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

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

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.

En plus des deux classes, unité et double, il peut y avoir éventuellement des couples de classes conjuguées inégales, donc en tout un nombre pair.

Si un groupe, dont l'ordre est de la forme indiquée, n'est pas cyclique, il a une décomposition minimum en un produit de deux groupes cycliques, de générateurs **I** et **J**, dont les ordres, l'un étant diviseur de l'autre sont nécessairement:

$$m = 2^u, \quad n = 2^v \times P; \qquad 0 < u \leqslant v;$$

il contiendrait alors au moins deux éléments d'ordre 2:

$$\mathbf{I}^{m:2} \qquad \mathbf{J}^{n:2};$$

ce ne peut donc être un groupe de classes de l'un des corps envisagés.

Le tableau XV, disposé comme le tableau XII, donne trois exemples de corps, dont le discriminant a deux facteurs premiers et dont le groupe de classes d'idéaux est cyclique. Pour chacun d'eux on a précisé la structure du groupe, en indiquant, pour chaque idéal réduit, sa congruence avec la puissance de l'un d'entre eux **I**, choisi (convenablement) pour définir une classe génératrice du groupe cyclique. On a limité à cette indication le prolongement de la table des valeurs en deça de O. On a aussi transcrit un sommaire des calculs qui établissent cette structure.

Pour le *premier exemple*, la décomposition du discriminant (impair) —299 = 13×(—23) entraîne l'existence d'un *idéal réduit réfléchi*, —congru à son conjugué— :

$$F(2) = 9^2 \qquad (\mathbf{9}, \quad \theta - 2) \sim (9, \theta + 3).$$

Il y a, d'autre part trois couples d'idéaux réduits conjugués, donc *huit classes*; leur groupe est cyclique, en raison de la remarque générale précédente (l'ordre n'a pas de facteur carré impair).

La table donne immédiatement des valeurs des idéaux conjugués **I** et **I**′, de *norme 5* (de racines minimum 0 et —1), qui sont réduits et de leurs carrés, de *norme 25* et de mêmes racines, qui ne sont pas réduits. La décomposition de $F(0) = 3^4 \times \mathbf{3}$ montre que ces carrés sont congrus aux idéaux réduits, de *norme 3*, de racines —1 et 0.

Tableau XV.

Exemples de corps imaginaires dont le discriminant a deux facteurs premiers.

$D = -299 = 13 \times (-23)$ $r = 5$; ordre **8**	
-2	$(\mathbf{7},\ \theta+2) \sim \mathbf{I}^5$
-1	$(\mathbf{5},\ \theta+1) \sim \mathbf{I}^7$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^2$
0	$75 = 5^2 \times \mathbf{3}$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{3},\ \theta-0) \sim \mathbf{I}^6$ $(\mathbf{5},\ \theta-0) = \mathbf{I}$
$+1$	$77 = 7 \times 11$ $(\mathbf{7},\ \theta-1) \sim \mathbf{I}^3$
$+2$	$81 = 3^4 = 9^2$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^4$
$+3$ $+4$	$87 = 3 \times 29$ $95 = 5 \times 19$
$+5$	$107 = 15 \times \mathbf{7}$

$\mathbf{I}^2 = (5^2,\ \theta-0)$
$\sim (\mathbf{3},\ \theta+1)$; $[F(0)]$
$\mathbf{I}^8 \sim (\mathbf{3},\ \theta+1)^4$
$\sim (1)$; $[F(2)]$
$\mathbf{I}^2 \times \mathbf{I} \sim (15,\ \theta-5)$
$\sim (\mathbf{7},\ \theta-1)$, $[F(5)]$

$D = -404 = (-4) \times 101$ $r = 6$; ordre **14**	
-4	$(\mathbf{9},\ \theta+4) \sim \mathbf{I}^{12}$
-3	$(\mathbf{10},\ \theta+3) \sim \mathbf{I}^3$
-2	$(\mathbf{7},\ \theta+2) \sim \mathbf{I}^9$ $(\mathbf{5},\ \theta+2) \sim \mathbf{I}^4$
-1	$(\mathbf{6},\ \theta+1) \sim \mathbf{I}^6$ $(\mathbf{3},\ \theta+1) \sim \mathbf{I}^{13}$
0	101 $(\mathbf{1},\ \theta-0) = (1)$
$+1$	$102 = 2 \times 3 \times 17$ $(\mathbf{2},\ \theta-1) \sim \mathbf{I}^7$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$ $(\mathbf{6},\ \theta-1) \sim \mathbf{I}^8$
$+2$	$105 = (3 \times 5) \times \mathbf{7}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^{10}$ $(\mathbf{7},\ \theta-2) \sim \mathbf{I}^5$
$+3$	$110 = 2 \times 5 \times 11$ $(\mathbf{10},\ \theta-3) \sim \mathbf{I}^{11}$
$+4$	$117 = 3^2 \times 13$ $(\mathbf{9},\ \theta-4) = \mathbf{I}^2$
$+5$	$122 = 2 \times 61$
$+7$ $+13$	$150 = 30 \times \mathbf{5}$ $270 = 27 \times \mathbf{10}$

$\mathbf{I}^3 = (3^3,\ \theta-13) \sim (\mathbf{10},\ \theta+3)$; $[F(13)]$
$\mathbf{I}^3 \times \mathbf{I} \sim (30,\ \theta-7) \sim (\mathbf{5},\ \theta+2)$; $[F(7)]$
$\mathbf{I}^3 \times \mathbf{I}^2 \sim (\mathbf{2},\ \theta-0)$

$D = -344 = 8 \times (-43)$ $r = 6$; ordre **10**	
-2	$(\mathbf{9},\ \theta+2) = \mathbf{I}^2$ $(\mathbf{6},\ \theta+2) \sim \mathbf{I}^6$ $(\mathbf{5},\ \theta+2) \sim \mathbf{I}^3$
-1	$(\mathbf{3},\ \theta+1) \sim \mathbf{I}^9$
0	$86 = 2 \times 43$ $(\mathbf{1},\ \theta-0) = (1)$ $(\mathbf{2},\ \theta-0) \sim \mathbf{I}^5$
$+1$	$87 = 3 \times 29$ $(\mathbf{3},\ \theta-1) = \mathbf{I}$
$+2$	$90 = (3^2 \times 5) \times \mathbf{2}$ $(\mathbf{5},\ \theta-2) \sim \mathbf{I}^7$ $(\mathbf{6},\ \theta-2) \sim \mathbf{I}^4$ $(\mathbf{9},\ \theta-2) \sim \mathbf{I}^8$
$+3$ $+4$ $+5$	$95 = 5 \times 19$ $102 = 2 \times 3 \times 17$ $111 = 3 \times 37$
$+7$	$135 = 27 \times \mathbf{5}$

$\mathbf{I}^3 = (3^3,\ \theta-7)$
$\sim (\mathbf{5},\ \theta+2)$; $[F(7)]$
$\mathbf{I}^3 \times \mathbf{I}^2 \sim (45,\ \theta+2)$
$\sim (\mathbf{2},\ \theta-0)$ $[F(2)]$

La décomposition de $F(2) = 3^4$ montre que ces idéaux ont leur puissance d'exposant 4, congrue à (1). Il en résulte que les classes définies par **I**, ou **I**$'$ sont d'*ordre 8* et peuvent (chacune) servir de générateur au groupe cyclique, qui a le même ordre. Ces considérations donnent les puissances de **I** qui sont congrues aux idéaux, de *normes 5*, *3*, *9* (idéal réfléchi). Les produits des idéaux, de normes 3 et 5 (congrus à $\mathbf{I}^2$ et **I**, et à leurs conjugués respectifs) donnent des idéaux de *norme 15* et de racines 5 et —6. La décomposition $F(5) = 15 \times \mathbf{7}$, adjointe à la table montre qu'ils sont congrus aux idéaux réduits de *norme 7*.

Dans le *deuxième exemple*, l'idéal de norme 2 est *réduit double* et il y a six couples d'idéaux réduits conjugués; en tout *quatorze classes*; leur groupe est cyclique, pour la même raison.

La table des valeurs donne immédiatement les couples d'idéaux conjugués réduits **I** et **I**$'$, de *norme 3* et de racines (minimum) 1 et —1 ainsi que leurs carrés, de *norme 9* et de racines 4 et —4. Un calcul de congruence arithmétique (**15**) donne la forme canonique de leurs cubes, de *norme 27* et de racines 13 et —13. La décomposition de $F(13) = 27 \times \mathbf{10}$, dont la valeur est adjointe à la table, montre que ces cubes sont congrus aux idéaux de *norme 10* et de racines —3 et 3.

En multipliant ces idéaux par ceux de norme 3, on obtient des idéaux congrus à $\mathbf{I}^4$ et $\mathbf{I}'^4$, qui sont de *norme 30* et de racines 7 et —7; la décomposition de $F(7) = 30 \times \mathbf{5}$, aussi adjointe à la table, montre qu'ils sont congrus aux idéaux réduits, de *norme 5*.

En multipliant les idéaux réduits, ainsi obtenus congrus à $\mathbf{I}^4$ et $\mathbf{I}^3$

$$(\mathbf{10},\ \theta+3)\times(\mathbf{5},\ \theta+2)$$
$$(\mathbf{2},\ \theta+1)\times(\mathbf{5},\ \theta-2)\times(\mathbf{5},\ \theta+2) \sim (\mathbf{2},\ \theta+1)$$

on constate que $\mathbf{I}^7$ est congru à l'idéal double (d'ordre 2). Les classes définies par **I** et **I**$'$ sont donc d'*ordre 14* et chacune d'elles est générateur du groupe.

On a obtenu, en même temps les puissances de **I** congrues aux idéaux réduits, de *normes 3*, *9*, *10*, *5*, *et 2* (double). Un calcul de multiplication, immédiat, donne les idéaux de *norme 6* et la décomposition de $F(2)$ donne ceux de *norme 7*.

Dans le *troisième exemple*, l'idéal de norme 2 est double et il y a quatre couples d'idéaux conjugués réduits, en tout *dix classes*; leur groupe est cyclique.

Tableau XVI.

Répartition, d'après l'ordre du groupe des classes des Corps quadratiques imaginaires, dont le discriminant D à deux facteurs premiers.

Ordre	$\|D\|$ impair		$\|D\| = 4p$	$\|D\| = 4\times(2p)$
	Idéal réduit réfléchi	Idéal réduit double	*p* premier impair	
2	3×5; 5×7; 7×13; 11×17; 13×31;	3×17; 5×23; 3×41; 5×47; 3×89; 7×61;	4×5; 4×13; 4×37;	8×3; 8×5; 8×11; 8×29;
4	5×11; 17×19; 23×29;	3×13; 5×31; 7×29; 3×73; 7×37; 3×97; 5×71; 3×241; 7×109; 5×191;	4×17; 4×73; 4×97; 4×193;	8×7; 8×17; 8×23; 8×41; 8×71;
6	13×19;	3×29; 3×113; 3×137; 11×41; 5×103; 7×101; 3×257; 5×167; 3×281;	4×29; 4×53; 4×61; 4×109; 4×157;	8×13; 8×19; 8×53; 8×59; 8×101; 8×107;
8	13×23;	5×19; 3×37; 3×61; 5×59; 7×53; 5×79; 3×193; 11×53; 3×313; 11×89; 5×199;	4×41; 4×113; 4×137;	8×31; 8×47; 8×79; 8×89; 8×113;
10	7×17; 11×13; 11×29; 19×41; 23×37;	3×53; 3×101; 5×83; 13×47; 5×127; 3×233; 11×73; 13×71;	4×181; 4×197; 4×229;	8×37; 8×43; 8×61; 8×83; 8×109;
12	17×43;	3×109; 3×181; 5×131; 3×229; 5×151;	4×89; 4×233; 4×241;	»
14	17×23; 19×37; 29×31;	5×43; 7×41; 3×149; 7×73; 5×107; 3×269;	4×101; 4×149; 4×173;	8×67;
16	17×47; 23×41;	11×37; 3×157; 13×43; 5×179;	»	8×73
18	17×31;	5×67; 3×173; 7×97;	»	»
20	»	»	»	8×97; 8×103;

Ordre	$\lvert D\rvert$ impair		$\lvert D\rvert$ pair
	Idéal réduit réfléchi	Idéal réduit double	
22	»	3×197; 7×89; 13×59; 13×67; 3×293;	»
24	»	5×139;	»
26	19×29;	3×317;	»
28	»	3×277;	»
30	»	11×61; 5×163;	»
32	»	7×113;	»
34	»	»	»
36	»	7×137.	»

$$F(x) = x^2+x+240; \quad D = -959 = (-7)\times137; \quad r = 9.$$

c	$F(c)$	Normes	
0	$240 = 2^4\times3\times5$	**2, 3, 4, 5, 6, 8, 10, 12, 15.**	$(\mathbf{2},\ \theta-0)^4\times(\mathbf{3},\ \theta-0)\times(\mathbf{5},\ \theta-0) \sim (1)$
1	$242 = 2\times11^2$	**11.**	
2	$246 = 2\times3\times41$	**6.**	
3	$252 = 2^2\times3^2\times7$	**7, 9, 12, 14.**	$(\mathbf{2},\ \theta+1)^4\times(\mathbf{3},\ \theta-0)^4 \sim (1)$
4	$260 = 2^2\times5\times13$	**10, 13.**	
5	$270 = 2\times3^3\times5$	**15.**	$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^3\times(\mathbf{5},\ \theta+1) \sim (1)$
6	$282 = 2\times3\times47$		
7	$296 = 2^3\times37$		$(\mathbf{2},\ \theta-0)\times(\mathbf{3},\ \theta-0)^8 \sim (1)$
8	$312 = 2^3\times3\times13$		$(\mathbf{3},\ \theta-0)^{36} \sim (1)$
9	$330 = 2\times3\times5\times11$		

La table des valeurs donne immédiatement les couples d'idéaux conjugués **I** et **I**$'$, réduits, de *norme 3* et de racines (minimum) 1 et —1, ainsi que leurs carrés, de *norme 9* et de racines —2 et 2. On calcule encore leurs cubes, qui sont de *normes 27* et de racines 7 et —7. La décomposition $F(7) = 27 \times \mathbf{5}$, adjointe à la table, montre qu'ils sont congrus aux idéaux, de *norme 5* et de racines —2 et 2.

Les produits des idéaux de norme 9 et 5, donnent des idéaux congrus à $\mathbf{I}^5$ et $\mathbf{I}'^5$; ils sont de *norme 45* et de racines $+2$ et -2; la décomposition de $F(2) = 45 \times \mathbf{2}$ montrent qu'ils sont congrus à l'*idéal double* (d'ordre 2). Les idéaux **I** et **I**$'$ définissent donc des classes d'ordre 10, qui peuvent servir chacune de générateur au groupe cyclique.

On a obtenu, en même temps les puissances de **I**, qui sont congrues aux idéaux, de *normes 3*, *9*, *5*, *2* (double); pour les idéaux de *norme 6*, elles s'obtiennent par un calcul immédiat de multiplication.

Comme dans ces exemples, on constate que, pour tous les corps, dont le discriminant est de valeur absolue inférieure à 1 000 et a seulement deux facteurs premiers différents, le groupe des classes d'idéaux est cyclique, son ordre étant un des nombres pairs de 2 à 36 [à l'exception des corps de discriminant —4 et —8, qui sont principaux; (**34**)]. Le tableau XVI en donne une répartition, d'après l'ordre de leur groupe, en distinguant, pour les discriminants pairs, ceux qui ont un *facteur* 4, ou 8 et, pour les discriminants impairs la nature de l'idéal (unique) réduit remarquable: *réfléchi*, ou *double* (**29**).

On peut affirmer à priori que les groupes de ces différents corps sont cycliques, par la seule considération de leur ordre qui n'a pas de facteur impair carré. Il y a exception pour les quatre corps dont le groupe est d'ordre 18 et pour celui dont cet ordre est 36; il convient alors de faire une vérification.

On peut à cet effet chercher les idéaux réduits qui sont congrus aux puissances de l'un d'entre eux, convenablement choisi; ou former deux sous-groupes cycliques *indépendants*, dont le produit des ordres est égal à celui du groupe; si ces ordres sont premiers entre eux, le groupe est cyclique (**26**).

C'est ainsi que dans le corps de polynôme fondamental:

$$F(x) = x^2+x+170, \qquad D = -679 = (-7)\times 97,$$

l'idéal réduit (**2**, θ—0) engendre un sous-groupe cyclique, d'ordre 9, qui ne contient pas la classe double définie par l'idéal réduit de norme 7, diviseur de D. Le groupe qui a dix-huit classes est égal au produit direct du sous-groupe cyclique d'ordre 9 et de celui d'ordre 2, engendré par la classe double. Il est donc cyclique d'ordre 18.

On peut dans certains cas faire une vérification plus rapide, qui n'exige pas le calcul complet de la structure. Un exemple en est donné pour le corps de *discriminant* $-959 = (-7)\times 137$, dont le groupe est d'ordre 36: (suite du *tableau XVI*).

On a seulement indiqué, dans le tableau de valeurs, les normes des idéaux réduits; il y en a six qui sont des nombres premiers 2, 3, 5, 7 (idéal double), 11, 13. On s'occupe d'abord des relations entre les idéaux correspondants. Les décompositions de:

$$F(0) = F(-1), \qquad F(3) = F(-4), \qquad F(5) = F(-6)$$

donnent des relations entre les idéaux, des quatre premières normes, sous formes de monômes congrus à (1). On peut remplacer chaque monôme par celui des idéaux conjugués; c'est ce qui a été fait en utilisant la décomposition de $F(-6)$ au lieu de $F(5)$. Le monôme qui résulte de la décomposition de $F(3)$ contient l'idéal double, de norme 7, dont le carré est congru à (1), le carré de ce monôme qui est toujours congru à (1), est alors congru à un monôme des seuls idéaux, de normes 2 et 3.

On a ainsi formé trois monômes, des idéaux de normes 2, 3, 5, respectivement congrus à (1). En les multipliant convenablement, on peut obtenir des relations plus simples (le produit de deux idéaux conjugués est congru à (1) et peut être supprimé dans un monôme). On obtient notamment en formant le produit des trois monômes [l'idéal $(3, \theta-0)$ étant désigné par $\mathbf{I}$]:

$$(2, \theta-0)\times\mathbf{I}^8 \sim (1) \quad \Leftrightarrow \quad (2, \theta+1) \sim \mathbf{I}^8;$$

puis par combinaison avec la deuxième relation:

$$\mathbf{I}^{36} \sim (1); \qquad (3, \theta+1) \sim \mathbf{I}^{35}; \qquad (2, \theta-0) \sim \mathbf{I}^{28}.$$

Les décompositions résultant de la table, permettent alors de former les puissances de $\mathbf{I}$, auxquelles sont congrus les idéaux réduits de normes: 5 [$F(0)$]; 13 [$F(8)$]; 11 [$F(9)$ adjoint à la table]; 7 [$F(3)$]; pour ce dernier dont l'ordre est 2, on peut affirmer à priori, qu'il est congru à $\mathbf{I}^{18}$. Les expressions des autres idéaux réduits dont les normes sont composées avec ces nombres premiers s'obtiennent par multiplication.

Comme dans le cas d'un discriminant premier, il semble que ce soit seulement pour des valeurs relativement grandes de $|D|$ qu'il soit possible d'obtenir des groupes de classes non cycliques. Un exemple en est donné dans le tableau XVII, disposé comme le tableau XIV, qui concerne le corps de discriminant —19 451 = (—43)×437.

Il a dix-huit classes d'idéaux, dont une classe double représentée par l'idéal réduit double de norme 43. Leur groupe n'est pas cyclique: il a une *décomposition minimum* en un produit direct de sous-groupes cycliques d'ordres 3 et 6 et ses éléments peuvent être représentés par les monômes (indiqués dans le tableau):

$$\mathbf{I}^x \times \mathbf{J}^y; \quad x, \quad \text{mod. } 3; \quad y, \quad \text{mod. } 6.$$

La vérification peut être faite comme suit: la décomposition de $F(0) = 17^3$ montre que les idéaux de norme 17, forment avec (1), un *sous-groupe cyclique*, d'ordre 3. La décomposition de $F(21) = 5^3 \times 43$ montre que les idéaux, de normes 5 et 25 ont leur troisième puissance congru à l'idéal double, de norme 7; ils définissent, par suite, avec cet idéal et (1), un *sous-groupe de six classes*, *cyclique*, indépendant du précédent (dont il ne contient pas d'élément, sauf (1)). Le groupe est donc égal au produit direct de ces deux sous-groupes; il n'a aucun élément d'ordre 18 et il n'est pas cyclique.

On peut préciser sa structure en calculant les idéaux réduits congrus aux divers monômes en **I** et **J**; c'est ce qui a été indiqué dans le tableau; la première congruence résulte d'un calcul de multiplication d'idéaux canoniques, de normes premières entre elles, obtenus successivement:

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

37. Corps imaginaires, dont le discriminant a plus de deux facteurs premiers.

Le discriminant est alors décomposable, au moins de deux façons, en un produit de deux facteurs. Il en résulte l'existence