Mathematics. — *Les systèmes hypercomplexes non commutatifs de deuxième ordre.* By F. LOONSTRA. (Communicated by Dr. A. HEYTING.)

(Communicated at the meeting of January 31, 1948.)

§ 1. Soient R un corps commutatif, **P** le système hypercomplexe de deuxième ordre induit par R. Les éléments de **P** s'écrivent sous la forme $a\, e_1 + b\, e_2$. En désignant une table de multiplication **P** est complètement défini. Il sera possible de caractériser les systèmes non commutatifs de deuxième ordre. Supposons en général:

$$e_1 e_1 = a_{11} e_1 + b_{11} e_2 \qquad e_2 e_1 = a_{21} e_1 + b_{21} e_2$$
$$e_1 e_2 = a_{12} e_1 + b_{12} e_2 \qquad e_2 e_2 = a_{22} e_1 + b_{22} e_2,$$

les conditions suffisantes et nécessaires pour les a_{ik} et b_{ik} s'expriment par $(e_m e_n) e_p = e_m (e_n e_p)$.

De $(e_1 e_1) e_1 = e_1 (e_1 e_1)$ il s'ensuit:

$$a_{11} e_1 e_1 + b_{11} e_2 e_1 = a_{11} e_1 e_1 + b_{11} e_1 e_2 \quad \text{ou} \quad b_{11} (e_1 e_2 - e_2 e_1) = 0.$$

De la supposition $b_{11} \neq 0$ il résulte en multipliant par b_{11}^{-1}: $e_1 e_2 = e_2 e_1$, alors **P** serait commutatif. Par conséquent:

$$b_{11} = 0. \qquad (1)$$

De $(e_2 e_2) e_2 = e_2 (e_2 e_2)$ il s'ensuit: $a_{22} (e_1 e_2 - e_2 e_1) = 0$, alors

$$a_{22} = 0. \qquad (2)$$

De $(e_1 e_1) e_2 = e_1 (e_1 e_2)$ il s'ensuit (à l'aide de (1) et (2)):

$$b_{12} (a_{11} - b_{12}) e_2 = b_{12} a_{12} e_1. \qquad (3)$$

En vertu de l'indépendance de e_1 et e_2 les coëfficients de e_1 et e_2 seront nuls, ce qui donne lieu aux cas suivants:

$$a_{12} = 0,\ a_{11} = b_{12} \quad (3a), \qquad b_{12} = 0 \qquad (3b)$$

Si nous poursuivons ($3a$), la condition $e_1 (e_2 e_2) = (e_1 e_2) e_2$ sera remplie; en effet, en multipliant on trouvera

$$(b_{22} - a_{12}) a_{12} e_1 = a_{12} b_{12} e_2.$$

En outre la validité de $(e_1 e_2) e_1 = e_1 (e_2 e_1)$ sera garantie, parce qu'on trouve $a_{11} (a_{12} - a_{21}) e_1 = (b_{21} a_{12} - b_{12} a_{21}) e_1$.

De $e_2 (e_1 e_1) = (e_2 e_1) e_1$ il s'ensuit $b_{21} (a_{11} - b_{21}) e_2 = b_{21} a_{21} e_1$ donnant lieu aux cas

$$a_{21} = 0,\ a_{11} = b_{21} \quad (4a), \qquad b_{21} = 0 \qquad (4b)$$

Continuons ($3a$, $4a$), il s'ensuit $a_{12} = a_{21} = 0$, $b_{12} = b_{21}$, de sorte que

$\mathbf{P}$ est commutatif. Poursuivant ($3a$, $4b$) il résulte de $(e_2e_1)e_2 = e_2(e_1e_2)$:

$$a_{12}b_{21} + b_{12}b_{22} - a_{21}b_{12} - b_{21}b_{22} = 0,$$

c'est à dire en vertu des dernières conditions: $b_{12}(a_{21} - b_{22}) = 0$, alors

$$b_{12} = 0 \quad (5a) \qquad \text{ou} \qquad a_{21} = b_{22} \quad \ldots\ldots \quad (5b)$$

Continuons ($3a$, $4b$, $5a$): De $(e_2e_2)e_1 = e_2(e_2e_1)$ il résulte

$$(b_{22} - a_{21})\,a_{21}\,e_1 = a_{21}\,b_{21}\,e_2 \quad \ldots\ldots\ldots \quad (6)$$

Le membre droit étant nul on a $(b_{22} - a_{21})a_{21} = 0$. De $a_{21} = 0$ il s'ensuit que $\mathbf{P}$ sera commutatif. Alors $b_{22} = a_{21}$, de sorte que ($3a$, $4b$, $5a$) conduit au système suivant:

$$a_{11} = a_{12} = a_{22} = b_{11} = b_{12} = b_{21} = 0, \; a_{21} = b_{22} \quad \ldots \quad (\mathrm{I}')$$

Poursuivons ($3a$, $4b$, $5b$), la condition (6) est remplie, alors on a

$$\underline{a_{12} = a_{22} = b_{11} = b_{21} = 0; \; a_{11} = b_{12}; \; a_{21} = b_{22}} \quad \ldots \quad (\mathrm{I})$$

Le système (I′) ressortit au système (I).

Continuons le deuxième cas ($3b$): $b_{12} = 0$.

De $(e_2e_1)e_1 = e_2(e_1e_1)$ il résulte

$$b_{21}(a_{11} - b_{21})\,e_2 = b_{21}\,a_{21}\,e_1,$$

de sorte que les coëfficients sont nuls, donnant lieu aux cas suivants:

$$a_{21} = 0, \; a_{11} = b_{21} \quad (7a), \qquad b_{21} = 0 \quad \ldots\ldots \quad (7b)$$

Poursuivons ($3b$, $7a$), la condition $(e_1e_2)e_1 = e_1(e_2e_1)$ est remplie. De $(e_1e_2)e_2 = e_1(e_2e_2)$ on trouve $(b_{22} - a_{12})a_{12}e_1 = a_{12}b_{12}e_2$, alors

$$(b_{22} - a_{12})\,a_{12} = 0, \quad \ldots\ldots\ldots\ldots \quad (8)$$

donnant lieu aux cas:

$$a_{12} = 0 \quad (8a), \qquad a_{12} = b_{22} \quad \ldots\ldots\ldots \quad (8b)$$

Poursuivons d'abord ($3b$, $7a$, $8a$); de $e_2(e_1e_2) = (e_2e_1)e_2$ il résulte $b_{22}b_{21} = 0$; de $b_{21} = 0$ il résulte un anneau $\mathbf{P}$ commutatif, alors

$$a_{12} = a_{21} = a_{22} = b_{11} = b_{12} = b_{22} = 0; \; a_{11} = b_{21} \quad \ldots \quad (\mathrm{II}')$$

Poursuivons ($3b$, $7a$, $8b$): alors on satisfera à la relation $e_2(e_1e_2) = (e_2e_1)e_2$ de même qu'à la relation $(e_2e_2)e_1 = e_2(e_2e_1)$, de sorte qu'on a un système:

$$\underline{a_{21} = a_{22} = b_{11} = b_{12} = 0; \; a_{11} = b_{21}; \; a_{12} = b_{22}} \quad \ldots \quad (\mathrm{II})$$

Le système (II′) ressortit au système (II).

Poursuivons encore ($3b$, $7b$): $b_{12} = b_{21} = 0$. De $e_1(e_2e_1) = (e_1e_2)e_1$ il résulte $a_{11}(a_{12} - a_{21}) = 0$. En excluant $a_{12} = a_{21}$, on a $a_{11} = 0$.

De $e_1(e_2e_2) = (e_1e_2)e_2$ on a: $(b_{22} - a_{12})a_{12} = 0$, alors

$$b_{22} = a_{12} \quad (9a), \qquad a_{12} = 0 \quad \ldots\ldots\ldots \quad (9b)$$

Poursuivons ($9a$), la condition $(e_2e_1)e_2 = e_2(e_1e_2)$ est remplie.

De $(e_2e_2)e_1 = e_2(e_2e_1)$ il s'ensuit $(b_{22} - a_{21})a_{21} = 0$; nous avons seulement $a_{21} = 0$, alors:

$$a_{11} = a_{21} = a_{22} = b_{11} = b_{12} = b_{21} = 0;\ b_{22} = a_{12}; \quad . \quad . \quad \text{(II}')$$

ce cas ressortit aussi au système (II).

En dernier lieu nous continuons (9*b*): $a_{12} = 0$; la condition $(e_2e_1)e_2 = e_2(e_1e_2)$ est remplie. De $(e_2e_2)e_1 = e_2(e_2e_1)$ on trouve $(b_{22} - a_{21})a_{21} = 0$. En excluant $a_{21} = 0$, on a $b_{22} = a_{21}$ donnant lieu de nouveau au système (I). Il résulte que les systèmes hypercomplexes non commutatifs possibles sont d'une structure suivante:

$$\text{(I)}\quad \begin{aligned} e_1e_1 &= a\,e_1 \\ e_1e_2 &= \qquad a\,e_2 \\ e_2e_1 &= b\,e_1 \\ e_2e_2 &= \qquad b\,e_2 \end{aligned} \qquad\qquad \text{(II)}\quad \begin{aligned} e_1e_1 &= a\,e_1 \\ e_1e_2 &= b\,e_1 \\ e_2e_1 &= \qquad a\,e_2 \\ e_2e_2 &= \qquad b\,e_2, \end{aligned}$$

a et b représentant des éléments de R. Les multiplications correspondantes sont:

(I) $(a_1e_1 + b_1e_2)(a_2e_1 + b_2e_2) = (a_1a + b_1b)(a_2e_1 + b_2e_2)$, en particulier pour $a = b = e$ ($=$ unité de R): $(a_1e_1 + b_1e_2)(a_2e_1 + b_2e_2) = (a_1 + b_1)(a_2e_1 + b_2e_2)$.

(II) $(a_1e_1 + b_1e_2)(a_2e_1 + b_2e_2) = (a_2a + b_2b)(a_1e_1 + b_1e_2)$, en particulier pour $a = b = e$: $(a_1e_1 + b_1e_2)(a_2e_1 + b_2e_2) = (a_2 + b_2)(a_1e_1 + b_1e_2)$.

§ 2. Pour la description de quelques propriétés notables de ces systèmes nous nous bornerons — à cause de la symétrie de (I) et (II) — au cas I, tandis que a et b ne sont pas nuls en même temps.

Supposons e l'unité de R, on a la possibilité que P contienne plusieurs unités gauches (par exemple si R contient une infinité d'éléments); une unité droite n'existe pas. En effet, les éléments $a_1e_1 + b_1e_2$ avec $a_1a + b_1b = e$ sont des unités gauches.

De $(a_1e_1 + b_1e_2)(a_2e_1 + b_2e_2) = (a_1a + b_1b)(a_2e_1 + b_2e_2)$ il s'ensuit qu'on ne peut satisfaire à la relation

$$(a_1\,e_1 + b_1\,e_2)(x_1\,e_1 + x_2\,e_2) = (a_1\,a + b_1\,b)(x_1\,e_1 + x_2\,e_2) = a_1\,e_1 + b_1\,e_2$$

pour aucune combinaison (a_1, b_1); alors une unité droite n'existe pas.

L'ensemble des diviseurs de nuls gauches de P *est un idéal premier, bilatère et maximal.* (Dans un anneau A — pas nécessairement commutatif — on dit qu'un idéal $\mathfrak{p} \neq A$ est premier, si la relation $xy \subset \mathfrak{p}$ entraîne au moins une des relations $x \subset \mathfrak{p}$, $y \subset \mathfrak{p}$).

On dit que l'élément $\alpha = a_1e_1 + b_1e_2$ est un diviseur de nul gauche, s'il existe un élément $\beta = a_2e_1 + b_2e_2 \neq 0$ de sorte que $\alpha\beta = 0$. Une condition nécessaire et suffisante pour que α soit un diviseur de nul gauche est $a_1a + b_1b = 0$. En désignant l'ensemble de ces diviseurs de nul par N_g, on a: N_g est un idéal; soient $\alpha = a_1e_1 + b_1e_2$ et $\beta = a_2e_1 + b_2e_2$ des éléments de N_g, c'est à dire $a_ia + b_ib = 0$ $(i = 1, 2)$, on a en outre

$(a_1 - a_2)a + (b_1 - b_2)b = 0$, alors $\alpha - \beta$ est un diviseur de nul gauche.

Soit $\alpha = a_1e_1 + b_1e_2$ un élément de N_g, $\beta = a_2e_1 + b_2e_2$ un élément quelconque, $\alpha\beta$ aussi bien que $\beta\alpha$ appartient à N_g: d'abord $\alpha\beta = 0$, tandis que $\beta\alpha = (a_2e_1 + b_2e_2)(a_1e_1 + b_1e_2) = (a_2a + b_2b)(a_1e_1 + b_1e_2)$, alors

$$(a_2 a + b_2 b) a_1 a + (a_2 a + b_2 b) b_1 b = (a_2 a + b_2 b)(a_1 a + b_1 b) = 0.$$

Il s'ensuit que N_g est un idéal bilatère. En outre il résulte que N_g soit un idéal premier; en effet, soit

$$(a_1 e_1 + b_1 e_2)(a_2 e_1 + b_2 e_2) = (a_1 a + b_1 b)(a_2 e_1 + b_2 e_2)$$

un élément de N_g, on a: $(a_1a + b_1b)(a_2a + b_2b) = 0$ et parce que R ne contient pas de diviseurs de nuls, on au moins une des possibilités $a_1a + b_1b = 0$ ou $a_2a + b_2b = 0$.

Quant à la propriété maximale de N_g nous remarquons: soit

$$\alpha = a_1e_1 + b_1e_2$$

un élément de P ($\not\subset N_g$), on a pour tout $\beta = a_2e_1 + b_2e_2$ de P une solution de l'équation $\alpha \cdot x = \beta$; en effet, de $(a_1a + b_1b)(x_1e_1 + x_2e_2) = a_2e_1 + b_2e_2$ il s'ensuit $x_1 = a_2 : (a_1a + b_1b)$, $x_2 = b_2 : (a_1a + b_1b)$. La solution est univoque, parce que de $\alpha x = \alpha y$ on tire $\alpha(x - y) = 0$ et α n'étant pas un diviseur de nul gauche, on a $x = y$. Chaque élément α ($\not\subset N_g$) engendra — en multipliant à droite par un élément de P convenable — tout l'anneau P. Maintenant il est évident que N_g est un idéal maximal de P.

L'anneau quotient P/N_g de P par la congruence modulo l'idéal N_g des diviseurs de nuls gauches est isomorphe au corps R.

Démonstration: La relation d'équivalence $x - y \subset N_g$, définie par l'idéal bilatère N_g, se note le plus souvent $x \equiv y \pmod{N_g}$, ou $x \equiv y(N_g)$. Les relations $x \equiv y(N_g)$, $x' \equiv y'(N_g)$ entraînent donc $x + x' \equiv y + y'(N_g)$, $xx' \equiv yy'(N_g)$ et $x'x \equiv y'y(N_g)$. La relation de congruence mod N_g donne lieu à une ensemble de classes de congruences. Soit $\alpha = a_1e_1 + b_1e_2$, $\beta = a_2e_1 + b_2e_2$, $\alpha \equiv \beta(N_g)$, on a: $a_1a + b_1b = a_2a + b_2b$, c'est à dire pour deux éléments d'une classe mod N_g la somme $a_1a + b_1b$ est constante. Inversément deux éléments ayant cette propriété appartiennent à la même classe mod N_g. Alors les classes de congruences seront caractérisées par l'élément $r = a_1a + b_1b$, en particulier la classe de nul N_g par 0. Désignons les classes de congruences par (r), N_g par (0), à toute classe correspond un symbole (r) et inversement à tout r de R correspond une une classe (r); (on peut toujours-pour a et b fixe-choisir a_1 et b_1 de sorte que $a_1a + b_1b = r$). Si l'on désigne par $(r) + (s)$ la classe de congruence à laquelle appartient la somme de deux représentants de (r) et (s), par $(r)(s)$ la classe de congruence à laquelle appartient le produit de deux représentants de (r) et (s), on a les propriétés suivantes: $(r) + (s) = (r + s)$, $(r)(s) = (rs)$. Il se trouve alors que ces propriétés valent indépendamment du choix des représentants. Alors, il s'ensuit l'isomorphie de P/N_g au corps R. L'unité de P/N_g est la classe (e) contenant toutes les unités gauches. L'élément inverse de la classe (r), $(r \neq 0)$, est la classe (r^{-1}).