# 54. Corps à deux classes doubles.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

Les seuls corps, de discriminant inférieur à 1000, vérifiant les conditions précédentes et qui ne sont pas principaux, sont ceux de discriminant:

$$321 = 3\times107,\quad 469 = 7\times67,\quad 473 = 11\times43,\quad 993 = 3\times331;$$
$$316 = 4\times79,\quad 892 = 4\times223;\quad 568 = 8\times71;$$

qui comprennent chacun un cycle principal et un couple de cycles conjugués formant par suite un *groupe d'ordre* 3, *cyclique*,

et le corps de discriminant $817 = 19\times43$, qui comprend, en plus du cycle principal, deux couples de cycles conjugués, formant *un groupe d'ordre* 5, *cyclique.*

## 54. Corps à deux classes doubles.

Par un raisonnement analogue aux précédents (**52** et **53**), on peut caractériser les corps qui ont deux et seulement deux classes doubles d'idéaux.

*Condition suffisante.* — Un corps réel a deux, et seulement deux, classes doubles d'idéaux lorsque son discriminant a l'une des formes suivantes:

1. il est impair, nécessairement congru à $+1$, mod. 4, *égal à un produit* $u\times v$, *de deux nombres premiers*, *congrus chacun à* $+1$, mod. 4;

2. il est pair, *égal au produit par* 4, *du double* $2d'$, *d'un nombre premier* $d'$, *congru à* $+1$, mod. 4;

[Dans ces deux cas les classes doubles sont caractérisées par *deux cycles*, soit du *type* 1 (d'un nombre impair de termes), soit *l'un du type* 2 *et l'autre du type* 3 (tous deux d'un nombre pair d'éléments).]

3. il est impair, *égal à un produit* $u\times v\times w$, *de trois nombres premiers*, *dont un est congru à* $+1$ *et chacun des deux autres à* $-1$, mod. 4;

4. il est pair, *égal au produit par* 4, *d'un produit* $d = u\times v$, ou du double $d = 2d'$, d'un produit $d' = u'\times v'$, *de deux nombres premiers*, *dont l'un est congru à* $+1$ *et l'autre à* $-1$, mod. 4;

5. il est pair, égal *au produit par 4 du double* $d = 2d'$, *d'un produit* $d' = u' \times v'$, *de deux nombres premiers, congrus chacun à* —1, mod. 4.

[Dans ces trois cas, les classes doubles sont caractérisées par deux cycles du type 2 (d'un nombre pair de termes).]

L'un des cycles contenant nécessairement l'idéal unité est principal; il peut exister, en outre, des cycles du type 4, répartis par couples de cycles conjugués, chacun ayant un nombre de termes de même parité que celui des termes du cycle principal.

Dans les cas 1 et 2, $D$ ou $d = 2d'$, considéré dans le corps $\mathbf{R}(i)$, est la norme d'un produit de deux idéaux premiers du premier degré (non rationnels); il est donc décomposable de deux façons en une somme de deux carrés et le corps contient deux idéaux semi réduits réfléchis.

D'autre part, dans chaque cas il existe deux (et seulement deux) idéaux doubles, dont les normes sont les diviseurs du discriminant: 1 et le plus petit des entiers $u$ et $v$, pour le premier cas; 1 et 2 pour le second cas (d'après le raisonnement déjà fait ci-dessus lorsque $d'$ est congru à —1; **53**).

Il y a donc quatre (et seulement quatre) idéaux semi réduits remarquables donc deux cycles contenant chacun deux d'entre eux. Ils sont du type 1 si chacun contient un idéal double et un idéal réfléchi; ils sont l'un du type 2, l'autre du type 3, dans le cas contraire.

Dans les cas 3 à 5, $D$ ou $d$, qui contient au moins un facteur premier, congru à —1, mod. 4, n'est pas égal à une somme de deux carrés; le corps ne contient pas d'idéal semi réduit réfléchi.

Par contre il y a quatre (et seulement quatre) idéaux semi réduits doubles dont les normes sont, suivant le cas:

3 — 1, $u$ ou $v \times w$, $v$ ou $w \times u$, $w$ ou $u \times v$;
4 — 1, 2, $u$ ou $v$, $2u$ ou $2v$;
5 — 1, 2, $u'$ ou $2v'$, $v'$ ou $2u'$.

Il y a donc encore quatre idéaux semi réduits remarquables, donc deux cycles, mais chacun d'eux est du type 2.

Dans chacun des 5 cas, le corps a donc deux classes doubles. Si ces classes (ou ces cycles) existent seules, elles constituent *un groupe, d'ordre* 2, *cyclique*.

Dans le cas contraire, *l'ordre du groupe des classes est pair* (deux classes doubles et des couples de classes conjuguées). Si cet ordre est le double d'un produit de nombres premiers impairs différents, le groupe est cyclique. Il l'est encore si ces nombres premiers comprennent un facteur 2 (notamment si l'ordre est égal à 4); car un produit direct d'un groupe d'ordre pair par un

TABLEAU XXIX.

Exemples de corps à deux classes doubles.

| $c$ | $D = 685 = 5 \times 137$<br>$-(x^2+x-171)$ | $D = 689 = 13 \times 53$<br>$-(x^2+x-172)$ | $D = 904 = 8 \times 113$<br>$-(x^2-226)$ | $c$ |
|---|---|---|---|---|
| 0 | 171 | 172 | 226 | 0 |
| 1 | $169 = 13 \times 13;\ \mathbf{V}_2 \times \mathbf{V}_2$ | 170 | $225 = 15 \times 15;\ \mathbf{V}_1 \times \mathbf{V}_1$ | 1 |
| 2 | $165 = 15 \times 11;\ \mathbf{U}_1 \times \mathbf{U}_5$ | 166 | 222 | 2 |
| 3 | 159 | $160 = 16 \times 10;\ \mathbf{U}_1 \times \mathbf{U}_4$ | 217 | 3 |
| 4 | 151 | 152 | $210 = 15 \times 14;\ \mathbf{K}_1 \times \mathbf{K}'_3$ | 4 |
| 5 | 141 | 142 | 201 | 5 |
| 6 | 129 | $130 = 10 \times 13;\ \mathbf{U}_2 \times \mathbf{U}_3$ | $190 = 10 \times 19;\ \mathbf{J}_1 \times \mathbf{J}'_1$ | 6 |
| 7 | 115 | 116 | 177 | 7 |
| 8 | $99 = 11 \times 9;\ \mathbf{U}_2 \times \mathbf{U}_4$ | $100 = 5 \times 20;\ \mathbf{I}_2 \times \mathbf{I}'_2$<br>$= 10 \times 10;\ \mathbf{V}_2 \times \mathbf{V}_2$ | $162 = 9 \times 18;\ \mathbf{K}_3 \times \mathbf{K}'_1$ | 8 |
| 9 | $81 = 9 \times 9;\ \mathbf{U}_3 \times \mathbf{U}_3$ | 82 | 145 | 9 |
| 10 | 61 | 62 | $126 = 6 \times 21;\ \mathbf{I}_1 \times \mathbf{I}'_1$<br>$= 18 \times 7;\ \mathbf{K}_4 \times \mathbf{K}'_0$<br>$= 14 \times 9;\ \mathbf{K}_2 \times \mathbf{K}'_2$ | 10 |
| 11 | $39 = 3 \times 13;\ \mathbf{V}_1 \times \mathbf{V}_3$ | $40 = 20 \times 2;\ \mathbf{I}_3 \times \mathbf{I}'_0$<br>$= 4 \times 10;\ \mathbf{V}_1 \times \mathbf{V}_3$<br>$= 8 \times 5;\ \mathbf{I}_1 \times \mathbf{I}'_2$ | $105 = 21 \times 5;\ \mathbf{I}_2 \times \mathbf{I}'_0$<br>$= 7 \times 15;\ \mathbf{K}_0 \times \mathbf{K}'_4$ | 11 |
| 12 | $15 = 1 \times 15;\ \mathbf{U}_0 \times \mathbf{U}_6$<br>$= 5 \times 3;\ \mathbf{V}_0 \times \mathbf{V}_4$<br>. . . . . . . . . . . . | $16 = 1 \times 16;\ \mathbf{U}_0 \times \mathbf{U}_5$<br>$= 2 \times 8;\ \mathbf{I}_0 \times \mathbf{I}'_3$<br>$= 4 \times 4;\ \mathbf{V}_0 \times \mathbf{V}_0$<br>. . . . . . . . . . . . | 82 | 12 |
| 13 | | | $57 = 19 \times 3;\ \mathbf{J}_2 \times \mathbf{J}'_0$ | 13 |
| 14 | | | $30 = 2 \times 15;\ \mathbf{V}_0 \times \mathbf{V}_2$<br>$= 3 \times 10;\ \mathbf{J}_0 \times \mathbf{J}'_2$<br>$= 5 \times 6;\ \mathbf{I}_0 \times \mathbf{I}'_2$ | 14 |
| 15 | | | $1 = 1 \times 1;\ \mathbf{U}_0 \times \mathbf{U}_0$ | 15 |
| | Ordre 2 | Ordre 4 | Ordre 8 | |
| | $(\theta-1) = \mathbf{V}_2 \times \mathbf{V}_2$<br>$\mathbf{V}^2 \sim 1$ | $(\theta-12) = \mathbf{I}_0'^4$<br>$\mathbf{I}^4 \sim 1$ | $(\theta-8) = \mathbf{J}_0'^4 \times \mathbf{V}_0$<br>$\mathbf{J}^8 \sim \mathbf{V}^2 \sim 1$ | |

groupe d'ordre 2 contient au moins deux termes d'ordre 2; or la classe double non principale est le seul terme d'ordre 2, du groupe des classes.

Pour des discriminants peu élevés, on constate encore que, pour une assez grande proportion d'entre eux, il n'y a pas de cycles de type 4, et que, par suite leur groupe est d'ordre 2 et cyclique. Pour les discriminants inférieurs à 1000, il y a ainsi 91 corps qui n'ont que deux classes d'idéaux [la classe principale et une classe égale à sa conjuguée et de carré égal à la classe principale]. Ils se répartissent suivant les cinq conditions précédentes en:

21 (condition 1); 12 (2°); 20 (3°); 32 (4°); 6 (5°).

Les seuls corps qui, en vérifiant les conditions précédentes ont un groupe d'ordre supérieur à 2 (ou contiennent des cycles de type 4) sont: ceux de discriminants:

$$145 = 5 \times 29, \quad 445 = 5 \times 89, \quad 505 = 5 \times 101, \quad 689 = 13 \times 53,$$

$$793 = 13 \times 61, \quad 901 = 17 \times 53, \quad 905 = 5 \times 181; \quad 328 = 8 \times 41;$$

$$777 = 3 \times 7 \times 37; \quad 897 = 3 \times 13 \times 23; \quad 876 = 4 \times 3 \times 73;$$

qui ont un *groupe*, *d'ordre* 4, *cyclique;*

ceux de discriminants:

$$785 = 5 \times 157, \quad 985 = 5 \times 197; \quad 940 = 4 \times 235;$$

qui ont un *groupe d'ordre* 6, *cyclique*;

et celui de discriminant $904 = 8 \times 113$, qui a un *groupe d'ordre* 8, et qui est *cyclique*, car il ne contient qu'un seul terme d'ordre 2.

Le tableau XIX donne des exemples de calcul des idéaux semi réduits et de vérification de la structure des groupes pour trois corps, [deux classes doubles] dont les discriminants sont:

$685 = 5 \times 137$ (premier cas de la condition) qui a deux cycles d'un nombre impair d'idéaux (7 et 5), du type 1;

$689 = 13 \times 53$ (même cas) qui a deux cycles de type 2 et 3, d'un nombre pair d'idéaux (6 et 4) et un couple de cycles conjugués de type 4, de chacun quatre idéaux. Son groupe est d'ordre 4, cyclique;

$904 = 8 \times 113$ (deuxième cas), qui a deux cycles de type 1 contenant un et trois idéaux et trois couples de cycles conjugués de type 4, contenant respectivement trois, trois et cinq idéaux. Son groupe est d'ordre $2+2 \times 3 = 8$, cyclique.

### 55. Corps à plus de deux classes doubles.

Les conditions, énoncées ci-dessus, *suffisantes* pour qu'un corps contienne seulement une ou deux classes doubles d'idéaux, sont aussi *nécessaires:* si elles ne sont pas vérifiées par le discriminant, le corps a au moins trois classes doubles. Cette propriété peut être explicitée sous forme d'une condition suffisante analogue aux précédentes.

Un corps réel a *au moins trois classes doubles* d'idéaux lorsque son discriminant $D$ a l'une des formes suivantes:

1. il est impair, nécessairement congru à $+1$, mod. 4, *égal à un produit* $u \times v \times w$, de trois nombres premiers, *congrus chacun à* $+1$, mod. 4;

2. il est pair, égal au *produit par* 4, *du double* $2d'$ d'un produit $d' = u' \times v'$, de deux nombres premiers, *congrus chacun à* $+1$, mod. 4;

3. Il est impair, nécessairement congru à $+1$, mod. 4, égal à un *produit de plus de trois nombres premiers impairs.*

4. Il est pair, produit par 4 d'un nombre impair $d$, congru à $-1$, mod. 4, ou du double $2d'$ d'un nombre impair $d'$, *produit d'au moins trois nombres premiers impairs.*

Il est équivalent de dire que $D$ vérifie ces conditions, ou ne vérifie pas les conditions précédentes; c'est ce qui résulte du tableau des diverses conditions: