# 23. Congruence et classes d'idéaux

On obtient 8 progressions arithmétiques, dont on donne encore les premiers nombres premiers (inférieurs à 500), ainsi que la norme minimum positive de l'un des idéaux dont ils sont la norme:

$1+15\lambda$: 61 (25); 181 (14); 241 (16); 421 (65);
$7+15\lambda$: 7 (1); 67 (22); 127 (53); 307 (130); 367 (105); 487 (224);
$11+15\lambda$: 11 (2); 71 (21); 131 (43); 191 (46); 251 (39); 311 (126); 431 (51); 491 (83);
$17+15\lambda$: 17 (7); 137 (17); 197 (58); 257 (23); 317 (40);
$43+15\lambda$: 43 (12); 103 (18); 163 (34); 223 (98); 283 (79); 463 (101);
$49+15\lambda$: 109 (48); 229 (106); 349 (109); 409 (158);
$53+15\lambda$: 53 (11); 113 (44); 173 (19); 233 (99); 293 (111); 353 (108);
$59+15\lambda$: 59 (29); 179 (33); 239 (60); 359 (71); 419 (68); 479 (203).

*Il y a une infinité* de nombres premiers vérifiant les conditions précédentes, donc d'*idéaux premiers du premier degré*, dans tout corps quadratique.

On peut le démontrer en s'inspirant du raisonnement arithmétique qui est utilisé couramment pour démontrer l'existence d'une infinité de nombres premiers. On forme le produit $C$, des $m$ premiers nombres premiers $p_i$, à l'exception des diviseurs du discriminant $D$. Le nombre entier $C^2-D$ admet un diviseur premier $p$, supérieur à tous les $p_i$, et qui vérifie la condition imposée [1]).

## 23. Congruence et classes d'idéaux.

De même qu'on a construit le groupe quotient $\mathcal{G}|\mathfrak{L}$, des classes du groupe $\mathcal{G}(\theta)$, relativement au sous-groupe $\mathfrak{L}$, des

[1]) Cette propriété résulte aussi du *théorème de la progression arithmétique*, qui affirme l'existence d'une infinité de nombres premiers dans chacune des progressions arithmétiques, construites comme il a été dit, de raison $|D|$ et dont les premiers termes sont premiers avec $|D|$. Ceci montre aussi bien l'existence d'une infinité d'idéaux premiers du second degré —ou de nombres premiers ne vérifiant pas la condition imposée—. On pourrait aussi en donner une démonstration directe, mais sans distinguer l'appartenance des normes aux différentes progressions.

idéaux principaux rationnels (**14 bis**), on peut construire le groupe quotient $\mathcal{G}|\mathcal{R}$, relativement au sous-groupe $\mathcal{R}$, des idéaux principaux $(\rho)$. Il peut être utile de donner une construction directe de cette répartition, en définissant d'abord une *congruence* —ou un mode d'égalité— .

DÉFINITION. — *Deux idéaux*, non nuls, d'un corps $\mathbf{R}(\theta)$, *sont* **congrus** [sous entendu, mod. $\mathcal{R}$] *lorsque leur quotient est égal à un idéal principal.*

Cette relation est désignée par le signe $\sim$, séparant les idéaux congrus; elle a les qualités d'une égalité. Elle est *réflexive* ($\mathbf{I} \sim \mathbf{I}$) le quotient d'un idéal par lui-même est l'idéal unité qui est principal. Elle est *symétrique*, l'ordre du quotient est indifférent: si $\mathbf{I}\times\mathbf{J}^{-1}$ est principal, il en est de même de $\mathbf{J}\times\mathbf{I}^{-1}$, qui est l'idéal inverse. Elle est *transitive*:

$$\{\mathbf{I} \sim \mathbf{J} \quad \text{et} \quad \mathbf{J} \sim \mathbf{K}\} \quad \Rightarrow \quad \mathbf{I} \sim \mathbf{K};$$

car si les quotients $\mathbf{I}\times\mathbf{J}^{-1}$ et $\mathbf{J}\times\mathbf{K}^{-1}$ sont des idéaux principaux, il en est de même de $\mathbf{I}\times\mathbf{K}^{-1}$, qui est égal à leur produit.

Il est équivalent de dire que deux idéaux sont congrus, si l'un d'eux, et, par suite, chacun d'eux, est égal au produit de l'autre par un idéal principal $(\rho)$ non nul, ou par la base $\rho$ de cet idéal:

$$\mathbf{I} \sim \mathbf{J} \quad \Leftrightarrow \quad \text{Existe } \rho \neq 0 \quad \text{et} \quad \mathbf{I} = (\rho)\times\mathbf{J} \quad \text{ou} \quad \rho\times\mathbf{J}.$$

*La multiplication et la division conservent —ou sont compatibles avec— la congruence*: des produits et des quotients d'idéaux respectivement congrus, sont des idéaux congrus.

En effet si $\mathbf{I}\times\mathbf{I}_1^{-1}$ et $\mathbf{J}\times\mathbf{J}_1^{-1}$ sont des idéaux principaux, il en est de même des idéaux:

$$(\mathbf{I}\times\mathbf{J})\times(\mathbf{I}_1\times\mathbf{J}_1)^{-1} = (\mathbf{I}\times\mathbf{I}_1^{-1})\times(\mathbf{J}\times\mathbf{J}_1^{-1});$$

$$(\mathbf{I}\times\mathbf{J}^{-1})\times(\mathbf{I}_1\times\mathbf{J}_1^{-1})^{-1} = (\mathbf{I}\times\mathbf{I}_1^{-1})\times(\mathbf{J}\times\mathbf{J}_1^{-1})^{-1};$$

qui en sont un produit et un quotient.

*La conjugaison conserve —ou est compatible avec— la congruence*: les idéaux conjugués de deux idéaux congrus sont congrus: si $\mathbf{I}\times\mathbf{J}^{-1}$ est principal, il en est de même de $\mathbf{I}'\times(\mathbf{J}')^{-1}$, qui est son conjugué.

DÉFINITION. — Dans un corps quadratique, on appelle **classe d'idéaux** (sous-entendu mod. $\mathcal{R}$) toute famille d'idéaux formée par *ceux qui sont congrus à un idéal non nul.*

En raison de la transitivité de la congruence, les idéaux d'une classe sont congrus entre eux, deux à deux; la classe peut être définie —ou engendrée— par un de ses idéaux, choisi arbitrairement.

Les classes d'idéaux, dans un corps constituent une *répartition* de l'ensemble —ou du groupe $\mathcal{G}$— des idéaux non nuls: tout idéal appartient à une classe (celle qu'il engendre); deux classes qui ont un idéal commun sont égales.

On peut **multiplier** les classes d'idéaux d'un corps: l'ensemble des produits de tout idéal **A**, d'une classe $\mathcal{A}$, par tout idéal **B**, d'une classe $\mathcal{B}$ (éventuellement égale à $\mathcal{A}$) est une classe, qui est appelée le **produit** (de la multiplication) des classes et qui est désignée par $\mathcal{A}\times\mathcal{B}$.

Les produits $\mathbf{A}\times\mathbf{B}$ sont congrus entre eux, en raison de la conservation de la congruence dans la multiplication. En outre tout idéal **I** congru à un produit $\mathbf{A}\times\mathbf{B}$ est lui-même égal à un produit, puisque:

$$\mathbf{I} = (\mathbf{A}\times\mathbf{B})\times\rho = \mathbf{A}\times(\mathbf{B}\times\rho);$$

et $\mathbf{B}\times\rho$ appartient à $\mathcal{B}$.

La multiplication des classes ainsi définie, s'étend à plusieurs facteurs; elle est manifestement *associative* et *commutative*, comme celle des idéaux (**12**), qui sert à la définir. Elle permet de définir les puissances (d'exposants entiers positifs) d'une classe.

La **classe principale** est la famille —ou le groupe— $\mathcal{R}$, de tous les idéaux principaux $(\rho)$, non nuls, qui sont manifestement tous ceux qui sont congrus à l'un quelconque d'entre eux.

Cette classe est un *élément neutre* —ou *unité*— pour la multiplication (des classes): toute classe est égale à son produit par $\mathcal{R}$:

$$\mathcal{A}\times\mathcal{R} = \mathcal{A}; \quad \text{notamment} \quad \mathcal{R}^2 = \mathcal{R}\times\mathcal{R} = \mathcal{R}.$$

*Deux classes* $\mathcal{A}$ et $\mathcal{A}'$ (notées par une même lettre avec et sans accent) *sont* **conjuguées**, *lorsque l'une*, et, par suite, chacune d'elles, *est constituée par les idéaux conjugués de tous les idéaux de l'autre.*

Les conjugués des idéaux d'une classe sont en effet congrus entre eux, en raison de la conservation de la congruence dans la conjugaison, et la relation est réciproque. Pour que deux classes soient conjuguées, il suffit que l'une contienne le conjugué d'*un* idéal de l'autre.

*Deux classes sont* **inverses** (au sens général de ce qualificatif) —ou chacune d'elles est l'inverse de l'autre— *lorsque leur produit est égal à la classe principale* —ou classe unité— .

*Deux classes conjuguées sont inverses et réciproquement*:

$$\mathcal{A}\times\mathcal{A}' = \mathcal{R} \quad \text{et} \quad \mathcal{A}\times\mathcal{A}^{-1} = \mathcal{R} \quad \Rightarrow \quad \mathcal{A}^{-1} = \mathcal{A}'.$$

D'une part, le produit $\mathcal{A}\times\mathcal{A}'$ de deux classes conjuguées contient le produit $\mathbf{A}\times\mathbf{A}'$ de deux idéaux conjugués, qui est égal à l'idéal principal (rationnel), $(N(\mathbf{A}))$, dont la base est la norme (commune) des idéaux conjugués (**13**); c'est donc la classe $\mathcal{R}$, des idéaux principaux. Inversement si deux idéaux sont inverses, l'associativité de la multiplication montre qu'ils sont conjugués:

$$\mathcal{A}\times\mathcal{A}^{-1} = \mathcal{R} \quad \Rightarrow \quad (\mathcal{A}'\times\mathcal{A})\times\mathcal{A}^{-1} = \mathcal{A}'\times\mathcal{R} \quad \Rightarrow \quad \mathcal{A}^{-1} = \mathcal{A}'.$$

Deux classes conjuguées sont donc, chacune constituée par les inverses des idéaux de l'autre. C'est aussi bien une conséquence de la construction de l'inverse (**14**); l'idéal $\mathbf{A}'\times(N(\mathbf{A}))^{-1}$ est à la fois inverse de $\mathbf{A}$ et congru à son conjugué $\mathbf{A}'$.

Un raisonnement général (déjà utilisé ci-dessus pour la division des idéaux; **14**) permet de déduire de l'*existence* d'une classe inverse, *la possibilité et la détermination de la division* des classes.

Etant données une classe dividende $\mathcal{D}$ et une classe diviseur $\mathcal{A}$, *il existe une et une seule classe* $\mathcal{B}$, appelée **quotient** de $\mathcal{D}$ par $\mathcal{A}$, *dont le produit* (de la multiplication) *par* $\mathcal{A}$ *est égal à* $\mathcal{D}$.

Ce quotient est égal au *produit de la classe dividende par l'inverse* —ou la conjuguée— *de la classe diviseur.*

C'est une conséquence de l'associativité de la multiplication:

$$\mathcal{A}\times\mathcal{B} = \mathcal{D} \quad \Leftrightarrow \quad (\mathcal{A}'\times\mathcal{A})\times\mathcal{B} = \mathcal{A}'\times\mathcal{D} \quad \Leftrightarrow \quad \mathcal{B} = \mathcal{A}'\times\mathcal{D}.$$

Cette règle comprend, comme cas particulier, la construction, déjà faite, du quotient de la classe principale —ou unité— $\mathcal{R}$, par une classe $\mathcal{A}$, qui est égal à la classe conjuguée —ou inverse— $\mathcal{A}'$.

*Une classe est* **double**, *lorsqu'elle est égale à sa conjuguée*, qui est aussi son inverse, son carré est égal à $\mathcal{R}$.

Pour qu'une classe soit double, il suffit qu'elle contienne deux idéaux conjugués; notamment un idéal double.

Les qualités de la multiplication et de la division des classes peuvent encore être exprimées (partiellement) par la constitution d'un *groupe* (ainsi qu'il a déjà été dit, dans un corps $\mathbf{R}(\theta)$, pour ses éléments non nuls (**1**); pour ses idéaux non nuls (groupe $\mathcal{G}$) et pour ses idéaux principaux rationnels (groupe $\mathfrak{Q}$) [**14** et **14** *bis*].

Dans un corps quadratique, *les classes d'idéaux* (mod. $\mathcal{R}$) *forment un groupe multiplicatif abélien*, dont l'élément unité est la classe principale $\mathcal{R}$, qui peut être aussi désignée par (1).

Ce groupe contient les *puissances* $\mathcal{A}^x$, d'exposant $x$, entier quelconque (**14**), d'une classe $\mathcal{A}$, et les *monômes* —ou produits— de puissances de classes $\mathcal{A}^x \times \mathcal{B}^y \times \ldots$ Toutes les puissances de $\mathcal{R}$ sont égales à elle-même.

On aurait pu construire ce groupe des classes en utilisant des *propriétés générales des groupes abéliens.*

Dans le groupe multiplicatif $\mathcal{G}(\theta)$, des idéaux non nuls (**14 bis**), les idéaux principaux ($\rho$) constituent évidemment un sous-groupe $\mathcal{R}$, (contenant lui-même le sous-groupe $\mathfrak{Q}$ des idéaux principaux rationnels). Deux idéaux de $\mathcal{G}$ sont *congrus* lorsque leur quotient est dans $\mathcal{R}$, ce qui est une propriété réciproque en raison de la commutativité de la multiplication.

Les *classes d'idéaux* sont les *classes de répartition* des éléments du groupe $\mathcal{G}$, relativement au sous-groupe $\mathcal{R}$; on vérifie d'une façon générale qu'elles se multiplient et se divisent et constituent par suite un groupe multiplicatif abélien, qui est appelé (généralement) *groupe quotient* $\mathcal{G}|\mathcal{R}$, de $\mathcal{G}$ par $\mathcal{R}$.

Un **corps principal** (**19**) ne contient que la seule classe principale, qui constitue, à elle seule, un groupe d'un seul élément unité.

On étudie ci-dessous la structure du *groupe des classes*, dans un corps quadratique quelconque et on montre notamment qu'il ne contient qu'*un nombre fini de classes* —ou qu'il est d'*ordre fini*— .