

**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>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 17.07.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

## 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 trinôme 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  $\mathbf{R}$ , des nombres rationnels, un symbole —ou générateur—, désigné par  $\theta$ , 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  $\theta$ , de l'indéterminée  $x$ . Toutefois chacune d'elles est (considérée comme) égale à la valeur  $r+s\theta$ , du binôme:

$$r+s\theta = f(x) - F(x) \times q(x),$$

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  $\mathbf{R}$ ; (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:

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

Les règles explicites des opérations internes (addition, de signe +, multiplication, de signe  $\times$ ) se déduisent du « comportement » de  $\theta$  ou de la règle du reste (qui revient à remplacer  $\theta^2$  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<sup>1)</sup>.

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

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

dont les *variables*, ou *multiplicateurs*, des symboles 1 et  $\theta$ , désignées par des lettres latines:  $r, s, a, b, \dots$  sont des *nombre 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:

$$\begin{aligned} (1) \times (1) &= (1); & (1) \times (\theta) &= (\theta) \times (1) = (\theta); \\ (\theta) \times (\theta) &= -N + S\theta. \end{aligned}$$

Les éléments, pour lesquels le multiplicateur de  $\theta$  est nul:

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

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*:

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

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

<sup>1)</sup> 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  $\theta'$ , 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  $\rho^{-1}$ , 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  $\rho$  entraîne *la possibilité et la détermination* <sup>1)</sup>; *de la division par*  $\rho$  (inverse de la multiplication) et, notamment la détermination de cet inverse lui-même (*quotient* de la division par  $\rho$  de l'élément unité):

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

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**.

<sup>1)</sup> 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*  $\mathbf{R}$ , des nombres rationnels (inversement  $\mathbf{R}(\theta)$  est **sur corps** de  $\mathbf{R}$ ).

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. Éléments 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  $1, \theta$  et de  $1, \theta'$ , avec les mêmes multiplicateurs (nombres rationnels). Ils sont désignés par la même lettre, avec et sans accent (comme  $\theta$  et  $\theta'$ , qui sont des éléments conjugués particuliers):

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

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

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

Les éléments  $\theta$  et  $\theta'$  sont conjugués et inégaux.

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