Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 6 (1960)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: L'ARITHMÉTIQUE DES CORPS QUADRATIQUES
Autor: Châtelet, Albert
Kapitel: 1. Construction d'un corps quadratique.
DOI: https://doi.org/10.5169/seals-36338

CHAPITRE I

IDÉAUX D'UN CORPS QUADRATIQUE

1. Construction d'un corps quadratique.

Un *corps quadratique est caractérisé par un nombre entier*, d, différent de 0 et de $+1$, sans facteur carré; ou, plus précisément, *par le trinome du second degré normé* (de premier coefficient égal à $+1$), *appelé* **polynôme fondamental** *du corps*:

$$F(x) = x^2 - Sx + N,$$

dont les coefficients sont, suivant la divisibilité de $d-1$ par 4:

$d-1$ div. par 4:

$$S = -1, \quad N = (1-d):4, \quad 4F(x) = (2x+1)^2 - d;$$

$d-1$ non div. par 4:

$$S = 0, \quad N = -d, \quad F(x) = x^2 - d.$$

Ce trinôme peut être mis sous la forme (commune aux deux cas):

$$4F(x) = (2x-S)^2 - D; \quad D = S^2 - 4N = \begin{cases} d \\ 4d \end{cases};$$

D est appelé le **discriminant** du corps.

Le trinôme est *irréductible* —ou sans zéro rationnel—, puisque D n'est pas carré parfait (le cas $d = +1$ —ou $D = +4$— étant exclus).

Si d —donc aussi D— est positif, le trinôme a deux zéros *réels*, (non rationnels), on dit que le corps est *réel*; si d —donc D— est négatif, le trinôme a deux zéros *complexes*, le corps est dit *imaginaire*.

On peut donner du corps diverses *constructions* équivalentes:

Le **corps quadratique**, caractérisé par le polynôme fondamental $F(x)$, désigné par $\mathbf{R}(\theta)$, *peut être obtenu en « adjoignant »*, par addition, soustraction et multiplication, *au corps* **R**, des nombres rationnels, *un symbole* —ou *générateur*—, désigné par θ, *qui se comporte comme un zéro de* $F(x)$.

On peut entendre par là que ce corps $\mathbf{R}(\theta)$ est l'ensemble des valeurs $f(\theta)$, des expressions entières —ou polynômes— $f(x)$, à coefficients rationnels, pour la valeur θ, de l'indéterminée x. Toutefois chacune d'elles est (considérée comme) *égale* à la valeur $r+s\theta$, du binôme:

$$r+sx = f(x)—F(x)\times q(x),$$

reste de la division (euclidienne) de $f(x)$ par le polynôme $F(x)$.

Il est équivalent de dire qu'un *élément* de $\mathbf{R}(\theta)$ est l'*ensemble des expressions* (considérées comme) *égales entre elles*:

$r+s\theta+F(\theta)\times q(\theta)$; $q(x)$ polynôme à coefficients dans **R**; (la valeur $F(\theta)$ se comportant comme un *élément nul*).

On se borne, ordinairement, à utiliser les expressions linéaires $r+s\theta$, les autres servant seulement à définir, [ou à justifier], leur calcul. Deux éléments sont égaux, si et seulement si leurs expressions linéaires ont des *coefficients* (rationnels) égaux:

$$(r+s\theta) = (r'+s'\theta) \quad \Leftrightarrow \quad \{r = r' \quad \text{et} \quad s = s'\}.$$

Les règles explicites des *opérations internes* (*addition*, de signe $+$, *multiplication*, de signe $\times$) se déduisent du « comportement » de θ ou de la règle du reste (qui revient à remplacer θ^2 par $S\theta—N$):

$$(r+s\theta)+(r'+s'\theta) = (r+r')+(s+s')\theta;$$
$$(r+s\theta)\times(r'+s'\theta) = (rr'—Nss')+(rs'+sr'+Sss')\theta.$$

Ces règles (ou le calcul des expressions entières et la règle du reste), montrent que ces deux opérations ont les qualités usuelles: elles sont *associatives*, *commutatives* et la multiplication est *distributive* relativement à l'addition.

Les binômes $0+0\theta$ (en abrégé 0) et $1+0\theta$ (en abrégé 1), sont les éléments *nul* (neutre pour l'addition) et *unité* (neutre pour la multiplication). Chaque élément $r+s\theta$ a un *opposé* déterminé:

$$(-r)+(-s)\theta = (-1+0\theta)\times(r+s\theta), \text{ en abrégé } -(r+s\theta).$$

La somme de deux opposés est égale à l'élément nul, la *soustraction* (opération inverse de l'addition) est possible et déterminée: soustraire un élément est équivalent à additionner son opposé [1]).

On peut aussi considérer que *le corps quadratique* $\mathbf{R}(\theta)$ *est un ensemble d'éléments*, désignés par les lettres grecques $\rho,\alpha,\beta,\ldots$, qui sont des *formes* (linéaires) de deux symboles: 1 (*unité*) et θ *générateur*:

$$\rho = r\times(1)+s\times(\theta), \quad \text{en abrégé } r+s\theta;$$

dont les *variables*, ou *multiplicateurs*, des symboles 1 et θ, désignées par des lettres latines: $r,s,a,b,\ldots$ sont des *nombres rationnels.*

Les opérations (addition, soustraction, multiplication), entre ces éléments sont les mêmes qu'entre les formes; toutefois la multiplication, distributive relativement à l'addition, est définie par la table de multiplication (commutative et associative) des symboles:

$$(1)\times(1) = (1); \quad (1)\times(\theta) = (\theta)\times(1) = (\theta);$$
$$(\theta)\times(\theta) = -N+S\theta.$$

Les éléments, pour lesquels le multiplicateur de θ est nul:

$$r\times(1)+0\times\theta, \quad \text{en abrégé } r,$$

qui comprennent les éléments nul, et unité, sont appelés les *éléments rationnels* du corps; ils se calculent entre eux (égalité et opérations) comme les nombres rationnels (éléments du corps $\mathbf{R}$).

De la construction adoptée pour $\mathbf{R}(\theta)$, il résulte que, dans cet ensemble, *le polynôme fondamental* $F(x)$ *est décomposable en* —ou égal à— *un produit de deux binômes linéaires normés*:

$$F(x) = (x-\theta)\times(x-\theta'); \quad \theta' = S\times(1)+(-1)\times\theta, \quad \text{ou} \quad S-\theta.$$

On peut dire que, dans $\mathbf{R}(\theta)$, $F(x)$ a deux *zéros* θ *et* θ', tels que:

[1]) On reconnaît, dans ce calcul, une construction analogue à celle des *nombres complexes*, dans le corps des nombres réels, par les congruences de Cauchy. Plus généralement, on peut dire que $\mathbf{R}(\theta)$ est isomorphe à l'anneau quotient $\mathbf{R}(x)|F(x)$; [$\mathbf{R}(x)$ anneau des polynômes à coefficients rationnels; $F(x)$ polynôme fondamental].

$$\theta+\theta' = S; \quad \theta\times\theta' = N; \quad (\theta—\theta')^2 = S^2—4N = D.$$

Le corps $\mathbf{R}(\theta)$ peut être construit aussi avec les deux symboles: l'unité 1 et le générateur θ', moyennant la correspondance (biunivoque) suivante des multiplicateurs:

$$r+s\theta = r'+s'\theta' \Leftrightarrow r' = r+sS \quad \text{et} \quad s' = —s.$$

1. 2. *Inverses et division.*

L'irréductibilité de $F(x)$ —ou l'inexistence de zéro rationnel— permet d'affirmer que: *tout élément* $\rho = r+s\theta$, *non nul*, de $\mathbf{R}(\theta)$, *a un et un seul* **inverse**, c'est-à-dire qu'*il existe un élément* (unique), désigné (suivant la notation habituelle) par ρ^{-1}, *tel que le produit* $\rho\times\rho^{-1}$ *soit égal à l'élément unité* $+1$.

Pour obtenir cet inverse, on peut calculer le produit:

$$(r+s\theta)\times(r+s\theta') = r^2+Srs+Ns^2 = s^2\times F(—r:s) = q;$$

c'est un *élément rationnel* du corps, qui n'est pas nul (r et s ne l'étant pas simultanément), puisque $F(x)$ n'a pas de zéro rationnel. Le quotient de $r+s\theta'$ par ce nombre rationnel q:

$$\rho^{-1} = \frac{r}{q}+\frac{s}{q}\theta', \quad \text{ou} \quad \frac{r+Ss}{q}—\frac{s}{q}\theta;$$

est l'inverse cherché puisque $\rho\times\rho^{-1} = q:q = +1$.

Un raisonnement (de caractère général) montre que l'existence de l'inverse de ρ entraîne *la possibilité et la détermination* [1]), *de la* **division** *par* ρ (inverse de la multiplication) et, notamment la détermination de cet inverse lui-même (*quotient* de la division par ρ de l'élément unité):

$$\xi\times\rho = \sigma \quad \Leftrightarrow \quad (\xi\times\rho)\times\rho^{-1} = \sigma\times\rho^{-1} \quad \Leftrightarrow \quad \xi = \sigma\times\rho^{-1}.$$

L'ensemble des *éléments non nuls*, de $\mathbf{R}(\theta)$, entre lesquels existe une *multiplication* associative, et commutative, ainsi que l'opération inverse de *division*, est un **groupe** *multiplicatif abélien.*

[1]) Par *possibilité* on entend qu'il existe un quotient; par *détermination*, on entend que ce quotient est unique.

L'ensemble $\mathbf{R}(\theta)$, formé de ce groupe et de l'élément nul, est un **corps**, au sens général de ce terme (ce qui justifie le nom de *corps quadratique*). L'ensemble des éléments rationnels r, de $\mathbf{R}(\theta)$, en est un **sous-corps**, **isomorphe** —ou, par abréviation, égal— *au corps* **R**, des nombres rationnels (inversement $\mathbf{R}(\theta)$ est **sur corps** de **R**).

La construction de l'addition, de la soustraction et de la multiplication et les qualités de ces opérations resteraient valables, même sans l'hypothèse d'irréductibilité de $F(x)$; les inverses n'existeraient alors que pour certains des éléments $r+s\theta$ (ceux pour lesquels $-r:s$ n'annule pas $F(x)$). L'ensemble construit serait seulement un **anneau**, commutatif avec une unité, —ou au sens restreint— .

On peut aussi considérer que $\mathbf{R}(\theta)$ est un *sous-corps* du *corps* des nombres: *réels* si D est positif; *complexes* si D est négatif. Cette conception fournit encore une justification des règles de calcul, y compris la division. Elle sera utilisée ci-dessous pour établir la détermination des cycles d'idéaux semi-réduits, dans un corps réel (**46** et **47**).

2. Eléments conjugués.

DÉFINITION. — Dans le corps quadratique $\mathbf{R}(\theta)$, *deux éléments sont appelés* **conjugués**, ou chacun d'eux est le conjugué de l'autre, *lorsqu'ils sont égaux*, respectivement, *à des formes de* 1, θ *et de* 1, θ', *avec les mêmes multiplicateurs* (nombres rationnels). Ils sont désignés par la même lettre, avec et sans accent (comme θ et θ', qui sont des éléments conjugués particuliers):

$$\rho = r+s\theta = (r+Ss)-s\theta' \quad \Leftrightarrow \quad \rho' = r+s\theta' = (r-Ss)-s\theta.$$

Un élément du corps est *égal à son conjugué*, si et seulement si c'est un *élément rationnel* (coefficient de θ nul). Pour le vérifier, il suffit de former la différence de deux conjugués:

$$0 = \rho-\rho' = s\times(\theta-\theta') = -Ss+2s\theta = Ss-2s\theta' \quad \Leftrightarrow \quad s = 0.$$

Les éléments θ et θ' sont conjugués et inégaux.

Deux éléments de $\mathbf{R}(\theta)$, *obtenus en remplacant* x *par* θ *et* θ',