5. Congruence fondamentale (module premier).

5. Congruence fondamentale (module premier).

L'arithmétique d'un corps quadratique $\mathbf{R}(\theta)$ est intimement liée à l'étude de son polynôme fondamental, considéré dans l'*anneau des nombres entiers, définis à un module entier m près*, —ou des *classes d'entiers*, mod. *m*—. C'est cette étude que précisent les définitions et les propriétés suivantes.

DÉFINITIONS. — On appellera **congruence fondamentale**, mod. m, de $\mathbf{R}(\theta)$, l'équation congruentielle, obtenue en écrivant que le polynôme fondamental du corps $F(x)$, est *congru* à 0, mod. m:

$$x^2 - Sx + N \equiv 0, \quad (\text{mod. } m).$$

L'étude de cette équation en x, consiste à chercher les valeurs entières c, de la variable x, telles que $F(c)$, qui est un nombre entier, soit divisible par m. S'il en existe, elles se répartissent en progressions arithmétiques, de raison m, doublement illimitées:

$$c + \lambda m; \qquad \lambda \text{ nombre entier quelconque.}$$

En effet l'égalité:

$$F(c+\lambda m) = F(c) + m \times (\text{un nombre entier}),$$

montre que tous les nombres entiers $F(c+\lambda m)$ sont divisibles par m, s'il en est ainsi de l'un d'eux.

Une telle progression, $c+\lambda m$, est couramment appelée une *classe d'entiers, mod. m* —ou un *entier défini, mod. m*— .

On appellera **zéro, mod.** m, de $F(x)$ —ou *solution* de la congruence fondamentale— indifféremment: *une progression* $c+\lambda m$, dont chaque terme donne à $F(x)$ une valeur $F(c+\lambda m)$ divisible par m; ou *un seul des termes* de cette progression, choisi arbitrairement, ou précisé par une condition convenable.

On peut d'abord établir une propriété générale, valable pour tout module m.

THÉORÈME des zéros conjugués. — Les solutions de la congruence fondamentale, s'il en existe, forment *un, ou plusieurs*,

couples de zéros mod. m, de $F(x)$. *Les deux zéros d'un couple ont une somme congrue à* S, mod. m:

$$c = c_0+\lambda m, \quad c' = c'_0+\lambda' m; \qquad c+c' \equiv S, \quad (\text{mod. } m);$$

ils sont appelés **conjugués** et désignés par une même lettre avec et sans accent (comme les éléments conjugués du corps).

Deux zéros conjugués sont égaux si et seulement si m est diviseur du discriminant D; leur valeur commune est alors appelée **zéro double.**

L'existence d'un zéro c entraîne celle de son conjugué c', car, d'après les calculs évidents de congruences, mod. m:

$$\left.\begin{array}{l} c+c' \equiv S, \\ \text{et} \\ c^2-Sc+N \equiv 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} c\times c' \equiv c\times(S-c) \equiv \mathrm{N} \\ \qquad\qquad\qquad\qquad (\text{mod. } m) \\ F(x) \equiv (x-c)\times(x-c') \end{array}\right.$$

En outre la congruence:

$$(c-c')^2 \equiv S^2-4N = D, \quad (\text{mod. } m),$$

montre que les deux zéros sont congrus —ou les deux progressions sont égales—, si et seulement si D est congru à 0, mod. m.

Pour qu'un zéro soit double il faut et il suffit qu'il annule, mod. m, le polynôme dérivé:

car:
$$\dot{F}(x) = 2x-S;$$
$$c \equiv c' \Leftrightarrow 2c \equiv S, \quad (\text{mod. } m).$$

On peut remarquer que ces calculs de congruences peuvent, aussi bien, être considérés comme des calculs [d'addition, soustraction et multiplication] entre les m classes d'entiers, mod. m:

$$0+\lambda m,\ 1+\lambda m,\ \ldots,\ (m-1)+\lambda m,$$

qui constituent un *anneau commutatif avec unité* —ou au sens restreint— .

Théorème de la congruence fondamentale pour un module premier. — Lorsque le module de la congruence fondamentale est un nombre premier p,

1. Si p *ne divise pas* le discriminant D:
ou bien la congruence est *impossible*;

ou bien elle a un et un seul couple de solutions inégales —ou $F(x)$ a *un et un seul couple de zéros conjugués incongrus*— ;

2. Si p *est diviseur* de D (notamment si $p = 1$), la congruence a deux solutions confondues —ou $F(x)$ a *un et un seul zéro double*— .

La première partie du théorème peut être complétée par des *propriétés caractéristiques de possibilité*:

pour un module premier p *impair*, ne divisant pas le discriminant D, la congruence fondamentale est possible, si, et seulement si, *il existe un entier, dont le carré soit congru à* D, *mod.* p. On exprime parfois cette existence en disant que D est **résidu quadratique** du nombre premier p.

pour le *module premier* 2, si le discriminant est impair, le polynôme fondamental est de la forme:

$$F(x) = x^2+x+N; \quad [S = -1; \quad D = 1-4N];$$

la congruence fondamentale est possible si, et seulement si, N *est pair*. Les deux zéros conjugués de $F(x)$ sont 0 et 1, (mod. 2).

1. Lorsque m est égal à un nombre premier p, pair ou impair, si la congruence est possible, le polynôme $F(x)$ a, au moins, un couple de zéros (conjugués), c et c', peut être égaux, et il est congru à un produit de binômes. *Il n'a pas alors d'autre zéro*, car la congruence

$$(x-c)\times(x-c') \equiv 0, \quad (\text{mod. } p),$$

exige que l'un au moins des facteurs soit divisible par p, c'est-à-dire que x soit congru à c ou à c'.

On peut exprimer ce raisonnement en disant que l'*anneau des* p *classes d'entiers, mod.* p, est un **domaine d'intégrité**, c'est-à-dire qu'un produit de deux facteurs ne peut être nul, que s'il en est ainsi de (au moins) l'un des facteurs. [C'est même un **corps**, car tout élément non nul, y possède un inverse.]

Pour un module p, *premier impair*, on peut utiliser le produit du polynôme $F(x)$ par 4:

$$4F(x) = (2x-S)^2-D;$$

l'existence d'un zéro est équivalente à celle d'un nombre entier $(2c—S)$, dont le carré est congru à D, mod. p.

Pour le *module premier* $p = 2$, il n'y a que deux classes d'entiers, représentés respectivement par 0 et 1; il suffit de former les valeurs qu'elles donnent à $F(x) = x^2+x+N$:

$$F(0) \equiv F(1) \equiv N, \quad (\text{mod. } 2);$$

d'où la condition d'existence.

2. Pour un *module premier impair* p, *diviseur de* D, l'expression de $4F(x)$ est congrue à:

$$4F(x) = (2x—S)^2—D \equiv (2x—S)^2, \quad (\text{mod. } p);$$

elle montre qu'il existe un et un seul zéro c, mod. p, qui rend $(2c—S)$ divisible par p. Suivant le cas, il est congru à:

$$c \equiv 0, \quad \text{si } S = 0; \qquad c \equiv \frac{p—1}{2}, \quad \text{si } S = —1.$$

Pour le *module* 2, lorsque D est pair, S est nul, la congruence:

$$x^2+N \equiv 0, \quad (\text{mod. } 2)$$

a une et une seule solution (zéro double), congrue à:

$$0, \quad \text{si } N \text{ est pair}; \qquad 1, \quad \text{si } N \text{ est impair}.$$

Pour $p = 1$, la propriété est triviale, il n'y a qu'une seule classe, formée de tous les nombres entiers et elle est zéro double de $F(x)$.

6. Congruence fondamentale (module composé).

On considère d'abord un *module primaire* —ou puissance d'un nombre premier > 1— .

Théorème de la congruence fondamentale pour un module primaire. Relativement à un *module* p^h, puissance (d'exposant h, entier positif), d'un nombre premier p, différent de 1, le polynôme fondamental $F(x)$: