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>

SEMINAIRE DE MATHEMATIQUES

Année I933-I934

Théorie des Groupes et des Algèbres

G.- Théorie des Corps Gauches

Exposé fait par Monsieur Jean DIEUDONNE, le 26 Février I934.

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 $\mathcal{Z}$ de degré fini n sur ρ est engendré par une racine ϑ d'une équation irréductible de degré n

$$f(x) = 0$$

à coefficients dans ρ . Le corps $\mathcal{Z}$ est dit galoisien s'il contient aussi les n-1 autres racines de $f(x) = 0$. Le groupe des 1-automorphismes de $\mathcal{Z}$ laissant fixes les nombres de ρ est le groupe de Galois G de $\mathcal{Z}$. C'est un groupe d'ordre n dont chaque substitution change ϑ en une autre racine de $f(x) = 0$. Si S est une substitution de G, z un nombre de $\mathcal{Z}$, 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 a de A par rapport à K, le degré minimum du polynome $\varphi(x)$ à coefficients dans K, tel que $\varphi(a) = 0$. 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 Z un corps galoisien de degré n sur ρ , G le groupe de Galois de Z ; on désignera par S, T, U ... les substitutions de G, par E la substitution unité .

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

$$A = u_E Z + u_S Z + \dots + u_T Z$$

$u_E, u_S \dots u_T$ désignent la 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 :

$$(1) \quad \begin{cases} z\, u_S = u_S z^S & \text{si } z \in Z \\ u_S u_T = u_{ST}\, a_{ST} \end{cases}$$

où a_{ST} est un élément $\neq 0$ de 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

$$(2) \quad a_{ST}^{U} = \frac{a_{STU}\, a_{TU}}{a_{STU}}$$

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

$u_s z_k$.

On écrit : $A = (a, \mathcal{Z})$

Propriétés élémentaires des produits croisés

1°- A possède une unité

$$e = u_E a^{-1}_{EE}$$

comme on le vérifie sans difficulté à l'aide de (1) et (2)

On identifie cette unité avec celle de $\mathcal{Z}$, en écrivant

$e = 1$, et par suite :

$$u_E = a_{E\bar{E}}$$

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

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

Soit a un élément de A

$$a = \Sigma\, u_S z_S \qquad z_S \in \mathcal{Z}$$

tel que : $a z = z a$ quel que soit $z \in \mathcal{Z}$

on en tire d'après (1)

$$\Sigma\, u_S z_S (z - z^S) = 0$$

ou $$z_S (z - z^S) = 0$$

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

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

3°- u_S possède un inverse u^{-1}_S

$$u^{-1}_S = u_{S^{-1}} a^{-1}_{SS^{-1}} a^{-1}_{EE}$$

comme on le vérifie sans peine .

4°- La condition nécessaire et suffisante pour que

$$(a, \mathfrak{Z}) = (\bar{a}, \mathfrak{Z})$$

est que l'on ait

$$(3) \qquad \bar{a}_{sT} = a_{sT} \frac{c_T c_s^{\tau}}{c_{sT}} \qquad c_s \neq 0 \text{ et dans } \mathfrak{Z}$$

ce qui peut encore s'exprimer en disant que l'on a entre les deux $\mathfrak{Z}$-bases de A la relation

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

a) la condition est nécessaire, car les relations

$$z\, u_{s-1} = u_{s-1}\, z^{s-1} \quad , \quad z\, \bar{u}_s = \bar{u}_s\, z^{s}$$

valables pour tout $z \in \mathfrak{Z}$, on en tire que $u_{s-1}\, \bar{u}_s$ est commutatif avec tous les éléments de $\mathfrak{Z}$, donc est dans $\mathfrak{Z}$ d'après 2°- ; par suite,

$u_s^{-1}\, \bar{u}_s$ est aussi dans $\mathfrak{Z}$, donc :

$$\bar{u}_s = u_s\, c_s$$

d'où la relation (3)

b) la condition est évidemment suffisante , car de (3') on tire que A est un $\mathfrak{Z}$-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 $(\bar{a}, \ )$.

3.- Structure des produits croisés

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

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

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

$$b = \sum u_s y_s \qquad y_s \in \mathfrak{Z}$$

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

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

Prenons z primitif dans $\mathfrak{Z}$, et $\bar{z} = z^U$; b_1 ne contient plus u_U ; on recommence l'opération et on arrive finalement à $u_R y_R \in B$; donc aussi u_R , et

$$u_s = u_R\, u_{RR^{-1}s}\, a^{-1}_{RR^{-1}s}$$

ce qui montre que B = A

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

$$\mathcal{M} = (u_E, u_s \ldots u_T)$$

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

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

(ζ_{ST}) étant la matrice carrée d'ordre n

$$\zeta_{ST} = a_{S\,T^{-1}T}\; z^{T}_{ST^{-1}}$$

On a ainsi une représentation $\mathcal{O}$ de A dans l'anneau total de matrices $\mathfrak{Z}_n$. Si $\bar{\mathfrak{Z}}$ est un corps isomorphe de $\mathfrak{Z}$, on en déduit aussi une représentation de A dans $\bar{\mathfrak{Z}}_n$ par l'isomorphie $\mathfrak{Z} \rightleftarrows \bar{\mathfrak{Z}}$.

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

$$A \times \bar{\mathfrak{Z}} = \sum u_s z_k \cdot \bar{z}$$

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

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

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

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

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

le $\overline{\zeta}$-rang de R est m, et le rang de $\overline{\zeta}$ sur ρ étant n, le ρ- 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 ρ , semblable à K, contient un sous-corps commutatif maximum ζ isomorphe à $\overline{\ }$.

Soit $\mathcal{W} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ une K-base de R, considéré comme K-module à droite $(\alpha_i \in (K \times \overline{\zeta}))$

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

$$\zeta\,\alpha_i = \alpha_1 x_1^i + \alpha_2 x_2^i + \ldots + \alpha_n x_n^i \qquad x_i^\delta \in K$$

ou (5) $\zeta\,\mathcal{W} = \mathcal{W}\,z_\zeta$

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

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

c) Jusqu'ici, on n'a pas utilisé le fait que $\overline{\zeta}$ est galoisien . Soit Γ le groupe de Galois de $\overline{\zeta}$, Σ une de ses substitutions .

Par définition, on pose

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

ce qui définit les substitutions S du groupe de Galois G

de $\mathcal{Z}$, isomorphe à Γ.

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

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

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

$$e^{\Sigma}_{ik} = q_{\Sigma}\, e_{ik}\, q_{\Sigma}^{-1} \qquad q_{\Sigma} \in (K \times \overline{\mathcal{Z}})$$ et possède un inverse.

On en déduit

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

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

$$q_{\Sigma}\mathcal{W} = \mathcal{W}^{\Sigma} u_s \tag{7}$$

u_s matrice inversible dans $K_z = A$

Appliquons à (5) l'automorphisme Σ ; on a :

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

ou, d'après (7)

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

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

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

ou d'après (6)

$$z^S = u_S^{-1} z u_S \quad \text{pour tout} \quad z \in Z$$

(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 $u_S u_T u_{ST}^{-1} z = z u_S u_T u_{ST}^{-1}$ quels que soit $z \in Z$

comme Z est sous-corps maximum de A, il n'y a pas d'éléments de A commutatifs avec tous les éléments de Z en dehors des éléments de Z , donc :

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

D'où on tire

$$u_S u_T = u_{ST} \alpha_{ST} = u_{ST} a_{ST} \qquad a_{ST} \neq 0 \text{ et dans } Z$$

(c'est la 2ème condition (1)).

d) Pour montrer que

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

il suffit maintenant d'établir que les u_S forment une Z-base de A, considérée comme Z-module à droite .

Montrons d'abord que les u_S sont linéairement indépendants . De

$$\Sigma u_S y_S = 0 \qquad y_S \in Z$$

on tire

$$\Sigma u_S y_S (z^S - \bar{z}) = 0 \text{ quels que soient } z \text{ et } \bar{z}$$

dans Z .

On procède comme ci-dessus (Th.I, première partie) et on en tire :

$$u_R\, y_R\, a_R = 0 \qquad a_R \neq 0 \text{ dans } ,$$

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

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

5.- Théorie générale des corps de décomposition

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

I°) Si $\overline{\mathfrak{Z}}$ 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 $\mathfrak{Z}$ isomorphe à $\overline{\mathfrak{Z}}$.

Quand ρ est un corps algébrique de degré fini, on peut énoncer les réciproques suivantes (voir Van der Waerden t.II, p.2IO)

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

2°) Tout corps isomorphe à $\mathfrak{Z}$ 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 ρ est isomorphe à un anneau total de matrices ρ_k sur ρ, on écrit $A \sim 1$ au lieu de $A \sim \rho$.

Théorème III.- Si $(a) \sim (1)$, $(a, \mathfrak{Z}) \sim 1$

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

Considérons la représentation isomorphe $\mathcal{H}$ de $A = (a, \mathfrak{Z})$ dans l'anneau $\mathfrak{Z}_n$, donnée par la relation (4)

Posons

$$(\zeta_{ST}) = A$$

d'où (4') $\qquad a\,\mathcal{U} = \mathcal{U}\,A_a$

Soit C la matrice carrée inversible

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

On en tire de (4')

$$a\,\mathcal{U}\,C = \mathcal{U}\,C\,C^{-1}A_a\,C = \mathcal{U}\,C\,\overline{A}_a$$

en posant

$$\overline{A}_a = C^{-1}A_a\,C$$

Les $\overline{A}_a$ constituent une représentation $\overline{\mathcal{A}}$ de A dans $\mathfrak{Z}_n$ équivalente à $\mathcal{A}$, donc isomorphe à A.

Or, on a :

$$C\,u_R = u_R\,C^R$$

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

donc $a(\mathcal{U} u_R C^R) = a(\mathcal{U} C u_R)$

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

Mais $C^R = (z_k^{sR})$

$$\mathcal{U} u_R C^R = \left(\sum_P u_P u_R z_k^{PR}\right) \quad \text{(matrice à 1 ligne)}$$

$$= \left(\sum_P u_{PR} z_k^{PR}\right) = \left(\sum_Q u_Q z_k^Q\right) = \mathcal{U} C$$

d'où

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

et par suite

$\bar{A}_a^R = \bar{A}_a$ quel que soit R, les éléments de $\bar{A}_a$ sont donc dans ρ. $\bar{\mathcal{A}}$ est un sous-anneau de ρ_n ; mais comme le ρ-rang de $\bar{\mathcal{A}}$ est égal à n^2, $\bar{\mathcal{A}}$ est identique à ρ_n, donc

$$(a, \zeta) \sim 1$$

Théorème 4.- Si l'algèbre simple (a, ζ) a pour indice (degré du corps semblable à (a, ζ)) m, on a :

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

(c'est une réciproque du théorème précédent).

Soit K le corps gauche de degré m, semblable à $A = (a\zeta)$ On a donc

$$A = K \times \rho_r \qquad \text{si } n = r\,m \ .$$

Soit e_{ik} le système d'unités matricielles de A, $R = e_{11} A$ un idéal à droite minimum de A.

Si k est le ζ-rang de R (considéré comme ζ-module à droite), le ρ-rang de R est égal à k n ; d'autre part, le

K-rang de R est r , donc on a

$$k\,n = r\,m^2 \qquad k = m$$

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

$$\mathcal{W}\,u_s = \mathcal{W}\,B_s$$

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

$$\mathcal{W}\,u_s\,u_T = \mathcal{W}\,B_s\,u_T = \mathcal{W}\,u_t\,B_s^T = \mathcal{W}\,B_T\,B_S^T$$
$$= \mathcal{W}\,u_{sT}\;a_{sT} = \mathcal{W}\,B_{sT}\;a_{sT}$$

et par suite

$$(8) \qquad B_T\,B_S^T = B_{sT}\;a_{sT}$$

les matrices B_s , représentations des u_s dans $\mathcal{Z}_m$, 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 $(a, \mathcal{Z}) \times (\bar{a}, \mathcal{Z}) \sim (a\bar{a}, \mathcal{Z})$

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

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

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

de $\overline{A}$

a) $A \times \overline{A}$ contient $Z \times \overline{Z}$; ce dernier produit est une somme directe de corps commutatifs, la décomposition étant unique Soit Z' un des corps composants, e son unité ; on a :

$$Z' = e\,(Z \times \overline{Z}) = (eZ \times e\overline{Z})$$

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

$$Z' = eZ = e\overline{Z}$$

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

On verra plus bas que les n unités de ces corps peuvent être complétées par un système de $n^2 - n$ éléments de $A \times \overline{A}$ formant un système d'unités matricielles , donc $A \times \overline{A}$ est un anneau complet de matrices d'ordre n sur un corps gauche isomorphe à $e\,(A \times \overline{A})\,e$. Donc :

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

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

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

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

$$e_{k_1} + e_{k_2} + \ldots + e_{k_r} ;$$

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

Les n corps $\mathfrak{Z}'^{R}$ (R parcourant toutes les substitutions de G) sont <u>distincts</u> ; si on avait en effet, $e^R = e$ les éléments de $e\overline{\mathfrak{Z}}$ seraient invariants par la substitution R, donc aussi ceux de $e\mathfrak{Z}$ et par suite ceux de $\mathfrak{Z}$, ce qui ne se peut que si $R = E$.

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

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

$$z^* = \sum_R e^R z_R \qquad z_R \in \mathfrak{Z}$$

En particulier, pour $z^* = \overline{z} \in \overline{\mathfrak{Z}}$

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

$$\overline{z}^S = \overline{z} = \sum_R e^{RS} z_R$$

Donc, $z_R^S = z_{RS}$ et en particulier, si $R = E$, $z_R = z_E^R = z^R$

en posant $z_\varepsilon = z$. Donc :

$$(9) \qquad \overline{z} = \sum_R e^R z^R \qquad z \in \mathfrak{z}$$

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

Soit maintenant $\overline{G}$ le groupe de Galois de $\overline{\mathfrak{z}}$ et prolongeons-le à $\mathfrak{z} * \overline{\mathfrak{z}}$ en lui imposant la condition de laisser fixes les éléments de $\mathfrak{z}$. Soit $\overline{S}$ la substitution de $\overline{G}$ qui correspond à S de G, par l'isomorphisme J , c'est à dire tel le que

$$\overline{z}^{\overline{S}} = z^{SJ}$$

ou encore

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

comme d'autre part

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

On a

$$(10) \qquad e^{R\overline{S}} = e^{S^{-1}R}$$

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

$$a\, u_S = u_S\, a^S \qquad a\, u_S = \overline{u}_S\, a^{\overline{S}}$$

car u_S est commutatif avec les éléments de $\overline{A}$ et $\overline{u}_S$ avec ceux de A . En particulier :

$$(11) \qquad e^R u_S = u_S\, e^{RS}$$

$$(12) \qquad e^R \overline{u}_S = \overline{u}_S\, e^{R\overline{S}} = \overline{u}\; e^{S^{-1}R}$$

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 $A \times \overline{A}$ ce qui justifie l'assertion de la première partie de la démonstration.

c) Considérons le corps gauche

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

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

$$a^* = \sum_{S,T} u_S \overline{u}_T z_{ST} \qquad z_{ST} \in \mathfrak{Z} \times \overline{\mathfrak{Z}}$$

ou $$a^* = \sum_{R,S,T} u_S \overline{u}_T e^R z_{RST} \qquad z_{RST} \in \mathfrak{Z}$$

cette représentation étant unique.

L'élément correspondant de A' est donc

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

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

Posons $u'_S = u_S \overline{u}_S e \qquad z'_S = e\, z_{ESS} \qquad z'_S \in \mathfrak{Z}' = e\mathfrak{Z}$

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

et la représentation est encore unique, le ρ-rang de A' étant n^2. Les u'_S sont donc une $\mathfrak{Z}'$- base de A'. De plus, quel que soit $z' = e\, z$

$$z'\, u'_S = e\, z\, u_S \overline{u}_S e = u_S \overline{u}_S e\, z^S = u'_S\, z'^{S'}$$

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

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

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

$$= u_{s\tau}\,\overline{u}_{s\tau}\,e\,a'_{s\tau}\,\overline{a}'_{s\tau}$$

où

$$a'_{s\tau} = e\,a_{s\tau} \qquad \overline{a}'_{s\tau} = e\,\overline{a}_{s\tau}$$

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

$$A' = (a'\overline{a}', \Sigma')$$

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

On sait que si entre des algèbres simples A, B, A', B' on a les relations

$$A \sim A' \qquad B \sim B'$$

il en résulte

$$A \times B \sim A' \times B'$$

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 A du groupe a un exposant fini ℓ diviseur de l'indice m de A.

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

En effet, soit $\mathcal{Z}$ 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, $\mathcal{Z}$ possède un sous-corps Σ de degré n' sur ρ . Σ n'est pas un corps de décomposition pour A, car son degré n'est pas multiple de m . Mais $A \times \Sigma$, considéré comme une algèbre sur Σ , admet le corps de décomposition $\mathcal{Z}$, de degré p^{ν} par rapport à Σ , donc l'indice de $A \times \Sigma$ est p^{μ} $(\mu \leq \nu)$; l'exposant de $A \times \Sigma$ est donc $p^{\lambda} \neq 1$ car $A \times \Sigma$ n'est pas ~ 1 . D'autre part, on a

$$(A \times \Sigma)^{\ell} = A^{\ell} \times \Sigma \sim 1$$

Donc ℓ est multiple de p^{λ} . 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 $\ell = \prod_i p_i^{\lambda_i}$ l'exposant du corps gauche K

Les nombres $\frac{\ell}{p_1^{\lambda_1}}$ $\frac{\ell}{p_2^{\lambda_2}}$ ..... $\frac{\ell}{p_K^{\lambda_K}}$ étant premiers entre eux dans leur ensemble , on peut trouver k nombres $q_1\ q_2 \ldots q_K$ tels que

$$q_i \equiv 1 \pmod{p_i^{\lambda_i}} \qquad q \equiv 0 \pmod{\frac{\ell}{p_i^{\lambda_i}}}$$

$$\Sigma q_i \equiv 1 \pmod{\ell}$$

On a donc $$K \sim K^{\sum_i q_i} = \prod_i K^{q_i} \sim \prod_i K_i$$

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 $$\prod_i K_i = K \times \rho_r$$

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

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 $\prod_i p_i^{\mu_i}$, et par suite $r = 1$

$$K = \prod_i K_i$$

8.- Extension du corps de base ρ.

Soit Φ un corps commutatif, extension parfaite du corps de base ρ.

Théorème 7.- On a

$$(a, \mathcal{Z}) \times \Phi \sim (a^{\Phi}, \mathcal{Z}\Phi)$$

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

Soit $A = (a, \mathcal{Z})$ de degré n . (La démonstration est

tout à fait analogue à celle du théorème 5)

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

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

$$(I3) \qquad A \times \Phi \sim \bar{A} = e\,(A \times \Phi)\,e$$

b) Soit G le groupe de Galois de $\mathfrak{Z}$: prolongeons-le en un groupe d'automorphismes de $\mathfrak{Z} \times \Phi$ en imposant à ses substitutions de laisser invariants les éléments de Φ.
Si S est une substitution de G , e^S est un idempotent de $\mathfrak{Z} \times \Phi$, et

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

est un/des corps dont la somme directe est égale à $\mathfrak{Z} \times \Phi$
Soit H le sous-groupe de G qui laisse invariant $\bar{\mathfrak{Z}}$
Si P est une substitution de H, on a, en particulier, $e^P = e$, par suite les éléments de $e\Phi$ sont invariants par P ; soit F le sous-corps de $\mathfrak{Z}$ qui est isomorphe au sous-corps commun à $e\mathfrak{Z}$ et $e\Phi$; P laisse invariants les éléments de F, donc appartient au sous-groupes H' de G qui correspond au corps F ; on a donc :

$$H \subset H'$$

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

$$H = H'$$

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

$$\mathfrak{Z} \times \Phi = \sum_{S \bmod .H} \bar{\mathfrak{Z}}^{S} = \sum_{S .\bmod .H} e^{S} (\mathfrak{Z} \times \Phi)$$

Comme $\quad e^{R} u_{S} = u_{S} e^{RS}$

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 $A \times \Phi$, ce qui justifie la relation(I3)

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

$$a^{*} = \sum_{S} u_{S} z_{S}^{*} \qquad z_{S}^{*} \in (\mathfrak{Z} \times \Phi)$$

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

$$\bar{a} = e\, a^{*}\, e = \sum_{S} e\, u_{S}\, z_{S}^{*}\, e = \sum_{S} u_{S}\, e^{S}\, e\, z_{S}^{*}$$

$$= \sum_{P \in H} u_{P}\, \bar{z}_{P} \qquad \bar{z}_{P} \in \bar{\mathfrak{Z}}$$

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

$$\overline{z}\, u_\rho = u_\rho\, \overline{z}^{\rho} \quad \text{pour tout } \overline{z} \in \overline{\mathcal{Z}}$$

$$u_\rho\, u_\sigma = u_{\rho\sigma}\, a_{\rho\sigma}$$

Donc $\overline{A} = (\overline{a}, \overline{\mathcal{Z}})$

$(\overline{a})$ 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 $\overline{u}_S = u$ est une $\mathcal{Z}$ -base du produit croisé $(a, \mathcal{Z})$ on a :

$$u^\mu = \overline{u}_{S^\mu}\, c_\mu \qquad c_\mu \in \mathcal{Z} \qquad (\mu = 1,2.....)$$

On peut donc prendre comme nouvelle base

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

et on a : $u^n = \alpha \qquad \alpha \in \mathcal{Z}$

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

$$u^{\mu+\nu} = u_{S^\mu S^\nu}\, a_{S^\mu S^\nu} = u^{\mu+\nu}\, a_{S^\mu S^\nu}\, a_{S^\mu S^\nu} = 1 \qquad (I4)$$

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

$$u^{\mu+\nu} = u_{S^\mu S^\nu}\, a_{S^\mu S^\nu} = u^{\mu+\nu-n}\, a_{S^\mu S^\nu}\, a_{S^\mu S^\nu} = \alpha \qquad (I5)$$

Ensuite, d'après (2) on a :

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

Donc α est un élément de ρ . Et inversement, si $\alpha \in \rho$, la condition d'associativité est bien satisfaite.

On pose, dans ce cas,

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

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

que α soit la norme d'un élément de $\mathcal{Z}$.

a) La condition est nécessaire

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

(I6) $$s_{s^\mu s^\nu} = \frac{c_{s^\nu}\, c_{s^\mu}^{s^\nu}}{c_{s^{\mu+\nu}}} \qquad c_{s^\mu} \neq 0 \text{ et } \in \mathcal{Z}$$

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

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

b) La condition est suffisante, car si

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

en posant

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

on vérifie sans peine que les nombres données par (I6) vérifient bien (I4) et (I5) , donc constituent le système de facteurs de (, , S).