

# SÉMINAIRE DE MATHÉMATIQUES

JEAN DIEUDONNÉ

## **Théorie des corps gauches**

*Séminaire de Mathématiques (Julia)*, tome 1 (1933-1934), exp. n° 7, p. 1-24

[http://www.numdam.org/item?id=SMJ\\_1933-1934\\_\\_1\\_\\_A7\\_0](http://www.numdam.org/item?id=SMJ_1933-1934__1__A7_0)

© École normale supérieure, Paris, 1933-1934, tous droits réservés.

L'accès aux archives du séminaire de mathématiques implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

Exemplaire N° 4

Institut Henri Poincaré -  
Ne peut quitter la salle de travail

SEMINAIRE DE MATHÉMATIQUES

I. - Rappel de définitions et résultats antérieurs.

Tous les corps et algèbres envisagés sont pris sur un même corps de base commutatif et parfait.

Année 1933-1934

On sait qu'un corps commutatif algébrique  $Z$  de degré fini  $n$  sur  $\rho$  est engendré par une racine  $\theta$  d'une équation irréductible de degré  $n$ .

Théorie des Groupes et des Algèbres

Soit  $f(x) = 0$  une équation algébrique à coefficients dans  $\rho$ .

G. - Théorie des Corps Gauches dit galoisien s'il contient aussi les  $n-1$  autres racines de  $f(x) = 0$ . Le groupe des 1-automorphismes de  $Z$  laissant fixes les nombres de  $\rho$  est le groupe de Galois  $G$  de  $Z$ . C'est un groupe d'ordre  $n$  dont chaque substitution change  $\theta$  en une autre racine de  $f(x) = 0$ . Si  $S$  est une substitution de  $G$ , et un nombre de  $Z$ , on désigne par  $s^S$  le transformé de  $s$  par  $S$ .

Exposé fait par Monsieur Jean DIEUDONNE, le 26 Février 1934.

Soit  $A$  une algèbre sur un corps  $K$  (commutatif ou non). Le  $K$ -rang de  $A$  est le nombre d'éléments de base de  $A$ , considéré comme  $K$ -module. On définit de même le  $K$ -rang des idéaux de  $A$ .

Si  $A$  est une algèbre simple, et  $K$  le centre de  $A$ , on sait que le  $K$ -rang de  $A$  est un carré parfait  $m^2$ . On appelle degré d'un élément  $\alpha$  de  $A$  par rapport à  $K$ , le degré minimum du polynôme  $\varphi(x)$  à coefficients dans  $K$ , tel que  $\varphi(\alpha) = 0$ .

On démontre que le degré maximum des éléments de  $A$  est égal à  $m$ .  $m$  est dit le degré de l'algèbre  $A$  par rapport à  $K$ .



K.

2. - Théorie des Produits croisés . ( dGe à Mlle E. Nöther).I. - Rappel de définitions et résultats antérieurs.

Tous les corps et algèbres envisagés sont pris sur un même corps de base commutatif et parfait.

On sait qu'un corps commutatif algébrique  $\zeta$  de degré fini  $n$  sur  $\rho$  est engendré par une racine  $\theta$  d'une équation irréductible de degré  $n$  sur  $\zeta$  est

une algèbre  $A$  comme  $\zeta$ -module à droite de rang  $n$ .  
 $f(x) = 0$   
 à coefficients dans  $\rho$ . Le corps  $\zeta$  est dit galoisien s'il contient aussi les  $n-1$  autres racines de  $f(x) = 0$ . Le groupe des  $\rho$ -automorphismes de  $\zeta$  laissant fixes les nombres de  $\rho$  est le groupe de Galois  $G$  de  $\zeta$ . C'est un groupe d'ordre  $n$  dont chaque substitution change  $\theta$  en une autre racine de  $f(x) = 0$ . Si  $S$  est une substitution de  $G$ ,  $z$  un nombre de  $\zeta$ , on désigne par  $z^S$  le transformé de  $z$  par  $S$ .

Soit  $A$  une algèbre sur un corps  $K$  (commutatif ou non). Le  $K$ -rang de  $A$  est le nombre d'éléments de base de  $A$ , considéré comme  $K$ -module. On définit de même le  $K$ -rang des idéaux de  $A$ .

Si  $A$  est une algèbre simple, et  $K$  le centre de  $A$ , on sait que le  $K$ -rang de  $A$  est un carré parfait  $m^2$ . On appelle degré d'un élément  $\alpha$  de  $A$  par rapport à  $K$ , le degré minimum du polynôme  $\varphi(x)$  à coefficients dans  $K$ , tel que  $\varphi(\alpha) = 0$ . On démontre que le degré maximum des éléments de  $A$  est égal à  $m$ .  $m$  est dit le degré de l'algèbre  $A$  par rapport à



K.

2.- Théorie des Produits croisés. (dûe à Mlle E. Nöther), exposée d'après un mémoire de Hasse, Transactions of the American mathematical society, 1932, t. 34).

Soit  $\mathcal{Z}$  un corps galoisien de degré  $n$  sur  $\rho$ ,  $G$  le groupe de Galois de  $\mathcal{Z}$ ; on désignera par  $S, T, U \dots$  les substitutions de  $G$ , par  $E$  la substitution unité (1) et (2)

Un produit croisé (verschränktes Produkt) sur  $\mathcal{Z}$  est une algèbre  $A$  définie comme  $\mathcal{Z}$ -module à droite de rang  $n$ .

$$A = u_E \mathcal{Z} + u_S \mathcal{Z} + \dots + u_T \mathcal{Z}$$

$u_E, u_S \dots u_T$  désignent la  $\mathcal{Z}$ -base de  $A$  (chaque  $u$  correspondant à une substitution de  $G$ ), la loi de multiplication des deux éléments de  $A$  étant définie par les conditions :

$$(1) \left\{ \begin{array}{l} z u_S = u_S z^S \quad \text{si } z \in \mathcal{Z} \\ u_S u_T = u_{ST} a_{ST} \end{array} \right.$$

où  $a_{ST}$  est un élément  $\neq 0$  de  $\mathcal{Z}$ . L'ensemble des  $n^2$  nombres  $a_{ST}$  constitue le système de facteurs qui définit le produit croisé, et qu'on désigne par (a). Ces  $n^2$  nombres ne sont pas arbitraires : on vérifie que pour que la multiplication soit associative, ils doivent satisfaire aux conditions

$$(2) \quad a_{ST}^U = \frac{a_{STU} a_{TU}}{a_{STU}} \quad \text{pour } S = E, \text{ d'où}$$

Si  $z_1, z_2, \dots, z_n$  est une  $\rho$ -base de  $\mathcal{Z}$ , on voit immédiatement que  $A$  est un système hypercomplexe de rang  $n^2$  sur  $\rho$ , la  $\rho$ -base de  $A$  étant constituée par les éléments



comme on le vérifie sans peine :

$u_s z_k$  La condition nécessaire et suffisante pour que

On écrit :  $A = ( a, \mathbb{Z} )$

Propriétés élémentaires des produits croisés

1°- A possède une unité

$$e = u_E a_{EE}^{-1}$$

comme on le vérifie sans difficulté à l'aide de (1) et (2)  
 On identifie cette unité avec celle de  $\mathbb{Z}$ , en écrivant

$e = 1$ , et par suite :

$$u_E = a_{EE}$$

$\mathbb{Z}$  est donc contenu dans A.

2°-  $\mathbb{Z}$  est un sous-corps commutatif maximum de A; les éléments de  $\mathbb{Z}$  sont les seuls éléments de A commutatifs avec tous les éléments de  $\mathbb{Z}$ .

Soit a un élément de A

$$a = \sum u_s z_s \quad z_s \in \mathbb{Z}$$

tel que :  $az = za$  quel que soit  $z \in \mathbb{Z}$

on en tire d'après (1)

$$\sum u_s z_s (z - z^s) = 0$$

ou  $z_s (z - z^s) = 0$

En prenant pour z un élément primitif de  $\mathbb{Z}$ ,  $z \neq z^s$   
 si  $s \neq E$ , donc  $z_s = 0$ , sauf pour  $s = E$ , d'où

$$a = u_E z_E = a_{EE} z_E \in \mathbb{Z}$$

3°-  $u_s$  possède un inverse  $u_s^{-1}$

$$u_s^{-1} = u_{s^{-1}} a_{ss}^{-1} a_{EE}^{-1}$$

le corps  $\mathbb{Z}$  isomorphe à  $\mathbb{Z}$  est un corps de décomposition de A.



comme on le vérifie sans peine.  $a, b$  un nombre de  $B$

4°- La condition nécessaire et suffisante pour que

soient R.T. ...  $(a, \mathcal{Z}) = (\bar{a}, \mathcal{Z})$  dans  $\mathcal{G}$  pour lesquelles  
est que l'on ait  $\bar{a}$  sont dans  $B$ , quels que soient  $a$  et  $\mathcal{Z}$

$$(3) \quad \bar{a}_{sT} = a_{sT} \frac{c_T c_s^T}{c_s} \quad c_s \neq 0 \text{ et dans } \mathcal{Z}$$

ce qui peut encore s'exprimer en disant que l'on a entre les  
deux  $\mathcal{Z}$ -bases de  $A$  la relation  $\bar{a} = a \frac{c_T c_s^T}{c_s}$  et on arrive finalement

$$(3') \quad \bar{u}_s = u_s c_s. \text{ On écrit dans ce cas } (\bar{a}) \sim (a)$$

a) la condition est nécessaire, car les relations

ce qui montre  $z u_{s-1} = u_{s-1} z^{s-1}$ ,  $z \bar{u}_s = \bar{u}_s z^s$   
valables pour tout  $z \in \mathcal{Z}$ , on en tire que  $u_{s-1}, \bar{u}_s$  est com-  
mutatif avec tous les éléments de  $\mathcal{Z}$ , donc est dans  $\mathcal{Z}$  d'a-  
près 2°- ; par suite, un nombre quelconque de  $A$ . On a

$$(4) \quad u_{s-1} \bar{u}_s = \text{est aussi dans } \mathcal{Z}, \text{ donc :}$$

$(c_{sT})$  étant  $\bar{u}_s = u_s c_s$  ce carré d'ordre  $n$   
d'où la relation (3)

b) la condition est évidemment suffisante, car de (3') on  
tire que  $A$  est un  $\mathcal{Z}$ -module de base  $\bar{u}_s$ , satisfaisant aux  
relations (1) où on remplace les  $a$  par les  $\bar{a}$ , donc que  $A$   
est égal au produit croisé  $(\bar{a}, \mathcal{Z})$ .

### 3.- Structure des produits croisés

Théorème I. 1°) Tout produit croisé est une algèbre simple

2°) Tout corps  $\bar{\mathcal{Z}}$  isomorphe à  $\mathcal{Z}$  est un corps  
de décomposition de  $A$ .



1°)- Soit  $B$  un idéal bilatère de  $A$ ,  $b$  un nombre de  $B$

$$b = \sum u_s y_s \quad y_s \in \bar{Z}$$

Soient  $R, T, \dots, U$  les substitutions de  $G$  pour lesquelles  $y_s \neq 0$ ,  $z b$  et  $b \bar{z}$  sont dans  $B$ , quels que soient  $z$  et  $\bar{z}$  et aussi

$$b_1 = z b - b \bar{z} = \sum u_s y_s (z - \bar{z})$$

Prenons  $z$  primitif dans  $\bar{Z}$ , et  $\bar{z} = z^u$ ;  $b$  ne contient plus  $u$ ; on recommence l'opération et on arrive finalement à

$$u_R y_R \in B \quad ; \quad \text{donc aussi } u_R, \text{ et}$$

$$u_s = u_R u_{R^{-1}S} a^{-1} R R^{-1} S$$

ce qui montre que  $B = A$

2°)- Désignons par  $\mathcal{M}$  la matrice à une ligne

$$\mathcal{M} = (u_E, u_S, \dots, u_T)$$

soit  $a = \sum u_s z_s$  un nombre quelconque de  $A$ . On a

$$(4) \quad a \mathcal{M} = \mathcal{M} (\zeta_{ST})$$

$(\zeta_{ST})$  étant la matrice carrée d'ordre  $n$

$$\zeta_{ST} = a_{S T^{-1} T} z_{ST}^T$$

On a ainsi une représentation  $\mathcal{A}$  de  $A$  dans l'anneau total

de matrices  $Z_n$ . Si  $\bar{Z}$  est un corps isomorphe de  $Z$ , on

en déduit aussi une représentation de  $A$  dans  $\bar{Z}_n$  par l'i-

somorphisme  $Z \cong \bar{Z}$ .

Considérons maintenant l'algèbre  $A \times \bar{Z}$  ( $Z$  et  $\bar{Z}$  doivent être considérés comme indépendants). On a

$$R = e_{11} (K \times A \times \bar{Z} = \sum u_s z_k \cdot \bar{z} \dots e_{1n}) \text{ un idéal à droite}$$

minimum de  $K \times \bar{Z}$ . Soit  $x$  le rang  $K$ -rang de  $R$ ;  $K$  étant de rang  $m^2$  sur  $P$ , le  $P$ -rang de  $R$  est  $x m^2$ ; d'autre part,



et en passant de  $u_s z_k$  à sa représentation dans  $\bar{z}_n$  on a une représentation de  $A \times \bar{z}$  dans  $\bar{z}_n$ . Cette représentation est une isomorphie de  $A \times \bar{z}$  sur un sous-anneau de  $\bar{z}_n$  car  $A \times \bar{z}$  est simple, et si ce n'était pas une isomorphie,  $A \times \bar{z}$  serait représenté sur le seul élément 0, ce qui n'est pas. Mais  $A \times \bar{z}$  est de rang  $n^2$  sur  $\bar{z}$ , donc aussi le sous-anneau de  $\bar{z}_n$  qui lui est isomorphe, et comme  $\bar{z}_n$  est lui-même de rang  $n^2$  sur  $\bar{z}$ , ce sous-anneau coïncide avec  $\bar{z}_n$ , ce qui montre que  $\bar{z}$  est (corps de) décomposition de  $A \times \bar{z}$ .

4.- On peut donner du théorème précédent une réciproque qui montre l'intérêt de l'introduction des produits croisés pour l'étude des corps gauches.

Théorème II .- 1°)- Tout corps gauche  $K$  ( et par suite , toute algèbre simple) est semblable à un produit croisé.

2°)- A chaque corps galoisien de décomposition  $\bar{z}$  , de  $K$ , correspond un produit croisé  $A = ( a, \bar{z} )$  semblable à  $K$ ,  $\bar{z}$  étant un corps isomorphe à  $\bar{z}$ .

a) Le degré  $n$  de  $\bar{z}$  est un multiple du degré  $m$  de  $K$

En effet, par hypothèse,  $K \times \bar{z}$  est isomorphe à un anneau complet de matrices d'ordre  $m$  dans  $\bar{z}$  : soit  $e_{i,k}$  le système d'unités matricielles correspondant, et soit  $R = e_{11} (K \times \bar{z}) = ( e_{11}, e_{12}, \dots, e_{1m} )$  un idéal à droite minimum de  $K \times \bar{z}$ . Soit  $r$  le  $K$ -rang de  $R$ ;  $K$  étant de rang  $m^2$  sur  $\rho$ , le  $\rho$ -rang de  $R$  est  $r m^2$ ; d'autre part,



le  $\bar{Z}$ -rang de  $R$  est  $m$ , et le rang de  $\bar{Z}$  sur  $\rho$  étant  $n$ , le  $\rho$ -rang de  $R$  est aussi  $n m$ , d'où

$$r m^2 = n m$$

$$n = r m$$

b) L'algèbre simple  $A$ , de rang  $n^2 = r^2 m^2$  sur  $\rho$ , semblable à  $K$ , contient un sous-corps commutatif maximum  $\bar{Z}$  isomorphe à  $\bar{K}$ .

Soit  $W = (\alpha_1, \alpha_2, \dots, \alpha_r)$  une  $K$ -base de  $R$ , considéré comme  $K$ -module à droite  $(\alpha_i \in (K \times \bar{Z}))$

Si  $\zeta \in \bar{Z}$ ,  $\zeta \alpha_i = \alpha_i \zeta \in R$ , donc

$$\zeta \alpha_i = \alpha_1 x_1^i + \alpha_2 x_2^i + \dots + \alpha_r x_r^i \quad x_i^i \in K$$

ou (5)  $\zeta W = W z_\zeta$

en posant  $z_\zeta = (x_i^j)$  matrices d'ordre  $r$  sur  $K$ .

Ces matrices donnant une représentation isomorphe de  $\bar{Z}$  sur un sous-corps  $\bar{Z}$  de l'algèbre  $A = K_r$ , anneau de matrices total sur  $K$ ; or,  $\bar{Z}$  est de degré  $r m$  sur  $\rho$  et  $K$ , algèbre de rang  $r^2 m^2$  sur  $\rho$ , ne peut contenir de sous-corps commutatif de degré  $> r m$ .

c) Jusqu'ici, on n'a pas utilisé le fait que  $\bar{Z}$  est galoisien. Soit  $\Gamma$  le groupe de Galois de  $\bar{Z}$ ,  $\Sigma$  une de ses substitutions.

Par définition, on pose

$$(6) \quad z_\zeta^S = z_{\zeta \Sigma}$$

ce qui définit les substitutions  $S$  du groupe de Galois  $G$

ou d'après (6)



de  $\bar{Z}$ , isomorphe à  $\bar{\Gamma}$ .

D'autre part, prolongeons  $\Gamma$  en un groupe d'automorphismes de  $K \times \bar{Z}$ ; en lui imposant la condition de laisser invariants les éléments de  $K$ .

Si  $\Sigma \in \Gamma$ , les  $e_{ik}$  se changent par  $\Sigma$  en un nouveau système d'unités matricielles  $e_{ik}^\Sigma$ ;  $R = e_{-11}(K \times \bar{Z})$  se change en  $R^\Sigma = e_{-11}^\Sigma(K \times \bar{Z})$ , la  $K$ -base  $\mathcal{W}$  de  $R$  se change en une  $K$ -base  $\mathcal{W}^\Sigma$  de  $R^\Sigma$ .

Or, on sait que ( Voir Van der Waerden, t.III, p.209) pour tout automorphisme de  $K \times \bar{Z}$  laissant invariant  $K$ , on a :

$$e_{ik}^\Sigma = q_\Sigma e_{ik} q_\Sigma^{-1} \quad q_\Sigma \in (K \times \bar{Z}) \text{ et } q_\Sigma \text{ possède un inverse.}$$

On en déduit

$$R^\Sigma = q_\Sigma e_{-11} q_\Sigma^{-1} (K \times \bar{Z}) = q_\Sigma e_{-11} (K \times \bar{Z}) = q_\Sigma R$$

Donc  $q_\Sigma \mathcal{W}$  est une  $K$ -base de  $R^\Sigma$ , et par suite

$$(7) \quad q_\Sigma \mathcal{W} = \mathcal{W}^\Sigma u_s$$

$u_s$  matrice inversible dans  $K \times \bar{Z} = A$

Appliquons à (5) l'automorphisme  $\Sigma$ ; on a :

$$\zeta^\Sigma \mathcal{W}^\Sigma = \mathcal{W}^\Sigma z_\zeta \quad (K \text{ invariant par } \Sigma)$$

ou, d'après (7)

$$\zeta^\Sigma q_\Sigma \mathcal{W} u_s^{-1} = q_\Sigma \mathcal{W} u_s^{-1} z_\zeta$$

et comme  $\zeta^\Sigma \in \bar{Z}$ , centre de  $K \times \bar{Z}$

$$\zeta^\Sigma \mathcal{W} = \mathcal{W} u_s^{-1} z_\zeta u_s$$

ou d'après (6)



$$z^S = u_S^{-1} z u_S \text{ pour tout } z \in \bar{\mathcal{Z}} \text{ dans } A$$

(c'est la 1ère condition (1)).

Ensuite :  $z^{ST} = (z^S)^T = u_T^{-1} z^S u_T = u_T^{-1} u_S^{-1} z u_S u_T$   
 $= u_{ST}^{-1} z u_{ST}$

D'où relation  $u_S u_T u_{ST}^{-1} z = z u_S u_T u_{ST}^{-1}$  quels que soit  $z \in \bar{\mathcal{Z}}$   
 comme  $\bar{\mathcal{Z}}$  est sous-corps maximum de  $A$ , il n'y a pas d'éléments de  $A$  commutatifs avec tous les éléments de  $\bar{\mathcal{Z}}$  en dehors des éléments de  $\bar{\mathcal{Z}}$ , donc :

$$u_S u_T u_{ST}^{-1} = \alpha_{ST} \quad \alpha_{ST} \neq 0 \text{ et dans } \bar{\mathcal{Z}}.$$

D'où on tire

1°) Si  $\bar{\mathcal{Z}}$  est un corps de décomposition d'un corps gauche  $K$  son degré  $n$  est multiple du degré de  $K$   
 $u_S u_T = u_{ST} \alpha_{ST} = u_{ST} a_{ST} \quad a_{ST} \neq 0 \text{ et dans } \bar{\mathcal{Z}}$   
 (c'est la 2ème condition (1)).

2°) L'algèbre simple  $A$  de degré  $n$ , semblable à  $K$ , contient

d) Pour montrer que

un sous-corps commutatif maximum  $\bar{\mathcal{Z}}$  isomorphe à  $\bar{\mathcal{Z}}$ .

$$A = (a, \bar{\mathcal{Z}}) \quad \text{où } a = (a_{ST})$$

Quand  $\bar{\mathcal{P}}$  est un corps algébrique de degré fini, on peut il suffit maintenant d'établir que les  $u_S$  forment une  $\bar{\mathcal{Z}}$ -base de  $A$ , considérée comme  $\bar{\mathcal{Z}}$ -module à droite.

t. II, p. 210)

Montrons d'abord que les  $u_S$  sont linéairement indé-

pendants. De

1°) Si  $\bar{\mathcal{Z}}$  est un sous-corps commutatif maximum d'une algèbre simple  $A$ , le degré de  $\bar{\mathcal{Z}}$  est égal à celui de  $A$ .

$$\sum u_S y_S = 0 \quad y_S \in \bar{\mathcal{Z}}$$

2°) Tout corps isomorphe à  $\bar{\mathcal{P}}$  est corps de décomposition on tire

$$\sum u_S y_S (z^S - \bar{z}) = 0 \text{ quels que soient } z \text{ et } \bar{z} \text{ dans } \bar{\mathcal{Z}}.$$

Ces propositions déterminent dans ce cas tous les corps de décomposition des algèbres simples.

On procède comme ci-dessus (Th. I, première partie) et

on en tire : algèbres simples et classes de systèmes de



facteurs associés.

$$u_R y_R a_R = 0 \quad a_R \neq 0 \text{ dans } \mathcal{P}$$

pour toute substitution  $R$  de  $G$ , d'où  $y_R = 0$

Le  $\mathcal{Z}$ -module à droite  $\sum u_s \mathcal{Z}$  est contenu dans  $A$  et a même  $\mathcal{P}$ -rang  $n^2$  que  $A$ , donc est identique à  $A$ . D'après les relations (1) qui ont été démontrées plus haut, on a bien  $a = (a, \mathcal{Z})$

### 5.- Théorie générale des corps de décomposition

Dans le cours de la démonstration précédente, on a établi les propositions suivantes :

- 1°) Si  $\bar{\mathcal{Z}}$  est un corps de décomposition d'un corps gauche  $K$  son degré  $n$  est multiple du degré de  $K$
- 2°) L'algèbre simple  $A$  de degré  $n$ , semblable à  $K$ , contient un sous-corps commutatif maximum  $\mathcal{Z}$  isomorphe à  $\bar{\mathcal{Z}}$ .

Quand  $\mathcal{P}$  est un corps algébrique de degré fini, on peut énoncer les réciproques suivantes ( voir Van der Waerden t. II, p. 210)

- 1°) Si  $\mathcal{Z}$  est un sous-corps commutatif maximum d'une algèbre simple  $A$ , le degré de  $\mathcal{Z}$  est égal à celui de  $A$ .
- 2°) Tout corps isomorphe à  $\mathcal{Z}$  est corps de décomposition pour  $A$ .

Ces propositions déterminent dans ce cas tous les corps de décomposition des algèbres simples.

### 6.- Classes d'algèbres simples et classes de systèmes de



facteurs associés.

Si une algèbre simple  $A$  sur  $\rho$  est isomorphe à un anneau total de matrices  $P_k$  sur  $\rho$ , on écrit  $A \sim 1$  au lieu de  $A \sim P$ .

Théorème III. - Si  $(a) \sim (1)$ ,  $(a, z) \sim 1$

On peut évidemment supposer que  $a_{sT} = 1$  quels que soient  $S$  et  $T$ .

Considérons la représentation isomorphe  $\mathcal{N}$  de  $A = (a, z)$  dans l'anneau  $Z_n$ , donnée par la relation (4)

Posons

(4')  $(\sum_{sT} z_{sT}) = A$   
 d'où  $a \mathcal{U} = \mathcal{U} A a$

Soit  $C$  la matrice carrée inversible

$C = \begin{pmatrix} E & E & \dots & E \\ z_1 & z_2 & \dots & z_n \\ S & S & \dots & S \\ z_1 & z_2 & \dots & z_n \\ \dots & \dots & \dots & \dots \\ T & T & \dots & T \\ z_1 & z_2 & \dots & z_n \end{pmatrix} = \begin{pmatrix} S \\ z_k \end{pmatrix}$

On en tire de (4')

$a \mathcal{U} C = \mathcal{U} C C^{-1} A a C = \mathcal{U} C \bar{A} a$

On a donc en posant

$\bar{A} a = C^{-1} A a C$  si  $n = r m$

Les  $\bar{A} a$  constituent une représentation  $\bar{\mathcal{U}}$  de  $A$  dans  $Z_n$  équivalente à  $\mathcal{U}$ , donc isomorphe à  $A$ .

Or, on a: est le rang de  $R$  (considéré comme  $Z$ -module à droite), le  $C u = u R C^R$  est égal à  $k n$ ; d'autre part, le



$$\bar{A}_a u_R = u_R \bar{A}_a^R$$

donc de  $a (M u_R C^R) = a (M C u_R)$

$$= M C \bar{A}_a u_R = (M C u_R) \bar{A}_a^R = (M u_R C^R) \bar{A}_a^R$$

Mais  $u_R C^R = (z_{\ell}^{SR})$  ; les éléments de  $u_R$  sont dans  $P$

donc  $M u_R C^R = (\sum_P u_P u_R z_{\ell}^{PR})$  (matrice à 1 ligne)

$$= (\sum_P u_P z_{\ell}^{PR}) = (\sum_Q u_Q z_{\ell}^{Q}) = M C$$

d'où

$$a (M C) = (M C) \bar{A}_a^R$$

et par suite

et par suite  $\bar{A}_a^R = \bar{A}_a$  quel que soit R, les éléments

de  $\bar{A}_a$  sont donc dans  $P$ ,  $\bar{A}$  est un sous-anneau de  $P_n$  ; mais

comme le  $P$ -rang de  $\bar{A}$  est égal à  $n^2$ ,  $\bar{A}$  est identique à

$P_n$ , donc de déterminant  $\neq 0$ . Soit :

$$(a, \bar{z}) \sim 1 \neq 0$$

Théorème 4 .- Si l'algèbre simple  $(a, \bar{z})$  a pour indice

(degré du corps semblable à  $(a, \bar{z})$ ) m, on a :

et d'après  $(a^m) \sim 1$

(c'est une réciproque du théorème précédent).

Soit K le corps gauche de degré m, semblable à  $A = (a \bar{z})$

Théorème 5 .- On a  $(a, \bar{z}) \times (a, \bar{z}) \sim (a \bar{a}, \bar{z})$

On a donc

Pour faire le produit des deux systèmes hypercomplexes

$$A = K \times P_n \quad \text{si } n = r m$$

$(a, \bar{z})$  et  $(a, \bar{z})$ , il faut y considérer les deux corps

Soit  $e_{i\ell}$  le système d'unités matricielles de A,  $R = e_{11}$  A

un idéal à droite minimum de A.

Si k est le  $\bar{z}$ -rang de R (considéré comme  $\bar{z}$ -module à

droite), le  $P$ -rang de R est égal à  $k n$  ; d'autre part, le

$u$  et  $\bar{u}$  étant respectivement la  $\bar{z}$ -base de A et la  $\bar{z}$ -base



et on écrit :

k-rang de R est r, donc on a

$$kn = r m^2 \quad k = m$$

Soit  $W$  une  $\bar{Z}$ -base de R ; les éléments de  $W u_s$  sont dans R donc

$$W u_s = W B_s$$

$B_s$ , matrice d'ordre m à éléments dans  $\bar{Z}$ . On a, de plus

$$\begin{aligned} W u_s u_T &= W B_s u_T = W u_{sT} B_s^T = W B_T B_s^T \\ &= W u_{sT} a_{sT} = W B_{sT} a_{sT} \end{aligned}$$

et par suite

$$(8) \quad B_T B_s^T = B_{sT} a_{sT}$$

les matrices  $B_s$ , représentations des  $u_s$  dans  $\bar{Z}_m$ , sont inversibles, donc de déterminant  $\neq 0$ . Soit :

$$c_s = |B_s| \neq 0$$

En égalant les déterminants des deux membres de (8) on a :

$$c_T c_s^T = c_{sT} a_{sT}^m$$

et d'après (3), on en tire

$$(a^m) \sim 1$$

Théorème 5.- On a  $(a, \bar{Z}) \times (\bar{a}, \bar{Z}) \sim (a\bar{a}, \bar{Z})$

b) Pour faire le produit des deux systèmes hypercomplexes  $(a, \bar{Z})$  et  $(\bar{a}, \bar{Z})$ , il faut y considérer les deux corps  $\bar{Z}$  qui y figurent comme isomorphes mais distincts ; dans  $(\bar{a}, \bar{Z})$  on remplacera donc  $\bar{Z}$  par un corps isomorphe  $\bar{\bar{Z}}$  et on écrira :

$$A = (a, \bar{Z}) \quad \bar{A} = (\bar{a}, \bar{\bar{Z}})$$

$u_s$  et  $\bar{u}_s$  étant respectivement la  $\bar{Z}$ -base de A et la  $\bar{\bar{Z}}$ -base



de  $\bar{A} : K$  est donc un corps isomorphe à  $\bar{Z}$  contenu dans  $\bar{Z} \times \bar{Z}$   
 a)  $A \times \bar{A}$  contient  $\bar{Z} \times \bar{Z}$  ; ce dernier produit est une somme  
 directe de corps commutatifs, la décomposition étant unique

Soit  $\bar{Z}'$  un des corps composants,  $e$  son unité ; on a :

$$\bar{Z}' = e (\bar{Z} \times \bar{Z}) = (e \bar{Z} \times e \bar{Z})$$

$\bar{Z}'$  contient donc les deux corps,  $e \bar{Z}$ ,  $e \bar{Z}$ , isomorphes  
 à  $\bar{Z}$  ; ces deux corps, sous-corps isomorphes d'un même  
 corps, sont conjugués ; étant galoisiens, ils sont identiques  
 donc :

$$\bar{Z}' = e \bar{Z} = e \bar{Z}$$

$\bar{Z}'$  est donc un corps de degré  $n$ , isomorphe à  $\bar{Z}$ . Comme  
 $\bar{Z} \times \bar{Z}$  est de rang  $n^2$  sur  $\rho$ , c'est la somme directe de  $n$   
 corps isomorphes à  $\bar{Z}$ .

On verra plus bas que les  $n$  unités de ces corps peu-  
 vent être complétées par un système de  $n^2 - n$  éléments de

$A \times \bar{A}$  forment un système d'unités matricielles, donc  
 $A \times \bar{A}$  est un anneau complet de matrices d'ordre  $n$  sur

un corps gauche isomorphe à  $e (A \times \bar{A}) e$ . Donc :

$$A \times \bar{A} \sim A' = e (A \times \bar{A}) e$$

b) Soit  $G$  le groupe de Galois de  $\bar{Z}$ . On le prolonge en  
 un groupe d'automorphismes de  $\bar{Z} \times \bar{Z}$  en lui imposant de  
 laisser invariants les éléments de  $\bar{Z}$ . Si  $R$  est une subs-  
 titution de  $G$ ,  $e^R$  le transformé de  $e$  par  $R$ , on a :

$$\bar{Z}'^R = e^R (\bar{Z} \times \bar{Z}) = e^R \bar{Z} = e^R \bar{Z}$$



$\mathbb{Z}^R$  est donc un corps isomorphe à  $\mathbb{Z}$  contenu dans  $\mathbb{Z} \times \bar{\mathbb{Z}}$   
 c'est donc nécessairement un des corps dont  $\mathbb{Z} \times \bar{\mathbb{Z}}$  est la  
 somme directe. ( En effet, si  $\mathbb{Z} \times \bar{\mathbb{Z}} = e_1 \mathbb{Z} \oplus e_2 \bar{\mathbb{Z}} \oplus \dots \oplus e_n \mathbb{Z}$   
 les  $e_i$  tels que  $e_i^2 = e_i$ ,  $e_i e_j = 0$ , les seuls idem-  
 potents de  $\mathbb{Z} \times \bar{\mathbb{Z}}$  sont des nombres de la forme

$$e^{k_1} + e^{k_2} + \dots + e^{k_r};$$

$e^R$  est donc un tel nombre, et par suite  $\mathbb{Z}^R$  est la somme  
 directe d'un certain nombre des corps composants de  $\mathbb{Z} \times \bar{\mathbb{Z}}$   
 Mais étant lui-même un corps, il se réduit à l'un de ses  
 composants ).

Les  $n$  corps  $\mathbb{Z}^R$  ( $R$  parcourant toutes les substitu-  
 tions de  $G$ ) sont distincts; si on avait en effet,  $e^R = e$   
 les éléments de  $e \bar{\mathbb{Z}}$  seraient invariants par la substitution  
 $R$ , donc aussi ceux de  $e \mathbb{Z}$  et par suite ceux de  $\mathbb{Z}$ , ce qui  
 ne se peut que si  $R = E$ .

Par suite, 
$$\mathbb{Z} \times \bar{\mathbb{Z}} = \sum_R e^R \mathbb{Z} \quad (\text{somme directe})$$

et si  $z^*$  est un nombre de  $\mathbb{Z} \times \bar{\mathbb{Z}}$  on a l'unique représentation

$$z^* = \sum_R e^R z_R \quad z_R \in \mathbb{Z}$$

En particulier, pour  $z^* = \bar{z} \in \bar{\mathbb{Z}}$

$$\bar{z} = \sum_R e^R z_R$$

$$\bar{z}^S = \bar{z} = \sum_R e^{k^S} z_R$$

Donc,  $z_R^S = z_R$  et en particulier, si  $R = E$ ,  $z_R = z_R^E = z_R$

De la relation (11) on déduit que :



en posant  $z^E = z$ . Donc :

$$(9) \quad \bar{z} = \sum_R e^R z^R \quad z \in \mathbb{Z}$$

Cette relation définit un isomorphisme de  $\mathbb{Z}$  et  $\bar{\mathbb{Z}}$  qu'on désignera par  $J$ , en posant  $\bar{z} = z^J$

Soit maintenant  $\bar{G}$  le groupe de Galois de  $\bar{\mathbb{Z}}$  et prolongeons-le à  $\mathbb{Z} \times \bar{\mathbb{Z}}$  en lui imposant la condition de laisser fixes les éléments de  $\mathbb{Z}$ . Soit  $\bar{S}$  la substitution de  $\bar{G}$  qui correspond à  $S$  de  $G$ , par l'isomorphisme  $J$ , c'est à dire telle que

$$\bar{z}^{\bar{S}} = z^{S^J}$$

ou encore

$$\bar{z}^{\bar{S}} = \sum_R e^R z^{SR} = \sum_R e^{S^{-1}R} z^R$$

comme d'autre part

$$\bar{z}^{\bar{S}} = \sum_R e^{R\bar{S}} z^R$$

On a

$$(10) \quad e^{R\bar{S}} = e^{S^{-1}R}$$

Ceci posé,  $a$  étant un élément quelconque de  $A \times \bar{A}$  on a d'après (1)

$$a u_s = u_s a^S \quad a \bar{u}_s = \bar{u}_s a^{\bar{S}}$$

car  $u_s$  est commutatif avec les éléments de  $\bar{A}$  et  $\bar{u}_s$  avec ceux de  $A$ . En particulier :

$$(11) \quad e^R u_s = u_s e^{RS}$$

$$(12) \quad e^R \bar{u}_s = \bar{u}_s e^{R\bar{S}} = \bar{u}_s e^{S^{-1}R}$$

De la relation (11) on déduit que :



$$e_{ST} = u_S^{-1} u_T e^T$$

forment un système de  $n^2$  unités matricielles de  $A \times \bar{A}$  ce qui justifie l'assertion de la première partie de la démonstration. Ceci établit donc bien que :

c) Considérons le corps gauche

$$A' = e (A \times \bar{A}) e,$$

et soit  $a^*$  un élément de  $A \times \bar{A}$

$$a^* = \sum_{S,T} u_S \bar{u}_T z_{ST} \quad z_{ST} \in \mathbb{Z} \times \mathbb{Z}$$

ou 
$$a^* = \sum_{R,S,T} u_S \bar{u}_T e^R z_{RST} \quad z_{RST} \in \mathbb{Z}$$

cette représentation étant unique.

L'élément correspondant de  $A'$  est donc

$$a' = e a^* e = \sum_{R,S,T} e u_S \bar{u}_T e^R z_{RST} e$$

$$= \sum_{RST} u_S \bar{u}_T e^{T-1S} e^R e z_{RST} = \sum_S u_S \bar{u}_S e z_{ESS}$$

Posons  $u'_S = u_S \bar{u}_S e$   $z'_S = e z_{ESS}$   $z'_S \in \mathbb{Z}' = e \mathbb{Z}$

On a 
$$a' = \sum_S u'_S z'_S$$

et la représentation est encore unique, le  $\rho$ -rang de  $A'$  étant  $n^2$ . Les  $u'_S$  sont donc une  $\mathbb{Z}'$ -base de  $A'$ . De plus,

quel que soit  $z' = e z$ , isomorphe au groupe des systèmes de facteurs  $z' u'_S = e z u_S \bar{u}_S e = u_S \bar{u}_S e z = u'_S z'^S$

$S'$  étant l'automorphisme de  $\mathbb{Z}'$  qui correspond à  $S$ . Enfin,

$$e u'_S u'_T = u_S \bar{u}_S e u_T \bar{u}_T e = u_S u_T \bar{u}_S \bar{u}_T e$$

$$= u_{ST} \bar{u}_{ST} e a_{ST} = u_{ST} \bar{u}_{ST} e a_{ST} \bar{a}_{ST}$$



$$= u_{ST} \bar{u}_{ST} e a'_{ST} \bar{a}'_{ST}$$

où  $l$  est divisible par tout facteur premier  $p$  de  $n$ .

$$a'_{ST} = e a_{ST} \quad \bar{a}'_{ST} = e \bar{a}_{ST}$$

sont des nombres de  $Z'$ . Ceci établit donc bien que :

$$A' = ( a' \bar{a}', z')$$

7.- Groupe de classes d'algèbres simples semblables.

On sait que si entre des algèbres simples  $A, B, A', B'$  on a les relations  $A \sim A'$  de  $B \sim B'$  par rapport à  $\Sigma$ , admet le corps de décomposition  $\Sigma$ , donc il en résulte  $A \times B \sim A' \times B'$  par rapport à  $\Sigma$ . D'autre part, si ces produits sont simples.

Toutes les algèbres simples semblables forment une classe dont chacune est un représentant ; le produit des deux classes est la classe définie par le produit d'un représentant de l'une par un représentant de l'autre . Ceci posé, les résultats précédents peuvent encore s'énoncer en disant que les classes d'algèbres simples qui admettent un même corps galoisien de décomposition forment un groupe abélien, isomorphe au groupe des systèmes de facteurs des produits croisés qui représentent chaque classe (le produit de deux tels systèmes étant défini comme ci-dessus) . De plus, tout élément  $\alpha$  du groupe a un exposant fini  $l$  diviseur de l'indice  $m$  de  $A$ .



$\sum q_i = 1 \pmod{l}$

On peut établir de plus que l'exposant  $l$  est divisible par tout facteur premier  $p$  de  $m$ .

En effet, soit  $Z$  un corps galoisien de décomposition de l'algèbre  $A$ ; son degré  $n = r m = p^{\nu} n'$ ,  $n'$  premier avec  $p$ . D'après un théorème de Sylow,  $Z$  possède un sous-corps  $\Sigma$  de degré  $n'$  sur  $\mathcal{P}$ .  $\Sigma$  n'est pas un corps de décomposition pour  $A$ , car son degré  $n'$  n'est pas multiple de  $m$ . Mais  $A \times \Sigma$ , considéré comme une algèbre sur  $\Sigma$ , admet le corps de décomposition  $Z$ , de degré  $p^{\nu}$  par rapport à  $\Sigma$ , donc l'indice de  $A \times \Sigma$  est  $p^{\lambda}$  ( $\lambda \leq \nu$ ); l'exposant de  $A \times \Sigma$  est donc  $p^{\lambda} \neq 1$  car  $A \times \Sigma$  n'est pas  $\sim 1$ . D'autre part, on a

$$(A \times \Sigma)^l = A^l \times \Sigma \sim 1$$

Donc  $l$  est multiple de  $p^{\lambda}$ . c.q.f.d.

On peut enfin établir la proposition suivante :

Théorème 6.- Tout corps gauche est égal à un produit de corps gauches dont les degrés sont des puissances de nombres premiers

Soit  $l = \prod_{i=1}^k p_i^{\lambda_i}$  l'exposant du corps gauche  $K$

Les nombres  $\frac{l}{p_1^{\lambda_1}}, \frac{l}{p_2^{\lambda_2}}, \dots, \frac{l}{p_k^{\lambda_k}}$  étant premiers entre eux

dans leur ensemble, on peut trouver  $k$  nombres  $q_1, q_2, \dots, q_k$  tels que

$$q_i \equiv 1 \pmod{p_i^{\lambda_i}} \quad q \equiv 0 \pmod{\frac{l}{p_i^{\lambda_i}}}$$



tout à fait analogue  $\sum q_i \equiv 1 \pmod{l}$

On a donc  $K \sim K^{\sum q_i} = \prod_1 K^{q_i} \sim \prod_1 K_i$

où  $K_i$  est le corps gauche semblable à  $K^{q_i}$ ; comme  $K^{q_i}$  a pour exposant  $p_i^{\lambda_i}$  le degré de  $K_i$  est une puissance  $p_i^{\mu_i}$ .

On a donc  $\prod_1 K_i = K \times P_r$  de  $Z\Phi$  sur  $\Phi$ ; on a donc

et par suite  $\prod_1 p_i^{\mu_i} = r m$

Mais d'après la définition de  $K_i$ , tout corps de décomposition de  $K$  est aussi corps de décomposition de  $K_i$ ; comme  $K$  a des corps de décomposition de degré  $m$ , tout  $p_i^{\mu_i}$  est diviseur de  $m$ , donc aussi  $\prod_1 p_i^{\mu_i}$ , et par suite  $r = 1$

b) Soit  $G$  le groupe des Galois de  $Z$ ; prolongeons-le en un groupe d'automorphismes de  $Z \times \Phi$  en imposant à ses substitutions de laisser invariants les éléments de  $\Phi$ .

### 8.- Extension du corps de base $P$ .

Soit  $\Phi$  un corps commutatif, extension parfaite du corps de base  $P$ .

Théorème 7.- On a

$$(a, Z) \times \Phi \sim (a^\Phi, Z\Phi)$$

où  $Z\Phi$  désigne le plus petit corps contenant  $Z$  et  $\Phi$ , considéré comme corps sur  $\Phi$ ,  $(a^\Phi)$  le système de facteurs formé des facteurs de  $(a)$  correspondant aux automorphismes de  $Z\Phi$  par rapport à  $\Phi$ .

Soit  $A = (a, Z)$  de degré  $n$ . (La démonstration est élémentaire de  $P$ , donc appartient au sous-groupe  $H$  de  $G$  qui correspond au corps  $P$ ; on a donc :



tout à fait analogue à celle du théorème 5 )

a)  $A \times \Phi$  contient  $Z \times \Phi$ , qui est somme directe de corps commutatifs. Si  $\bar{Z}$  est l'un de ces corps,  $e$  son unité, on a  $\bar{Z} = e (Z \times \Phi)$ ; donc  $\bar{Z}$  contient les corps  $eZ$  et  $e\Phi$ , et, d'après la manière dont il est formé, il est isomorphe à  $Z\Phi$ . Soit  $h$  le degré de  $Z\Phi$  sur  $\Phi$ ; on a donc  $n = hk$ ,  $k$  étant le nombre de corps isomorphes à  $Z\Phi$  dont la somme directe est égale à  $Z \times \Phi$ .

On montrera plus loin que l'on peut former à l'aide des  $e$  un système de  $k$  unités matricielles dans  $A \times \Phi$  on en déduit

$$(13) \quad A \times \Phi \sim \bar{A} = e (A \times \Phi) e$$

b) Soit  $G$  le groupe de Galois de  $Z$ : prolongeons-le en un groupe d'automorphismes de  $Z \times \Phi$  en imposant à ses substitutions de laisser invariants les éléments de  $\Phi$ .

Si  $S$  est une substitution de  $G$ ,  $e^S$  est un idempotent de  $Z \times \Phi$ , et

$$\bar{Z}^S = e^S (Z \times \Phi)$$

des est un corps dont la somme directe est égale à  $Z \times \Phi$

Soit  $H$  le sous-groupe de  $G$  qui laisse invariant  $\bar{Z}$

Si  $P$  est une substitution de  $H$ , on a, en particulier,

$$e^P = e, \text{ par suite les éléments de } e\Phi \text{ sont invariants}$$

par  $P$ ; soit  $F$  le sous-corps de  $Z$  qui est isomorphe au sous-corps commun à  $eZ$  et  $e\Phi$ ;  $P$  laisse invariants les éléments de  $F$ , donc appartient au sous-groupe  $H'$  de  $G$  qui correspond au corps  $F$ ; on a donc :



correspondant  $\bar{H} = H' \bar{H}^{-1}$  pour tout  $\bar{H} \in \bar{Z}$

Mais inversement,  $H'$  est isomorphe au groupe des automorphismes de  $e\bar{Z}$  qui laissent invariants les éléments de  $eF$  et par suite au groupe des automorphismes de  $\bar{Z}$  par rapport à  $e\bar{\Phi}$ , donc à  $H$ , ce qui entraîne :

$$H = H'$$

Comme  $e^{H^s} = e^s$   $\bar{Z}^{H^s} = \bar{Z}^s$ , donc l'ordre de  $H$  est égal à  $h$ , et par suite

$$\bar{Z} \times \bar{\Phi} = \sum_{S \text{ mod. } H} \bar{Z}^s = \sum_{S \text{ mod. } H} e^s (\bar{Z} \times \bar{\Phi})$$

Comme  $e^R u_s = u_s e^{R^s}$  ( $\mu = 1, 2, \dots$ )  
on voit que les  $k^2$  quantités

$$e_{sT} = u_s^{-1} u_T e^T$$

correspondant à  $k$  substitutions de  $G$  choisies chacune dans une classe différente (mod.  $H$ ) forment un système d'unités matricielles dans  $A \times \bar{\Phi}$ , ce qui justifie la relation (13)

c) Si  $a^*$  appartient à  $A \times \bar{\Phi}$ , on a

$$a^* = \sum u_s z_s^* \quad z_s^* \in (\bar{Z} \times \bar{\Phi}) \quad (15)$$

et cette représentation est unique. L'élément correspondant de  $\bar{A}$  s'écrit

$$\bar{a} = e a^* e = \sum e u_s z_s^* e = \sum u_s e^s e z_s^*$$

$$= \sum_{P \in H} u_P \bar{z}_P \quad \bar{z}_P \in \bar{Z}$$

et cette représentation est unique d'après le  $\bar{\Phi}$ -rang de  $A$ . Les  $u_P$  forment donc une  $\bar{Z}$ -base de  $\bar{A}$ , et de plus,



que  $\alpha$  soit le nombre  $\bar{z} u_P = u_P \bar{z}^P$  pour tout  $\bar{z} \in \bar{Z}$

a) La condition  $u_P u_Q = u_{PQ} a_{PQ}$

Donc si (a)  $\bar{A} = (\bar{a}, \bar{Z})$

Si  $(\bar{a})$  étant le système partiel du système (a) qui correspond aux substitutions du sous-groupe H, ce qui établit le théorème.

9.- Cas cyclique.- Si G est un groupe cyclique, engendré par les puissances d'une substitution S, et si  $\bar{u}_S = u$  est une  $\bar{Z}$ -base du produit croisé (a,  $\bar{Z}$ ) on a :

$$u^\mu = \bar{u}_{S^\mu} c_\mu \quad c_\mu \in \bar{Z} \quad (\mu = 1, 2, \dots)$$

On peut donc prendre comme nouvelle base

$$u_S = 1, \quad u_S = u_1, \quad u_{S^\mu} = u^\mu \quad (\mu = 1, 2, \dots, n-1)$$

et on a :  $u = \alpha \quad \alpha \in \bar{Z}$

Donc si  $\mu < n, \nu < n, \mu + \nu < n$  on a

$$u^{\mu+\nu} = u_{S^{\mu+\nu}} a_{S^{\mu+\nu}} = u_{S^\mu S^\nu} a_{S^\mu S^\nu} = u_{S^\mu} a_{S^\nu} = u^\mu u^\nu = 1 \quad (14)$$

Si  $\mu < n, \nu < n, \mu + \nu \geq n$

$$u^{\mu+\nu} = u_{S^{\mu+\nu}} a_{S^{\mu+\nu}} = u_{S^{\mu+\nu-n}} a_{S^{\mu+\nu-n}} = u_{S^\mu S^\nu} a_{S^\mu S^\nu} = \alpha \quad (15)$$

Ensuite, d'après (2) on a :

$$\alpha^S = a_{SS^{n-1}}^S = \frac{a_{SE} a_{S^{n-1}S}}{a_{ES}} = \alpha$$

Donc  $\alpha$  est un élément de  $\mathcal{P}$ . Et inversement, si

$\alpha \in \mathcal{P}$ , la condition d'associativité est bien satisfaite.

On pose, dans ce cas,

$$A = (a, \bar{Z}) = (\alpha, \bar{Z}, S)$$

La condition nécessaire et suffisante pour que  $A \sim 1$  est



Exemple n° 4  
 Institut Henri Poincaré  
 (Ne peut quitter le  
 salle de travail)

que  $\alpha$  soit la norme d'un élément de  $\mathcal{E}$ .

a) La condition est nécessaire

Si  $(a) \sim 1$ , on a :

$$(16) \quad a_{s^\mu s^\nu} = \frac{c_{s^\nu} c_{s^\mu}}{c_{s^{\mu+\nu}}} \quad c_{s^\mu} \neq 0 \text{ et } \in \mathcal{E}$$

Faisons  $\mu = 1$ , donnons à  $\nu$  toutes les valeurs de 0 à  $n-1$ , et multiplions les égalités obtenues membre à membre ; il vient

$$\alpha = N(c) \quad \text{où } c = c_s \in \mathcal{E}$$

b) La condition est suffisante, car si

$$\alpha = N(c) = c \cdot c^s \cdot c^{s^2} \dots c^{s^{n-1}}$$

en posent

$$c_{s^\mu} = \prod_{\rho=0}^{\mu-1} c$$

on vérifie sans peine que les nombres donnés par (16) vérifient bien (14) et (15), donc constituent le système de facteurs de  $(\quad, \quad, S)$ .