34. Corps imaginaires principaux.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Le troisième est sous-groupe de $\mathcal{J}$, les deux premiers en sont *indépendants* (**26**). On obtient le sous-groupe en formant le produit direct de l'un d'eux avec $\mathcal{J}$.

On a choisi le premier, défini par l'idéal de norme 3, désigné par **J**. Les calculs des produits:

$$\mathbf{I}\times\mathbf{J} = (6,\ \theta-2); \qquad \mathbf{I}^2\times\mathbf{J} = (12,\ \theta+2) \sim (5,\ \theta-1),$$

sont indiqués dans la table; le second utilise la décomposition $F(-2) = 5\times 12$. On en déduit les expressions des classes conjuguées:

$$\mathbf{I}'\times\mathbf{J}' \sim \mathbf{I}^5\times\mathbf{J}, \qquad \mathbf{I}'^2\times\mathbf{J}' \sim \mathbf{I}^4\times\mathbf{J}.$$

Le monôme $\mathbf{I}^3\times\mathbf{J}$, congru à son conjugué, est naturellement congru au seul idéal réduit restant, de norme 7, d'ailleurs remarquable. On en a aussi indiqué un calcul de vérification, qui utilise la décomposition adjointe à la table: $F(10 = 7\times 24$.

34. Corps imaginaires principaux.

On va examiner sommairement quelques-unes des circonstances générales, qui peuvent se présenter dans la structure du groupe des classes des idéaux d'un corps imaginaire.

Pour qu'un corps imaginaire soit *principal* (**19**), ou ne contienne que la seule classe principale (groupe des classes d'ordre 1), il faut et il suffit que *l'idéal unité soit le seul idéal réduit.*

Il est équivalent de dire que, la limite r étant calculée par la condition (**25** et **26**):

$$3\ .\ (2x-S)^2 > |D| \quad\Leftrightarrow\quad x > r;$$

les r *premières valeurs* $F(c)$, du polynôme fondamental $(0 \leqslant c < r)$ *sont toutes des nombres premiers.*

Pour $|D|$ pair, *les seuls corps principaux sont ceux de discriminants* -4 et -8; il n'y a qu'une valeur $F(c)$ à considérer $(r = 1)$, qui est égale, respectivement à 1 et à 2. Pour tout autre corps, l'idéal de norme 2 et de racine minimum 0 ou 1 est réduit double et n'est pas principal.

Pour $|D|$ *impair*, il est nécessaire que ce soit un nombre premier, si non sa décomposition, non triviale, entraînerait l'existence d'au moins un idéal réduit remarquable, différent de (1) (double ou réfléchi) (**29**), donc d'une classe double, non principale.

Le tableau XI suivant donne les *sept corps imaginaires principaux*, qui sont connus et, pour chacun d'eux, les r valeurs de leur polynôme fondamental qui sont, comme il vient d'être dit, des nombres premiers. Le polynôme x^2+x+41 a déjà été indiqué comme générateur d'une suite de nombres premiers (**28**); il en est de même des polynômes, de discriminants —43 et —67, qui donnent respectivement des suites de 10 et 16 nombres premiers.

Tableau XI.

Corps imaginaires principaux.

Discriminant impair.

$D =$ $r =$	—3 1	—7 1	—11 1	—19 1	—43 2	—67 2	—163 4
$F(0) = N =$	1	2	3	5	11	17	41
$F(1) =$	....				13	19	43
$F(2) =$	....						47
$F(3) =$	....						53

pair.

$D =$ $r =$	—4 1	—8 1
$F(0) = N$	1	2

On peut établir méthodiquement l'existence de ces corps principaux et vérifier qu'il n'y en a pas d'autre, au moins jusqu'à une valeur relativement grande de $|D|$ par les considérations suivantes.

On peut d'abord comparer $|D|$ aux nombres premiers successifs:

$$p_0 = 1, \; p_1 = 2, \; p_2 = 3, \; \dots \; p_i, \; \dots$$

Un corps, de discriminant $|D|$, *compris entre:*

$$3p_k^2 \leqslant |D| < 3p_{k+1}^2 ,$$

est principal, si et seulement si *D n'est pas congru à un carré* —ou n'est pas résidu quadratique— *relativement aux k premiers nombres premiers* (i de 1 à k).

La condition est *nécessaire*: le corps n'ayant pas d'idéal premier réduit, en dehors de (1), donc de norme p_i antérieur à p_{k+1}, la congruence fondamentale doit être impossible pour chacun des nombres premiers p_i.

La condition est *suffisante*: si elle est remplie, il n'y a aucun idéal réduit, différent de (1), car son existence entraînerait celle d'au moins un idéal premier réduit (**32**).

Les valeurs absolues $|D|$. des discriminants qui ne sont pas congrus à un carré, relativement aux nombres premiers successifs, de 2 à p_i, appartiennent à des *progressions arithmétiques*:

de raison: $4P$; $P = 1 \times 2 \times ... \times p_k = \Pi p_i$; ($i$ de 0 à k);

en nombre: $\varphi(4P) : 2^{k+1} = (3-1) \times ... \times (p_k - 1) : 2^{k-1}$.

Leur détermination peut se faire de proche en proche, en cherchant, pour les valeurs successives de p_i, les valeurs de $|D|$, pour lesquelles D est un discriminant, non congru à un carré; puis en conjuguant les systèmes successifs de relations ainsi formées. On obtient ainsi:

	successivement:		collectivement:	
	$\|D\| \equiv$,	mod.:	$\|D\| \equiv$,	mod.:
(1)	3	4		
(2)	3	8	3	8
(3)	1	3	19	$8 \times 3 = 24$
(4)	2, ou 3	5	43, ou 67	$24 \times 5 = 120$
(5)	3, ou 5, ou 6	7	43, ou 163, ou 403 ou 67, ou 547, ou 667	$120 \times 7 = 840$

La condition (1) exprime seulement que D est un discriminant. La condition (6) suivante exprimerait que $|D|$ est congru à:

$$2, \quad \text{ou } 6, \quad \text{ou } 7, \quad \text{ou } 8, \quad \text{ou } 10; \quad (\text{mod. } 11);$$

sa conjonction avec les précédentes conditions exprimerait que $|D|$ est congru, à l'un des trente nombres:

$$\begin{array}{rrrrrrrrrr}
883, & 3403, & 5083, & 5923, & 6763; & 163, & 3523, & 6043, & 7723, & 8563; \\
2083, & 3763, & 4603, & 5443, & 8803; & 67, & 907, & 1747, & 5107, & 7627; \\
1387, & 2227, & 3067, & 6427, & 8947; & 2347, & 4027, & 4867, & 5707, & 9067;
\end{array}$$
$$(\text{mod. } 9240).$$

En rapprochant la limitation de $|D|$ et son appartenance aux progressions, on obtient les résultats suivants:

$$k = 0; \quad 3 \leqslant |D| < 3\times 2^2 = 12; \quad |D| = 3+4\lambda;$$

les seuls nombres premiers vérifiant ces conditions sont:

$$\mathbf{3}, \quad 3+4 = \mathbf{7}, \quad 3+4\times 2 = \mathbf{11};$$

ce sont les trois premières valeurs du tableau XI.

$$k = 1; \quad 12 \leqslant |D| < 3\times 3^2 = 27; \quad |D| = 3+8\lambda;$$

le seul nombre premier vérifiant ces conditions est:

$$3 + 8\times 2 = \mathbf{19}; \quad \text{quatrième valeur du tableau.}$$

$$k = 2; \quad 27 \leqslant |D| < 3\times 5^2 = 75; \quad |D| = 19+24\lambda;$$

les seuls nombres premiers vérifiant ces conditions sont:

$$19+24 = \mathbf{43}, \quad 19+24\times 2 = \mathbf{67};$$

ce sont les cinquième et sixième valeurs du tableau XI.

$$k = 3; \quad 75 \leqslant |D| < 3\times 7^2 = 147 \quad 43 + 120\lambda \quad \text{ou} \quad 67+120\lambda$$

aucun nombre premier ne remplit ces conditions.

$$k = 5; \quad 147 \leqslant |D| < 3\times 11^2 = 363;$$

et $|D|$ doit appartenir à une des six progressions indiquées de raison 840. Il n'y a qu'un nombre premier vérifiant ces conditions:

$$\mathbf{163}, \quad \text{dernière valeur du tableau.}$$

$$k = 6; \quad 363 \leqslant |D| < 3\times 13^2 = 507;$$

aucun nombre premier des trois progressions, mod. 9240, ne vérifie cette limitation.

TABLEAU XII.

Corps imaginaires de discriminant premier.

$D = -263;\ r = 5$

c	F(c)
-5	$86 = 2\times 43$
-4	$78 = 2\times 3\times 13$
-3	$72 = 2^3\times 3^2$ $(\mathbf{8},\ \theta+3) \sim \mathbf{I}^{10}$ $(\mathbf{6},\ \theta+3) \sim \mathbf{I}^{7}$
-2	$68 = 2^2\times 17$ $(\mathbf{4},\ \theta+2) = \mathbf{I}^{2}$
-1	$66 = 2\times 3\times 11 = 6\times 11$ $(\mathbf{6},\ \theta+1) \sim \mathbf{I}^{4}$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{5}$ $(\mathbf{2},\ \theta+1) \sim \mathbf{I}^{12}$
0	$66 = 2\times 3\times 11 = 11\times \mathbf{6}$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) = \mathbf{I}$ $(\mathbf{3},\ \theta-0) \sim \mathbf{I}^{8}$ $(\mathbf{6},\ \theta-0) \sim \mathbf{I}^{9}$
$+1$	$68 = 2^2\times 17$ $(\mathbf{4},\ \theta-1) \sim \mathbf{I}^{11}$
$+2$	$72 = 2^3\times 3^2$ $(\mathbf{6},\ \theta-2) \sim \mathbf{I}^{6}$ $(\mathbf{8},\ \theta-2) = \mathbf{I}^{3}$
$+3$	$78 = 2\times 3\times 13$
$+4$	$86 = 2\times 43$
...	
10	$176 = 2^4\times \mathbf{11}$

Ordre 13

$D = -439;\ r = 6$

c	F(c)
-6	$140 = 2^2\times 5\times 7$
-5	$130 = 2\times 5\times 13$ $(\mathbf{10},\ \theta+5) \sim \mathbf{I}^{5}$
-4	$122 = 2\times 61$
-3	$116 = 2^2\times 29$
-2	$112 = 2^4\times \mathbf{7}$ $(\mathbf{8},\ \theta+2) = \mathbf{I}^{3}$ $(\mathbf{7},\ \theta+2) \sim \mathbf{I}^{11}$ $(\mathbf{4},\ \theta+2) = \mathbf{I}^{2}$
-1	$110 = 2\times 5\times 11$ $(\mathbf{10},\ \theta+1) \sim \mathbf{I}^{8}$ $(\mathbf{5},\ \theta+1) \sim \mathbf{I}^{9}$ $(\mathbf{2},\ \theta+1) \sim \mathbf{I}^{14}$
0	$110 = 2\times 5\times 11$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) = \mathbf{I}$ $(\mathbf{5},\ \theta-0) \sim \mathbf{I}^{6}$ $(\mathbf{10},\ \theta-0) \sim \mathbf{I}^{7}$
$+1$	$112 = 2^4\times 7$ $(\mathbf{4},\ \theta-1) \sim \mathbf{I}^{13}$ $(\mathbf{7},\ \theta-1) \sim \mathbf{I}^{4}$ $(\mathbf{8},\ \theta-1) \sim \mathbf{I}^{12}$
$+2$	$116 = 2^2\times 29$
$+3$	$122 = 2\times 61$
$+4$	$130 = 2\times 5\times 13$ $(\mathbf{10},\ \theta-4) \sim \mathbf{I}^{10}$
$+5$	$140 = 2^2\times 5\times 7$
...	
14	$320 = 2^6\times \mathbf{5} = 2^5\times \mathbf{10}$

Ordre 15

$D = -419;\ r = 6$

c	F(c)
-6	$135 = 3^3\times \mathbf{5}$
-5	$125 = 5^3$
-4	$117 = 3^2\times 13$ $(\mathbf{9},\ \theta+4) \sim \mathbf{I}^{7}$
-3	$111 = 3\times 37$
-2	107
-1	$105 = 3\times 5\times 7$ $(\mathbf{7},\ \theta+1) \sim \mathbf{I}^{4}$ $(\mathbf{5},\ \theta+1) \sim \mathbf{I}^{6}$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{8}$
0	$105 = 3\times 5\times 7 = 15\times \mathbf{7}$ $(\mathbf{1},\ \theta-0 = (1)$ $(\mathbf{3},\ \theta-0) = \mathbf{I}$ $(\mathbf{5},\ \theta-0) \sim \mathbf{I}^{3}$ $(\mathbf{7},\ \theta-0) \sim \mathbf{I}^{5}$
$+1$	107
$+2$	$111 = 3\times 37$
$+3$	$117 = 3^2\times 13$ $(\mathbf{9},\ \theta-3) = \mathbf{I}^{2}$
$+4$	$125 = 5^3$
$+5$	$135 = 3^3\times 5$

Ordre 9

Calcul des idéaux réduits

congrus aux puissances de l'idéal générateur.

$D = -263$; 13 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{2},\ \theta-0)$, $\mathbf{I}^{12} \sim (\mathbf{2},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{4},\ \theta+2)$, $\mathbf{I}^{11} \sim (\mathbf{4},\ \theta-1)$;

$\mathbf{I}^3 = (\mathbf{8},\ \theta-2)$, $\mathbf{I}^{10} \sim (\mathbf{8},\ \theta+3)$;

$\mathbf{I}^4 = (2^4,\ \theta-10) \sim (11,\ \theta+11)$ [$F(10)$]

$= (11,\ \theta-0) \sim (\mathbf{6},\ \theta+1)$, $\mathbf{I}^9 \sim (\mathbf{6},\ \theta-0)$; [$F(0)$]

$\mathbf{I}^5 = \mathbf{I}^4 \times \mathbf{I} \sim (\mathbf{6},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (2) \times (\mathbf{3},\ \theta+1)$, $\mathbf{I}^8 \sim (\mathbf{3},\ \theta-0)$;

$\mathbf{I}^6 = \mathbf{I}^5 \times \mathbf{I} \sim (\mathbf{3},\ \theta+1) \times (\mathbf{2},\ \theta-0) = (\mathbf{6},\ \theta-2)$, $\mathbf{I}^7 \sim (\mathbf{6},\ \theta+3)$;

$D = -439$; 15 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{2},\ \theta-0)$, $\mathbf{I}^{14} \sim (\mathbf{2},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{4},\ \theta+2)$, $\mathbf{I}^{13} \sim (\mathbf{4},\ \theta-1)$;

$\mathbf{I}^3 = (\mathbf{8},\ \theta+2)$, $\mathbf{I}^{12} \sim (\mathbf{8},\ \theta-1)$;

$\mathbf{I}^4 = (2^4,\ \theta+2) \sim (\mathbf{7},\ \theta-1)$, $\mathbf{I}^{11} \sim (\mathbf{7},\ \theta+2)$; [$F(-2)$]

$\mathbf{I}^5 = (2^5,\ \theta-14) \sim (10,\ \theta+15) = (\mathbf{10},\ \theta+5)$, $\mathbf{I}^{10} \sim (\mathbf{10},\ \theta-4)$; [$F(14)$]

$\mathbf{I}^6 = (2^6,\ \theta-14) \sim (\mathbf{5},\ \theta+15) = (\mathbf{5},\ \theta-0)$, $\mathbf{I}^9 \sim (\mathbf{5},\ \theta+1)$; [$F(14)$]

$\mathbf{I}^7 = \mathbf{I}^6 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{2},\ \theta-0) = (\mathbf{10},\ \theta-0)$, $\mathbf{I}^8 \sim (\mathbf{10},\ \theta+1)$;

$D = -419$; 9 classes; groupe cyclique.

$\mathbf{I} = (\mathbf{3},\ \theta-0)$, $\mathbf{I}^8 \sim (\mathbf{3},\ \theta+1)$;

$\mathbf{I}^2 = (\mathbf{9},\ \theta-3)$, $\mathbf{I}^7 \sim (\mathbf{9},\ \theta+4)$;

$\mathbf{I}^3 = (3^3,\ \theta+6) \sim (\mathbf{5},\ \theta-0)$, $\mathbf{I}^6 \sim (\mathbf{5},\ \theta+1)$; [$F(-6)$]

$\mathbf{I}^4 = \mathbf{I}^3 \times \mathbf{I} \sim (\mathbf{5},\ \theta-0) \times (\mathbf{3},\ \theta-0) = (15,\ \theta-0)$

$\sim (\mathbf{7},\ \theta+1)$, $\mathbf{I}^5 \sim (\mathbf{7},\ \theta-0)$; [$F(0)$]

$$k = 7; \quad 507 \leqslant |D| < 3 \times 17^2 = 867;$$

cette limitation n'est vérifiée par aucun nombre des trente progressions donc, à fortiori par aucun des $30 \times 6 = 180$ progressions construites en adjoignant une condition, mod. 13.

Au lieu de continuer ce raisonnement, on peut étudier directement les nombres premiers contenus dans les trente progressions, limités, par exemple à 100.000. Un calcul de congruences permet d'éliminer ceux qui sont congrus à un carré, mod. 13 ou mod. 17. Pour ceux qui restent, la construction directe des corps qui les admettent comme discriminants, montre qu'ils ne sont pas principaux.

35. Corps imaginaires, de discriminant premier.

On a signalé ci-dessus (**34**) que les corps, de discriminant (négatif) premier, sont les seuls, pour lesquels *l'idéal unité est l'unique idéal réduit* remarquable. Les classes contiennent donc, en plus de la classe principale, des couples de classes conjuguées; *l'ordre g du groupe des classes est un nombre impair*; il est égal à 1 pour les sept corps principaux indiqués.

Ce groupe des classes peut être *cyclique*; il en est toujours ainsi si son ordre g est *premier*, ou *produit de nombres premiers différents* —ou sans facteur carré— .

Dans les trois exemples du *tableau XII*, le groupe des classes est *cyclique*. Pour chacun d'eux, on a dressé les valeurs de $F(c)$ pour c inférieur au rang r; pour des raisons de clarté, on a prolongé le tableau en deçà de 0, de façon à indiquer les idéaux réduits devant leur racine minimum.

On a choisi un idéal réduit (convenable) désigné par **I**; définissant une classe génératrice du groupe. Devant chaque idéal réduit, on a indiqué à quelle puissance de **I**, il est congru, ou éventuellement égal. Les calculs sont détaillés en face; on a indiqué simultanément les idéaux réduits congrus aux classes inverses, —ou d'exposants opposés— .

Dans le *premier exemple*, le nombre de classes est premier, le groupe est cyclique et on peut choisir arbitrairement un générateur. On a utilisé l'idéal de norme 2, dont le tableau donne immédiatement