Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 7 (1961)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LES CORPS QUADRATIQUES

Autor: Châtelet, A.

Kapitel: 35. Corps imaginaires, de discriminant premier.

DOI: https://doi.org/10.5169/seals-37125

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

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

Tableau XIII.

Répartition des *corps quadratiques imaginaires* de discriminant D premier (négatif, congru à $+1$, mod. 4)

d'après le nombre de leurs *classes d'ideaux* (ordre du groupe).

Ordre	$\lvert D \rvert$
1	3, 7, 11, 19, 43, 67, 163. (Corps principaux.)
3	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 883, 907.
5	47, 79, 103, 127, 131, 179, 227, 347, 443, 523, 571, 619, 643, 683, 691, 739, 787, 947.
7	71, 151, 223, 251, 463, 467, 487, 587, 811, 827, 859.
9	199, 367, 419, 491, 563, 823.
11	167, 271, 659, 967.
13	191, 263, 607, 631, 727.
15	239, 439, 751, 971.
17	383, 991.
19	311, 359, 919.
21	431, 503, 743, 863.
23	647.
25	479, 599.
27	983.
29	887.
31	719, 911.
33	839.

les idéaux réduits égaux aux trois premières puissances de cet idéal et de son conjugué.

Dans le *deuxième exemple*, le nombre de classes est $15 = 3 \times 5$, nombre composé sans facteur carré. Le groupe est cyclique, mais on ne peut choisir arbitrairement le générateur. Le tableau donne immédiatement le cube de $\mathbf{I} = (\mathbf{2},\ \theta—0)$, qui n'est pas congru à 1. La décomposition de $F(14)$, formé pour étudier la puissance d'exposant 5 de **I**, montre qu'elle n'est pas non plus congrue à (1). On peut donc prendre comme générateur la classe définie par **I**, qui, n'étant pas d'ordre 3 ou 5, est d'ordre 15.

Dans le *troisième exemple*, il y a neuf classes et le groupe pourrait être un produit direct de deux groupes cycliques d'ordre 3. Mais la décomposition de $F(—6)$ montre que le cube de l'idéal $\mathbf{I} = (\mathbf{3},\ \theta—0)$ n'est pas congru à (1); il définit une classe qui, n'étant pas d'ordre 3, est d'ordre 9 et peut être prise comme générateur.

On constate que, pour tous les corps quadratiques imaginaires, dont *le discriminant est un nombre premier*, *inférieur à* 1000, le groupe des classes d'idéaux est *cyclique*. On donne ci-dessous le tableau XIII de leur répartition, d'après l'ordre du groupe.

On remarquera que, pour les groupes dont l'ordre est un carré (six groupes d'ordre 9 et deux groupes d'ordre 25), il convient de vérifier qu'ils sont bien cycliques, alors que pour les autres, cette qualité résulte de la seule nature arithmétique de leur ordre (nombre premier, ou produit de nombres premiers différents). Cette vérification a été explicitement indiquée dans le troisième exemple du tableau XII, concernant le corps de discriminant —419, qui comprend neuf classes d'idéaux.

La complexité de la structure paraît bien augmenter avec la grandeur du discriminant: il semble que ce soit seulement pour des valeurs relativement grandes (de sa valeur absolue) qu'il existe des groupes de classes non cycliques. Un exemple en est donné dans le tableau XIV, qui concerne le corps de discriminant premier —12 451.

L'exemple comprend, comme pour les précédents, une table des valeurs du polynôme fondamental $F(x)$, limitée toutefois aux valeurs

Tableau XIV.

Structure d'un groupe de classes d'idéaux.

$F(x) = x^5 + x + 3\,113; \quad D = -12\,451; \quad r = 32.$

0	$3\,113 = 11 \times 283$
	$(\mathbf{1}, \theta-0) = (1)$
	$(\mathbf{11}, \theta-0) \sim \mathbf{I}^3 \times \mathbf{J}^3$
1	$3\,115 = 5 \times 7 \times 89$
	$(\mathbf{5}, \theta-1) = \mathbf{I}$
	$(\mathbf{7}, \theta-1) = \mathbf{J}$
	$(\mathbf{35}, \theta-1) = \mathbf{I} \times \mathbf{J}$
2	$3\,119$
3	$3\,125 = 5^5 = 5^3 \times \mathbf{25}$
	$(\mathbf{25}, \theta-3) \sim \mathbf{I}^3$
4	$3\,133 = 13 \times 241$
	$(\mathbf{13}, \theta-4) \sim \mathbf{I}^4 \times \mathbf{J}^2$
5	$3\,143 = 7 \times 449$
6	$3\,155 = 5 \times 631$
7	$3\,169$
8	$3\,185 = (5 \times 7^2) \times \mathbf{13} = 65 \times \mathbf{49}$
	$(\mathbf{35}, \theta-8) \sim \mathbf{I}^4 \times \mathbf{J}$
	$(\mathbf{49}, \theta-8) = \mathbf{J}^2$
9	$3\,203$
10	$3\,223 = 11 \times 293$
11	$3\,245 = 5 \times 11 \times 59 = 59 \times \mathbf{55}$
	$(\mathbf{55}, \theta-11) \sim \mathbf{I}^4 \times \mathbf{J}^3$
12	$3\,269 = 7 \times 467$
13	$3\,295 = 5 \times 659$
14	$3\,323$
15	$3\,353 = 7 \times 479$
16	$3\,385 = 5 \times 677$
17	$3\,419 = 13 \times 263$
18	$3\,455 = 5 \times 691$
19	$3\,493 = 7 \times 499$
20	$3\,533$
21	$3\,575 = 5^2 \times 11 \times 13 = 65 \times \mathbf{55}$
	$(\mathbf{55}, \theta-21) \sim \mathbf{I}^3 \times \mathbf{J}^2$
22	$3\,619 = 7 \times 11 \times 47 = (7 \times 47) \times \mathbf{11}$
	$(\mathbf{47}, \theta-22) \sim \mathbf{I}^2 \times \mathbf{J}$
23	$3\,665 = 5 \times 733$
24	$3\,713 = 47 \times 79$
25	$3\,763 = 53 \times 71$
	$(\mathbf{53}, \theta-25) \sim \mathbf{I}^2 \times \mathbf{J}^4$
26	$3\,815 = 5 \times 7 \times 109$
27	$3\,869 = 53 \times 73$
28	$3\,925 = 5^2 \times 157$
29	$3\,983 = 7 \times 569$
30	$4\,043 = 13 \times 311$
31	$4\,105 = 5 \times 821$

$F(71) = 7\,225 = (5^2 \times 7) \times \mathbf{47}$

$F(-79) = F(78) = 9\,275 = (5^2 \times 7) \times \mathbf{55}$

$F(106) = 14\,455 = (5 \times 7^2) \times \mathbf{59}$

$F(-139) = F(138) = 22\,295 = 7^3 \times \mathbf{65}$

entières de x, entre 0 et la limite r. Elle est complétée sur la page, de face, par une *table de Pythagore, de la multiplication des classes*, caractérisées par les idéaux réduits, et par un *détail des calculs* de sa construction.

Dans ce détail, les couples d'idéaux réduits conjugués, écrits avec leurs racines minimum (de somme —1), ont leurs normes en caractères gras, pour les distinguer des idéaux servant d'intermédiaires. Par contre, dans la table de multiplication cette distinction d'écriture a été conservée aux seuls idéaux réduits, de racine minimum non négative et ce sont les seuls qui ont été inscrits dans la table des valeurs, en face de leur racine.

Les monômes $\mathbf{I}^x \times \mathbf{J}^y$ (x,y prenant les valeurs de 0, sous-entendu à 4), inscrits dans la table des valeurs et dans celle de multiplication, montrent que le groupe des classes est un *produit direct* (**26**) *de deux sous-groupes cycliques*, d'ordre 5, pour lesquels on peut prendre pour générateurs respectifs, les classes définies par les idéaux réduits de normes 5 et 7, notés **I** et **J**.

Pour les calculs l'ordre adopté est le suivant: la décomposition $F(3) = F(—4) = 5^5$, montre que les idéaux réduits, conjugués, de norme 5 ont leur puissance, d'exposant 5, congrue à (1). Les classes définies par les quatre idéaux réduits de normes 5 et 25, avec la classe (1) constituent par suite un *sous-groupe cyclique, d'ordre 5.*

Le calcul du cube $\mathbf{J}^3$, de l'idéal $\mathbf{J} = (7,\ \theta—1)$ montre qu'il est congru au carré $\mathbf{J}'^2$, de son idéal conjugué $\mathbf{J}' = (7, \theta+2)$. Il en résulte que les puissances d'exposant 5, de **J** et **J**′ (ainsi que de leurs carrés) sont aussi congrues à (1). Les quatre idéaux, de forme 7 et 49, définissent des classes, qui avec la classe (1) forment *un sous-groupe cyclique, d'ordre* 5, *indépendant du précédent* [sans élément commun, sauf (1)]. Le *produit direct de ces deux sous-groupes cyliques*, qui a vingt-cinq éléments, *est donc égal au groupe*, dont il est une décomposition minimum (**26**).

On a calculé ensuite les produits $\mathbf{I} \times \mathbf{J}$ et $\mathbf{I} \times \mathbf{J}^4$ (en remplaçant $\mathbf{J}^4$ par l'idéal réduit congru **J**′, conjugué de **J**). Leurs expressions obtenues par un calcul de congruences arithmétiques sont directement dans la table des valeurs.

Pour les autres produits, on passe par des idéaux intermédiaires dont les décompositions de valeurs de $F(x)$, permettent comme il a été dit, de trouver des idéaux congrus, de norme inférieure. En fait,

Table de pythagore de multiplication des classes d'idéaux

(Produit direct de 2 sous-groupes cycliques d'ordre 5).

	$\mathbf{J}^5 \sim (1)$	$\mathbf{J}$	$\mathbf{J}^2$	$\mathbf{J}^3$	$\mathbf{J}^4$
$\mathbf{I}^5 \sim (1)$	(1)	$(\mathbf{7}, \theta-1)$	$(\mathbf{49}, \theta-8)$	$(49, \theta+9)$	$(7, \theta+2)$
$\mathbf{I}$	$(\mathbf{5}, \theta-1)$	$(\mathbf{35}, \theta-1)$	$(55, \theta+12)$	$(13, \theta+5)$	$(35, \theta+9)$
$\mathbf{I}^2$	$(25, \theta+4)$	$(\mathbf{47}, \theta-22)$	$(11, \theta+1)$	$(55, \theta+22)$	$(\mathbf{53}, \theta-25)$
$\mathbf{I}^3$	$(\mathbf{25}, \theta-3)$	$(53, \theta+26)$	$(\mathbf{55}, \theta-21)$	$(\mathbf{11}, \theta-0)$	$(47, \theta+23)$
$\mathbf{I}^4$	$(5, \theta+2)$	$(\mathbf{35}, \theta-8)$	$(\mathbf{13}, \theta-4)$	$(\mathbf{55}, \theta-11)$	$(35, \theta+2)$

Calculs

$$
\begin{array}{llllll}
\mathbf{J}^3 = (\mathbf{7}, \theta-1)^3 = (7^3, \theta+139) & \sim (65, \theta-138) & = (65, \theta-8) & & & F(-139) \\
 & \sim (\mathbf{49}, \theta+9) & = (\mathbf{7}, \theta+2)^2; & & & F(8) \\
\mathbf{I}\times\mathbf{J} = (\mathbf{5}, \theta-1)\times(\mathbf{7}, \theta-1) & = (\mathbf{35}, \theta-1); & & & & \\
\mathbf{I}\times\mathbf{J}^4 \sim (\mathbf{5}, \theta-1)\times(\mathbf{7}, \theta+2) & = (\mathbf{35}, \theta+9); & & & & \\
\mathbf{I}\times\mathbf{J}^2 = (\mathbf{5}, \theta-1)\times(\mathbf{49}, \theta-8) & = (5\times 7^2, \theta-106) & \sim (59, \theta+107) & & & F(106) \\
 & = (59, \theta-11) & \sim (\mathbf{55}, \theta+12); & & & \\
\mathbf{I}\times\mathbf{J}^3 \sim (\mathbf{5}, \theta-1)\times(\mathbf{49}, \theta+9) & = (5\times 7^2, \theta+9) & \sim (13, \theta-8) & & & F(-9) \\
 & & = (\mathbf{13}, \theta+5); & & & F(11) \\
\mathbf{I}^2\times\mathbf{J} \sim (\mathbf{7}, \theta-1)\times(\mathbf{25}, \theta+4) & = (7\times 5^2, \theta-71) & \sim (47, \theta+72) & & & F(71) \\
 & & = (\mathbf{47}, \theta-22); & & & \\
\mathbf{I}^2\times\mathbf{J}^4 \sim (\mathbf{7}, \theta+1)\times(\mathbf{25}, \theta+4) & = (7\times 5^2, \theta+79) & \sim (53, \theta-78) & & & F(-79) \\
 & & = (\mathbf{53}, \theta-25); & & & \\
\mathbf{I}^2\times\mathbf{J}^2 \sim (\mathbf{7}, \theta-1)\times(\mathbf{47}, \theta-22) & = (7\times 47, \theta-22) & \sim (11, \theta+23) & & & F(22) \\
 & & = (\mathbf{11}, \theta+1); & & & \\
\mathbf{I}^3\times\mathbf{J}^2 \sim (\mathbf{5}, \theta-1)\times(\mathbf{11}, \theta+1) & = (\mathbf{55}, \theta-21); & & & &
\end{array}
$$

au cours des déterminations successives, on a remplacé certains produits par des idéaux congrus, déjà calculés:

$$\mathbf{I}\times\mathbf{J}^3 \text{ par } \mathbf{I}\times\mathbf{J}'^2; \quad \mathbf{J}^4 \text{ par } \mathbf{J}'; \quad \mathbf{I}^2\times\mathbf{J}^2 \text{ par } \mathbf{J}\times(\mathbf{I}^2\times\mathbf{J});$$
$$\mathbf{I}^3\times\mathbf{J}^2 \text{ par } \mathbf{I}\times(\mathbf{I}^2\times\mathbf{J}^2).$$

On aurait aussi bien pu faire des calculs, en apparence plus directs. Par exemple un calcul de congruences arithmétiques donne:

$$\mathbf{I}^2\times\mathbf{J}^2 = (25,\ \theta+4)\times(49,\ \theta-8) = (25\times 49,\ \theta-596).$$

La décomposition de $F(596)$ donne la congruence:

$$F(596) = 358\,925 = (25\times 49)\times 293 \Rightarrow \mathbf{I}^2\times\mathbf{J}^2 \sim (293,\ \theta-597).$$

Dans ce dernier idéal la racine minimum est -11; la décomposition de $F(-11) = F(10)$ donne alors la congruence:

$$F(-11) = 3\,223 = 293\times 11 \Rightarrow \mathbf{I}^2\times\mathbf{J}^2 \sim (11,\ \theta-10) = (11,\ \theta+1).$$

36. Corps imaginaires dont le discriminant a deux facteurs premiers.

Dans un corps quadratique imaginaire, *le groupe*, des classes d'idéaux, *ne contient qu'un seul élément d'ordre* 2, qui est une classe double, définie par un idéal réduit remarquable, si et seulement si *le discriminant n'a que deux facteurs premiers différents*, dont l'un peut être 2, à l'exposant 2 ou 3.

S'il en est ainsi *l'ordre du groupe* —ou le nombre des classes— *est pair.*

Si cet ordre n'a pas de facteur carré impair —ou est de la forme:

$2^h\times P$; $\quad h \geqslant 0$;

P produit de nombres premiers impairs différents—

le groupe est cyclique.

La première propriété résulte du théorème d'existence des idéaux réduits remarquables (**30**). L'élément double unique est la classe définie, suivant les cas, par un idéal: double, ou réfléchi, de norme impaire (si $|D|$ est impair); double, de norme 2, si $|D|$ est pair.