

51. Structure du groupe des classes d'idéaux.

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.09.2024**

Nutzungsbedingungen

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

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

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

Haftungsausschluss

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

indices des idéaux associés ont alors pour somme constante $a-1$ (notamment $-1, \text{ mod. } h$). Ce sont ces constantes 0 et -1 qui ont été adoptées dans l'exemple des tableaux XXII et XXIV.

La constante de la somme des indices d'idéaux correspondants, dont, par ailleurs les points correspondants ont même abscisse, ou même ordonnée, explique la différence des sens de parcours sur les schémas. On peut aussi remarquer que les conjugués d'un idéal et de son suivant sont un idéal et son précédent.

51. Structure du groupe des classes d'idéaux.

Dans un corps réel, pour établir la table de PYTHAGORE (de la multiplication) des classes d'idéaux, il suffit d'établir celle des cycles qui les caractérisent, ou les représentent proprement.

Pour multiplier deux cycles, on en choisit des représentants, qui figurent dans des décompositions (convenables) de valeurs de la table (éventuellement prolongée). Comme, dans le cas d'un corps imaginaire, on cherche, au besoin par récurrence, un idéal semi réduit qui soit congru à ce produit; le cycle auquel appartient cet idéal est le produit des cycles considérés; ou, plus exactement, détermine la classe qui est le produit des classes représentées par les cycles multipliés.

Dans un corps qui n'a qu'un petit nombre de cycles (ce qui est le cas pour des discriminants relativement petits), la détermination de la structure du groupe des classes (ou des cycles) est, en général aisée; elle peut être facilitée par la considération du nombre de cycles, qui est l'ordre du groupe. Si cet ordre est un nombre premier le groupe est cyclique et chacun de ses termes, différent de l'unité (ou de la classe principale) en est un générateur. Si l'ordre est un produit de nombres premiers différents, le groupe est encore cyclique, mais il y a lieu de chercher ses générateurs; ce sont les termes dont l'ordre est égal à celui du groupe. Dans le cas général, la comparaison de l'ordre de certains termes à l'ordre du groupe peut permettre d'affirmer que le groupe est, ou n'est pas cyclique.

Le tableau XXVII donne un exemple de recherche de la structure du groupe des classes, pour un corps de discriminant assez élevé; 62 501; dont le polynôme fondamental est $F(x) = x^2 + x - 15\ 625$.

TABLEAU XXVII.

$$F(x) = x^2 + x - 15\,625; \quad D = 62\,501; \quad r = 56.$$

c	-F(c)
0	15 625 = 5 × 25 × 125
1	623 = 17 × 919
2	619
3	613 = 13 × 1201
4	605 = 5 × 3121
5	15 595 = 5 × 3119
6	583
7	569
8	553 = 103 × 151
9	535 = 5 × 13 × 239
10	15 515 = 5 × 29 × 107
11	493
12	469 = 31 × 499
13	443
14	415 = 5 × 3083
15	15 385 = 5 × 17 × 181
16	353 = 13 × 1181
17	319
18	283 = 17 × 29 × 31
19	245 = 5 × 3049
20	15 205 = 5 × 3041
21	163 = 59 × 257
22	119 = 13 × 1163
23	073
24	025 = 5 ² × 601
25	14 975 = 5 ² × 599
26	923
27	869
28	813
29	755 = 5 × 13 × 227
30	14 695 = 5 × 2939
31	633
32	569 = 17 × 857
33	503
34	435 = 5 × 2885

125²; U₁²

c	-F(c)
35	14 365 = 5 × 17 × 13 ²
36	293
37	219 = 59 × 241
38	143
39	065 = 5 × 29 × 97
40	13 985 = 5 × 2797
41	903
42	819 = 13 × 1063
43	733 = 31 × 443
44	645 = 5 × 2729
45	13 555 = 5 × 2711
46	463
47	369 = 29 × 461
48	273 = 13 × 1021
49	175 = 5 ² × 17 × 31
50	13 075 = 5 ² × 523
51	12 973
52	869 = 17 × 757
53	763
54	655 = 5 × 2531
55	12 545 = 5 × 13 × 593
56	433
57	319 = 97 × 127
58	203
59	085 = 5 × 2437
60	11 965 = 5 × 2393
61	843 = 13 × 911
62	719
63	593
64	465 = 5 × 2293
65	11 335 = 5 × 2287
66	203 = 17 × 659
67	069
68	10 933 = 13 × 29 ²
69	795 = 5 × 17 × 127

97 × 145; K₅ × K₁¹

85 × 155; L₁ × L₃¹

127 × 97; K₄ × K₂¹

85 × 127; K₃ × K₃¹

c	-F(c)
70	10 655 = 5 × 2131
71	513
72	369
73	223
74	075 = 5 ² × 13 × 31
75	9 925 = 5 ² × 397
76	773 = 29 × 337
77	619
78	463
79	305 = 5 × 1861
80	9 145 = 5 × 31 × 59
81	8 983 = 13 × 691
82	819
83	653 = 17 × 509
84	485 = 5 × 1697
85	8 315 = 5 × 1663
86	143 = 17 × 479
87	7 969 = 13 × 613
88	793
89	615 = 5 × 1523
90	7 435 = 5 × 1487
91	253
92	069
93	6 883
94	695 = 5 × 13 × 103
95	6 505 = 5 × 1301
96	313 = 59 × 107
97	119 = 29 × 211
98	5 923
99	725 = 5 ² × 229
100	5 525 = 5 ² × 13 × 17
101	323
102	119
103	4 913 = 17 ³
104	705 = 5 × 941

155 × 65; J₄ × J'₀
59 × 155; J₃ × J'₁
103 × 65; K₁ × K'₅
107 × 59; J₂ × J'₂
29 × 211; L₃ × L'₁
25 × 221; I₁ × I'₁
65 × 85; K₂ × K'₄

c	-F(c)
105	4 495 = 5 × 29 × 31
106	283
107	069 = 13 × 313
108	3 853
109	635 = 5 × 727
110	3 415 = 5 × 683
111	193 = 31 × 103
112	2969
113	743 = 13 × 211
114	515 = 5 × 503
115	2 285 = 5 × 457
116	053
117	1 819 = 17 × 107
118	583
119	345 = 5 × 269
120	1 105 = 5 × 13 × 17
121	0 863
122	619
123	373
124	125 = 5 ³
125	-125

155 × 29; L₂ × L'₂
145 × 31; K₆ × K'₀
31 × 103; K₀ × K'₀
211 × 13; L₄ × L'₀
17 × 107; J₁ × J'₃
65 × 17; J₀ × J'₄
13 × 85; L₀ × L'₄
221 × 5; I₂ × I'₀
1 × 125; U₀ × U₂
5 × 25; I₀ × I'₂

$(\theta-124) = I_0^3 \sim 1;$
 $(\theta-103) = J_1^3 \sim 1;$
 $(\theta-49) = I_2' \times J_1 \times K_0 \sim 1;$
 $(\theta-120) = I_0' \times L_0 \times J_4' \sim 1.$

Devant chaque valeur $-F(c)$, est inscrite sa décomposition en facteurs premiers et une sous ligne indique ceux de ces facteurs, ou produits de facteurs qui sont des normes d'idéaux réduits (38); la majorante de leurs racines est $r = 56$.

D'autre part, devant certaines valeurs (positives de $-F(c)$), l'indication d'un produit égal, de deux *nombres* (en caractères gras), est celle de normes d'un couple d'idéaux semi réduits associés, de racine finale c . Le produit suivant de deux *lettres*, est une représentation de ces idéaux: la lettre (**U, I, J, K, L**) désigne le cycle; l'indice désigne la succession dans ce cycle. On peut vérifier que chacun de ces couples renferme au moins un des idéaux réduits, signalés par ailleurs.

Il y a neuf cycles; l'un d'eux de trois termes, désignés par la lettre **U** est du type 1; il contient un idéal double $(1, \theta-124)$ et un idéal réfléchi $(125, \theta)$; ses idéaux sont principaux, c'est le cycle principal.

Les autres cycles se répartissent en quatre couples de cycles conjugués; désignés respectivement par la même lettre, avec et sans accent, dont les nombres de termes sont: trois pour **I** et **I'**; cinq pour **J** et **J'**; sept pour **K** et **K'**; cinq pour **L** et **L'**; ces nombres sont impairs, comme celui des idéaux du cycle **U**. La somme des indices des idéaux conjugués est congrue à 0, celle des idéaux associés est congrue à -1 (49).

Dans le groupe chacun des huit termes, différents de l'unité **U**, est d'ordre 3. Le groupe est *produit direct de deux groupes cycliques d'ordre 3*, engendrés respectivement par les puissances de deux cycles, non conjugués, par exemple **I** et **J**.

Cette structure résulte immédiatement des décompositions de certaines des valeurs de la table. Celles de:

$$F(124) = 5^3 \Rightarrow (\theta-124) = (5, \theta-124)^3 = \mathbf{I}_0^3;$$

$$F(103) = 17^3 \Rightarrow (\theta-103) = (17, \theta-103)^3 = (17, \theta-117)^3 = \mathbf{J}_1^3$$

montrent que les cycles **I** et **J**, ainsi que leurs conjuguées **I'** et **J'** sont des termes d'ordre 3 du groupe. Par suite ce groupe qui est d'ordre 9, ne peut être cyclique (si non il ne contiendrait que deux termes d'ordre 3, puissances 3 et 6 d'une base). Il est donc produit de deux groupes cycliques, d'ordre 3. Ses termes peuvent notamment être exprimés par:

$$\mathbf{I}^x \times \mathbf{J}^y; \quad x, y \text{ entiers, mod. } 3.$$

On peut compléter cette indication en cherchant les expressions de \mathbf{K} et de \mathbf{L} . Elles résultent notamment des décompositions :

$$F(49) = 25 \times 17 \times 31 \Rightarrow (25, \theta-49) \times (17, \theta-49) \times (31, \theta-49) \\ = (25, \theta-124) \times (17, \theta-117) \times (31, \theta-111) \sim 1$$

$$F(120) = 5 \times 13 \times 17 \Rightarrow (5, \theta-120) \times (13, \theta-120) \times (17, \theta-120) \sim 1.$$

Elles entraînent :

$$\mathbf{K} = \mathbf{I} \times \mathbf{J}^2; \quad \mathbf{L} = \mathbf{I} \times \mathbf{J}.$$

Les cycles conjugués sont aussi inverses, l'un de l'autre, de sorte que chacun d'eux est égal au carré de l'autre (exposant 2, mod. 3).

52. Corps de discriminant premier.

On va examiner quelques unes des circonstances qui peuvent se présenter dans la structure du groupe des classes des idéaux semi réduits, ou des cycles.

Dans un corps réel, dont le discriminant est un nombre premier, nécessairement congru à $+1$, mod. 4, il n'y a qu'une seule classe double, caractérisée par un cycle, du type 1, d'un nombre impair d'idéaux. Il peut exister en outre des couples de cycles conjugués, et associés, du type 4, qui ont aussi un nombre impair d'idéaux.

Si le cycle principal existe seul, le corps est principal. Dans le cas contraire l'ordre du groupe des classes est impair et supérieur à 1 ; si cet ordre est un nombre premier, ou un produit de nombres premiers différents, le groupe est cyclique, mais cette condition suffisante n'est pas nécessaire.

Un corps, de discriminant premier ne contient qu'un idéal double de norme 1, qui engendre un cycle de type 1, évidemment principal. Ce cycle doit donc contenir un idéal semi réduit réfléchi, ce qui entraîne l'existence d'une décomposition du discriminant en une somme de carrés de deux nombres entiers.

C'est là une nouvelle preuve de la propriété déjà établie par la considération du corps $\mathbf{R}(i)$: un nombre premier, congru à $+1$, mod. 4 ; est égal à une somme de carrés de deux nombres entiers (20).

Cette démonstration établissait aussi la détermination de ces deux carrés ; il est possible de le vérifier également par des considéra-