LE SÉMINAIRE DE MATHÉMATIQUES 1933–1939

édition réalisée et annotée par
Michèle Audin

1. Année 1933-1934
Théorie des groupes et des algèbres

Jean Dieudonné

Théorie des Corps Gauches

Séminaire de mathématiques (1933-1934), Exposé 1-G, 17 p.

<http://books.cedram.org/MALSM/SMA_1933-1934__1__G_0.pdf>

Séminaire de mathématiques 26 février 1934
Exposé 1-G, p. 1 à 17

THÉORIE DES CORPS GAUCHES

par **Jean Dieudonné**

1.– Rappel de définitions et résultats antérieurs. Tous[1] les corps et algèbres envisagés sont pris sur un même *corps de base* commutatif et parfait.

On sait qu'un corps commutatif $\mathfrak{Z}$, de degré fini n sur P est engendré par une racine θ d'une équation irréductible de degré n :

$$f(x) = 0$$

à coefficients dans P. Le corps $\mathfrak{Z}$ est dit *galoisien* s'il contient aussi les $n-1$ autres racines de $f(x)=0$. Le groupe des 1-automorphismes de $\mathfrak{Z}$ laissant fixes les nombres[2] de P est le *groupe de Galois* G de $\mathfrak{Z}$. C'est un groupe d'ordre n[3] dont chaque substitution change θ en une autre racine de $f(x)=0$. Si S est une substitution de G, z un nombre de $\mathfrak{Z}$, 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[4] le *degré de l'algèbre* A par rapport à K. 1/2

2.– Théorie des produits croisés. (dûe [sic] à Mlle E.Nöther [re-sic]) exposée d'après un mémoire de Hasse, Transactions of the American mathematical Société [sic], 1932, t.34.)[5]

Soit $\mathfrak{Z}$ un corps *galoisien* de degré n sur P, G le groupe de Galois de $\mathfrak{Z}$; on désignera par $S, T, U, \ldots$ les substitutions de G, par E la substitution unité.

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

$$A = u_E\mathfrak{Z} + u_S\mathfrak{Z} + \cdots + u_T\mathfrak{Z}$$

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

$$\begin{cases} zu_S = u_S z^S & \text{si } z \in \mathfrak{Z} \\ u_S u_T = u_{ST} a_{S,T} \end{cases} \tag{1}$$

où $a_{S,T}$ est un élément $\neq 0$ de $\mathfrak{Z}$. L'ensemble des n^2 nombres $a_{S,T}$ 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 :

$$a_{S,T}^{U} = \frac{a_{ST,U} a_{T,U}}{a_{ST,U}} \tag{2}$$

Si $z_1, z_2, \ldots, z_n$ est une P-base de $\mathfrak{Z}$, on voit immédiatement que A est un *système hypercomplexe de rang* n^2 sur P, la P-base de A étant constituée par les éléments
2/3 $u_S z_k$.

On écrit : $A = (a, \mathfrak{Z})$

Propriétés élémentaires des produits croisés.

1e – *A possède une unité.*

$$e = u_E a_{E,E}^{-1}$$

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

$$e = 1, \text{ et pas suite: } u_E = a_{E,E}$$

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

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

Soit a un élément de A

$$a = \sum u_S z_S \qquad z_S \in \mathfrak{Z}$$

tel que : $az = za$ quel que soit $z \in \mathfrak{Z}$, on en tire d'après (1) :

$$\sum u_S z_S (z - z^S) = 0$$
$$\text{ou} \quad z_S (z - z^S) = 0$$

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

$$a = u_E z_E = a_{E,E} z_E \in \mathfrak{Z}$$

3e – *u_S possède un inverse u_S^{-1}.*

$$u_S^{-1} = u_{S^{-1}} a_{S,S^{-1}}^{-1} a_{E,E}^{-1}$$

3/4 comme on le vérifie sans peine.

4e – *La condition nécessaire et suffisante pour que :*

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

est que l'on ait

$$\overline{a}_{S,T} = a_{S,T}\frac{c_T c_S^T}{c_{ST}} \qquad c_S \neq 0 \text{ et dans } \mathfrak{Z} \tag{3}$$

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

$$\overline{u}_S = u_S c_S. \tag{3'}$$

On écrit dans ce cas : $(\overline{a}) \sim (a)$.

a) la condition est *nécessaire*, car des relations

$$z u_{S^{-1}} = u_{S^{-1}} z^{S^{-1}}, \qquad z\overline{u}_S = \overline{u}_S z^S$$

valables pour tout $z \in \mathfrak{Z}$, on tire que $u_{S^{-1}}\overline{u}_S$ est commutatif avec tous les éléments de $\mathfrak{Z}$, donc est dans $\mathfrak{Z}$ d'après 2e ; par suite : $u_S^{-1}\overline{u}_S$ est aussi dans $\mathfrak{Z}$, donc :

$$\overline{u}_S = u_S c_S$$

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 $\overline{u}_S$, satisfaisant aux relations (1) où l'on remplace les a par des $\overline{a}$, donc que A est égal au produit croisé $(\overline{a}, \mathfrak{Z})$.

3.– Structure des produits croisés.

Théorème I.

1e) Tout produit croisé est une algèbre simple.

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

4/5

1e) 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 $R, T, \ldots, U$ les substitutions de G pour lesquelles $y_S \neq 0$, zb et $b\overline{z}$ sont dans B, quelque soient z et $\overline{z}$ et aussi

$$b_1 = zb - b\overline{z} = \sum u_S y_S (z^S - z)$$

Prenons z primitif dans $\mathfrak{Z}$, et $\overline{z} = z^U$; b_1 ne contient plus u_U ; on recommence l'opération et on arrive finalement à

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

$$u_S = u_R u_{R^{-1}S} a_{R,R^{-1}S}^{-1}$$

ce qui montre que $B = A$.

2e) Désignons par $\mathfrak{M}$ la matrice à une ligne

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

soit $a = \sum u_S z_S$ un nombre quelconque de A. On a :

$$a\mathfrak{M} = M(\zeta_{S,T}) \tag{4}$$

$(\zeta_{S,T})$ étant la matrice carrée d'ordre n.

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

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

Considérons maintenant l'algèbre $A \times \overline{\mathfrak{Z}}$ ($\mathfrak{Z}$ et $\overline{\mathfrak{Z}}$ doivent être considérés comme *indépendants*).[6] On a :

$$A \times \overline{\mathfrak{Z}} = \sum u_S z_k \cdot \overline{\mathfrak{Z}}$$

5/6 et en passant de $u_S z_k$ à sa représentation dans $\overline{\mathfrak{Z}}_n$ on a une représentation de $A \times \overline{\mathfrak{Z}}$ dans $\overline{\mathfrak{Z}}_n$. Cette représentation est une *isomorphie de $A \times \overline{\mathfrak{Z}}$ sur un sous-anneau de $\overline{\mathfrak{Z}}_n$*, car $A \times \overline{\mathfrak{Z}}$ est *simple*, et si ce n'était pas une isomorphie $A \times \overline{\mathfrak{Z}}$ serait représenté sur le seul élément 0, ce qui n'est pas. Mais $A \times \overline{\mathfrak{Z}}$ est de rang n^2 sur $\overline{\mathfrak{Z}}$, donc aussi le sous-anneau de $\overline{\mathfrak{Z}}_n$ qui lui est isomorphe, et comme $\overline{\mathfrak{Z}}_n$ est lui-même de rang n^2 sur $\overline{\mathfrak{Z}}$, ce sous-anneau coïncide avec $\overline{\mathfrak{Z}}_n$, ce qui montre que $\overline{\mathfrak{Z}}$ est *corps de décomposition* de A.[7]

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.

1e) Tout corps gauche K (et par suite, toute algèbre simple) est semblable à un produit croisé.

2e) À chaque corps galoisien de décomposition $\overline{\mathfrak{Z}}$ de K, correspond un produit croisé $A = (a, \mathfrak{Z})$ semblable à K, $\mathfrak{Z}$ étant un corps isomorphe à $\overline{\mathfrak{Z}}$.

a) *Le degré n de $\overline{\mathfrak{Z}}$ est un multiple du degré m de K.*

En effet, par hypothèse, $K \times \overline{\mathfrak{Z}}$ est isomorphe à un anneau complet de matrices d'ordre m dans $\overline{\mathfrak{Z}}$: soit e_{ik} le système d'unités matricielles correspondant, et soit $R = e_{11}(K \times \overline{\mathfrak{Z}}) = (e_{11}, e_{12}, \dots, e_{1m})$ un idéal à droite minimum de $K \times \overline{\mathfrak{Z}}$. Soit r *le K-rang de R*; K étant de rang m^2 sur P, le P-*rang* de R est rm^2;
6/7 d'autre part le $\overline{\mathfrak{Z}}$-*rang* de R est m, et le rang de $\overline{\mathfrak{Z}}$ sur P étant n, le P-*rang* de R est aussi nm, d'où

$$rm^2 = nm$$
$$n = rm$$

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

Soit $\mathfrak{w} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ une *K-base de R*, considéré comme K-module à droite ($\alpha_i \in (K \times \overline{\mathfrak{Z}})$). Si $\zeta \in \overline{\mathfrak{Z}}$, $\zeta\alpha_i = \alpha_i\zeta \in R$, donc

$$\zeta\alpha_i = \alpha_1 x_1^i + \alpha_2 x_2^i + \cdots + \alpha_r x_r^i \qquad x_i^j \in K$$

ou

$$\zeta\mathfrak{w} = \mathfrak{w} z_\zeta \tag{5}$$

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

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

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

Par définition, on pose

$$z_\zeta^S = z_{\zeta\Sigma} \tag{6}$$

ce qui définit les substitutions S du groupe de Galois G de $\mathfrak{Z}$, isomorphe à Γ. 7/8

D'autre part, *prolongeons* Γ en un groupe d'automorphismes de $K \times \overline{\mathfrak{Z}}$, en lui imposant 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_{ik}^Σ ; $R = e_{11}(K \times \overline{\mathfrak{Z}})$ se change en $R^\Sigma = e_{11}^\Sigma(K \times \overline{\mathfrak{Z}})$, la K-base $\mathfrak{w}$ de R se change en une K-base $\mathfrak{w}^\Sigma$ de R^Σ.

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

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

On en déduit

$$\begin{aligned} R^\Sigma &= q_\Sigma e_{11} q_\Sigma^{-1}(R \times \overline{\mathfrak{Z}}) = q_\Sigma e_{11}(K \times \overline{\mathfrak{Z}}) \\ &= q_\Sigma R \end{aligned}$$

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

$$q_\Sigma\mathfrak{w} = \mathfrak{w}^\Sigma u_S \tag{7}$$

u_S matrice inversible dans $K_r = A$.

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

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

ou d'après (7)

$$\zeta^\Sigma q_\Sigma \mathfrak{w} u_S^{-1} = q_\Sigma \mathfrak{w} u_S^{-1} z_\zeta$$

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

$$\zeta^\Sigma \mathfrak{w} = \mathfrak{w} u_S^{-1} z_\zeta u_S$$

8/9 ou d'après (6) :

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

(c'est la 1ère condition (1)).

Ensuite :

$$\begin{aligned} z^{ST} = (z^S)^T = u_T^{-1} z^S u_T = u_T^{-1} u_S^{-1} z u_S u_T \\ = u_{ST}^{-1} z u_{ST} \end{aligned}$$

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

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

D'où on tire

$$u_S u_T = u_{ST} \alpha_{S,T}^{ST} = u_{ST} a_{S,T} \qquad a_{S,T} \neq 0 \text{ et dans } \mathfrak{Z}$$

(c'est la 2ème condition (1)).

d) Pour montrer que

$$A = (a, \mathfrak{Z}) \text{ où } a = (a_{S,T})$$

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

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

$$\sum u_S y_S = 0 \qquad y_S \in \mathfrak{Z}$$

on tire

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

9/10 On procède comme ci-dessus (Th.I, première partie) et on en tire :

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

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 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 :

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

5.– Théorie générale des corps de décomposition. Dans le cours de la démonstration précédente, on a établi les propositions suivantes :

1. *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 dgré n, semblable à K, contient un sous-corps commutatif maximum $\mathfrak{Z}$ isomorphe à $\overline{\mathfrak{Z}}$.*

Quand P est un corps *algébrique de degré fini*, on peut énoncer les réciproques suivantes (voir Van der Waerden t.II, p.210) :

1. *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.

10/11

6.– Classes d'algèbres simples et classes de systèmes de facteurs associés. Si une algèbre simple A sur P est isomorphe à un anneau total de matrices P_k sur P, on écrit $A \sim 1$ au lieu de $A \sim \mathsf{P}$.

Théorème 3. *Si $(a) \sim 1$, $(a, \mathfrak{Z}) \sim 1$.*

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

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

$$(\zeta_a) = A_a$$

d'où

$$a\mathcal{M} = \mathcal{M}A_a \tag{4'}$$

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 tire de (4')

$$a\mathcal{M}C = \mathcal{M}CC^{-1}A_aC = \mathcal{M}C\overline{A}_a$$

en posant

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

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

$$Cu_R = u_RC^R$$

11/12

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

$$\text{donc} \qquad a(\mathcal{M}u_R C^R) = a(\mathcal{M}Cu_R)$$

$$= \mathcal{M}C\overline{A}_a u_R = (\mathcal{M}Cu_R)\overline{A}_a^R = (\mathcal{M}u_R C^R)\overline{A}_a^R$$

$$\text{Mais} \qquad C^R = (z_k^{SR})$$

$$\mathcal{M}u_R C^R = (\sum_P u_P u_R z_k^{PR}) \qquad \text{(matrice à 1 ligne)}$$

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

d'où

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

et par suite

$$\overline{A}_a^R = \overline{A}_a \qquad \text{quel que soit } R,$$

les éléments de $\overline{A}_a$ sont donc dans P. $\overline{\mathfrak{A}}$ est un sous-anneau de P_n ; mais comme le P-rang de $\overline{\mathfrak{A}}$ est égal à n^2, $\overline{\mathfrak{A}}$ *est identique à* P_n, donc

$$(a, \mathfrak{Z}) \sim 1$$

Théorème 4. *Si l'algèbre simple $(a, \mathfrak{Z})$ a pour indice (degré du corps semblable à $(a, \mathfrak{Z})$), m, on a :*

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

(c'est donc une réciproque du théorème précédent).

Soit K le corps gauche de degré m, semblable à $A = (a, \mathfrak{Z})$. On a donc :

$$A = K \times \mathsf{P}_r \qquad \text{si } n = rm$$

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 $\mathfrak{Z}$-*rang* de R (considéré comme $\mathfrak{Z}$-module à droite), le P-*rang* de R est
12/13 égal à kn ; d'autre part, le K-*rang* de R est r, donc on a :

$$kn = rm^2 \qquad k = m$$

Soit $\mathfrak{w}$ une $\mathfrak{Z}$-*base* de R ; les éléments de $\mathfrak{w}u_S$ sont dans R, donc

$$\mathfrak{w}u_S = \mathfrak{w}B_S$$

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

$$\mathfrak{w}u_S u_T = \mathfrak{w}B_S u_T = \mathfrak{w}u_T B_S^T = \mathfrak{w}B_T B_S^T$$

$$= \mathfrak{w}u_{ST}a_{S,T} = \mathfrak{w}B_{ST}a_{S,T}$$

et par suite

$$B_T B_S^T = B_{ST}a_{S,T} \tag{8}$$

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 :

$$c_T c_S^T = c_{ST} a_{S,T}^m$$

et d'après (3) on en tire

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

Théorème 5. *On a* $(a, \mathcal{Z}) \times (\overline{a}, \mathcal{Z}) \sim (a\overline{a}, \mathcal{Z})$.

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

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

u_S et $\overline{u}_S$ étant respectivement la $\mathcal{Z}$-base de A et la $\overline{\mathcal{Z}}$-base de $\overline{A}$. 13/14

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

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

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

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

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

On verra plus bas que les n unités de ces n 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 $\mathcal{Z}$. On le prolonge en un groupe d'automorphismes de $\mathcal{Z} \times \overline{\mathcal{Z}}$ en lui imposant de laisser invariants les éléments de $\overline{\mathcal{Z}}$. Si R est une substitution de G, e^R le transformé de e par R, on a :

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

$\mathcal{Z}'^R$ est donc un corps isomorphe à $\mathcal{Z}$ contenu dans $\mathcal{Z} \times \overline{\mathcal{Z}}$: c'est donc nécessairement un des corps dont $\mathcal{Z} \times \overline{\mathcal{Z}}$ est la somme directe. (En effet, si $\mathcal{Z} \times \overline{\mathcal{Z}} =$ 14/15

$e_1\mathfrak{Z} \oplus e_2\mathfrak{Z} \oplus \cdots \oplus e_n\mathfrak{Z}$, les e_i tels que $e_i^2 = e_i$ $e_ie_j = 0$, les seuls idempotents de $\mathfrak{Z} \times \overline{\mathfrak{Z}}$ sont des nombres de la forme :

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

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 tel corps, il se réduit à l'un de ses composants).

Les n corps $\mathfrak{Z}'^R$ (R parcourant toutes les substitutions de G) sont *distincts* ; 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, $\mathfrak{Z} \times \overline{\mathfrak{Z}} = \sum_R e^R\mathfrak{Z}$ (somme directe) et si $s^\star$ est un nombre de $\mathfrak{Z} \times \overline{\mathfrak{Z}}$, on a l'*unique* représentation :

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

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

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

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

15/16 Donc, $z_R^S = z_{RS}$ et en particulier, si $R = E$, $z_R = z_E^R = z^R$ en posant $z_E = z$. Donc

$$\overline{z} = \sum_R e^R z^R \qquad z \in \mathfrak{Z} \tag{9}$$

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 $\mathfrak{Z} \times \overline{\mathfrak{Z}}$ en lui imposant 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 telle 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

$$e^{R\overline{S}} = e^{S^{-1}R} \tag{10}$$

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

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

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

$$e^R u_S = u_S e^{RS} \tag{11}$$

$$e^R \overline{u}_S = \overline{u}_S e^{R\overline{S}} = \overline{u}_S e^{S^{-1}R} \tag{12}$$

De la relation (11), on en déduit que : 16/17

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

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 $a^\star$ un élément de $A \times \overline{A}$

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

$$\text{ou} \quad a^\star = \sum_{R,S,T} u_S \overline{u}_T e^R z_{RST} \qquad z_{RST} \in \mathcal{Z}$$

cette représentation étant *unique*. L'élément correspondant de A' est donc

$$\begin{aligned} a' = ea^\star e &= \sum_{R,S,T} eu_S \overline{u}_T e^R z_{RST} e \\ &= \sum_{R,S,T} u_S \overline{u}_T e^{T^{-1}S} \cdot e^R \cdot e \cdot z_{RST} = \sum_S u_S \overline{u}_S e z_{ESS} \end{aligned}$$

Posons

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

On a $a' = \sum_S u'_S z'_S$ et la représentation est encore *unique*, le P-rang de A' étant n^2. Les u'_S sont donc une $\mathcal{Z}'$-base de A'. De plus, quel que soit $z' = ez$

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

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

$$\begin{aligned} u'_S u'_T &= u_S \overline{u}_S e u_T \overline{u}_T e = u_S u_T \overline{u}_S \overline{u}_T e \\ &= u_{ST} a_{S,T} \overline{u}_{ST} \overline{a}_{S,T} e = u_{ST} \overline{u}_{ST} e a_{S,T} \overline{a}_{S,T} \\ &= u_{ST} \overline{u}_{ST} e a'_{S,T} \overline{a}'_{S,T} \end{aligned}$$

où 17/18

$$a'_{S,T} = e a_{S,T} \qquad \overline{a}'_{S,T} = e \overline{a}_{S,T}$$

sont des nombres de $\mathcal{Z}'$. Ceci établit donc bien que :

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

7.– Groupe de classes d'algèbres simples semblables. On sait que si entre des algèbres simples, A, B, A', B' on a les relations

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

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* 18/19 *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 $n = rm = p^\nu n'$, n' premier avec p. D'après un théorème de Sylow, $\mathcal{Z}$ possède un sous-corps Σ de degré n' sur P. Σ *n'est pas un corps de décomposition* pour A, car son degré n'est pas un 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 $(\mu \leqslant \nu)$; 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 $\frac{\ell}{p_1^{\lambda_1}}, \frac{\ell}{p_2^{\lambda_2}}, \ldots, \frac{\ell}{p_k^{\lambda_k}}$ étant premiers entre eux dans leur ensemble, on peut trouver k nombres $q_1, q_2, \ldots, q_k$ tels que

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

19/20

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

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

$$\prod_i K_i = K \times \mathsf{P}_r$$

et par suite

$$\prod_i p_i^{\mu_i} = rm$$

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 $r = 1$

$$K = \prod_i K_i$$

6.– Extension du corps de base P. Soit Φ un corps commutatif, extension parfaite du corps de base P.

Théorème 7. *On a :*

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

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

Soit $A = (a, \mathfrak{Z})$ de degré n. (La démonstration est tout à fait analogue à celle du théorème 5). 20/21

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

$$A \times \Phi \sim \overline{A} = e(A \times \Phi)e \tag{13}$$

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

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

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 $\overline{\mathfrak{Z}}$. 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-groupe H' de G qui correspond au
21/22 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 eF et par suite au groupe des automorphismes de $\overline{\mathfrak{Z}}$ par rapport à $e\Phi$, donc à H, ce qui entraîne :

$$H = H'$$

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

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

Comme $e^R u_S = u_S e^{RS}$ on voit que les k^2 quantités

$$a_{S,T} = u_S^{-1} u_T e^T$$

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 (13)

c) Si $a^\star$ appartient à $A \times \Phi$, on a

$$a^\star = \sum_S u_s z_S^\star \qquad z_S^\star \in (\mathfrak{Z} \times \Phi)$$

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

$$\overline{a} = e a^\star e = \sum_S e u_S z_S^\star e = \sum_S u_S e^S e z_S^\star$$
$$= \sum_{P \in H} u_P \overline{z}_P \qquad \overline{z}_P \in \overline{\mathfrak{Z}}$$

et cette représentation est unique d'après le Φ-rang de A. Les u_P forment donc
22/23 une $\overline{\mathfrak{Z}}$-base de $\overline{A}$, et de plus,

$$\overline{z} u_P = u_P \overline{z}^P \quad \text{pour tout } \overline{z} \in \overline{\mathfrak{Z}}$$
$$u_P u_Q = u_{PQ} a_{P,Q}$$

Donc $\overline{A} = (\overline{a}, \overline{\mathfrak{Z}})$, $(\overline{a})$ 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 $\mathfrak{Z}$-base du produit croisé $(a, \mathfrak{Z})$, on a :

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

On peut prendre comme nouvelle base

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

et on a : $u^n = \alpha \in \mathfrak{Z}$. Donc si $\mu < n$, $\nu < n$, $\mu + \nu < n$, on a

$$u^{\mu+\nu} = u_{S^\mu S^\nu} a_{S^\mu, S^\nu} = u^{\mu+\nu} a_{S^\mu, S^\nu} \qquad a_{S^\mu, S^\nu} = 1 \tag{14}$$

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

$$u^{\mu+\nu} = u_{S^\mu S^\nu} a_{S^\mu, S^\nu} = u^{\mu+\nu-n} a_{S^\mu, S^\nu} \qquad a_{S^\mu, S^\nu} = \alpha \tag{15}$$

Ensuite, d'après (2) on a :

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

Donc α *est un élément de* P. Et inversement, si $\alpha \in \mathsf{P}$ la condition d'associativité est bien satisfaite. On pose, dans ce cas,

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

La condition nécessaire et suffisante pour que $A \sim 1$ *est que* α *soit la norme d'un élément de* $\mathfrak{Z}$. 23/24

a) La condition est *nécessaire*

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

$$a_{S^\mu, S^\nu} = \frac{c_{S^\nu} c^{S^\nu}_{S^\mu}}{c_{S^{\mu+\nu}}} \qquad c_{S^\mu} \neq 0 \text{ et } \in \mathfrak{Z} \tag{16}$$

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

$$\alpha = N(c) \text{ où } c = c_S \in \mathfrak{Z}$$

b) La condition est *suffisante*, car si

$$\alpha = N(c) = c \cdot c^S \cdots c^{S^{n-1}}$$

en posant

$$c_{S^\mu} = \prod_{P=0}^{\mu-1} c^{SP}$$

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

Notes

1. Les travaux utilisés dans cet exposé sont l'article [Has32] de Hasse, dont le texte est très fortement inspiré, et toujours le livre [vdW31].
2. En conformité avec les hésitations sur les notations ($\in$, $\subset$...), noter que la pensée « ensembliste » n'est pas encore formée. Comme Élie Cartan, le jeune Dieudonné appelle les éléments d'un corps les « nombres » de ce corps.
3. Il est difficile d'imaginer que Dieudonné ait vraiment cru que le groupe de Galois était d'ordre n. À sa décharge : dans l'article de Hasse, l'extension considérée est cyclique. L'entier n va vraiment désigner l'ordre du groupe dans l'exposé.
4. Le « commandement » de ne pas commencer une phrase par un symbole mathématique, dont la pertinence apparaît ici, n'était pas respecté par ces auteurs non plus.
5. L'article « américain » [Has32] de Hasse a été écrit en anglais et publié aux États-Unis parce que son auteur voulait faire connaître aux Américains ce qui se faisait en Allemagne. Dans cet article est introduite la traduction *crossed product* du terme allemand *verschränktes Produkt*, qu'Emmy Noether avait appréciée. Voir [Roq05, Note 21].
6. Rappelons (voir les notes de l'exposé 1-D) que la notation $\times$ désigne le produit tensoriel.
7. L'expression « corps de décomposition » a pris depuis un sens différent. Ici (elle n'est pas définie dans l'exposé) elle désigne un $\mathfrak{Z}$ dans une écriture $A = (a, \mathfrak{Z})$.

Des archives du séminaire...

Compte-rendu de la séance du 26 Février 1934

1. La séance est ouverte à 16h.30. MM.Cartan et Hadamard, retenus, n'y assistent pas [1].

2. La parole est donnée à Dieudonné, qui fait un exposé sur les corps gauches.

3. À la fin de l'exposé et sur la demande même de Dieudonné une discussion s'engage sur la terminologie : le mot de produit croisé, traduction littérale de l'allemand, lui paraît fâcheuse [sic]. La question n'est pas résolue.

La rédaction de cet exposé contiendra les démonstrations qui, faute de temps, n'ont pu être indiquées ces démonstrations sont celles qu'a données Hasse dans le mémoire cité mémoire dont la lecture est rendue difficile par de nombreuses fautes d'impression.

Un autre exposé de la question se trouvera d'ailleurs dans un ouvrage, à paraître prochainement, de Döring [Deuring].

Enfin M.Julia remercie en son nom et pour tous Dieudonné.

4. Thé. Conversations. Discussions. La séance est levée à 18h.30 [2].

1. Rappelons que ce jour-là s'est tenue une réunion de l'Académie des sciences en « comité secret », préparant l'élection d'un nouveau membre (qui fut Gaston Julia), et que cette réunion dura jusqu'à $17^{\text{h}}45$. Voir le § 2.1.1.

2. Une page ronéotypée, archives de l'IHP.

Références

[Has32] H. Hasse – « Theory of cyclic algebras over an algebraic number field », *Trans. Am. Math. Soc.* **34** (1932), p. 171–214.

[Roq05] P. Roquette – *The Brauer-Hasse-Noether theorem in historical perspective*, Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences], vol. 15, Springer-Verlag, Berlin, 2005.

[vdW31] B. van der Waerden – *Moderne Algebra. Unter Benutzung von Vorlesungen von E. Artin und E. Noether. Bd. II*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Springer, 1931.