *groupe quotient* $\mathcal{G}|\mathcal{R}$, de $\mathcal{G}$ par $\mathcal{R}$.

Un **corps principal** (**19**) ne contient que la seule classe principale, qui constitue, à elle seule, un groupe d'un seul élément unité.

On étudie ci-dessous la structure du *groupe des classes*, dans un corps quadratique quelconque et on montre notamment qu'il ne contient qu'*un nombre fini de classes* —ou qu'il est d'*ordre fini*— .

24. Congruence d'idéaux canoniques.

La congruence des idéaux et la formation des classes peuvent être ramenées *à une congruence et à un calcul d'idéaux canoniques*, en utilisant la remarque suivante:

Un idéal fractionnaire $\mathbf{I} = q \times \mathbf{M}$ *est congru à son facteur canonique* **M**.

La forme canonique d'un idéal **I** (**8**) est en effet le produit de son facteur canonique **M** par le facteur rationnel q, —ou l'idéal principal (rationnel) (q)— (**12**).

Donc deux idéaux, non nuls, sont congrus, si et seulement si il en est ainsi de leurs facteurs canoniques (puisque la congruence est transitive).

Ces considérations sont encore des conséquences des *propriétés générales des groupes*. Le groupe $\mathcal{R}$, des idéaux principaux admet comme sous-groupe, le groupe $\mathfrak{Q}$ des idéaux principaux rationnels. Dans chaque classe de $\mathcal{G}$ et de $\mathcal{R}$, mod. $\mathfrak{Q}$, il y a un et un seul idéal canonique. La répartition des idéaux canoniques en classes est donc équivalente à la formation du groupe quotient des groupes quotients $(\mathcal{G}|\mathfrak{Q})|(\mathcal{R}|\mathfrak{Q})$.

La relation d'*association* (**16**) d'idéaux canoniques, qui se présente naturellement, comme il a été dit (**21**), dans l'*algorithme du tableau de valeurs*, entraîne une relation entre les classes.

Théorème des idéaux associés. — *Deux idéaux canoniques associés*, relativement à une racine c, *définissent* —ou engendrent— *des classes inverses*, donc conjuguées (**23**). En particulier un *idéal réfléchi* définit une *classe double* (**23**).

En effet, le produit de deux idéaux associés, suivant une racine c, étant l'idéal principal $(\theta—c)$, le produit des classes qu'ils définissent est la classe principale —ou chacun est congru à l'idéal conjugué de l'autre— :

$$\mathbf{M} \times \mathbf{N} = (\theta—c) \quad \Rightarrow \quad \mathbf{M} \sim \mathbf{N}' \quad \text{et} \quad \mathbf{M}' \sim \mathbf{N}.$$

On peut expliciter cette relation de congruence en précisant une base de l'idéal principal multiplicateur. Les expressions:

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

entraînent:

$$\mathbf{M}\times[(\theta'—c): m] = \mathbf{N}'; \qquad \mathbf{M} = \mathbf{N}'\times[(\theta—c): n].$$

En appliquant la règle du produit d'idéaux, définis l'un par une *base arithmétique*, l'autre par une *base algébrique* (**13**), on obtient:

$$\begin{aligned}\mathbf{M}\times(\theta'—c) &= (m, \theta—c)\times(\theta'—c) = (m\times(\theta'—c),\ (\theta—c)\times(\theta'—c))\\ &= (m\times(\theta'—c), F(c)) = (m\times(\theta'—c), m\times n)=(m)\times\mathbf{N}'.\end{aligned}$$

On peut vérifier de même la seconde formule; on peut aussi bien former le produit des deux multiplicateurs indiqués qui doivent être inverses:

$$[(\theta'—c): m]\times[(\theta—c): n] = [(\theta'—c)\times(\theta—c)]: (m\times n) = [F(c)]: (m\times n);$$

le résultat est bien égal à $+1$ ou à -1 (suivant le signe de $F(c)$).

La congruence de deux idéaux canoniques établit entre leurs éléments une correspondance biunivoque qui conserve l'addition —ou est un *isomorphisme des modules*— . Elle fait par suite corespondre des bases arithmétiques libres (**9**).

Théorème des bases des idéaux congrus. — *Une congruence entre des idéaux canoniques* $\mathbf{M}$ *et* $\mathbf{M}_1$, *fait correspondre à une base arithmétique libre*, de l'un $\mathbf{M}_1$ (qui peut être sa base canonique), *une base arithmétique libre de l'autre* $\mathbf{M}$ (donc équivalente arithmétiquement à sa base canonique (**9**).

Les éléments ξ, de l'idéal canonique $\mathbf{M}_1$, sont des entiers algébriques, représentés proprement, au moyen d'une base arithmétique libre de deux éléments α_1 β_1 par les expressions:

$$\xi = x\times\alpha_1+y\times\beta_1; \qquad x,y \text{ entiers rationnels.}$$

La congruence étant définie par un multiplicateur (élément du corps) ρ, non nul, les produits:

$$\rho\times\xi = \rho\times(x\times\alpha_1+y\times\beta_1) = x\times(\rho\times\alpha_1)+y\times(\rho\times\beta_1),$$

sont des éléments de $\mathbf{M} = \rho\mathbf{M}_1$, donc des entiers algébriques, qui sont représentés ainsi au moyen de la *base arithmétique* $\rho\times\alpha_1$ $\rho\times\beta_1$. Cette représentation est propre et la *base est libre*, car l'annulation de $\rho\times\xi$ est équivalente à celle de ξ; donc à celle de x et de y.

En outre les éléments de $\mathbf{M}$ et de $\mathbf{M}_1$ se correspondent, en étant *représentés par les mêmes coefficients* (entiers rationnels) relativement aux bases correspondantes, $\alpha_1\ \beta_1$ et $\rho\times\alpha_1\ \rho\times\beta_1$.

Cette correspondance peut notamment être appliquée à des idéaux congrus, construits par l'intermédiaire d'idéaux associés:

$$\mathbf{M} = (m,\ \theta\text{—}c),\quad \mathbf{N} = (n,\ \theta\text{—}c);\qquad \mathbf{M}_1 = \mathbf{N}'.$$

La congruence de $\mathbf{M}_1$ à $\mathbf{M}$ est réalisée par le multiplicateur $(\theta\text{—}c)\colon n$. Appliqué à la base $(n,\ \theta'\text{—}c)$, de $\mathbf{M}_1$ il donnerait la base canonique de $\mathbf{M}$. Mais, appliqué à une base $(n,\ \theta\text{—}c_1)$, (où c_1 est une racine conjuguée de c, suivant le module n), il donne une base arithmétique libre de $\mathbf{M}_1$:

$$n\times[(\theta\text{—}c)\colon n] = (\theta\text{—}c),\quad [(\theta\text{—}c_1)\times(\theta\text{—}c)]\colon n$$

qui peut être différente de la base canonique, mais lui est arithmétiquement équivalente.

Dans l'exemple du tableau I, on peut considérer les idéaux associés:

$$\mathbf{M} = (3,\ \theta\text{—}1),\quad \mathbf{N} = (4,\ \theta\text{—}1),\qquad \mathbf{M}_1 = \mathbf{N}' = (4,\ \theta\text{—}2);$$

le multiplicateur de $\mathbf{M}_1$ étant $(\theta\text{—}1)\colon 4$, à la base choisie de $\mathbf{M}_1$, il fait correspondre:

$$4\times[(\theta\text{—}1)\colon 4] = \theta\text{—}1,\quad [(\theta\text{—}1)\times(\theta\text{—}2)]\colon 4 = \text{—}\theta\text{—}2.$$

On vérifie bien que ce couple d'éléments est bien arithmétiquement équivalent à la base canonique de $\mathbf{M}$:

$$\left\|\begin{matrix}\theta\text{—}1\\ \text{—}\theta\text{—}2\end{matrix}\right\| = \left\|\begin{matrix}0 & 1\\ \text{—}1 & \text{—}1\end{matrix}\right\| \times \left\|\begin{matrix}3\\ \theta\text{—}1\end{matrix}\right\|$$

25. Idéaux canoniques réduits.

THÉORÈME du nombre de classes d'idéaux. — Dans un corps quadratique, *le nombre de classes d'idéaux*, (mod. $\mathcal{R}$) —ou l'ordre du groupe quotient $\mathcal{G}|\mathcal{R}$— *est fini.*

Pour démontrer cette propriété, on peut ramener la construction des classes à celle d'idéaux canoniques particuliers, appelés *réduits*, pour lesquels on vérifie que:

1. Toute classe contient au moins un idéal réduit —ou *tout idéal canonique est congru à* (au moins) *un idéal réduit*— .

2. *Le nombre total d'idéaux* (canoniques) *réduits est fini.* Il en est, à fortiori, de même du nombre de classes, qui lui est au plus égal, et chacune d'elles ne renferme qu'un nombre fini d'idéaux réduits.

Le choix d'une définition d'un idéal réduit présente évidemment un certain caractère arbitraire; il est justifié, à posteriori, par la vérification des deux qualités précédentes.

Définition. — Un idéal canonique réduit, ou, par abréviation, *un* **idéal réduit**, *est un idéal canonique* $(m,\ \theta\text{—}\overline{c})$, *dont le carré de la norme est au plus égal à la valeur absolue du polynôme fondamental,* $|F(\overline{c})|$ pour la *racine minimum* $\overline{c}$ (de cet idéal):

$$|2\overline{c}\text{—}S| < m, \quad \text{ou bien} \quad 2\overline{c}\text{—}S = m; \qquad m^2 \leqslant |F(\overline{c})|.$$

Deux idéaux (canoniques) *conjugués* (**7**), *distincts*, dont les racines minimum sont $\overline{c}$ et $S\text{—}\overline{c}$ (**21**), *sont simultanément réduits*, puisque $F(\overline{c})$ et $F(S\text{—}\overline{c})$ sont égaux.

Pour un *idéal double*, la norme m étant diviseur du discriminant, d'après la valeur de la racine minimum indiquée ci-dessus (**21**), la condition de réduction est équivalente, suivant les cas à:

$$\overline{c} = 0: \qquad m^2 \leqslant |F(0)|, \quad \text{ou} \quad 4m^2 \leqslant |D|;$$

$$2\overline{c}\text{—}S = m; \quad 4m^2 \leqslant |m^2\text{—}D|; \qquad \begin{cases} 3m^2 \leqslant |D|; & D < 0 \\ 5m^2 \leqslant D; & D > 0. \end{cases}$$

L'*idéal unité* $(1,\ \theta\text{—}0)$ *est manifestement réduit.*

1. Pour tout idéal canonique **M**, *on peut construire*, au moins *un idéal congru, qui soit réduit.*

On peut raisonner par récurrence sur la norme. La construction est triviale si **M** vérifie les conditions de réduction; il est congru à lui-même.

La construction est encore évidente s'il existe une racine c, de l'idéal, pour laquelle $|F(c)| = m$. Alors l'idéal est principal (**11**):

$$(m,\ \theta—c) = (|F(c)|,\ \theta—c) = (\theta—c);$$

il est congru à l'idéal unité qui est réduit.

La construction existe pour la valeur 1, de la norme, puisque l'idéal est alors l'idéal unité, qui est réduit. Il suffit d'établir, par récurrence, qu'*un idéal canonique*, qui ne vérifie pas les deux constructions triviales précédentes, *est congru à un idéal canonique, de norme plus petite.*

Un tel idéal, a, au moins, une racine c (notamment sa racine minimum) telle que:

$$m^2 > |F(c)| \quad \text{et} \quad m < |F(c)|.$$

L'idéal $\mathbf{N} = (n, \theta—c)$, de norme $|F(c)| : m = n$, qui lui est associé, vérifie les conditions de comparaison:

$$1 < n = |F(c)| : m < m.$$

Or l'idéal **M** est congru à l'idéal $\mathbf{N}'$ conjugué de **N** (**22**), dont la norme n est bien inférieure à m.

Si la racine c est minimum pour **N**, cet idéal et son conjugué $\mathbf{N}'$ sont réduits, et la récurrence est terminée.

2. *Les conditions de réduction entraînent une limitation des racines minimum*, donc aussi des normes des idéaux réduits, dont le nombre est, par suite, fini.

Cette limitation est exprimée par la comparaison (générale):

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

qui est équivalente, suivant le signe du discriminant D, à:

$$\begin{array}{lllll} D > 0: & F(\bar{c}) < 0; & 5(2\bar{c}—S)^2 \leqslant D\ ; & \text{et} & 4m^2 \leqslant D\ ; \\ D < 0: & & 3(2\bar{c}—S)^2 \leqslant |D|; & \text{et} & 3m^2 \leqslant |D|. \end{array}$$

La condition générale résulte immédiatement de l'élimination de m entre les conditions de réduction.

Si D est *positif*, les valeurs de c qui rendent $F(c)$ *positif* ne vérifient pas cette condition, car:

$$4F(c) = (2c—S)^2—D \quad \Rightarrow \quad (2c—S)^2 > 4F(c) > F(c).$$

Pour les valeurs de c qui rendent $F(c)$ *négatif*, l'expression du polynôme entraîne l'équivalence:

$$4(2c—S)^2 \leqslant 4|F(c)| = D—(2c—S)^2 \Leftrightarrow 5(2c—S)^2 \leqslant D.$$

En outre:

$$4m^2 \leqslant D—(2c—S)^2 \leqslant D \Rightarrow 4m^2 \leqslant D.$$

Si D est négatif, l'expression du polynôme, dont la valeur est toujours positive, entraîne l'équivalence:

$$4(2c—S)^2 \leqslant 4F(c) = (2c—S)^2+|D| \Leftrightarrow 3(2c—S)^2 \leqslant |D|;$$

en outre:

$$4m^2 \leqslant (2c—S)^2+|D| \leqslant m^2+|D| \Rightarrow 3m^2 \leqslant |D|.$$

Ceci acquis, pour obtenir les idéaux réduits, en utilisant le tableau des valeurs de $F(c)$, pour c entier croissant à partir de 0, on peut:

I. *Déterminer la limite* r des entiers, à partir de laquelle la condition de limitation n'est plus vérifiée, c'est-à-dire telle que

$$(2c—S)^2 > |F(c)| \Leftrightarrow c \geqslant r;$$

ce qui est équivalent, suivant le signe de D, à:

$$D > 0: \quad 5(2c—S)^2 > D \Leftrightarrow c \geqslant r;$$
$$D < 0: \quad 3(2c—S)^2 > |D| \Leftrightarrow c \geqslant r.$$

II. Pour les valeurs entières de c, limitées par:

$$0 \leqslant c < r;$$

chercher les diviseurs m (entiers positifs) des valeurs $F(\overline{c})$, tels que

$$(2\overline{c}—S) \leqslant m \leqslant |F(\overline{c})|: m.$$

III. A *chaque couple d'entiers* $\overline{c}$ *et* m, ainsi obtenus, *correspond*

1° si m est diviseur du discriminant D, un *idéal double réduit*:

$$(m, \ \theta—\overline{c}), \quad 2\overline{c}—S = 0 \quad \text{ou} \quad m.$$

2° si m n'est pas diviseur de D, *deux idéaux réduits conjugués*, différents:

$$(m, \ \theta—\overline{c}), \quad (m, \ \theta—\overline{c'}); \quad \overline{c'} = S—\overline{c}.$$

On peut remplacer la racine minimum négative $\overline{c'}$ par la plus petite racine positive $\overline{c'}+m = m+S-\overline{c}$.

Exemple 1 (tableau I). — Dans le corps de discriminant $D = -39$, la valeur de r, déterminée par comparaison avec $|D|$ est 2:

$$3.(2\times 1+1)^2 = 27 < 39 < 3.(2\times 2+1)^2 = 75.$$

Il suffit de chercher les diviseurs de $F(0) = 10$ et de $F(1) = 12$, qui vérifient les conditions de réduction (compris entre $2c+1$ et la racine carrée de $|F(c)|$). On obtient deux idéaux doubles, de normes 1 et 3 (diviseurs de 39):

$$(1,\ \theta-0),\qquad (3,\ \theta-1)$$

et deux idéaux conjugués distincts, de norme 2:

$$(2,\ \theta-0)\qquad (2,\ \theta+1) = (2,\ \theta-1).$$

Il y a quatre idéaux réduits différents, donc au plus quatre classes, on vérifie ci-dessous que c'est effectivement le nombre de classes.

Exemple 2 (tableau II) — Dans le corps de discriminant $D = +60$ la valeur de r est 2:

$$5\times(2\times 1)^2 = 20 < 60 < 5\times(2\times 2)^2 = 80.$$

Il suffit de chercher les diviseurs de $|F(0)| = 15$ et de $|F(1)| = 14$, qui vérifient les conditions de réduction. On obtient ainsi trois idéaux doubles, de normes 1, 3, 2 (diviseurs de 60):

$$(1,\ \theta-0),\qquad (3,\ \theta-0),\qquad (2,\ \theta-1).$$

Il y a au plus trois classes; on vérifie ci-dessous qu'il n'y en a que deux, la classe principale contenant l'idéal de norme 1, d'ailleurs égal à (1) et une classe double contenant les deux idéaux de normes 3 et 2 (dont on peut vérifier qu'ils sont congrus).

26. Propriétés générales des groupes de classes d'idéaux.

Certaines relations entre les classes d'idéaux, d'un corps quadratique, sont des applications de propriétés générales des groupes abéliens d'ordre fini qu'on va indiquer sommairement [1]).

---

[1]) Ces propriétés sont exposées et démontrées dans de nombreux ouvrages. Je me permets de citer: *Arithmétique et Algèbre modernes*, ch. II, § 5 et 7; ch. III, n° 35 (1954 et 1955), ou, pour plus de développements: *Les groupes abéliens finis* (1925).

Deux puissances, d'exposants entiers quelconques, *d'une même classe* (**23**) —ou plus généralement d'un élément A, appartenant à un groupe $\mathfrak{A}$, d'ordre fini, (même non commutatif)— *sont égales*, si et seulement si *les exposants sont congrus*, suivant un certain module n:

$$A^x = A^{x'} \Leftrightarrow \{x \equiv x', \quad (\text{mod. } n)\}$$

On peut exprimer cette condition caractéristique d'égalité en disant que:

la (valeur de la) *puissance* A^x *est caractérisée* —ou représentée proprement— *par l'exposant* x, *entier défini* mod. n —ou par la progression arithmétique $x+\lambda n$, de raison n; ou par la classe d'entiers mod. n (**5**)— .

L'entier (positif) n est appelé l'**ordre** de l'élément A, —ou de la classe— dans le groupe $\mathfrak{A}$ ou $\mathcal{G}|\mathcal{R}$. Si A est l'*élément unité* du groupe, désigné par E, ou (1) —ou $\mathcal{R}$ dans $\mathcal{G}|\mathcal{R}$— son ordre est égal à 1, il est égal à toutes ses puissances, dont les expressions forment la progression arithmétique, de raison 1.

Cette propriété est bien connue et sa vérification est immédiate. Les puissances A^x, x entier quelconque, ne constituent qu'un nombre fini d'éléments différents, au plus égal à l'ordre —ou au nombre d'éléments— du groupe $\mathfrak{A}$. Il y a donc des puissances, d'exposants différents égales entre elles; en choisissant l'une d'elles A^h, on peut construire le plus petit entier positif n, tel que:

$A^{h+n} = A^h$; donc $A^n = A^{-n} = E$, ou (1), élément unité.

La conséquence est obtenue en multipliant les deux membres de l'égalité par l'inverse $(A^h)^{-1} = A^{-h}$. On en déduit, λ étant un entier quelconque:

$$A^{n\lambda} = E^\lambda = E \quad \text{et} \quad x' = x+n\lambda \Rightarrow A^{x'} = A^x \times A^{n\lambda} = A^x;$$

c'est la condition *suffisante* d'égalité.

D'autre part, pour tout entier positif r, la puissance A^{h+r} ne peut être égale à A^h et A^r ne peut être égal à E. On en déduit l'implication réciproque de la précédente:

$$A^{x'} = A^x \Rightarrow A^{(x'-x)} = E \Rightarrow \{x'-x = \lambda n; \quad \lambda \text{ entier}\}.$$

Il suffit de former le reste de la division (arithmétique) de $x'—x$ par n:

$$x'—x = \lambda n+r; \quad 0 \leqslant r < n; \quad \lambda \text{ entier};$$

la puissance d'exposant $x'—x$ est égale à celle d'exposant r, elle ne peut être égale à E, que si r est nul.

L'entier n, dont l'existence est ainsi établie, est indépendant de la puissance A^h, choisie pour le construire. Comme il y a n progressions arithmétiques, de raison n, définies notamment par les entiers de 0 à $n—1$, il y a n éléments différents, égaux aux puissances de A. On justifie ainsi la définition suivante.

DÉFINITION. — *On appelle* **groupe cyclique**, de *générateur* A, et d'*ordre* n, *le système de* n *valeurs des puissances* A^x (x entier défini mod. n), d'un élément A, d'ordre n, dans le groupe $\mathfrak{A}$ —ou $\mathcal{G}|\mathcal{R}$—. Ces valeurs se composent par multiplication dans $\mathfrak{A}$; leur groupe qui sera désigné par **A**, est un *sous-groupe* de $\mathfrak{A}$.

Un groupe cyclique, multiplicatif —ou noté comme tel— d'ordre n, est *isomorphe* au *groupe additif* de ses exposants, définis mod. n.

Il est manifeste que les n valeurs des puissances de A forment un groupe (multiplicatif) puisque leur multiplication, définie dans $\mathfrak{A}$, et réalisée par l'addition des exposants, est associative et que deux puissances d'*exposants opposés* sont *inverses* —ou de produit égal à l'élément unité E— :

$A^x \times A^y = A^{x+y}$, $A^{-x} \times A^x = E$; $x,y,x+y,(—x)$, définis mod. n.

La représentation d'un élément A^x par son exposant x, mod. n, est *propre* —ou est une correspondance biunivoque— elle fait correspondre l'opération de multiplication (alors nécessairement commutative) avec l'addition; ce sont ces deux qualités qu'exprime le terme d'*isomorphisme*.

On peut représenter le groupe additif des entiers, mod. n, par les *rotations*, autour d'un axe —ou autour d'un point dans un plan— d'angles multiples de $(2\pi : n)$. Au produit —ou composition— commutatif de deux rotations correspond la somme des arcs —ou de leurs mesures, au module 2π près—. Cette représentation explique le qualificatif *cyclique*.

On peut aussi bien construire le groupe cyclique **A**, de générateur A et d'ordre n, en formant *les puissances d'un de ses éléments* A^a, construit toutefois avec un exposant a, *premier avec* n:

$$(A^a)^y = A^{a\times y}; \quad y \text{ défini mod. } n;$$

on peut notamment prendre pour valeurs de y, les n entiers de 0 à n—1.

On constate en effet que les nouveaux exposants y vérifient la même condition caractéristique d'égalité des puissances:

$$\{(ay'—ay) = a(y'—y) \equiv 0, \pmod{n}\} \Leftrightarrow \{y' \equiv y, \pmod{n}\}.$$

L'équivalence résulte du fait que n, premier avec a, ne peut diviser le produit $a(y'—y)$ qu'en divisant le second facteur.

Une telle puissance A^a est encore un *générateur* du groupe cyclique **A**. Un groupe cyclique, d'ordre n, a ainsi $\varphi(n)$ générateurs.

On rappelle que la fonction $\varphi(n)$, de l'entier (positif) n, appelée l'*indicateur* d'EULER, est le nombre d'entiers, positifs, inférieurs à n —ou d'entiers, définis mod. n— premiers avec n.

Sa valeur, pour n égal à une puissance p^h, d'un nombre premier, est

$$\varphi(p^h) = (p—1)\times p^{h-1}; \quad \varphi(2^h) = 2^{h-1}.$$

Pour un produit de puissances de nombres premiers différents —et, plus généralement, pour un produit de nombres m_i premiers entre eux, deux à deux— sa valeur est égale au produit des valeurs pour chacun des facteurs:

$$\varphi(\Pi m_i) = \Pi(\varphi(m_i)); \quad m_i = p_i^{hi}.$$

Il est équivalent de dire qu'*une puissance* A^h, d'un élément A, d'ordre n, *est aussi un élément d'ordre* n, lorsque h *est premier avec* n. Dans le cas général, il est aisé de constater que l'ordre de cette puissance est égal au quotient de n par le p.g.c.d. de h et n.

Lorsque, dans un groupe $\mathfrak{A}$, d'ordre fini —notamment dans $\mathcal{G}|\mathcal{R}$— *il existe un élément A dont l'ordre est égal à celui du groupe* —ou au nombre de ses éléments— le groupe, qui est alors

évidemment formé des seules puissances de A, est, lui-même, *un groupe cyclique, de générateur A* —ou est égal à **A**— .

Un raisonnement, usuel et simple, montre que, dans un groupe, même non commutatif, d'ordre fini, l'ordre de tout sous-groupe, et, notamment, *l'ordre de tout élément est diviseur de* (et éventuellement égal à) *l'ordre du groupe.*

Un sous-groupe définit une *répartition* des éléments du groupe en classes, dont chacune est formée des produits des éléments du sous-groupe par un élément du groupe n'appartenant pas à une autre classe —et défini lui-même au produit près par un élément du sous-groupe—. L'ordre du groupe est, par suite, égal au produit de l'ordre du sous-groupe par le nombre de classes, ainsi constituées.

En rapprochant ces deux propriétés, on constate que: *un groupe, dont l'ordre g est un nombre premier, est cyclique*, puisque l'ordre de tout élément, à l'exception de E, ou (1), étant diviseur de g, ne peut que lui être égal, en sorte que cet élément est un générateur du groupe, qui en a $\varphi(g) = g-1$.

DÉFINITION. — *Dans un groupe abélien* —ou commutatif— $\mathfrak{A}$, d'ordre fini —notamment dans $\mathfrak{G}|\mathfrak{R}$—, *deux éléments*, différents de l'unité E:

$$A, \text{ d'ordre } u; \qquad B, \text{ d'ordre } v;$$

—ou *les sous-groupes cycliques* **A** et **B**, qu'ils engendrent— *sont* qualifiés **indépendants**, lorsque *ces sous-groupes n'ont, en commun, que le seul élément unité E*:

$$A^x = B^y \iff \{x \equiv 0, \pmod{u} \text{ et } y \equiv 0, \pmod{v}\};$$

dans le vocabulaire de l'algèbre des ensembles: l'intersection [**A**,**B**] des deux sous-groupes est égal au sous-groupe trivial, formé du seul élément unité E.

Il est équivalent de dire que le monôme $A^x \times B^y$ n'est égal à l'élément unité E que si x et y sont respectivement congrus à 0, suivant les modules u et v.

Deux éléments sont notamment indépendants, lorsque leurs

ordres u et v sont *premiers entre eux*. Car, dans ce cas:

$$A^x = B^y \Rightarrow A^{xv} = B^{yv} = E$$
$$\Rightarrow xv \equiv 0, \pmod{u} \Rightarrow x \equiv 0;$$
$$\Rightarrow B^y = E \Rightarrow y \equiv 0, \pmod{v}.$$

DÉFINITION. — On appelle **produit direct** *de deux sous-groupes cycliques indépendants*, **A** de générateur A, d'ordre u et **B** de générateur B, d'ordre v, *le sous-groupe constitué par le système de monômes*;

$$A^x \times B^y; \quad x, \text{ mod. } u, \quad y, \text{ mod. v};$$

—ou par les produits, en nombre $u \times v$, de chaque élément de **A** par chaque élément de **B** (dans un ordre quelconque, puisque $\mathfrak{A}$ est *abélien*)— .

Ce produit direct est désigné par $\mathbf{A} \times \mathbf{B}$ et le *couple* de générateurs A,B en est appelé une *base*.

Les monômes ainsi constitués sont bien inégaux, car, en raison de la *commutativité de la multiplication*, dans le groupe $\mathfrak{A}$ et de l'*indépendance des générateurs*:

$$A^x \times B^y = A^{x'} \times B^{y'}$$
$$\Rightarrow A^{x'-x} \times B^{y'-y} = E \quad \text{ou} \quad (1)$$
$$\Rightarrow \{x'-x \equiv 0, \pmod{u} \text{ et } y'-y \equiv 0, \pmod{v}\}.$$

Ils constituent un groupe, car le produit (ou le quotient) de deux monômes est encore un monôme, obtenu par les sommes (ou les différences) des exposants respectifs:

$$(A^x \times B^y) \times (A^{x'} \times B^{y'}) = A^{x+x'} \times B^{y+y'};$$
$$(A^x \times B^y) \times (A^{-x} \times B^{-y}) = E.$$

Les monômes sont représentés proprement par les couples d'exposants $\|x\ y\|$. On dit encore que le produit direct $\mathbf{A} \times \mathbf{B}$, des groupes cycliques multiplicatifs est isomorphe au *produit direct des groupes additifs*, des entiers, mod. u et mod. v.

Le sous-groupe cyclique **A**, de générateur A, peut être considéré comme égal à son produit direct par le sous-groupe trivial (E), formé du seul élément unité E.

On peut étendre par *récurrence* les notions d'*indépendance* et de *produit direct* à un nombre quelconque s, d'éléments d'un groupe abélien et aux sous-groupes cycliques qu'ils engendrent.

Des éléments d'un groupe abélien, en nombre s:

$$A_i, \quad \text{d'ordre } u_i, \qquad (i \text{ de } 1 \text{ à } s);$$

—ou les sous-groupes cycliques $\mathbf{A}_i$, qu'ils engendrent— sont qualifiés **indépendants**, lorsque: les s—1 premiers le sont et que *leur produit direct* $\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}$ *et le groupe cyclique* $\mathbf{A}_s$, engendré par le dernier élément A_s, *n'ont en commun que le seul élément unité* E; [l'intersection $[\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}, \ \mathbf{A}_s]$ est égal à (E)].

On appelle **produit direct** de s sous-groupes cycliques indépendants, $\mathbf{A}_i$ engendré par l'élément A_i, le système des produits de tout élément du produit direct $\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}$ par tout élément de $\mathbf{A}_s$.

L'indépendance et le produit direct ayant été définis pour $s = 2$, sont ainsi définis, ou construits, de proche en proche pour $s = 3$, puis 4, ... puis s. On en déduit des propriétés caractéristiques, indépendantes de l'ordre adopté pour les éléments.

Les éléments A_i —ou les sous-groupes $\mathbf{A}_i$— sont *indépendants* si un monôme formé avec les A_i n'est égal à l'élément unité E, que pour des exposants respectivement congrus à 0, relativement à l'ordre de l'élément qu'ils affectent:

$$A_1^{x_1} \times \ldots A_s^{x_s} = E \quad \Leftrightarrow \quad \{x_i \equiv 0, \pmod{u_i}; \quad \text{tout } i\}$$

Le *produit direct* des sous-groupes cycliques $\mathbf{A}_i$, est le système des monômes, en nombre $u_1 \times \ldots \times u_s$;

$$A_1^{x_1} \times \ldots \times A_s^{x_s}; \quad x_i \text{ défini mod. } u_i.$$

Ces monômes sont inégaux; ils constituent un sous-groupe de $\mathfrak{A}$, leur multiplication, définie dans $\mathfrak{A}$, est réalisée par l'addition des exposants respectifs. Ils sont représentés proprement par les systèmes —ou le s-uple— de leurs exposants. On dit encore que leur groupe est

isomorphe au *produit direct des s groupes additifs*, des entiers définis respectivement suivant les modules u_i.

On généralise aisément les propriétés indiquées pour $s = 2$ et $s = 1$.

1. *Des éléments* A_i, d'ordre u_i, *sont*, notamment, *indépendants lorsque leurs ordres* u_i *sont premiers entre eux, deux à deux*, chacun d'eux étant, par suite, premier avec le produit des autres.

2. *L'ordre d'un produit direct*, de s sous-groupes cycliques indépendants (dans un groupe abélien $\mathfrak{A}$) est égal au produit Πu_i, des ordres u_i, des sous-groupes composants.

3. Si, dans un groupe abélien $\mathfrak{A}$, d'ordre fini g, il existe s éléments indépendants A_i, dont le produit des ordres Πu_i est égal à l'ordre g, de $\mathfrak{A}$, ce groupe, qui est évidemment formé des seuls monômes des A_i, est égal au produit direct des groupes cycliques $\mathbf{A}_i$, qu'ils engendrent:

$$u_1 \times \ldots \times u_s = g \quad \Rightarrow \quad \mathfrak{A} = \mathbf{A}_1 \times \ldots \times \mathbf{A}_s.$$

En particulier *un groupe cyclique* $\mathbf{A}$, de générateur A, dont l'ordre g est décomposable en un produit d'entiers g_i (i de 1 à s), premiers entre eux, deux à deux, —notamment puissances de nombres premiers différents— *est égal au produit direct des sous-groupes cycliques*, engendrés par les s générateurs:

$$A_i^{g:g_i}, \quad \text{d'ordre } g_i.$$

Exemple. — Dans un groupe cyclique, d'ordre $15 = 3 \times 5$:

$$A^z, \quad [z, \text{ mod. } 15] = (A^3)^x \times (A^5)^y; \quad [x, \text{ mod. } 5; \ y, \text{ mod. } 3].$$

La relation entre les entiers z et x,y est exprimée par les congruences:

$$z \equiv 3x+5y, \quad (\text{mod. } 15)$$

$$\Rightarrow \quad \{z \equiv 3x, \quad (\text{mod. } 5) \quad \text{et} \quad z \equiv 5y, \quad (\text{mod. } 3)\}$$

$$\Rightarrow \quad \{x \equiv 2z, \quad (\text{mod. } 5) \quad \text{et} \quad y \equiv 2z, \quad (\text{mod. } 3)\}.$$

Réciproquement, *un produit direct de groupes cycliques, d'ordres premiers entre eux, deux à deux,* —notamment de puissances de nombres premiers différents— *est égal à un groupe cyclique*, dont un générateur est égal au produit des générateurs des groupes composants.

THÉORÈME de decomposition des groupes abéliens d'ordre fini. *Tout groupe abélien* $\mathfrak{A}$, d'ordre fini, *est égal à un produit direct de groupes cycliques*, dont les générateurs sont des éléments indépendants, convenablement choisis dans $\mathfrak{A}$, différents de **E**.

Pour cette construction qui peut, en général être réalisée de diverses façons, on peut toujours disposer des sous-groupes composants $\mathbf{A}_i$ et de leur numérotage, de façon que *l'ordre* g_i, de chacun d'eux, *soit diviseur de* —ou égal à— *l'ordre* g^{i+1} *du suivant* [1]).

Ceci peut encore être réalisé, en général, par divers choix possibles des sous-groupes cycliques; toutefois *leur nombre* r, *est déterminé, ainsi que leurs ordres* g_i. Toute décomposition du groupe en produit cyclique comporte alors au moins r groupes composants et *la décomposition*, ainsi formée, *est*, en quelque sorte, *minimum.*

D'une façon opposée, on peut construire une *décomposition maximum*, en un produit direct de groupes cycliques, *dont les ordres sont des puissances de nombres premiers*, en remplaçant dans la décomposition minimum éventuellement chaque sous-groupe cyclique par un produit de cette forme. Les ordres ainsi obtenus sont encore déterminés.

EXEMPLE. — Un groupe abélien, d'ordre 12, produit direct de groupes cycliques d'ordre 2 et 6 a pour éléments 12 monômes:

$$A^x \times B^y; \quad x, \text{ mod. } 2; \quad y, \text{ mod. } 6.$$

Aucun n'est d'ordre 12 (leurs ordres étant 6, ou 3, ou 2 —ou 1 pour

---

[1]) La démonstration de ce théorème et des précisions qui en sont données est plus complexe que celles des propriétés précédentes. On peut la rattacher à une analyse linéaire diophantienne, ou à des propriétés générales de décomposition d'un module —ou groupe additif— en somme —ou produit— directe. Je renvoie aux ouvrages cités ci-dessus.

l'élément unité—, le groupe n'est donc pas cyclique et sa décomposition est *minimum*. Elle peut être réalisée en remplaçant A par un des trois éléments d'ordre 2, et B par un des quatre éléments d'ordre 6, dont les puissances ne contiennent pas A; ceci donne 12 décompositions possibles:

A et B;	A et B^5;	A et $A\times B$;	A et $A\times B^5$
B^3 et $A\times B$;	B^3 et $A\times B^5$;	B^3 et $A\times B^2$;	B^3 et $A\times B^4$
$B^3\times A$ et $B^2\times A$;	$B^3\times A$ et $B^4\times A$;	$B^3\times A$ et A;	$B^3\times A$ et A^5

On peut encore construire une décomposition *maximum*, en groupes cycliques d'ordres 2, 2, 3, par exemple:

$$A^x\times(B^3)^{y'}\times(B^2)^{y''};\quad x,y',\ \text{mod. } 2,\quad y''\ \text{mod. } 3.$$