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.
DOI: https://doi.org/10.5169/seals-36342

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

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

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

Download PDF: 10.12.2025

ETH-Bibliothek Zürich, E-Periodica, https://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* $\bar{c}'$ négative et $\bar{c}$ symétrique, qui ont été caractérisées (**7. 4**) par les limitations:

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

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

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

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 $\bar{c}'$ est négative, par sa *plus petite racine positive*, qui est $\bar{c}'+m$; les limitations des racines ainsi distinguées sont alors, pour un couple d'idéaux conjugués:

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

Si les idéaux sont égaux (idéal double), $\bar{c}$ 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:

$$-(m+1):2 \qquad (m-1):2;$$

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:

$$(1,\ \theta-0), \qquad (3,\ \theta-1), \qquad (13,\ \theta-6).$$

TABLEAU I.

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

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:

$$-1 \text{ et } 0, \quad -2 \text{ et } +1, \quad -3 \text{ et } +2;$$

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 $\bar{c}$ et de norme m:

$\bar{c}$:	—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 ;	$+65$;	...
$D =$	-3;	$+5$;	$(-3)\times(-7)$;	$(-3)\times(+5)$;	$(+5)\times(+13)$;	...

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 ;	...
$D =$	-4;	$(-4)\times(-3)$;	$(-4)\times(+5)$;	$(-4)\times(-3)\times(-7)$;	...

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 ;	$+10$;	...
$D =$	$+8$;	-8;	$(-8)\times(-3)$;	$(+8)\times(-3)$;	$(+8)\times(+5)$;	...

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: $\left(\frac{\delta}{p}\right) = \left(\frac{p}{|\delta|}\right)$;

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

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

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

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. $|\delta_i|$:

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

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

$$\varphi(|D|) = \Pi\varphi(|\delta_i|) \quad \text{valeurs incongrues}, \quad \text{mod. } |D| = \Pi|\delta_i|.$$

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 $\mathcal{G}|\mathfrak{Q}$, des classes du groupe $\mathcal{G}(\theta)$, relativement au sous-groupe $\mathfrak{Q}$, 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 $\mathcal{Q}$) [**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 $\mathcal{Q}$ 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 $\mathcal{Q}$ des idéaux principaux rationnels. Dans chaque classe de $\mathcal{G}$ et de $\mathcal{R}$, mod. $\mathcal{Q}$, 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 $(\mathcal{G}|\mathcal{Q})|(\mathcal{R}|\mathcal{Q})$.

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 **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:

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

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

$$n\times[(\theta-c):n] = (\theta-c),\quad [(\theta-c_1)\times(\theta-c)]:n$$

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:

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

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

$$4\times[(\theta-1):4] = \theta-1,\quad [(\theta-1)\times(\theta-2)]:4 = -\theta-2.$$

On vérifie bien que ce couple d'éléments est bien arithmétiquement équivalent à la base canonique de **M**:

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

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* $(m, \theta-\bar{c})$, *dont le carré de la norme est au plus égal à la valeur absolue du polynôme fondamental*, $|F(\bar{c})|$ pour la *racine minimum* $\bar{c}$ (de cet idéal):

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

Deux idéaux (canoniques) *conjugués* (**7**), *distincts*, dont les racines minimum sont $\bar{c}$ et $S-\bar{c}$ (**21**), *sont simultanément réduits*, puisque $F(\bar{c})$ et $F(S-\bar{c})$ 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:

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

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

L'*idéal unité* $(1, \theta-0)$ *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 $\mathbf{M}$ est congru à l'idéal $\mathbf{N}'$ conjugué de $\mathbf{N}$ (**22**), dont la norme n est bien inférieure à m.

Si la racine c est minimum pour $\mathbf{N}$, 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:

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

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:

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

En outre:

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

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

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

en outre:

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

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

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

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

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

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*:

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

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

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

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:

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

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 $\mathfrak{G}|\mathfrak{R}$. Si A est l'*élément unité* du groupe, désigné par E, ou (1) —ou $\mathfrak{R}$ dans $\mathfrak{G}|\mathfrak{R}$— 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:

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

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:

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

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:

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

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 $\mathfrak{G}|\mathfrak{R}$—. 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— :

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

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:

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

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:

$$\{(ay'-ay) = a(y'-y) \equiv 0, \quad (\text{mod. } n)\} \Leftrightarrow \{y' \equiv y, \quad (\text{mod. } n)\}.$$

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

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

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:

$$\varphi(\Pi m_i) = \Pi(\varphi(m_i)); \qquad m_i = p_i^{h_i}.$$

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 $\mathfrak{G}|\mathfrak{R}$— *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— $\mathcal{A}$, d'ordre fini —notamment dans $\mathcal{G}|\mathcal{R}$—, *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:

$$A^x = B^y \quad \Leftrightarrow \quad \{x \equiv 0, \quad (\text{mod. } u) \quad \text{et} \quad y \equiv 0, \quad (\text{mod. } v)\};$$

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:

$$A^x = B^y \quad \Rightarrow \quad A^{xv} = B^{yv} = E$$

$$\Rightarrow \quad xv \equiv 0, \quad (\text{mod. } u) \quad \Rightarrow \quad x \equiv 0;$$
$$\Rightarrow \quad B^y = E \quad \Rightarrow \quad y \equiv 0, \quad (\text{mod. } v).$$

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*;

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

—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*:

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

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:

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

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:

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

CHAPITRE IV

CRIBLES

27. Calcul des diviseurs premiers.

Les propriétés des idéaux canoniques, dans un corps quadratique, et des idéaux réduits, peuvent être interprétées sous la forme de propriétés des *nombres premiers* (rationnels), analogues à celles du « crible d'Eratosthène ». On reprend, en se plaçant à ce point de vue, les constructions et définitions déjà indiquées, en sorte que le chapitre actuel peut être considéré comme indépendant des autres.

On forme, pour les valeurs entières de x, croissantes à partir de 0, *la suite des valeurs d'un trinôme du second degré:*

$$F(x) = x^2+Sx+N; \begin{cases} S = -1; & N \text{ quelconque}; \\ S = 0; & N \not\equiv +1; \quad (\text{mod. } 4); \end{cases}$$

sous la réserve que *le discriminant* $D = S^2-4N$, *n'ait pas de facteur carré*, à l'exclusion de 4 (si $S = 0$); et ne soit pas égal à $+4$.

On se propose de chercher *les facteurs premiers qui sont des diviseurs des valeurs de cette suite.*

A cet effet, on détermine un *rang* r, tel que pour tout x, au moins égal à r:

$$|F(x)| < (2x-S)^2.$$

Cette condition est d'ailleurs équivalente, suivant le cas **(25)** à:

$$D>0; \quad 5(2x-S)^2>D \Leftrightarrow x\geqslant r;$$
$$D<0; \quad 3(2x-S)^2>|D| \Leftrightarrow x\geqslant r$$

(dans le cas de D positif, $F(x)$ est négatif, notamment pour toutes les valeurs de x strictement inférieures à r).

On appelle **racine minimum** $\bar{c}_p$, d'un nombre (entier rationnel) premier p, *la plus petite valeur entière de* x (nulle ou positive) s'il en existe, *telle que* $|F(x)|$ *soit divisible par* p.

Les valeurs de x pour lesquelles $|F(x)|$ est divisible par p (zéros de la congruence fondamentale; (**5**), sont alors les termes de deux progressions arithmétiques, de raison p:

$$\bar{c}_p+\lambda p; \quad S-\bar{c}_p+(\lambda+1)p; \qquad (\lambda \text{ entier } \geqslant 0).$$

Ces deux progressions sont confondues si $2\bar{c}_p-S = p$; alors p est diviseur du discriminant.

Ces propriétés résultent de la construction des idéaux (**7** et **21**) les valeurs de x sont les racines des deux idéaux canoniques conjugués, de norme p, donc premiers et de produit égal à l'idéal principal (p). On peut aussi les établir directement comme conséquences de l'étude de la *congruence fondamentale* (**5**) pour un module premier.

On peut alors prendre comme base de l'algorithme du crible, la propriété fondamentale suivante.

Pour chaque valeur de x, au moins égale au rang r, *si un nombre premier p est diviseur de* $F(x)$ *et si son carré est au plus égal à* $|F(x)|$, *sa racine minimum* $\bar{c}_p$ *est* (strictement) *inférieure à* x —ou il est diviseur d'une valeur antérieure du tableau— .

$$x \geqslant \mathrm{r}; \ p \text{ diviseur de } |F(x)|; \ p^2 \leqslant |F(x)|:$$
$$\Rightarrow \text{ Existe } \bar{c}_p < x \quad \text{et} \quad p \text{ diviseur de } |F(\bar{c}_p)|.$$

On peut vérifier directement cette propriété en conjuguant la définition de r et la limitation de p^2:

$$x \geqslant r \quad \Rightarrow \quad p^2 \leqslant |F(x)| < (2x-S)^2$$
$$\Rightarrow \quad (2\bar{c}_p-S)^2 \leqslant p^2 < (2x-S)^2 \quad \Rightarrow \quad \bar{c}_p < x.$$

On peut aussi bien considérer l'idéal canonique de norme p, de racines $x+\lambda p$ et sa racine minimum (non négative) $\bar{c}_p$. S'il est réduit, $\bar{c}_p$ est inférieur à r, donc à x. S'il n'est pas réduit $|F(\bar{c}_p)|$ est inférieur à p^2, de sorte que x ne peut être égal à $\bar{c}_p$, donc lui est supérieur.

On choisit un nombre h, au moins égal à $r-1$ ($r-1 \leqslant h < H$), on considère les h premières valeurs de la suite et on décompose chacune d'elles en un produit de facteurs premiers p.

On détermine, pour chacune des valeurs successives de x ($h < x \leqslant H$), les puissances des nombres premiers p, précédemment obtenus, qui divisent exactement $|F(x)|$; on forme, pour chaque x, le quotient q_x de $|F(x)|$ par le produit de ces puissances.

1. *Le premier quotient* q_c, ainsi obtenu ($c > h$), *qui soit différent de* 1 *est un nombre premier.*

2. *Les quotients suivants*, pour les valeurs de x, ($h < x < h_1$), vérifiant la condition (c déterminé comme il vient d'être dit):

$$|F(x)| < (2c-S)^2;$$

sont égaux à 1, *ou sont des nombres premiers.*

1. Quel que soit le diviseur premier p, du quotient q_c, il n'est pas diviseur d'une valeur antérieure $|F(x)|$, sa racine minimum est c et p^2 est supérieur à $|F(c)|$ (c étant au moins égal à r). Donc:

$$p^2 > |F(c)| \geqslant q_c.$$

Or il y a au plus un diviseur de q_c, dont le carré lui est supérieur; de sorte que si q_x est différent de 1, il est égal à son seul facteur premier p.

2. Si un quotient q_x, pour $x > c$, est différent de 1 et n'est pas premier, il admet au moins un facteur premier p_1 dont le carré lui est au plus égal. Ce facteur ne divise aucune des valeurs antérieures à $F(c)$ et sa racine minimum c_1 est au moins égale à c, de sorte que:

$$(2c-S)^2 \leqslant (2c_1-S)^2 \leqslant p_1^2 \leqslant q_x \leqslant |F(x)|.$$

Ce quotient q_x ne peut donc être obtenu que pour une valeur de x, au delà des limites fixées par l'énoncé.

Ces règles peuvent s'appliquer par récurrence ascendante à des suites de valeurs croissantes $h_0 \geqslant r-1$; $h_1 > h_0$; ...

28. Exemples de calculs.

Le tableau V donne les valeurs pour x de 0 à $H = 100$, du trinôme $F(x)$ déjà utilisé (tableaux I et III), de discriminant $D = -39$. Le *rang* r (**25**) est égal à 2.

Les *deux premières valeurs* de $F(x)$, ont pour diviseurs premiers **2**, **3**, **5**, qui sont des diviseurs de $F(x)$, pour les valeurs respectives:

$$0+2\lambda,\ 1+2\lambda;\qquad 0+5\lambda,\ 4+5\lambda;\qquad 1+3\lambda.$$

Il n'y a qu'une progression pour 3, qui est diviseur de D.

On a inscrit devant chaque valeur de la table, le monôme des puissances des facteurs 2, 3, 5, qui en est diviseur, de façon à calculer les quotients q_x. Les périodicités, ou les progressions sont mises en évidence par l'alignement (vertical) de ces facteurs.

Le *premier quotient*, rencontré ensuite, qui soit différent de 1 est $F(3):2 = \mathbf{11}$. Il est premier, on l'a inscrit devant les valeurs dont il est diviseur et qui sont données par les progressions de raison 11 et de premiers termes 3 et 7. Deux seulement $F(51)$ et $F(69)$ sont divisibles par une puissance supérieure de 11; les autres appartenant à des progressions de raison 11^2 sont extérieures à la table.

Le premier quotient obtenu ensuite, qui soit différent de 1 est $F(6):2^2 = \mathbf{13}$. C'est un nombre premier, diviseur de D; il n'est obtenu que pour les valeurs d'une seule progression $6+13\lambda$, et seulement à la première puissance.

Les quotients suivants, jusqu'à $F(13)$ exclus, qui devient supérieur à $(2\times6+1)^2 = 169$, sont égaux à 1, ou sont premiers:

$F(7): (2\times3\times11) = 1$; $\quad F(8): 2 = \mathbf{41}$; $\quad F(9): (2^2\times5^2) = 1$;
$F(10): (2^3\times3\times5) = 1$; $\quad F(11): 2 = \mathbf{71}$; $\quad F(12):2 = \mathbf{83}$.

On inscrit ces nombres premiers devant les valeurs de la table, dont ils sont diviseurs, et qui sont données par:

41 pour $x = 8, 49, 90;\ 32, 73;$ **71** pour $x = 11, 82;\ 59;$
83 pour $x = 12, 95;\ 70;$

ils n'y figurent qu'à la première puissance.

Le premier quotient différent de 1, qui est rencontré ensuite est $F(16): (2\times3) = \mathbf{47}$; il est premier et il en est de même de ceux des

quotients suivants, qui sont différents de 1, jusqu'à $F(33)$ exclus, qui est supérieur à $(2\times 16 + 1)^2 = 1\,089$. Certains sont encore diviseurs d'autres valeurs du tableau, ce sont:

47 pour $x = 16, 63;\ 30, 77;$ **79** pour $x = 17, 96;\ 61;$
43 pour $x = 20, 63;\ 22, 65;$ **59** pour $x = 21, 80;\ 37, 96;$
61 pour $x = 24, 85;\ 36, 97;$ **89** pour $x = 26;\ 62.$

Par contre, les diviseurs premiers **281**, **383**, **137**, ne se rencontrent plus dans le tableau, limité à $H = 100$.

Le premier quotient rencontré ensuite, est $F(33) : 2^2 =$ **283**; il est premier et il en est de même de ceux des quotients suivants qui sont différents de 1 jusqu'à $F(67)$ exclus qui est supérieur à $(2\times 33 + 1)^2 = 4\,489$. Dans ces quotients, ceux qui figurent plus d'une fois dans le tableau, limité à $H = 100$, sont:

127 pour $x = 35;\ 91;$ **103** pour $x = 47;\ 55;$
149 pour $x = 54;\ 94;$ **139** pour $x = 64;\ 74.$

Le premier quotient rencontré ensuite est $F(67) : (2\times 3) =$ **761**; il est premier et il en est de même de tous les quotients suivants de la table, car $(2\times 67 + 1)^2 = 18\,225$ est supérieur à $F(100)$.

Dans la table, les nombres en caractères gras sont les facteurs p rencontrés pour leur racine minimum $\bar{c}_p$ (ou pour la première fois).

On rappelle qu'il a été indiqué ci-dessus que les nombres premiers ainsi obtenus sont ceux qui appartiennent à douze progressions arithmétiques de raison commune 39.

Le *deuxième exemple*, donné dans le tableau VI, est constitué par les valeurs pour x de O à $H = 100$, du trinôme, de discriminant D positif (définissant un corps réel):

$$F(x) = x^2 - 47; \qquad D = (-4)\times(-47) = 188.$$

Les valeurs sont négatives et de valeurs absolues décroissantes jusqu'à $F(6)$; elles sont ensuite positives et croissantes.

Le rang r est égal à 4, car:

$$5\times(2\times 3)^2 = 180 < 4\times 47 < 5\times(2\times 4)^2 = 320.$$

Les quatre premières valeurs de $F(x)$ ont pour diviseurs premiers: **2**, **47**, qui sont diviseurs de D, et **23**, **43**, **19**. On inscrit devant chaque valeur les monômes de ces facteurs qui en sont des diviseurs.

Tableau V.

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

c	$F(c)$	Diviseurs
0	10	**2. 5**
1	12	2^2. **3**
2	16	2^4
3	22	2. **11**
4	30	2. 3. 5
5	40	2^3. 5
6	52	2^2. **13**
7	66	2. 3 *11*
8	82	2. **41**
9	100	2^2. 5^2
10	120	2^3. 3. 5
11	142	2. **71**
12	166	2. **83**
13	192	2^6. 3
14	220	2^2. 5. 11
15	250	2. 5^3
16	282	2. 3 **47**
17	316	2^2. **79**
18	352	2^5. 11
19	390	2. 3. 5. 13
20	430	2. 5. **43**
21	472	2^3. **59**
22	516	2^2. 3. *43*
23	562	2. **281**
24	610	2. 5. **61**

c	$F(c)$	Diviseurs
25	660	2^2. 3. 5. 11
26	712	2^3. **89**
27	766	2. **383**
28	822	2. 3. **137**
29	880	2^4. 5. 11
30	940	2^2. 5. *47*
31	1 002	2. 3. **167**
32	1 066	2. 13. *41*
33	1 132	2^2. **283**
34	1 200	2^4. 3. 5^2.
35	1 270	2. 5. **127**
36	1 342	2. 11. *61*
37	1 416	2^3. 3. *59*
38	1 492	2^2. **373**
39	1 570	2. 5. **157**
40	1 650	2. 3. 5^2. 11
41	1 732	2^2. **433**
42	1 816	2^3. **227**
43	1 902	2. 3. **317**
44	1 990	2. 5. **199**
45	2 080	2^5. 5. 13
46	2 172	2^2. 3. **181**
47	2 266	2. 11. **103**
48	2 362	2. **1 181**
49	2 460	2^2. 3. 5. 41

c	$F(c)$	Diviseurs
50	2 560	2^9. 5.
51	2 662	2. 11^3
52	2 766	2. 3. **461**
53	2 872	2^3. **359**
54	2 980	2^2. 5. **149**
55	3 090	2. 3. 5. *103*
56	3 202	2. **1 601**
57	3 316	2^2. **829**
58	3 432	2^3. 3. 11. 13
59	3 550	2. 5^2. *71*
60	3 670	2. 5. **367**
61	3 792	2^4. 3. *79*
62	3 916	2^2. 11. *89*
63	4 042	2. 43. 47
64	4 170	2. 3. 5. **139**
65	4 300	2^2. 5^2. 43
66	4 432	2^4. **277**
67	4 566	2. 3. **761**
68	4 702	2. **2 351**
69	4 840	2^3. 5. 11^2
70	4 980	2^2. 3. 5. *83*
71	5 122	2. 13. **197**
72	5 266	2. **2 633**
73	5 412	2^2. 3. 11. 41
74	5 560	2^3. 5. *139*

c	$F(c)$	Diviseurs
75	5 710	2. 5. **571**
76	5 862	2. 3. **977**
77	6 016	2^7. 47
78	6 172	2^2. **1 543**
79	6 330	2. 3. 5. **211**
80	6 490	2. 5. 11. 59
81	6 652	2^2. **1 663**
82	6 816	2^5. 3. 71
83	6 982	2. **3 491**
84	7 150	2. 5^2. 11. 13
85	7 320	2^3. 3. 5. 61
86	7 492	2^2. **1 873**
87	7 666	2. **3 833**
88	7 842	2. 3. **1 307**
89	8 020	2^2. 5. **401**
90	8 200	2^3. 5^2. 41
91	8 382	2. 3. 11. *127*
92	8 566	2. **4 283**
93	8 752	2^4. **547**
94	8 940	2^2. 3. 5. *149*
95	9 130	2. 5. 11. 83
96	9 322	2. 59. 79
97	9 516	2^2. 3. 13. 61
98	9 712	2^4. **607**
99	9 910	2. 5. **991**
100	10 110	2. 3. 5. **337**

Les quotients suivants, pour les valeurs de x, définies par:

$$|F(x)| \leqslant (2\times 4)^2 \quad \Rightarrow \quad x \leqslant 10$$

sont uniquement des valeurs, ou des moitiés de valeurs du polynôme puisqu'à l'exception du diviseur 2, la première valeur devant laquelle on a inscrit un des diviseurs précédents est $F(16)$ divisible par 19. Ce sont:

$F(4) = -\mathbf{31}$; $F(5):2 = -\mathbf{11}$; $F(6) = -11$; $F(7):2 = +2$;
$F(8) = +\mathbf{17}$; $F(9):2 = +17$; $F(10) = +\mathbf{53}$.

On les inscrit devant les valeurs suivantes de la table qu'ils divisent, éventuellement avec l'exposant convenable.

Le quotient suivant $F(11):2 = +\mathbf{37}$ est premier; ceux qui suivent pour les valeurs de x:

$$|F(x)| \leqslant (2\times 11)^2 \quad \Rightarrow \quad x \leqslant 23,$$

sont égaux à 1, ou sont premiers. Ces derniers sont encore égaux aux valeurs, ou aux moitiés des valeurs du polynôme; les seuls quotients donnés par des diviseurs déjà inscrits, à l'exception de 2, sont:

$$F(16):(19\times 11) = +1; \qquad F(22):(23\times 19) = +1.$$

Les seuls nombres premiers ainsi obtenus qui figurent encore dans la table, limitée à $H = 100$, sont **37**, **97**, **61**, **89**.

Le premier quotient suivant qui est différent de 1 est $F(28):11 = \mathbf{67}$, ceux qui suivant pour les valeurs de x:

$$|F(x)| \leqslant (2\times 28)^2 \quad \Rightarrow \quad x \leqslant 56,$$

sont égaux à 1 ou premiers; ceux qui figurent plus d'une fois dans la table sont: **67**, **127**, **101**, **107**, **151**.

Au-delà de $x = 56$, tous les quotients sont premiers ou égaux à 1.

La disposition typographique est semblable à celle de l'exemple précédent, les nombres premiers obtenus pour la première fois (pour leur racine minimum) sont en caractères gras.

L'application de la loi de la réciprocité (**22**) montre que les nombres premiers ainsi obtenus sont ceux qui appartiennent à $\varphi(168):2 = 46$ progressions arithmétiques, de raison commune 168 et de premiers termes: 1, 9, 11, 15, 17, 19, 21, 23, 25, 31, 35, 37, 39, 43, 49, 53, 61, 65, 67, 81, 87, 89, 91, 97, 99, 101, 107, 121, 123, 127, 135, 139, 145, 149, 151, 153, 157, 163, 165, 167, 169, 171, 173, 177, 179, 187.

Tableau VI.

$F(x) = x^2 - 47 \qquad D = 188 = (-4) \times (-47) \qquad r = 4.$

c	F(c)	Diviseurs
0	— 47	**47**
1	— 46	**2. 23**
2	— 43	**43**
3	— 38	2. **19**
4	— 31	**31**
5	— 22	2. **11**
6	— 11	*11*
7	+ 2	2.
8	17	**17**
9	34	2. 17
10	53	**53**
11	74	2. **37**
12	97	**97**
13	122	2. **61**
14	149	**149**
15	178	2. **89**
16	209	*19.* 11
17	242	2. 11^2
18	277	**277**
19	314	2. **157**
20	353	**353**
21	394	2. **197**
22	437	*23.* 19
23	482	2. **241**
24	529	23^2

c	F(c)	Diviseurs
25	578	2. 17^2
26	629	17. *37*
27	682	2. *31.* 11
28	737	11. **67**
29	794	2. **397**
30	853	**853**
31	914	2. **457**
32	977	**977**
33	1 042	2. **521**
34	1 109	**1 109**
35	1 178	2. 19. 31
36	1 249	**1 249**
37	1 322	2. **661**
38	1 397	11. **127**
39	1 474	2. 11. *67*
40	1 553	1 **553**
41	1 634	2. *43.* 19
42	1 717	17. **101**
43	1 802	2. 17. *53*
44	1 889	**1 889**
45	1 978	2. 23. 43
46	2 069	**2 069**
47	2 162	2. 47. 23
48	2 257	37. *61*
49	2 354	2. 11. **107**

c	F(c)	Diviseurs
50	2 453	11. **223**
51	2 554	2. **1 277**
52	2 657	**2 657**
53	2 762	2. **1 381**
54	2 869	19. **151**
55	2 978	2. **1 489**
56	3 089	**3 089**
57	3 202	2. **1 601**
58	3 317	31. *107*
59	3 434	2. 17. *101*
60	3 553	19. 11. 17
61	3 674	2. 11. **167**
62	3 797	**3 797**
63	3 922	2. 53. 37
64	4 049	**4 049**
65	4 178	2. **2 089**
66	4 309	31. **139**
67	4 442	2. **2 221**
68	4 577	23. **199**
69	4 714	2. **2 357**
70	4 853	23. **211**
71	4 994	2. 11. **227**
72	5 137	11. **467**
73	5 282	2. 19. *139*
74	5 429	61. *89*

c	F(c)	Diviseurs
75	5 578	2. **2 789**
76	5 729	17. **337**
77	5 882	2. 17. **173**
78	6 037	**6 037**
79	6 194	2. 19. **163**
80	6 353	**6 353**
81	6 514	2. **3 257**
82	6 677	11. **607**
83	6 842	2. 11. **311**
84	7 009	43. *163*
85	7 178	2. 37. *97*
86	7 349	**7 349**
87	7 522	2. **3 761**
88	7 697	43. **179**
89	7 874	2. 31. *127*
90	8 053	**8 053**
91	8 234	2. 23. *179*
92	8 417	19. **443**
93	8 602	2. 23. 11. 17
94	8 789	47. 11. 17.
95	8 978	2. 67^2.
96	9 169	53. *173*
97	9 362	2. 31. *151*
98	9 557	19. **503**
99	9 754	2. **4 877**
100	9 953	37. **269**

29. Successions de nombres premiers.

Dans le deuxième exemple traité, les quinze premières valeurs de $|F(x)|$ sont des nombres premiers ou des doubles de nombres premiers. Cette particularité tient à ce que les valeurs de $|F(x)|$ pour $x < r$, sont des nombres premiers relativement grands, qui ne se retrouvent, par suite, dans la table, qu'à des rangs relativement éloignés. Il existe d'autres exemples de ce même phénomène.

Un exemple (bien connu, au moins depuis Euler) est constitué par les valeurs du trinôme (à discriminant D négatif):

$$F(x) = x^2+x+41; \quad D = -163.$$

Le tableau VII en donne les valeurs pour les valeurs entières de x, de 0 à 299; pour celles qui ne sont pas des nombres premiers, on a seulement inscrit leur décomposition en facteurs premiers.

Les quarantes premières valeurs de $F(x)$ sont des nombres premiers.

Le rang r est égal à 4; les quatre premières valeurs sont les nombres premiers:

$$41, \quad 43, \quad 47, \quad 53.$$

Ils ne se retrouvent comme facteurs qu'au-delà de $x = 39$. On peut montrer par récurrence sur c, compris entre 4 et 39 inclus, que $F(c)$ est un nombre premier, de racine minimum égale à c. Car, il en est ainsi pour $F(4)$, et, par hypothèse de récurrence, pour toute valeur $F(x)$, x étant compris entre 0 inclus et c exclus; en outre la racine conjuguée du nombre premier $F(x)$ est supérieure à 39, puisque

$$F(x)-x-1 = x^2+40 \geqslant 40.$$

Il s'en suit que $F(c)$ ne peut être divisible par aucun des nombres premiers $F(x)$, il est donc premier et de racine minimum c.

A l'exclusion des sept décompositions:

$$\begin{array}{lll} F(40) = 41^2, & F(41) = 41\times 43, & F(44) = 43\times 47, \\ F(49) = 47\times 53, & F(56) = 53\times 61, & F(65) = 61\times 71, \\ F(76) = 71\times 83 & & \end{array}$$

les valeurs de $F(40)$ à $F(80)$, sont des nombres premiers (soient 34 nombres premiers nouveaux).

Tableau VII.

$F(x) = x^2+x+41$; discriminant: —163; $r = 4$.

x	$F(x)$
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151
11	173
12	197
13	223
14	251
15	281
16	313
17	347
18	383
19	421
20	461
21	503
22	547
23	593
24	641
25	691
26	743
27	797
28	853
29	911
30	971
31	1 033
32	1 097
33	1 163
34	1 231
35	1 301
36	1 373
37	1 447
38	1 523
39	1 601
40	41^2
41	41×43

x	$F(x)$
42	1 847
43	1 933
44	43×47
45	2 111
46	2 203
47	2 297
48	2 393
49	47×53
50	2 591
51	2 693
52	2 797
53	2 903
54	3 011
55	3 121
56	53×61
57	3 347
58	3 463
59	3 581
60	3 701
61	3 823
62	3 947
63	4 073
64	4 201
65	61×71
66	4 463
67	4 597
68	4 733
69	4 871
70	5 011
71	5 153
72	5 297
73	5 443
74	5 591
75	5 741
76	71×83
77	6 047
78	6 203
79	6 361
80	6 521
81	$41 \times \mathbf{163}$
82	$41 \times \mathbf{167}$
83	7 013

x	$F(x)$
84	43×167
85	7 351
86	7 523
87	$43 \times \mathbf{179}$
88	7 873
89	83×97
90	8 231
91	47×179
92	8 597
93	8 783
94	8 971
95	9 161
96	$47 \times \mathbf{199}$
97	9 547
98	9 743
99	9 941
100	10 141
101	10 343
102	53×199
103	10 753
104	97×113
105	11 171
106	11 383
107	11 597
108	11 813
109	$53 \times \mathbf{227}$
110	12 251
111	12 473
112	12 697
113	12 923
114	13 151
115	13 381
116	13 613
117	61×227
118	14 083
119	14 321
120	14 561
121	113×131
122	$41 \times \mathbf{367}$
123	$41 \times \mathbf{373}$
124	15 541
125	15 791

x	$F(x)$
126	$61 \times \mathbf{263}$
127	$43 \times \mathbf{379}$
128	16 553
129	16 811
130	$43 \times \mathbf{397}$
131	17 333
132	17 597
133	17 863
134	18 131
135	18 401
136	71×263
137	18 947
138	$47 \times \mathbf{409}$
139	19 501
140	131×151
141	20 063
142	20 347
143	$47 \times \mathbf{439}$
144	20 921
145	21 211
146	21 503
147	$71 \times \mathbf{307}$
148	22 093
149	22 391
150	22 691
151	22 993
152	23 297
153	23 603
154	23 911
155	$53 \times \mathbf{457}$
156	24 533
157	24 847
158	25 163
159	83×307
160	25 801
161	151×173
162	$53 \times \mathbf{499}$
163	$41 \times \mathbf{653}$
164	$41 \times \mathbf{661}$
165	27 431
166	27 763
167	28 097

TABLEAU VII *(suite)*.

x	$F(x)$
168	28 433
169	28 771
170	43 × **677**
171	29 453
172	83 × **359**
173	43 × **701**
174	30 491
175	30 841
176	31 193
177	31 547
178	61 × **523**
179	32 261
180	32 621
181	32 983
182	33 347
183	33 713
184	*173 × 197*
185	47 × **733**
186	97 × *359*
187	61 × **577**
188	35 573
189	35 951
190	47 × **773**
191	36 713
192	37 097
193	37 483
194	37 871
195	38 261
196	38 653
197	39 047
198	39 443
199	39 841
200	40 241

x	$F(x)$
201	97 × **419**
202	41 047
203	41 453
204	41 × **1 021**
205	41 × **1 031**
206	42 683
207	71 × **607**
208	53 × **821**
209	197 × *223*
210	44 351
211	44 773
212	45 197
213	43 × **1 061**
214	46 051
215	53 × **877**
216	43 × **1 091**
217	113 × *419*
218	71 × **673**
219	48 221
220	48 661
221	49 103
222	49 547
223	49 993
224	50 441
225	50 891
226	51 343
227	51 797
228	52 253
229	52 711
230	53 171
231	53 633
232	47 × **1 151**
233	54 563

x	$F(x)$
234	113 × **487**
235	55 501
236	223 × *251*
237	47 × **1 201**
238	56 923
239	61 × **941**
240	57 881
241	58 363
242	83 × **709**
243	59 333
244	163 × *367*
245	41 × **1 471**
246	41 × **1 483**
247	61 297
248	61 × **1 013**
249	167 × *373*
250	62 791
251	167 × *379*
252	131 × *487*
253	64 303
254	64 811
255	83 × **787**
256	43 × **1 531**
257	66 347
258	66 863
259	43 × **1 567**
260	67 901
261	53 × **1 291**
262	68 947
263	69 473
264	70 001
265	251 × *281*
266	179 × *397*

x	$F(x)$
267	71 597
268	53 × **1 361**
269	72 671
270	179 × *409*
271	131 × **563**
272	74 297
273	74 843
274	75 391
275	75 941
276	76 493
277	77 047
278	71 × **1 093**
279	47 × **1 663**
280	78 721
281	79 283
282	79 847
283	97 × **829**
284	47 × **1 723**
285	81 551
286	41 × **2 003**
287	41 × **2 017**
288	83 273
289	71 × **1 181**
290	84 431
291	151 × *563*
292	85 597
293	86 183
294	86 771
295	199 × *439*
296	281 × *313*
297	88 547
298	97 × **919**
299	43 × **2 087**

Au-delà de $F(40)$, on inscrit les premiers nombres premiers de la table devant les valeurs qu'ils divisent, on obtient les sept décompositions indiquées; puis $F(81) = 41 \times \mathbf{163}$, qui comporte un diviseur premier non encore obtenu, ou de racine minimum 81.

A toute valeur $F(c)$, pour c compris entre 7 et 80 inclus, exception faite des valeurs de décomposition, on peut appliquer le raisonnement de récurrence précédent. Tout $F(x)$, de $F(6)$ à $F(c)$ exclus, étant

supposé premier, de racine minimum x, sa racine conjuguée est supérieure à 81, car:

$$F(x)-x-1 = x^2+40 \geqslant 49+40 = 89.$$

Il ne divise donc pas $F(c)$, qui n'étant pas divisible par les valeurs de $F(0)$ à $F(6)$ est un nombre premier de racine minium c.

Pour toutes les valeurs de x, au-delà de 80 et telles que:

$$F(x) \leqslant (2\times 80+1)^2 \quad \Rightarrow \quad x \leqslant 161,$$

les quotients obtenus (après division éventuelle par les monômes des nombres premiers précédents, qui peuvent être limités aux douze premiers), sont des nombres premiers ou sont égaux à 1.

Certains sont diviseurs de valeurs ultérieures du tableau concurremment avec des nombres premiers déjà trouvés. On les inscrit et on forme les quotients qui sont tous premiers ou égaux à 1, dans la limite de la table, dont les valeurs restantes sont inférieures à $(2\times 161+1)^2$.

On a indiqué, en caractère gras, les nombres premiers obtenus comme facteur d'une décomposition effective. Leur fréquence augmente naturellement, dans le prolongement de la table. On peut même trouver une suite de valeurs $F(x)$, en nombre H, arbitrairement grand, dont aucune ne soit un nombre premier.

Il suffit de prendre x compris entre P et $P+H$, le nombre P étant le produit des facteurs premiers qui divisent les H premières valeurs $|F(c)|$. Il est manifeste que chacune des valeurs $F(x)$, ainsi considérées est divisible par au moins un de ces nombres premiers, sans lui être égal (H étant pris au moins égal à r).

Cependant on ne peut pas affirmer qu'il n'y a qu'un nombre fini de valeurs $F(x)$ qui soient des nombres premiers.

Le *tableau VIII* donne *trois autres exemples*, de types différents, limités chacun aux soixante premières valeurs des trinômes.

Pour le trinôme, de discriminant D positif, impair;

$$F(x) = x^2+x-109; \qquad D = 347 = (-19)\times(-23);$$

les *vingt-huit premières valeurs sont des nombres premiers.*

Pour chacune d'elles la deuxième racine est supérieure à 27;

(pour $F(9) = -19$, et $F(11) = +23$, qui sont diviseurs du discriminant, les deux progressions sont confondues).

Dans les dix-neuf valeurs suivantes, seize *sont des nombres premiers*, les trois autres étant des produits de nombres premiers déjà obtenus:

$$F(28) = 19 \times 37; \quad F(34) = 23 \times 47; \quad F(45) = 37 \times 53.$$

(Le raisonnement fait par récurrence dans l'exemple précédent reste valable.)

La valeur suivante $F(47)$ est divisible par 19; mais le quotient est un nouveau nombre premier, ou de racine minimum 47.

Tous les *quotients* des valeurs restantes sont des nombres premiers ou sont égaux à 1.

Pour le trinôme de discriminant D positif, multiple de 4:

$$F(x) = x^2 - 83; \quad D = 332 = (-4) \times (-83)$$

2 étant diviseur du discriminant, toutes les valeurs, pour x impair sont divisibles par 2, mais non par 4.

Les *vingt-quatre premières valeurs* sont des *nombres premiers ou des doubles de nombres premiers*. Toutefois deux facteurs premiers se trouvent deux fois et un d'eux est égal à 1:

$$\mathbf{17} = |F(7)| : 2 = F(10); \quad \mathbf{19} = |F(8)| = F(11) : 2;$$
$$\mathbf{1} = |F(9)| : 2.$$

Dans les vingt valeurs suivantes: *treize sont des nombres premiers ou des doubles de nombres premiers*; les sept autres sont des produits ou des doubles de produits des nombres premiers impairs, précédemment obtenus.

Tous les quotients des valeurs restantes de la table, au-delà de $F(43)$, qui sont différents de 1 et de 2, sont des nombres premiers.

Pour le trinôme de discriminant négatif, multiple de 4:

$$F(x) = x^2 + 37; \quad D = -148 = (-4) \times (+37);$$

2 est encore diviseur du discriminant; toutes les valeurs pour x impair sont divisibles par 2, mais non par 4.

Les *dix-huit premières valeurs, ou leurs moitiés, sont des nombres premiers*. Dans les *trente-huit valeurs suivantes, vingt-neuf sont des nombres premiers ou des doubles de nombres premiers*; les neuf autres, ou leurs moitiés sont des produits des nombres premiers impairs déjà obtenus.

TABLEAU VIII.

$F(x)=x^2+x-109$;
$D=(-19)\times(-23)$

c	F(c)	c	F(c)
0	—109	30	821
1	—107	31	823
2	—103	32	947
3	— 97	33	1 013
4	— 89	34	23×*47*
5	— 79	35	1 151
6	— 67	36	1 223
7	— 53	37	1 297
8	— 37	38	1 373
9	— 19	39	1 451
10	+ 1	40	1 531
11	23	41	1 613
12	47	42	1 697
13	73	43	1 783
14	101	44	1 871
15	131	45	37×*53*
16	163	46	2 053
17	197	47	19×**113**
18	233	48	2 243
19	271	49	2 341
20	311	50	2 441
21	353	51	2 543
22	397	52	2 647
23	443	53	2 753
24	491	54	2 861
25	541	55	2 971
26	593	56	3 083
27	647	57	23×**139**
28	19×*37*	58	3 313
29	761	59	47×*73*

$F(x)=x^2-83$;
$D=(-4)\times(-83)$

c	F(c)	c	F(c)
0	— 83	30	19×*43*
1	—2×41	31	2×439
2	— 79	32	941
3	—2×37	33	2×503
4	— 67	34	29×*37*
5	—2×29	35	2×571
6	— 47	36	1 213
7	—2×17	37	2×643
8	— 19	38	1 361
9	— 2×1	39	2×719
10	+ *17*	40	37×*41*
11	2×*19*	41	2×17×*47*
12	61	42	41×41
13	2×43	43	2×883
14	113	44	17×**109**
15	2×71	45	2×971
16	173	46	19×**107**
17	2×103	47	2×1 063
18	241	48	2 221
19	2×139	49	2×19×*61*
20	317	50	2 417
21	2×179	51	2×1 259
22	401	52	2 621
23	2×223	53	2×29×47
24	17×*29*	54	2 833
25	2×271	55	2×1 471
26	593	56	43×*71*
27	2×17×19	57	2×1 583
28	701	58	17×**193**
29	2×379	59	2×1 699

$F(x)=x^2+37$;
$D=(-4)\times(+37)$

c	F(c)	c	F(c)
0	37	30	937
1	2×19	31	2×499
2	41	32	1 061
3	2×23	33	2×563
4	53	34	1 193
5	2×31	35	2×631
6	73	36	31×*43*
7	2×43	37	2×19×37
8	101	38	1 481
9	2×59	39	2×19×*41*
10	137	40	1 637
11	2×79	41	2×859
12	181	42	1 801
13	2×103	43	2×23×41
14	233	44	1 973
15	2×131	45	2×1 031
16	293	46	2 153
17	2×163	47	2×1 123
18	19×*19*	48	2 341
19	2×199	49	2×23×*53*
20	19×*23*	50	43×*59*
21	2×239	51	2×1 319
22	521	52	2 741
23	2×283	53	2×1 423
24	613	54	2 953
25	2×331	55	2×1 531
26	23×*31*	56	19×**167**
27	2×383	57	2×31×53
28	821	58	19×**179**
29	2×439	59	3 637

(à suivre)