Algèbre non commutative

Emmy Noether

Göttingen

Les principaux théorèmes de l'algèbre commutative sont, comme on le sait, contenus dans la théorie de Galois, elle-même précédée par la théorie des corps de décomposition et de factorisation – c'est-à-dire les corps suffisants pour qu'un polynôme donné puisse être décomposé en un facteur linéaire ou se factoriser complètement en facteurs linéaires.

Je développe ici les parties correspondantes de l'algèbre dans le domaine non commutatif, et plus particulièrement dans le domaine hypercomplexe. Plus précisément, je travaille principalement avec des méthodes non commutatives, notamment la représentation dans les corps non commutatifs. Enfin, je montre comment les théorèmes susmentionnés de l'algèbre commutative peuvent être obtenus parallèlement, à l'aide de la représentation dans les corps commutatifs.

La théorie des représentations sous-jacente – précédée d'une brève théorie des automorphismes (§ 1) – constitue un développement de la théorie des représentations basée sur la théorie des modules de représentation (voir E. Noether, "*Hypercomplex quantities and representation theory*", Math. Zeitschr. 30 (1929), p. 641–692, cité comme *Representation theory.* Cf. la reproduction de cet article dans van der Waerden, *Moderne Algebra* II). En particulier, je considère non seulement la représentation directe, mais aussi la représentation réciproque – l'une pouvant être réduite à l'autre – engendrée ici par le module de représentation réciproque. L'avantage est que ce module – qui est un module double – peut également être vu comme un module unilatéral dans l'anneau d'extension (§ 2). Ceci ramène la représentation dans les corps non commutatifs à la théorie des idéaux dans l'anneau d'extension. Les classes de représentation irréductibles correspondent aux classes d'idéaux irréductibles de l'anneau d'extension, en analogie exacte avec les faits qui s'appliquent au système lui-même lorsqu'il représente des systèmes hypercomplexes dans leur domaine de coefficients commutatifs (§ 3 et 4).

De là découlent les théorèmes de structure pour les anneaux de matrices sur les corps non commutatifs, à partir de la remarque (§ 5) selon laquelle chaque sous-anneau représente une représentation par ce corps, ou une représentation réciproque par le corps réciproquement isomorphe. Ce corps réciproquement isomorphe constitue un premier analogue des corps de décomposition et de scindage minimaux dans l'anneau commutatif, dans la mesure où il assure la médiation de toutes les représentations réciproques de degré un et, avec un centre de rang fini – ce qui n'était pas supposé auparavant –, également une décomposition complète en facteurs directs de rang 1. Ceci conduit à la théorie de Galois pour les corps (§ 6) et exprime simultanément le fait (§ 7) que les algèbres à division réciproquement isomorphes (corps de centre de rang fini) engendrent des classes inverses dans le groupe des classes d'algèbres de R. Brauer. Une seconde justification de la théorie galoisienne, qui s'applique plus généralement aux systèmes simples (qui précèdent dans le texte), est une conséquence presque immédiate d'un théorème sur les sous-anneaux commutatifs, qui est lui-même

Reçu le 8 juin 1932.

Référence : https://eudml.org/doc/168463.

: tentative de traduction avec les outils Google en n'étant pas germaniste : Denise Vella-Chemla, février 2026.

presque directement lié à la considération précédente des automorphismes.

Jusqu'ici, les considérations ont été exclusivement non commutatives. Cependant, la question des corps de décomposition commutatifs est également traitée de manière non commutative, du fait de la représentation du corps de décomposition par l'algèbre à division, conformément à la remarque faite au § 5 (§ 7). La conclusion consiste en le transfert susmentionné au domaine commutatif (§ 8) et la théorie des corps de décomposition pour des systèmes quelconques (§ 9), établissant simultanément le lien avec la théorie des représentations usuelle dans le domaine commutatif. R. Brauer a fondé sa théorie des corps de décomposition sur cette théorie de la représentation dans le domaine commutatif et sur les systèmes de facteurs "irrationnels" (Voir notre note commune : "*Sur les corps de décomposition minimaux des représentations irréductibles*", Sitz. Ber. d. Preuß. Ak. d. Wiss, 1927, p. 221-228 (La note p. 222 présente un compte-rendu de ces travaux). Les principaux théorèmes ont été écrits indépendamment et presque simultanément). Voir aussi R. Brauer, "*Sur les systèmes de nombres hypercomplexes*", S. 3. Math. Zeitschr. 30 (1929), p. 79-107. Albert a redécouvert ces théorèmes indépendamment par la suite. Du fait de cette justification commutative, il dut, comme Albert plus tard, supposer que le centre était un corps parfait, restriction inutile selon la justification non commutative. Avec la même restriction, et en utilisant également la théorie des représentations dans le domaine commutatif, R. Brauer et K. Shoda développèrent davantage la théorie après avoir pris connaissance de ma théorie galoisienne pour les corps non commutatifs : R. Brauer énonça le théorème susmentionné sur les sous-anneaux commutatifs, et K. Shoda développa indépendamment la théorie complète, y compris pour les systèmes semi-simples. (Voir : R. Brauer, *Über die algebraische Struktur von Seckfeldern*, 2. Journ. f. Math. 166 (1932), p. 241-252. K. Shoda, *Über die galoissche Theorie der halb-einfachen hyperkomplexen Systeme*. Math. Ann. 107 (1932), p. 252-258. Ces résultats avaient également été développés par J. Levitzki).

Enfin, il convient de mentionner qu'une brève présentation du cas des corps se trouve dans van der Waerden II (p. 128), faisant suite à ma conférence de l'été 1928, où j'ai abordé ces questions pour la première fois. La présentation de van der Waerden introduit un certain nombre de simplifications par rapport à cette conférence, dont certaines ont été reprises et développées dans une seconde conférence (à l'hiver 1929-1930), et d'autres sont seulement reprises ici. En particulier, le transfert de la méthode de démonstration hypercomplexe de la théorie galoisienne au domaine commutatif (§ 8) provient de la seconde conférence, où la démonstration non commutative (§ 6.3) a été considérablement simplifiée par rapport à la première conférence. Le théorème sur les sous-anneaux commutatifs (§ 5) et la deuxième méthode de preuve de la théorie galoisienne non commutative basée sur celui-ci (§ 6.1 et 6.2) n'ont été ajoutés qu'après la deuxième conférence, après connaissance de R. Brauer (cf note de bas de page n° 3) et van der Waerden p. 128 ; cependant, dans le § 5.3, il existe des hypothèses de finitude considérablement moins strictes que là.

Certaines inférences de la première conférence, la méthode d'intersection des idéaux de différence, bien que plus complexe, ont l'avantage d'être transposables aux systèmes de rang infini et aux systèmes entiers. Cette méthode est essentiellement reproduite dans G. Köthe, "*Skew Fields of Infinite Rank over the Center*" (§ 5, Math. Ann. 105 (1931), p. 15-39. Voir aussi la note de bas de page n° 10). Cette méthode d'intersection est alors remplacée par le fait presque trivial (§ 4.1), que van der Waerden a remarqué le premier, que les idéaux bilatères appartiennent aux modules invariants. Ceci permet de tout justifier par la décomposition en somme directe plus simple, qui, cependant,

échoue pour le rang infini et dans le cas entier. Pour les systèmes entiers commutatifs, on arrive ainsi au lien entre la différentiation idéale et les différences. Voir la conférence donnée à Prague, Jahresber. d. Deutsch. Math. Ver. 39 (1930), p. 17 (pagination oblique) que je discuterai plus en détail à un moment donné.

La théorie des corps de décomposition trouve son application principale dans la théorie des produits intriqués et de leurs systèmes de facteurs, qui constituent eux-mêmes le fondement d'applications en théorie des nombres ; ce sujet ne sera pas approfondi ici. La théorie des produits intriqués a été développée lors de la deuxième conférence ; elle est reproduite, avec quelques modifications mineures afin de ne pas présupposer la théorie présentée ici, dans H. Hasse : "*Theory of cyclic algebras over an algebraic numberfield*", chapitre II, *Transactions of the Amer. Math. Soc.* 34 (1932), 8, 171-214. Une présentation plus fidèle à la conférence paraîtra dans un compte rendu de M. Deuring dans les "*Ergebnisse der Mathematik*".

1. Automorphismes, modules et modules doubles.

La théorie des représentations basée sur les modules de représentation est connue (voir aussi le § 2) pour reposer sur la théorie des anneaux d'automorphismes des groupes abéliens, avec ou sans opérateurs. Afin d'éviter les répétitions, les relations d'inférence sous-jacentes entre les applications et les lois de calcul seront formulées dans quelques théorèmes simples.

1.1. Application multiplicative, loi associative.

Soit $\mathfrak{G}$ un groupe sans opérateurs, et $\mathfrak{A}$ son anneau d'automorphismes absolus, c'est-à-dire le système de tous les homomorphismes de $\mathfrak{G}$ dans lui-même. $\mathfrak{A}$ est multiplicativement clos, puisque le produit $\sigma\tau$ est défini par

$$g(\sigma\tau) = (g\sigma)\tau \quad \text{avec} \quad g \text{ dans } \mathfrak{G} \quad \text{et} \quad \sigma, \tau \text{ dans } \mathfrak{A} \tag{1}$$

est défini et vérifie l'associativité.

On sait que $\mathfrak{G}$ est un groupe muni d'opérateurs si un ensemble $\mathfrak{B}$ de symboles $\Theta, H, \ldots$ est donné, tel que les opérations $g\Theta, gH, \ldots$ produisent des éléments uniques de $\mathfrak{G}$ et engendrent des automorphismes (homomorphismes sur eux-mêmes) de $\mathfrak{G}$ – $(g \cdot h)\Theta = g\Theta \cdot h\Theta$; ainsi, il existe une application unique (généralement non inversiblement unique) de $\mathfrak{B}$ vers un sous-ensemble $\overline{\mathfrak{B}}$ de l'anneau des automorphismes absolus $\mathfrak{A}$. L'inférence mentionnée ci-dessus est donc :

Si le domaine d'opérateurs $\mathfrak{B}$ est multiplicativement clos, alors l'application bijective de $\mathfrak{B}$ vers $\overline{\mathfrak{B}}$ est multiplicativement homomorphe si et seulement si la relation associative correspondant à (1) est

$$g(\Theta H) = (g\Theta)H \quad \text{pour} \quad g \text{ dans } \mathfrak{G} \quad \text{et} \quad \Theta, H \text{ dans } \mathfrak{B} \quad \text{est satisfaite.} \tag{1a}$$

Par conséquent, un homomorphisme réciproque est défini lorsque les opérateurs sont des opérateurs à gauche.

L'application de $\mathfrak{B}$ vers $\overline{\mathfrak{B}}$ est donnée par $g\Theta = g\sigma$ pour tout g dans $\mathfrak{G}$, et donc également par $(g\Theta)H = (g\sigma)\tau = g(\sigma\tau)$, de sorte que (1a) devient une condition nécessaire et suffisante pour un homomorphisme multiplicatif. Le fait que les opérateurs à gauche engendrent des homomorphismes réciproques provient du fait que les automorphismes à gauche $\sigma^* g, \tau^*\sigma^* g$ se lisent de droite à gauche : $\tau^*\sigma^* g = g\sigma\tau$, tandis que les opérateurs se lisent toujours de gauche à droite.

1.2. Homomorphisme d'opérateurs.

Si $\mathfrak{G}$ est un groupe muni d'opérateurs, alors l'homomorphisme d'opérateurs est défini par

(2) $$(g\Theta)\sigma = (g\sigma)\Theta \text{ ou bien} \qquad (2^*)\ (\Theta g)\sigma = \Theta(g\sigma),$$

C'est-à-dire par interconnexion commutative ou par une loi d'associativité continue. De là, en suivant l'inférence 1 – application sur le domaine des automorphismes – pour deux domaines d'opérateurs différents, on obtient les résultats suivants :

Étant donnés deux domaines d'opérateurs $\mathfrak{B}$ et $\mathfrak{C}$ avec respectivement les éléments $\Theta, H, \ldots$ et $\overline{\Theta}, \overline{H}, \ldots$, alors les éléments de $\mathfrak{C}$ engendrent des automorphismes de $\mathfrak{B}$, et simultanément les éléments de $\mathfrak{B}$ engendrent des automorphismes de $\mathfrak{C}$, si et seulement si les domaines sont commutativement connexes à $\mathfrak{G}$, c'est-à-dire si la loi d'associativité continue est satisfaite :

(2a) $$(g\Theta)\overline{H} = (g\overline{H})\Theta, \qquad (2a^*)\quad (\Theta g)\overline{H} = \Theta(g\overline{H}).$$

1.3. Modules et doubles modules par anneaux.

Un module à droite $\mathfrak{M}$ par un anneau $\mathfrak{R}$ est défini comme un groupe abélien additif dont les éléments de $\mathfrak{R}$ sont les opérateurs à droite. Outre la relation d'associativité (1a) et la relation définissant les opérateurs $(g + h)\Theta = g\Theta + h\Theta$, la relation de distributivité

(3a) $$g(\Theta + H) = g\Theta + gH$$

est vérifiée ; il en va de même pour les modules à gauche.

Parmi les modules doubles, on peut distinguer deux types : les modules à droite, selon deux anneaux $\mathfrak{R}$ et $\mathfrak{S}$, sont appelés modules doubles si, outre les opérations (1a, 3a) qui s'appliquent individuellement à $\mathfrak{R}$ et $\mathfrak{S}$, $\mathfrak{R}$ et $\mathfrak{S}$ sont également commutativement liés à $\mathfrak{M}$ en vertu de (2a) ; Les modules $\mathfrak{R}$-gauche et $\mathfrak{S}$-droite sont appelés modules doubles si l'on ajoute (2a*), la loi d'associativité continue, aux autres opérations.

L'importance de ces opérations découle du fait que, dans le cas des groupes abéliens, le domaine des automorphismes absolus forme un anneau, l'anneau des automorphismes absolus. Pour les groupes non abéliens, il s'agit d'un anneau "généralisé" ; voir l'article de H. Fitting paru dans les *Math. Annalen* [*Math. Annalen* 107, p. 514-542]. Plus précisément, l'inférence d'applications donne :

Si le domaine d'opérateurs $\mathfrak{R}$ d'un groupe abélien (écrit de manière additive) $\mathfrak{M}$ est un anneau, alors l'application unique de $\mathfrak{R}$ vers un sous-ensemble $\overline{\mathfrak{R}}$ de l'anneau d'automorphismes absolus est homomorphe à l'anneau si et seulement si $\mathfrak{M}$ est un sous-module à droite de $\mathfrak{R}$ – c'est-à-dire si (1a) et (3a) sont satisfaits – et réciproquement pour "homomorphe à l'anneau sous module à gauche".

Si $\mathfrak{M}$ est un module à droite par rapport aux anneaux $\mathfrak{R}$ et $\mathfrak{S}$, alors $\mathfrak{M}$ devient un double module (2a) si et seulement si $\mathfrak{R}$ est envoyé sur un sous-anneau de l'anneau d'automorphismes de $\mathfrak{R}$. Le double module (2a*) désigne l'application homomorphe de $\mathfrak{S}$ sur un sous-anneau de l'anneau d'automorphismes de $\mathfrak{R}$ et qui, simultanément, envoie $\mathfrak{S}$ sur un sous-anneau de l'anneau d'automorphismes de $\mathfrak{R}$ de manière homomorphe. Si $\mathfrak{M}$ est un module à droite par rapport à $\mathfrak{S}$ et un module à gauche par rapport à $\mathfrak{R}$, alors le double module (2a*) désigne l'application homomorphe de $\mathfrak{S}$ vers un sous-anneau de l'anneau d'automorphismes $\mathfrak{R}$, et l'application homomorphe réciproque de $\mathfrak{R}$ vers un sous-anneau de l'anneau d'automorphismes $\mathfrak{S}$.

La dernière affirmation clarifie les conséquences connues : 1) Si $\mathfrak{R}$ est un anneau possédant un élément neutre, alors $\mathfrak{R}$ est non seulement directement isomorphe à son anneau d'automorphismes en tant que module à gauche de $\mathfrak{R}$, mais il est également réciproquement isomorphe à son anneau d'automorphismes en tant que module à droite de $\mathfrak{R}$. Ceci est dû au fait que la loi d'associativité (2a*) est satisfaite, et donc à l'énoncé d'homomorphisme. L'existence de l'élément neutre implique l'existence de tout automorphisme de la forme $e \to a$ de $\mathfrak{R}$, ce qui garantit l'isomorphisme et implique que $\mathfrak{R}$ épuise son anneau d'automorphismes.

2) $\mathfrak{R}$ est-il un anneau de matrices complet sur un corps généralement non commutatif A ?

$$\mathfrak{R} = \sum c_{ik}\ \mathsf{A} = \sum \mathsf{A}\ c_{ik},$$

Ainsi, A est réciproquement isomorphe au corps des automorphismes des idéaux simples à droite et directement isomorphe au corps des automorphismes des idéaux simples à gauche.

Puisque tout idéal simple à droite est opérateur-isomorphe à un module à gauche A et à un module à droite $\mathfrak{R}$, A épuise les automorphismes de $\mathfrak{R}$; il en va de même pour les idéaux à gauche.

1.4. Transition d'un module double à droite à un module unilatéral par un anneau produit.

L'importance du module double à droite repose essentiellement sur cette transition.

Théorème : Si $\mathfrak{M}$ est un module à droite par un anneau $\mathfrak{I}$ contenant deux sous-anneaux interchangeables élément par élément $\mathfrak{R}$ et $\mathfrak{S}$, alors $\mathfrak{M}$ peut également être exprimé comme un double module par $\mathfrak{R}$ et $\mathfrak{S}$. Réciproquement, s'il existe un double module selon $\mathfrak{R}$ et $\mathfrak{S}$, et un anneau

produit $\mathfrak{I}$ dans lequel $\mathfrak{R}$ et $\mathfrak{S}$ sont commutatifs élément par élément, alors $\mathfrak{M}$ peut également être ouvert comme un module à droite selon $\mathfrak{I}$ tel que l'opération selon $\mathfrak{I}$ soit une continuation de l'opération donnée selon $\mathfrak{R}$ et $\mathfrak{S}$.

La première affirmation découle du fait que $\mathfrak{I}$ peut, par définition, être transformé homomorphiquement en un sous-anneau $\overline{\mathfrak{I}}$ de l'anneau des automorphismes absolus, où $\mathfrak{R}$ et $\mathfrak{S}$ se transforment élément par élément en sous-anneaux commutatifs $\overline{\mathfrak{R}}$ et $\overline{\mathfrak{S}}$. Or, c'est précisément la relation (2a) qui caractérise le double module.

Réciproquement, si $\mathfrak{M}$ est défini comme $\mathfrak{R}$, un double module (module à droite), alors $\mathfrak{R}$ et $\mathfrak{S}$ peuvent être transformés homomorphiquement en sous-anneaux commutatifs élément par élément $\overline{\mathfrak{R}}$ et $\overline{\mathfrak{S}}$ de l'anneau des automorphismes absolus. Dans cet anneau, pour $\overline{\mathfrak{R}}$ et $\overline{\mathfrak{S}}$, il existe un anneau produit. (Le terme "anneau produit" désigne simplement l'anneau engendré par deux anneaux ayant un suranneau commun ; le produit n'est pas nécessairement direct). L'exemple suivant montre qu'un anneau produit n'existe pas toujours lorsqu'une intersection est donnée : soit $\mathfrak{o}$ l'anneau des entiers, et soient $\mathfrak{R} = \mathfrak{o}[x]$ et $\mathfrak{S} = \mathfrak{o}[y]$ avec $2x-1 = 0$ et $2y-1 = 0$, de sorte que $\mathfrak{o}$ soit l'intersection de $\mathfrak{R}$ et $\mathfrak{S}$ si aucune opération n'est imposée entre x et y. Cependant, si $\mathfrak{R}$ et $\mathfrak{S}$ appartiennent à un suranneau commun, alors : $(2x-1)y - x(2y-1) = 0$, Donc $x = y$. Par conséquent, il n'existe pas d'anneau produit d'intersection $\mathfrak{o}$. $\overline{\mathfrak{I}}$, qui, du fait de la commutativité élément par élément, est constitué de tous les éléments de la forme $\sum \overline{r}_i \overline{s}_i + \overline{r} + \overline{s}$ (si $\overline{\mathfrak{R}}$ et $\overline{\mathfrak{S}}$ possèdent des éléments neutres, alors les termes supplémentaires $\overline{r}$ et $\overline{s}$ sont omis). S'il existe également un anneau produit $\mathfrak{I}$ tel que $\mathfrak{R}$ et $\mathfrak{S}$ commutent élément par élément, alors il est constitué de tous les éléments de la forme $\sum r_i s_i + r + s$. Les homomorphismes $\mathfrak{R} \to \overline{\mathfrak{R}}, \mathfrak{S} \to \overline{\mathfrak{S}}$ peuvent donc être décrits par l'affectation

$$\sum r_i s_i + r + s \to \sum \overline{r}_i \overline{s}_i + \overline{r} + \overline{s}$$

à un homomorphisme $\mathfrak{I} \to \overline{\mathfrak{I}}$; ainsi, l'opération $m(\sum r_i s_i + r + s) = \sum (m r_i) s_i + mr + ms$ devient unique et, d'après le § 1.3, définit un $\mathfrak{I}$-module qui englobe le $\mathfrak{R}$-, $\mathfrak{S}$-module donné.

2. Représentation réciproque et directe.

2.1. Modules de formes linéaires.

La transition de la théorie développée dans le § 1 à la théorie des représentations repose sur la spécialisation des modules qui y sont présentés en modules de formes linéaires et sur la considération de leurs anneaux d'automorphismes.

Un module à droite $\mathfrak{S}$, $\mathfrak{M}$ – où $\mathfrak{S}$ est un anneau d'élément neutre – est appelé module de formes linéaires dans $\mathfrak{S}$ si $\mathfrak{M}$ est une somme directe de modules $\mathfrak{S}$ à un terme : $\mathfrak{M} = m_1\mathfrak{S} + \ldots + m_n\mathfrak{S}$ tels que $m_i\mathfrak{S}$ soit isomorphe à $\mathfrak{S}$ par opérateur, c'est-à-dire $s = 0$ pour $m_i = 0$. Il s'ensuit que $\mathfrak{S}$ peut être appliqué non seulement homomorphiquement, mais aussi isomorphiquement sur un sous-anneau de l'anneau d'automorphismes absolus,

Théorème 1. Si $\mathfrak{M}$ est un module de forme linéaire dans $\mathfrak{S}$, alors l'anneau d'automorphismes $\mathfrak{A}$ de $\mathfrak{M}$ dans $\mathfrak{S}$ est réciproquement isomorphe – et non seulement homomorphe – à l'anneau $\overline{\mathfrak{A}}$ de toutes les matrices à n lignes dans $\mathfrak{S}$.

Tout automorphisme α de $\mathfrak{M}$ dans $\mathfrak{S}$ est entièrement décrit par l'application $m_i \to \overline{m}_i = m_i\alpha$. Par définition, il s'ensuit que :

$$\sum m_i s_i \to \sum \overline{m}_i s_i = \sum (m_i\alpha)s_i = \sum (m_i s_i)\alpha.$$

Maintenant, en notation matricielle

$$(m_1\alpha, \ldots, m_n\alpha) = (m_1, \ldots, m_n)A,$$

Ainsi, si α parcourt tous les automorphismes, l'application $\alpha \to A$ établit une relation biunivoque entre $\mathfrak{A}$ et $\overline{\mathfrak{A}}$. Puisque $\mathfrak{M}$ est supposé être un module de forme linéaire, A est déterminé de manière unique par α, et chaque matrice A de degré n dans $\mathfrak{S}$ génère un automorphisme ; Il en découle également : $\alpha + \beta \to A + B, \alpha\beta \to BA$, cette dernière étant due à $(m_1\alpha\beta, \ldots m_n\alpha\beta) = (m_1, \ldots, m_n)A\beta = (m_1, \ldots, m_n)\beta A$ [car $ms\beta = m\beta s$] $= (m_1, \ldots, m_n)BA$.

2.2. Représentation et module de représentation.

Si l'on entend par représentation réciproque ou directe du n-ième degré de l'anneau $\mathfrak{R}$ dans $\mathfrak{S}$ un homomorphisme d'anneaux réciproque ou direct de $\mathfrak{R}$ vers un sous-anneau de l'anneau de toutes les matrices à n lignes dans $\mathfrak{S}$, alors le théorème 1 permet également la formulation :

Théorème 1'. L'anneau d'automorphismes $\mathfrak{A}$ d'un module de forme linéaire de degré n dans $\mathfrak{S}$ admet une représentation réciproque isomorphe (fidèle) par l'anneau de matrices plein $\overline{\mathfrak{A}}$ de toutes les matrices à n lignes dans $\mathfrak{S}$.

De ce fait, les théorèmes usuels pour les représentations directes s'appliquent également aux représentations réciproques.

Définition. Un module de forme linéaire $\mathfrak{M}$ dans $\mathfrak{S}$ est appelé module de représentation réciproque de $\mathfrak{R}$ dans $\mathfrak{S}$ si $\mathfrak{M}$ est un double module par rapport à $\mathfrak{R}$ ou $\mathfrak{S}$ et simultanément un module à droite de $\mathfrak{R}$ et de $\mathfrak{S}$. Un module de représentation directe est appelé module de représentation directe si $\mathfrak{M}$ est un double module et en même temps un module à gauche de $\mathfrak{R}$ et à droite de $\mathfrak{S}$.

Théorème 2. Tout module de représentation réciproque ou directe engendre une classe de représentations réciproques ou directes équivalentes de $\mathfrak{R}$ dans $\mathfrak{S}$, et toutes les représentations réciproques ou directes sont engendrées de cette manière.

Soit $\mathfrak{M}$ un module de représentation réciproque. D'après le § 1.3, $\mathfrak{R}$ peut alors être directement transformé par homomorphisme en un sous-anneau $\overline{\mathfrak{R}}$ de l'anneau d'automorphismes de $\mathfrak{S}$ de $\mathfrak{M}$; d'après le § 2, Théorème 1', $\overline{\mathfrak{R}}$ admet une représentation réciproque (fidèle), qui est aussi la représentation réciproque de $\mathfrak{R}$. Réciproquement, s'il existe une représentation réciproque $\mathfrak{R} \to \mathfrak{R}^*$,

alors par composition avec l'isomorphisme réciproque de $\mathfrak{R}^*$ vers un sous-anneau $\overline{\mathfrak{R}}$ de l'anneau d'automorphismes $\mathfrak{S}$, on obtient un homomorphisme direct de $\mathfrak{R}$ vers $\overline{\mathfrak{R}}$; ainsi, $\mathfrak{M}$ devient un module $\mathfrak{R}$, plus précisément un double module, c'est-à-dire un module de représentation selon le § 1.3. La transition vers d'autres bases $\mathfrak{S}$ donne la classe des représentations équivalentes.

Remarque. Bien entendu, les deux types de représentations sont réductibles l'un à l'autre : une représentation directe de $\mathfrak{R}$ est l'inverse de l'anneau réciproque de $\mathfrak{R}$, et réciproquement. Une autre réduction consiste à passer de $\mathfrak{S}$ à un anneau réciproque et à remplacer les matrices par leurs transposées. Ceci correspond au passage d'un module $\mathfrak{R}$-gauche, $\mathfrak{S}$-droite à un module $\mathfrak{R}$- et $\mathfrak{S}$-gauche.

2.3. Transition du module de représentation réciproque au module selon l'anneau d'extension.

L'avantage du module de représentation réciproque réside principalement dans la transition vers l'anneau d'extension possible selon le § 1.4.

Dans le cas particulier présenté ici – module de forme linéaire $\mathfrak{M}$ vers $\mathfrak{S}$ – voici donc le théorème de transition pour les modules de représentation :

Si $\mathfrak{M}$ est un module à droite par rapport à un anneau $\mathfrak{I}$ contenant deux sous-anneaux commutatifs élément par élément $\mathfrak{R}$ et $\mathfrak{S}$ tel que $\mathfrak{M}$ soit un module linéaire par rapport à $\mathfrak{S}$, alors $\mathfrak{M}$ peut également être vu comme le module de représentation réciproque de $\mathfrak{R}$ par rapport à $\mathfrak{S}$.

Réciproquement, si $\mathfrak{R}$ est un module de représentation réciproque par rapport à $\mathfrak{S}$, et s'il existe un anneau produit $\mathfrak{I}$ tel que $\mathfrak{R}$ et $\mathfrak{S}$ soient commutatifs élément par élément, alors $\mathfrak{M}$ peut également être vu comme un module de représentation réciproque de $\mathfrak{R}$ par rapport à $\mathfrak{S}$. Le module $\mathfrak{I}$ peut être interprété de telle sorte que l'opération $\mathfrak{I}$ soit le prolongement de l'opération $\mathfrak{R}$, $\mathfrak{S}$ donnée.

La conséquence du théorème de transition pour les modules de représentation est largement utilisée en théorie des représentations.

Si $\mathfrak{M}$ est un module de représentation réciproque de $\mathfrak{R}$ dans $\mathfrak{S}$ et simultanément un module $\mathfrak{I}$ dont l'anneau produit est $\mathfrak{I}$, alors l'isomorphisme $\mathfrak{R}$-, $\mathfrak{S}$- de $\mathfrak{M}$ vers un module $\mathfrak{N}$ est équivalent à l'isomorphisme $\mathfrak{I}$-. Chaque classe de modules $\mathfrak{I}$ isomorphes correspond à une classe de représentation réciproque de $\mathfrak{R}$ dans $\mathfrak{S}$ et réciproquement.

La combinaison de ces théorèmes avec les assertions des § 1.2 et 1.3 établit le lien fondamental entre les matrices échangeables avec une représentation et les automorphismes de $\mathfrak{R}$ et $\mathfrak{S}$.

Théorème sur les matrices échangeables.

Si $\mathfrak{R} \to \mathfrak{R}^*$ est une représentation réciproque de $\mathfrak{R}$ de degré $\mathfrak{S}$ dans $\mathfrak{S}$, et si $\mathfrak{B}^*$ désigne l'anneau de toutes les matrices (de degré $\mathfrak{S}$) commutativement interchangeables avec $\mathfrak{R}^*$, alors $\mathfrak{B}^*$ fournit une représentation réciproque isomorphe des $\mathfrak{R}$-, $\mathfrak{S}$-automorphismes – c'est-à-dire les $\mathfrak{S}$-

automorphismes qui sont aussi des $\mathfrak{R}$-automorphismes – du module de représentation générateur, ou, si l'anneau produit $\mathfrak{I}$ existe, des $\mathfrak{I}$-automorphismes.

Soit $\mathfrak{B}$ l'anneau de tous les $\mathfrak{R}$- et $\mathfrak{S}$-automorphismes de $\mathfrak{M}$. En tant que sous-anneau de l'anneau des $\mathfrak{S}$-automorphismes $\mathfrak{A}$, $\mathfrak{B}$ admet une représentation réciproquement isomorphe dans $\mathfrak{S}$. D'après les § 1.2 et 1.3, $\mathfrak{B}$ est constitué de tous les automorphismes de $\mathfrak{A}$ commutativement connexes à $\mathfrak{R}$, c'est-à-dire qui satisfont la relation (2a). L'ensemble $\mathfrak{B}$ est donc constitué de l'ensemble des automorphismes qui commutent élément par élément avec ceux de $\overline{\mathfrak{R}}$, où $\overline{\mathfrak{R}}$ désigne l'image de $\mathfrak{R}$ dans $\mathfrak{A}$. Puisque la représentation de $\mathfrak{B}$ et de $\overline{\mathfrak{R}}$ est un isomorphisme réciproque, et non un simple homomorphisme, c'est ce fait qu'il convient de démontrer.

Remarque. Les automorphismes $\mathfrak{R}$ et $\mathfrak{S}$ représentent une application $m_i \to m_i'$ telle que la même représentation $\mathfrak{R}^*$ soit obtenue grâce aux m_i. Les m_i ne fournissent pas nécessairement une base $\mathfrak{S}$ de $\mathfrak{M}$, ce qui correspond au fait que les matrices de $\mathfrak{B}^*$ ne sont pas nécessairement inversibles par indentation. Le terme "représentation" doit être compris métaphoriquement lorsque la somme $\sum m_i'\mathfrak{S}$ n'est plus directe :

$$(m_1', m_2', \ldots, m_n')a = (m_1', \ldots, m_n')A$$

L'équation reste vraie, mais A n'est plus uniquement déterminé par a.

Une autre remarque concernant le théorème de transition est la suivante : les matrices diagonales $E \cdot s$ fournissent une représentation directement isomorphe de $\mathfrak{S}$, la représentation "identique" de $\mathfrak{S}$. Le fait qu'il s'agisse d'un isomorphisme direct découle du fait que l'anneau d'automorphismes de $\mathfrak{M}$ par $\mathfrak{S}$ possède un sous-anneau réciproquement isomorphe à $\mathfrak{S}$, qui est sa représentation réciproque. Pour tout terme unique $m_i\mathfrak{S}$ de $\mathfrak{M}$, $\mathfrak{S}$ est opérateur-isomorphe à $\mathfrak{S}$ en tant que module à droite, et donc son anneau d'automorphismes $\mathfrak{S}$ est réciproquement isomorphe à $\mathfrak{S}$ (§ 1.3, Corollaire 1).

L'application de $\mathfrak{I}$ aux matrices de $\mathfrak{S}$ définies de manière unique par $\mathfrak{R}$ et $\mathfrak{S}$ n'est donc pas une représentation de l'anneau $\mathfrak{I}$, mais plutôt le prolongement de la représentation réciproque de $\mathfrak{R}$ en une représentation homomorphe par opérateurs de $\mathfrak{S}$: $\sum r_i s_i \to \sum R_i s_i$. En particulier, la représentation réciproque de $\mathfrak{R}$ est simultanément homomorphe par opérateurs par rapport à l'intersection $[\mathfrak{R}, \mathfrak{S}]$ de $\mathfrak{R}$ et $\mathfrak{S}$, qui se trouve au centre de $\mathfrak{R}$.

3. Modules par rapport à un corps.

Dans ce qui suit, nous ne traiterons que des représentations dans des corps généralement non commutatifs ; par conséquent, nous présenterons quelques théorèmes simples concernant les modules de formes linéaires par rapport à un corps.

3.1. Base normale d'un sous-module par rapport à une base donnée du module plein.

Soit A un corps et $\mathfrak{N} = x_1\,\mathsf{A} + ... + x_n\,\mathsf{A}$ un module de forme linéaire de rang n ; soit $\mathfrak{L} = z_1\,\mathsf{A} + ... + z_l\,\mathsf{A}$ un sous-module de rang $l \leq n$. Les z_i sont appelés bases normales par rapport à x s'ils sont de la forme :

$$z_i = x_i - (x_{l+1}\alpha_{i,l+1} + \ldots + x_n\alpha_{i,n}) \qquad (i = 1, \ldots, l).$$

Tout module $\mathfrak{L}$ possède une base normale après une numérotation appropriée des x.

En effet, après une numérotation appropriée, on obtient :

$$\mathfrak{N} = \mathfrak{L} + x_{l+1}\,\mathsf{A} + \ldots + x_n\,\mathsf{A}$$

et donc :

$$x_i \equiv x_{l+1}\alpha_{i,l+1} + \ldots + x_n\alpha_{i,n} \quad (\mathfrak{L}) \qquad (i = 1, \ldots, l).$$

Les l éléments $z_i = x_i - (x_{i+1}\alpha_{i,l+1} + \ldots)$ appartiennent donc à $\mathfrak{L}$ et épuisent $\mathfrak{L}$, puisqu'ensemble, $x_{l+1}, \ldots, x_n$ forment une base de $\mathfrak{N}$.

3.2. Module d'extension.

Soit A un corps et P un sous-corps. Un A-module $\mathfrak{N}$ de rang n est appelé module d'extension d'un P-module $\mathfrak{M}$; $\mathfrak{N} = \mathfrak{M}_\mathsf{A}$ si $\mathfrak{M}$ est un sous-module de même rang que $\mathfrak{N}$. Si $\mathfrak{M} = y_1\,\mathsf{P} + \ldots + y_n\,\mathsf{P}$, alors $\mathfrak{N} = \mathfrak{M}_\mathsf{A} = y_1\,\mathsf{A} + \ldots + y_n\,\mathsf{A}$. Réciproquement, pour tout P-module $\mathfrak{M} = y_1\,\mathsf{P} + \ldots + y_n\,\mathsf{P}$, le module d'extension $\mathfrak{M}_\mathsf{A}$ existe de manière unique à isomorphisme de modules près. Parce que le module $\overline{y}_1\,\mathsf{A} + \ldots + \overline{y}_n\,\mathsf{A}$ contient un sous-module $\overline{\mathfrak{M}}$ isomorphe à $\mathfrak{M}$, qui peut être identifié à $\mathfrak{M}$.

Conclusion a) Si $z_1, \ldots, z_t$ sont des éléments linéairement indépendants de $\mathfrak{M}$ par rapport à P, alors ils sont également linéairement indépendants par rapport à A dans $\mathfrak{N} = \mathfrak{M}_\mathsf{A}$ (car ils peuvent être étendus à une base de $\mathfrak{M}$ et donc de $\mathfrak{N}$). Tout P-module $\mathfrak{I} = z_1\,\mathsf{P} + \ldots + z_t\,\mathsf{P}$ de $\mathfrak{M}$ produit ainsi un module d'expansion $\mathfrak{I}_\mathsf{A} = z_1\,\mathsf{A} + \ldots + z_t\,\mathsf{A}$ dans $\mathfrak{M}_\mathsf{A}$.

Conclusion b) Tout P-module $\mathfrak{I} = z_1\,\mathsf{P} + \ldots + z_t\,\mathsf{P}$ de $\mathfrak{M}$ est un module de contraction. c'est-à-dire l'intersection de son module d'extension $\mathfrak{I}_\mathsf{A}$ avec $\mathfrak{M}$; $\mathfrak{I} = \mathrm{I}_\mathsf{A} \cap \mathfrak{M}$. Parce que $\mathfrak{I} \leq \mathfrak{I}_\mathsf{A} \cap \mathfrak{M}$; réciproquement, si a appartient à $\mathfrak{I}_\mathsf{A} \cap \mathfrak{M}$, alors $a = \sum z_i\alpha_i$, donc les éléments $\mathfrak{M}$ $a, z_1, \ldots, z_t$ dépendent de A, et par conséquent [conclusion a)] dépendent également de P ; Ainsi, a appartient à $\mathfrak{I}$.

3.3. Théorème sur les modules invariants.

Soit $\mathfrak{N} = \mathfrak{M}_\mathsf{A}$ un module d'extension d'un module P $\mathfrak{M}$ de rang n, et soit de plus P un corps plein d'invariants pour un groupe $\mathfrak{G}$ d'automorphismes d'anneaux de A. Le groupe $\mathfrak{G}$ est défini comme le domaine d'opérateurs de $\mathfrak{N} = \mathfrak{M}_\mathsf{A}$ par les assertions suivantes :

$$G \cdot m = m \quad \text{pour} \quad m \text{ de } \mathfrak{M} \quad \text{et} \quad G \text{ de } \mathfrak{G},$$

$$G \cdot \sum m_i \alpha_i = \sum m_i G(\alpha_i) \quad \text{pour} \quad m \text{ de } \mathfrak{M} \quad \text{et} \quad \alpha \text{ de } \mathsf{A}\,.$$

Théorème auxiliaire. Selon ces assertions, $\mathfrak{M}$ est constitué de la totalité des éléments de $\mathfrak{N}$ qui restent inchangés lorsque $\mathfrak{G}$ est présent. En effet, si $x_1, \ldots, x_n$ est une base P de $\mathfrak{M}$, c'est-à-dire $w = x_1\alpha_1 + \ldots + sx_n\alpha_n$, alors $G(w) = w$ pour tout vecteur de Gauss G dans $\mathfrak{G}$, il s'ensuit que $G(\alpha_i) = \alpha_i$, et donc, par hypothèse, α_i dans P.

Théorème. Seuls les modules d'extension $\mathfrak{L}_{\mathsf{A}}$ des sous-modules $\mathfrak{L}$ de $\mathfrak{M}$ sont admissibles par rapport à $\mathfrak{G}$, considéré comme le domaine des opérateurs. La première partie est claire. Réciproquement, supposons que $\mathfrak{L}$ soit admissible par rapport à $\mathfrak{G}$, et soit $z_1, \ldots, z_l$ une base normale de $\mathfrak{L}$ (voir 1) par rapport à x, où x est choisi comme la base P de $\mathfrak{M}$, c'est-à-dire que $\mathfrak{G}$ est autorisé élément par élément. Par hypothèse,

$$G(z_i) = x_i - (x_{l+1}G(\alpha_{i,l+1}) + \ldots + x_nG(\alpha_{i,n}))$$

est élément de $\mathfrak{L}$ pour chaque G de $\mathfrak{G}$, donc, pour un G fixé, linéairement exprimable en fonction de z et donc, comme on peut le voir en comparant les coefficients dans $x_1, \ldots, x_l : G(z_i) = z_i$ pour chaque G de $\mathfrak{G}$. Ainsi, d'après le lemme, les z appartiennent à $\mathfrak{M}$, et $\mathfrak{L}$ devient une extension du P-module $\mathfrak{I} = z_1\,\mathsf{P} + \ldots + z_l\,\mathsf{P}$ de $\mathfrak{M}$, où $\mathfrak{I} = \mathfrak{L} \cap \mathfrak{M}$ (par 2) [1].

4. Systèmes hypercomplexes et leurs classes de représentation.

4.1. Théorème d'extension.

Nous combinons maintenant les théorèmes de représentation du § 2 avec les théorèmes de module du § 3. Au lieu des anneaux généraux $\mathfrak{R}$, nous considérons des systèmes hypercomplexes avec éléments neutres - $S, T, \ldots$ - sur un corps commutatif P, c'est-à-dire

$$S = x_1\,\mathsf{P} + \ldots + x_n\,\mathsf{P}\,.$$

Au lieu d'anneaux de représentation arbitraires $\mathfrak{S}$, il n'existe que des corps $\mathsf{A}, \ldots$ et, sauf indication contraire, des corps de centre P. Dans ce cas, l'anneau produit dans lequel S et A sont interchangeables élément par élément existe toujours, avec une intersection P ; il s'agit du produit direct $S \times \mathsf{A}$, qui est simultanément le module d'extension S_{A} de S au sens de §.

$$S_{\mathsf{A}} = x_1\,\mathsf{A} + \ldots + x_n\,\mathsf{A}$$

et est donc également appelé anneau d'extension. Dans cette spécialisation, le théorème sur les modules invariants (§ 3.3) devient le suivant :

1. Les propositions de ce paragraphe restent valides en vertu d'inférences simples de bon ordre, même si le rang de $\mathfrak{M}$ devient infini par rapport à P (cf. G. Köthe : *Ein Beitrag zur Theorie der kommutativen Ringe ohne Finlichkeits-voraussetzung*, § 1, Gött. Nachr. 1931, p. 195-207).

Théorème d'extension : Tout idéal bilatère de S_{A} est un idéal d'extension d'un idéal de S, plus précisément une extension de son intersection avec S.

Si le groupe sous-jacent $\mathfrak{G}$ est celui des automorphismes intérieurs, alors P, en tant que centre de A, devient un corps invariant complet. L'interchangeabilité élément par élément de A avec S implique que $\mathfrak{G}$ est prolongé à S_{A} par le § 3.3, de sorte que S devienne un anneau invariant complet. Tout idéal bilatère $\mathfrak{a}$ de S_{A} est un sous-groupe admissible car $\alpha^{-1}\mathfrak{a}\alpha \leq \mathfrak{a}$ – c'est-à-dire, par le § 3, le troisième prolongement de son mode d'intersection $\mathfrak{a} \cap S$, qui devient un idéal de S.

Remarque complémentaire : Si S est commutatif, alors S est le centre de S_{A}. En effet, S est inclus dans le centre et constitue un anneau complet d'invariants par les automorphismes intérieurs engendrés par A. Plus généralement, le centre de S est également le centre de S_{A}.

Notation : $\mathsf{A}_r, \mathsf{B}_n, \ldots$ désignent toujours des anneaux de matrices du degré spécifié sur $\mathsf{A}, \mathsf{B}, \ldots$

$$\mathsf{A}_r = \sum \mathsf{A}\ c_{ik} = \sum c_{ik}\ \mathsf{A}\,.$$

Dans ce qui suit, on utilise un corollaire, le théorème d'extension pour les systèmes simples : si S est un système simple, alors S_{A} l'est aussi : $S_{\mathsf{A}} = \sum \mathsf{B}\ c_{ik} = \sum c_{ik}\ \mathsf{B}$, avec un corps associé B dont le centre est P. Ici, A, et donc B également, peuvent être de rang infini sur P ; seul S est supposé hypercomplexe. Si S et A ont le centre commun P, alors P devient également le centre de S_{A}.

Plus généralement, si S est un système hypercomplexe simple, alors le produit direct $S \times \mathsf{A}_r$ est également simple. En effet, $S \times \mathsf{A}_r$ est égal à $S_{\mathsf{A}} \times \mathsf{P}_r$, et donc égal à B_{ir} si $S_{\mathsf{A}} = \mathsf{B}_i$.

4.2. Classes de représentations.

Comme d'habitude, une représentation réciproque ou directe d'un système hypercomplexe est une représentation homomorphe aux opérateurs par rapport au domaine des coefficients P (§ 2, conclusion) et différente de la représentation nulle. La combinaison du théorème de transition et de son corollaire (§ 2.3) avec le théorème d'extension de 1 donne le

Théorème sur les classes de représentation : Si S est un hypercomplexe d'élément neutre, dont l'anneau des coefficients est P, et si A est un corps de centre P, alors S possède dans A autant de classes de représentations réciproques irréductibles distinctes de S qu'il y a de classes d'idéaux à droite simples dans l'anneau des classes résiduelles de S relativement à son radical. Si S est un système simple, alors il possède exactement une classe de représentation réciproque irréductible et une classe de représentation directe irréductible dans A.[2] En effet, d'après le corollaire du théorème de transition (§ 2.3), les classes de représentations réciproques simples et les classes de modules simples sont bijectives par rapport à S_{A}. Puisque S_{A} est de rang fini par rapport au corps A, il satisfait les conditions de maximum et de minimum pour les idéaux unilatéraux, Ainsi, la première partie de l'énoncé découle directement de la théorie des représentations, § 19. Si S est simple, alors S_{A} l'est aussi d'après le théorème d'extension. Du fait des conditions de maximum et de minimum, S est

2. Voir la théorie des représentations, et notamment la note de bas de page n° 20, pour le cas où A est le corps d'automorphismes associé à S.

également complètement réductible, c'est-à-dire qu'il ne possède qu'une classe d'idéaux unilatérale simple, ce qui signifie que S n'a qu'une classe de représentations réciproques irréductibles dans A. Avec S, le système réciproquement isomorphe à S est également simple, ne possédant qu'une classe de représentations réciproques irréductibles ; par conséquent, S n'a également qu'une classe de représentations directes simples.

4.3. Relation de rang.

Le fait que, si S est simple, $S_{\mathsf{A}} = \sum \mathsf{B} c_{ik}$ soit de rang fini à la fois par rapport à A et à B, donne la relation de rang :

(1) $$\begin{aligned} &n = rt \quad \text{avec} \quad n = (S : \mathsf{P}), \quad t^2 = (S_{\mathsf{A}} : \mathsf{B}), \\ &r = \text{degre de representation reciproque irreductible} \end{aligned}$$

Puisque S_{A} est lui-même le module de représentation réciproque de S dans A (la représentation étant déjà dans P), S_{A}, en tant qu'anneau de matrices sur B, se décompose en t idéaux à droite simples, il s'agit de S_{A} modules, dont le rang par rapport à A est égal au degré r de la représentation réciproque irréductible. Comme n est également le rang de S_{A} par rapport à A, la relation de rang s'ensuit.

4.4. Renforcement de la relation de rang.

Lorsque A est de rang fini par rapport à P, les trois relations sont vérifiées.

(1) $$(S : \mathsf{P}) \;=\; n = rt,$$

(2) $$(\mathsf{B} : \mathsf{P}) \cdot t \;=\; (\mathsf{A} : \mathsf{P}) \cdot r,$$

(3) $$(S : \mathsf{P}) \cdot (\mathsf{B} : \mathsf{P}) \;=\; (\mathsf{A} :) \cdot r^2.$$

Ici, (2) désigne le rang sous P d'un idéal à droite simple de S_{A}, exprimé selon (3) par le rang sous B ou A, tandis que (3) désigne le rang d'un idéal à droite simple dans un anneau de matrices B_n et est obtenu à partir de (2) par multiplication par r selon (1).

5. Application des théorèmes de représentation aux anneaux de matrices.

La représentation réciproque de S dans A considérée dans le § 4 peut également être vue comme un homomorphisme direct de S dans un sous-anneau de A_r, où A désigne le corps réciproquement isomorphe à A. Le principe des paragraphes suivants est, inversement, de réduire l'étude des anneaux de matrices A_r à la théorie des représentations dans le corps réciproque isomorphe A.

5.1. Plongement réductible et irréductible dans A_r.

Soient A et A deux corps isomorphes réciproques de rang fini ou infini sur leur centre P. En général, les corps ou systèmes réciproques seront notés par les lettres grecques et latines correspondantes. Le système simple S sur P est dit irréductible ou réductible dans A, et plongeable, si S admet une représentation réciproque irréductible ou réductible de degré f dans A. Si S est irréductiblement plongeable dans A_r, alors il est réductiblement plongeable dans tous les anneaux de matrices A_{rs} avec $s > 1$, puisqu'il admet des représentations réductibles de ces degrés et seulement de ces degrés (§ 4.2). S est donc directement isomorphe à certains sous-anneaux de A_r et A_{rs}. Cet isomorphisme devient un prolongement de l'identité de P. Comme pour les représentations déjà mentionnées, les isomorphismes qui apparaissent ci-dessous sont toujours des prolongements de l'identité de P – isomorphes à P – sans que cela soit explicitement indiqué à chaque fois ; d'après le § 4.3, r est un diviseur de rang n de S par P.

Ainsi, tous les sous-anneaux simples de rang fini englobant P sont obtenus dans P à partir des différents A_f $(f = 1, 2, \ldots)$; car chaque sous-anneau de ce type est réciproquement isomorphe à un sous-anneau de A_f, admettant ainsi une représentation réciproque réductible ou irréductible dans A.

5.2. Théorème sur les automorphismes intérieurs.

Si $S^{(1)}$ et $S^{(2)}$ sont deux sous-anneaux simples de P englobants les A_f de rang fini dans P, et si $S^{(1)}$ et $S^{(2)}$ sont isomorphes dans P, alors cet isomorphisme est engendré par un automorphisme intérieur de A_f.

Les systèmes $S^{(1)}$ et $S^{(2)}$ représentent, en général, des éléments de fondation réductibles d'un système simple S dans A_f, donc des représentations directes de degré f dans A. Ils appartiennent par conséquent à la même classe de représentations directes réductibles dans A. La matrice de transformation engendre l'automorphisme.

Si A est de rang fini pour P, c'est-à-dire s'il est hypercomplexe, le théorème se réduit au théorème bien connu suivant :

Deux sous-systèmes simples de A_f contenant le centre P et isomorphes à P sont transformés en eux-mêmes par un automorphisme interne de A_f. En particulier, tout automorphisme de A_f est intérieur [3].

5.3. Théorème sur les sous-anneaux commutant élément par élément.

Ce théorème découle du théorème sur les matrices commutatives du § 2.3, selon le principe énoncé au début du paragraphe :

3. Ceci n'est plus vrai si A est de rang infini selon P (cf. Köthe, dans le travail cité dans la note de bas de page n° 5).

Si S est un système simple de A_f englobant P, et si R désigne l'ensemble des éléments de A_f commutant élément par élément avec S, alors R est également un anneau de matrices : $R = B_s$. Les corps correspondants B de S_A et B de R sont réciproquement isomorphes. L'intersection de R et S est le centre de S. R est un corps si et seulement si S est irréductiblement plongé dans A_f.

Car selon le § 2.3, R devient directement isomorphe à l'anneau d'automorphismes du module de représentation réciproque $\mathfrak{M}$ de S dans A ; mais il s'agit de l'anneau d'automorphismes de $\mathfrak{M}$, considéré comme le module S_A. Si $\mathfrak{M}$ se décompose en s modules simples S_A, et si $S_\mathsf{A} = \sum \mathsf{B}\, c_{ik}$ est défini comme dans le § 4.1, alors R est isomorphe à $\sum \mathsf{B}\, c_{ik}$, où $\sum \mathsf{B}\, c_{ik}$ et R sont réciproquement isomorphes (car B et B sont réciproques isomorphes au corps des automorphismes des idéaux à droite simples de S_A, c'est-à-dire les modules simples S_A, d'après le § 1.3). R est un corps – $R = B$ – si et seulement si s vaut un, c'est-à-dire si S est irréductiblement plongé. Le fait que l'intersection de R et S soit le centre de S découle directement de la définition de R.

5.4. Théorème de commutation amélioré pour les anneaux de matrices hypercomplexes.

Dans ce cas, les relations de rang du § 4.4 permettent d'obtenir l'amélioration suivante :

Les sous-systèmes simples de A_f constituant P (où A est de rang fini par rapport à son centre P) se décomposent en paires S et $\overline{S}$ telles que $\overline{S}$ soit l'ensemble des éléments commutativement interchangeables avec S, et réciproquement. Les corps associés à S_A et $\overline{S}$ sont réciproquement isomorphes, de même que ceux de S et $\overline{S}_\mathsf{A}$. L'intersection de S et $\overline{S}$ est le centre commun. Un sous-anneau est un corps si et seulement si l'anneau est irréductiblement plongé dans le sous-anneau. Le produit des rangs de P de S et $\overline{S}$ est égal au rang de A_f. Si $f = rs = \overline{rs}$ (où S est irréductiblement plongeable dans A_r et $\overline{S}$ est irréductiblement plongeable dans $A_{\overline{r}}$), alors les corps associés à S et $\overline{S}$ sont isomorphes à une paire de sous-anneaux commutatifs de A_g tels que $f = gs\overline{s}$.

En substance, il suffit de démontrer l'énoncé concernant le produit des rangs. Si S est initialement plongé de manière irréductible, c'est-à-dire si $\overline{S}$ est un corps et réciproquement isomorphe à B (où $S_\mathsf{A} = \mathsf{B}_t$), alors la relation de rang (3) issue du § 4.4 permet d'obtenir l'énoncé du produit, puisque $f = r$ et que le rang de $\overline{S}$ est égal à celui de B. Si S est plongé de manière réductible, c'est-à-dire si $\overline{S} = B_s$, alors $f = rs$, et la multiplication de (3) par s^2 donne l'énoncé. Il en découle directement que S est constitué de l'ensemble des éléments qui sont commutativement interchangeables avec $\overline{S}$, et donc tout le reste de 3, découle, à l'exception de la dernière affirmation. Il découle directement de ce qui précède que S est constitué de l'ensemble des éléments commutativement interchangeables avec $\overline{S}$, et par conséquent, tout ce qui suit dans la section 3 s'ensuit, à l'exception de la dernière affirmation. Cette dernière affirmation est obtenue par deux transitions vers un plongement irréductible. Dans A_r – avec $f = rs$ – S est irréductiblement plongé ; S et R deviennent des systèmes commutatifs deux à deux, où R est isomorphe au corps B. De plus, du fait de la réciprocité entre S et $\overline{S}$, S est égal à $\overline{B}_{\overline{s}}$ – où $\overline{B}$ a la même signification pour $\overline{S}$ que B pour S – donc R est réductiblement plongé dans A_r et irréductiblement plongé dans A_g avec $r = g\overline{s}$. Ici, les systèmes interchangeables deux à deux sont B et $\overline{B}$ qui sont isomorphes.

6. Théorie de Galois des systèmes simples.

Le théorème de commutation intensifié du § 5.4 exprime la théorie de Galois des systèmes simples par rapport au centre, qui est l'anneau de référence. Nous considérons d'abord les corps, puis les systèmes simples en général.

6.1. Théorie de Galois des corps de rang fini par rapport au centre.

Le groupe de Galois $\mathfrak{G}$ de A est défini comme le groupe de tous les automorphismes qui sont des extensions de l'identité du centre P, c'est-à-dire (§ 5.2) comme le groupe de tous les automorphismes intérieurs. Ainsi, $\mathfrak{G}$ est isomorphe à A^* et P^*, où A^* et P^* sont les groupes multiplicatifs des éléments non nuls de A et P, respectivement. Les sous-groupes $\mathfrak{H}$ de $\mathfrak{G}$ correspondent donc biunivoquement aux sous-groupes englobants H^* de A^*, du fait que $\mathfrak{H} \simeq H^* / \mathsf{P}^*$. Un sous-groupe $\mathfrak{H}$ de $\mathfrak{G}$ est dit fermé si H^* devient un corps H après l'ajout de zéro. Le fait que C admette le groupe $\mathfrak{H}$ est équivalent au fait que C commute élément par élément avec H. Ainsi, le théorème de commutativité (§ 5.4) devient le

Théorème fondamental de la théorie de Galois des corps non commutatifs :

Les corps C compris entre P et A et les sous-groupes fermés $\mathfrak{H}$ de $\mathfrak{G}$ peuvent être envoyés l'un sur l'autre de manière unique de sorte que C soit le corps invariant complet de $\mathfrak{H}$ et $\mathfrak{H}$ soit le groupe invariant complet de C.

6.2. Théorie de Galois des systèmes simples.

Si A_f est un système simple de centre P, alors le groupe de Galois $\mathfrak{G}$ devient le groupe des automorphismes intérieurs, c'est-à-dire isomorphe à $A_f^* \, \mathsf{P}^*$, où A_f^* désigne maintenant le groupe multiplicatif des éléments réguliers de A_f. Un sous-groupe $\mathfrak{H} \simeq H^* \, \mathsf{P}^*$ de $\mathfrak{G}$ est dit simplement clos si le sous-anneau H engendré par H^* est un système simple et si H^* est constitué de l'ensemble des éléments réguliers de H. La transition du théorème de commutation à la théorie galoisienne est donnée ici par le théorème suivant :

Lemme : Tout système simple A_f contenant P est engendré par le groupe H^* de ses éléments réguliers. Ceci est évident si P possède une infinité d'éléments ; car l'élément général formé avec les indéterminées est régulier ; par une spécialisation appropriée, on peut former des éléments de base réguliers conformément à P. Cependant, selon Shoda, le lemme est valable en général [4].

En vertu du lemme, la commutativité de S avec un système simple $\overline{S}$ est à nouveau équivalente à ce que S admette les automorphismes induits par les éléments réguliers de $\overline{S}$. Ainsi, ici aussi, le théorème de commutativité (§ 5.4) se réduit au :

4. Shoda, voir l'ouvrage cité en note de bas de page n° 3. Dans ce cas, l'introduction des indéterminées est évitée.

Théorème fondamental de la théorie de Galois des systèmes simples : Les systèmes simples P-composants S de A_f et les sous-groupes simplement clos $\mathfrak{H}$ de $\mathfrak{G}$ peuvent être associés de manière unique de sorte que S devienne le domaine invariant complet de $\mathfrak{H}$ et que $\mathfrak{H}$ devienne le groupe invariant complet de S.

6.3. Démonstration par le principe de continuation.

Dans le cas d'un corps, je propose une seconde démonstration du théorème principal, fondée sur le principe de continuation des isomorphismes (représentations de degré un) et qui, par conséquent, s'affranchit du dénombrement des rangs et fait moins d'hypothèses de finitude. Elle montre notamment dans quelle direction un transfert vers des corps S de rang infini est possible. La démonstration n'utilise pas non plus le fait qu'il n'existe qu'une seule classe de représentations réciproques irréductibles et reste donc valable dans le cas commutatif (§ 8.2). Je présente d'abord quelques lemmes.

Lemmes : Le système simple S sur P admet une représentation réciproque de degré un dans A, et est donc un corps ; A peut être de rang fini ou infini sur son centre P. Une décomposition de S_A en idéaux à droite simples (isomorphes par opérateurs) (§ 4.3) est donnée par :

$$S_\mathsf{A} = r_1 + \ldots + r_n = e_1 S_\mathsf{A} + \ldots + e_n S_\mathsf{A} = e_1 \mathsf{A} + \ldots + e_n \mathsf{A} :$$

La représentation réciproque engendrée par e_i est ainsi définie par $e_i s = e_i \sigma$.

Théorème 1 : Les n représentations engendrées par $e_1, \ldots, e_n$ sont distinctes, c'est-à-dire que ce sont des représentations distinctes d'une même classe de représentations. Par conséquent, S possède au moins autant de représentations distinctes que son rang.

Pour le démontrer, nous étendons les représentations de S du § 2 aux applications de S_A qui deviennent homomorphes à A par opérateur. Ces applications sont définies ici par $e_i w = e_i \omega$ avec ω dans A pour tout w dans S_A. Si la même représentation était engendrée par e_i et e_j $(i \neq j)$, alors $e_i w = e_j w$ serait obtenu pour tout w dans S_A. Ceci est impossible car $e_i e_i = e_i, e_j e_i = 0$.

Théorème 2 : Si T est un corps compris entre P et S, et si s est le rang de S par rapport à T, alors tout isomorphisme réciproque de T vers A admet au moins s extensions différentes.

L'isomorphisme réciproque, c'est-à-dire la représentation réciproque de T dans A, est obtenu par une décomposition :

$$T_\mathsf{A} = E_1 T_\mathsf{A} + \ldots + E_h T_\mathsf{A} = E_1 \mathsf{A} + \ldots + E_h \mathsf{A} ; \quad E_\iota t = E_\iota \tau,$$

où les E_i sont des idempotents (ceci n'est pas une restriction de généralité, puisqu'une représentation engendrée par un élément de base $E_i \alpha$ est également engendrée par $\alpha^{-1} \cdot E_i \alpha$, c'est-à-dire que c'est un idempotent). La multiplication à droite par S donne $S_\mathsf{A} = E_1 S_\mathsf{A} + \ldots + E_h S_\mathsf{A}$. Ici, les $E_i S_\mathsf{A}$ sont tous de rang s par rapport à A ; car le rang de $E_i S_\mathsf{A}$ est au plus égal à s, comme le montre la substitution d'une base T dans S en vertu de la commutativité de S et A : $S = T w_1 + \ldots + T w_s$. $E_i S_\mathsf{A} = E_i T_\mathsf{A} w_1 + \ldots + E_i T_\mathsf{A} w_s = E_i w_1 \mathsf{A} + \ldots + E_i w_s \mathsf{A}$.

Puisque la somme S_{A} est de rang $n = hs$, chaque $E_i S_{\mathsf{A}}$ est exactement de rang s. Ainsi,

$$E_i S_{\mathsf{A}} = \mathfrak{r}_{i1} + \ldots + \mathfrak{r}_{is} = e_{i1}\,\mathsf{A} + \ldots + e_{is}\,\mathsf{A},$$

où, d'après le lemme 1, les s engendrés par $e_{i1}, \ldots, e_{is}$ sont tous distincts. Ce sont tous des prolongements de la représentation de T engendrée par les E_i. Comme $E_i t = E_i \tau$, il découle que $(e_{i1} + \ldots + e_{is}t = (e_{i1} + \ldots + {}_{is})\tau$ et donc $e_{i1}t = e_{il}\tau$ du fait de la décomposition en somme directe.

Définition. La division de classes $\mathfrak{I}_T$ induite par T des isomorphismes réciproques $\mathfrak{I}$ de S vers A est définie comme suit : seuls les isomorphismes de $\mathfrak{I}$ qui induisent le même isomorphisme sur T sont considérés comme équivalents.

Théorème fondamental : Si $\mathfrak{I}_T$ est la division de classes induite par T, alors T est sous-corps maximal en contraste avec cette division de classes.

Si L est un corps intermédiaire de T et S de degré l à T, alors, d'après le lemme 2, toute classe de $\mathfrak{I}_T$ se partitionne en au moins l classes de $\mathfrak{I}_L$.

La transition de cette version du théorème principal à la version usuelle provient du fait que l'ensemble d'isomorphismes $\mathfrak{I}$ est transformé en groupe d'automorphismes par multiplication de ses éléments par l'inverse d'un ensemble fixé, ce qui transforme une classe de $\mathfrak{I}_T$ en groupe invariant de T. L'affirmation que les sous-groupes fermés sont des groupes invariants complets est implicitement contenue dans ce résultat. Il suffit de substituer le corps H au corps intermédiaire T dans $\mathfrak{H} = H^*\,\mathsf{P}^*$.

7. La classe des algèbres semblables. Corps de décomposition.

Désormais, nous ne considérerons que les corps A et A, ainsi que les anneaux de matrices A_r de rang fini par rapport à leur centre P ; c'est-à-dire les algèbres simples et ordinaires sur P, que nous appellerons simplement algèbres sur P ou algèbres ; A et A sont alors des algèbres à division.

Tous les A_r ayant le même A associé sont regroupés dans une classe d'algèbres semblables : $A_r \sim A_s$. Les A isomorphes sont identifiés au cours de ce processus.

7.1. Le groupe des classes d'algèbres.

Si A_r et B_s sont des algèbres sur P, alors il en va de même pour leur produit (produit direct sur P) ; car, d'après la conclusion du § 3, on obtient : $A_r \times B_s = C_t$, où C est une algèbre à division de centre P, unique à isomorphisme près. La multiplication de A_r et B_s par des anneaux de matrices sur P montre que cette multiplication est unique pour les classes, qui forment ainsi un système multiplicativement clos et commutatif. De plus, le théorème de R. Brauer est vérifié : les classes d'algèbres semblables forment un groupe abélien pour le produit direct. Ceci est dû au fait que le système possède une classe unité constituée des anneaux de matrices sur P, c'est-à-dire des algèbres de type P. De plus, pour toute classe A, elle possède l'inverse $(A)^{-1}$, constitué des algèbres semblables à A, où A est réciproquement isomorphe à A. Ceci découle du théorème de commutation du § 5.3, grâce

à la spécialisation $S = A$. En effet, A peut être irréductiblement plongé dans A lui-même ; ainsi, $B = \mathsf{P}$ et $A_{\mathsf{A}} = \mathsf{P}_t$ en découle [5].

7.2. Corps de décomposition d'une classe d'algèbres.

La théorie des corps de décomposition repose entièrement sur le principe énoncé au début de la section 5 ; les corps d'extension commutatifs sont respectivement représentés dans A et A. Précisons ce qui suit :

Assertion : Si A est un corps de centre P, et Z un corps d'extension commutatif fini de P, alors A_{Z} se réduit à Z de centre Z.

En effet, d'après la section 4.1, cela est vrai pour le système Z_{A}, qui est réciproquement isomorphe à A_{Z}. Pour toute classe (A) d'algèbres semblables à A sur P, Z engendre une classe d'extension $(A)_{\mathsf{Z}}$ d'algèbres simples semblables à A_{Z} sur Z.

L'algèbre de division associée D d'une classe d'extension découle immédiatement du théorème de commutation dans le § 5.3 :

Théorème sur l'algèbre de division associée à une classe d'extension : Soit $(A)_{\mathsf{Z}}$ une classe d'extension, et Z une injection irréductible (représentation) de Z dans A_r. Alors $(A)_{\mathsf{Z}} = (D)$, où D est l'ensemble des éléments de A_r commutativement interchangeables avec Z.

Dans le § 5.3, on remplace simplement le système existant S par Z, en tenant compte du fait que Z_{A} et A_{Z} sont réciproquement isomorphes. Si Z est une injection réductible, alors l'ensemble des éléments commutativement interchangeables avec Z forme un anneau de matrices sur D.

Un corps d'extension commutatif Z de P est connu pour être un corps de partition de classes (A) si la classe d'extension $(A)_{\mathsf{Z}}$ partitionne complètement, c'est-à-dire devient égale à la classe d'unité sur Z, qui est la classe de tous les anneaux de matrices sur Z.

Théorème sur la caractérisation des corps de décomposition. Un corps d'extension commutatif fini Z de P est un corps de décomposition de classes (A) si et seulement si son plongement irréductible dans A_r induit un sous-corps commutatif maximal de A_r.

Pour que Z soit un corps de décomposition de (A), il faut que $(D) = (\mathsf{Z})$. Par conséquent, d'après le théorème sur l'algèbre de division associée, le plongement irréductible Z est nécessairement un sous-corps commutatif maximal. Si cette condition est satisfaite, alors $D = Z$ s'ensuit nécessairement, puisque tout a de D engendre un corps d'extension commutatif par adjonction avec Z.

5. Les théorèmes plus détaillés concernant le groupe des classes d'algèbre font appel à la théorie des systèmes de facteurs ; ils ne seront pas abordés ici. Il convient de noter que, jusqu'à présent, aucune considération relative aux corps commutatifs n'a été faite ; par exemple, le fait que le rang de $(A : \mathsf{P})$ soit un carré n'a été ni utilisé ni démontré.

Remarques.
1. Il s'ensuit qu'un sous-corps commutatif maximal Z, s'il est plongé de manière irréductible, engendre un sous-anneau commutatif maximal. En effet, l'ensemble des éléments commutatifs avec Z terme à terme forme un corps.

2. Ce théorème implique également l'existence de corps de décomposition, puisque l'algèbre à division associée A possède nécessairement des sous-corps maximalement commutatifs.

7.3. Relations de rang, indice, extensions commutatives infinies.

L'énoncé du rang du § 5.4 conduit initialement au fait bien connu que le rang d'une algèbre simple par rapport au centre est un carré parfait ; car si Z est maximalement commutative dans A, alors, puisque tout plongement dans A est irréductible : $(Z : \mathsf{P}) \cdot (Z : \mathsf{P}) = (A : \mathsf{P})$, donc $(A : \mathsf{P})m^2; (Z : \mathsf{P}) = m$, où m est l'indice de Schur, qui désigne donc également le degré de tous les corps de décomposition plongeables dans l'algèbre à division A elle-même. De plus, pour le degré n d'un corps de décomposition général : $n = m \cdot r$ [6], par exemple à cause de $(A_r : \mathsf{P}) = m^2 \cdot r^2$ Ou encore, d'après la relation de rang du § 4.3, puisque l'indice m est également égal au nombre de composantes simples de A_{Z}, l'anneau de matrices sur Z est de rang m^2. Plus généralement, si $A_{\mathsf{A}} \sim D$, alors L est l'injection irréductible de Λ dans A_r et d^2 est le rang $(D : L)$ de l'algèbre à division D sur son centre L. Ainsi, $l \cdot d = m \cdot r$, car d'après le § 5.4. Le théorème relatif à l'algèbre de division associée, présenté dans la section 4, conduit à : $(A_r : \mathsf{P}) = (L : \mathsf{P}) \cdot (D : \mathsf{P})$ ou $m^2 r^2 = l^2 d^2$.

De l'existence des corps de décomposition découle les propriétés suivantes pour les corps d'extension commutatifs (algébriques ou transcendants) infinis Ω de P :

La classe d'extension $(A)_\Omega$ est une classe d'algèbres simples de centre Ω. En particulier, si Ω est algébriquement clos, alors A_Ω est un anneau de matrices de degré m. L'indice m est donc égal au nombre absolu de composantes.

En effet, si Z est le corps de décomposition de A et de $\overline{\Omega}$, composé de Ω et de Z, alors $A_{\overline{\Omega}}$ est un anneau de matrices sur $\overline{\Omega}$, c'est-à-dire sans radical et de centre $\overline{\Omega}$. Ainsi, A_Ω est également sans radical, et son centre Ω (puisqu'un élément de A_Ω autre que Ω serait également au centre de $A_{\overline{\Omega}}$) est donc un corps. A_Ω est donc une algèbre simple sur Ω, et assurément un anneau de matrices sur Ω si Ω est algébriquement clos.

7.4. Existence de corps de décomposition séparables.

Chaque classe (A) possède des champs asymétriques séparables, même ceux qui sont intégrables dans A lui-même [7].

6. En général, il existe aussi des corps de décomposition "minimaux", c'est-à-dire ceux pour lesquels aucun sous-corps vrai n'est un corps de décroissance de tous les degrés. (Cf. Brauer-Noether, op. cit.

7. Cf. G. Köthe, *Über Schieffelder mit Unterfeldern zweiter Art über dem Centre*, Jour. f. Mathématiques. 166 (1932), 8. 182-184. La présente preuve, beaucoup plus simple, est basée sur une remarque de M. Zorn.

Soit P le corps de base de caractéristique p ; l'indice $m = s \cdot p^g$ avec s et p premiers entre eux. Si Z est un corps de décomposition de A de degré m et si Z_0 contient l'extension de première espèce dans A – c'est-à-dire $(\mathsf{Z} : \mathsf{Z}_0) = p^f$ –, alors l'indice de $A_{\mathsf{Z}_0} \sim D$ vaut p^f (d'après 3). Nous voulons démontrer l'existence d'un corps d'extension séparable Z_1 de Z_0 tel que l'indice de D_{Z_1} soit un diviseur propre de p^f. Or, D_Ω, avec Ω algébriquement clos, est, d'après 3, sans radical ; par conséquent, le discriminant réduit de D n'est pas nul. Il existe donc au moins un élément d de D dont la trace est réduite ; d ne peut appartenir au corps de base Z_0, puisque la trace de tout élément α de Z_0 devient $p^f\alpha$, c'est-à-dire qu'elle s'annule. $\mathsf{Z}_1 = \mathsf{Z}_0(d)$ devient ainsi un corps d'extension propre, et de fait séparable ; l'indice de D_{Z_1} devient un diviseur propre de p^f. La répétition finie conduit donc à un corps de décomposition séparable de (A), dont le degré m coïncide avec l'indice de A.

8. Corps de décomposition, et théorie de Galois dans le domaine commutatif.

Pour passer des corps de décomposition des systèmes simples sur leur centre à ceux des systèmes simples quelconques, il faut d'abord développer la théorie de décomposition du centre, à laquelle s'ajoutera une théorie de Galois parallèle à celle du § 6.3. (Tous les corps et systèmes mentionnés dans ce paragraphe sont commutatifs).

8.1. Décomposition et corps de décomposition des systèmes simples commutatifs.

Soit Z un système commutatif simplement défini sur P, c'est-à-dire un corps, et Ω un corps d'extension algébriquement clos de P. Alors, comme on le sait (§ 21 de *Representation theory*) :

Si Z est séparable (extension de première espèce) sur P, alors et seulement alors Z_Ω reste un système sans radicaux.

Car alors, et alors seulement, il possède autant d'applications isomorphes de degré un dans Ω que son rang dans Ω, et donc aussi autant de représentations différentes, qui correspondent ici à des classes de représentation.

Le fait qu'un radical puisse apparaître dans Z_Ω, ce qui signifie que la décomposition en sommes directes en composantes absolument simples n'a pas nécessairement lieu, conduit à ce qui suit :

Définitions : Un corps d'extension Λ de P est appelé un corps de scindage si Z_A se décompose en facteurs de composition de degré un ; autrement dit, si toutes les représentations absolument irréductibles sont déjà dans Λ. Un corps d'extension T de P est appelé un corps de scindage si Z_T décompose au moins un facteur de composition de degré un ; autrement dit, s'il existe au moins une représentation absolument irréductible de Z dans T.

Les champs de décroissance et de dédoublement peuvent être caractérisés selon le

Théorème : Un corps T est un corps de décomposition si et seulement s'il contient un sous-corps Z isomorphe à Z ; un corps Λ est un corps de division si et seulement s'il contient un sous-corps Γ qui devient isomorphe au corps de Galois appartenant à Z.

Ceci découle directement de la définition des corps de décomposition et des corps de division, en vertu des représentations absolument irréductibles. En particulier, par analogie avec le corps non commutatif, on aboutit à la :

Conclusion : Un corps Z est un corps de division minimal, c'est-à-dire qu'il n'est pas un corps de division propre, si et seulement s'il est isomorphe à Z (c'est-à-dire si son plongement commutatif irréductible dans Z représente un sous-corps commutatif maximal de Z). Un corps de décomposition minimal est un corps de décomposition si et seulement si Z est normal, c'est-à-dire un corps de Galois sur P.

C'est pourquoi on dit qu'une algèbre simple est normale sur son centre. Le fait que, dans un corps Ω fixé et algébriquement clos sur P, il n'existe qu'un seul corps de décomposition minimal, le corps de Galois appartenant à Z, contrairement à l'infinité générale de décompositions non isomorphes dans le corps non commutatif (voir R. Brauer-E. Noether, op. cit.), est dû à l'unique décomposition en somme directe dans le corps commutatif, par opposition à l'unique décomposition à isomorphisme d'opérateurs près dans le corps non commutatif. Autrement dit, il existe un nombre fini de représentations absolument irréductibles différentes, au lieu de l'infinité de représentations différentes dans le corps non commutatif, qui appartiennent cependant à la même classe (cf. 2).

8.2. Justification de la théorie galoisienne hypercomplexe dans le cas des corps séparables Z/P.

Par analogie exacte avec le § 6.3. la théorie des isomorphismes s'applique ici pour tout Z séparable sur P ; dans le cas d'un Z galoisien, la transition vers le groupe d'automorphismes usuel peut alors être effectuée.

Hypothèses : Soit Z, un corps d'extension fini et séparable sur P, Ω un corps de décomposition fini ou infini sur P, $\mathsf{Z} = \mathsf{Z}^{(1)}$ un sous-corps isomorphe à Z, et Γ le corps de Galois correspondant. Par conséquent, d'après la propriété 1 (Z est séparable !), la décomposition en somme directe est vérifiée :

$$\mathfrak{r}^{(1)} + \ldots + \mathfrak{r}^{(n)} = e^{(1)} Z_\Omega + \ldots + e^{(n)} Z_\Omega = e^{(1)}\Omega + \ldots + e^{(n)}\Omega.$$

La représentation $Z \to \mathsf{Z}^{(i)}$ engendrée par $e^{(1)}$ avec $\mathsf{Z}^{(i)} \leq \Gamma$ est donc définie par $e^{(i)} z = e^{(i)} \zeta^{(i)}$.

Leçon 1 : Les représentations engendrées par $e^{(1)}, \ldots, e^{(n)}$ sont toutes distinctes.

Démonstration : comme dans le § 6.3. ou bien également selon 1 ; car elles appartiennent à des classes de représentations différentes.

Leçon 2 : Si T est un corps intermédiaire entre P et Z, et s le rang de Z par rapport à T, alors tout isomorphisme de T vers Ω admet au moins s extensions, et donc exactement s extensions.

Démonstration : identique à celle du § 6.3. Le fait que la condition "au moins" soit ici trop restrictive découle de l'unique partition de Z_Ω, selon laquelle Z possède non pas au moins, mais exactement n isomorphismes dans Ω (voir les remarques à la fin de la section 1).

Comme dans le § 6.3, on définit maintenant la division de classes $\mathfrak{I}_T$ de l'ensemble (fini) $\mathfrak{I}$ des isomorphismes de Z induits par T – seuls les isomorphismes de $\mathfrak{I}$ qui induisent le même isomorphisme sur T sont considérés comme équivalents dans $\mathfrak{I}_T$ – et l'on démontre le théorème fondamental suivant :

Si $\mathfrak{I}_T$ est la division de classes induite par T, alors T est un sous-corps maximal par rapport à cette division de classes.

À partir de là, dans le cas d'un Z galoisien, on peut passer au groupe d'automorphismes et à la formulation usuelle par composition avec l'inverse d'un isomorphisme, comme dans le § 6.3. L'énoncé correspondant pour les sous-groupes découle de la considération des idempotents, qui présentent un intérêt en soi.

8.3. Les idempotents de Z_Ω.

Soit S soumis aux n substitutions qui transforment Z en chaque $\mathsf{Z}^{(i)}$, c'est-à-dire la composition des isomorphismes : $\mathsf{Z} \to Z$ et $Z \to \mathsf{Z}^{(i)}$, où le premier est donc l'inverse de $Z \to \mathsf{Z}$. Z n'est pas nécessairement galoisien. Pour les éléments a de Z_Z, les substitutions S sont définies comme des opérateurs par la condition qu'elles induisent l'identité sur Z ; ainsi, pour chaque a, le conjugué a^S appartenant à $Z_{\mathsf{Z}^{(i)}}$ est défini. Sous ces conditions, on a :

Théorème : Les n idempotents $e^{(i)}$ de Z_Ω sont conjugués : $e^{(i)} = e^S$ avec $e = e^{(1)}$. Ils appartiennent aux systèmes d'extension conjugués $Z_{\mathsf{Z}^{(i)}}$.

L'application de S transforme les relations de définition $ez = e\zeta^{(1)}$; $e^2 = e$ en $e^S z = e^S \zeta^{(i)}$; $(e^S)^2 = e^S$. Du fait de l'unicité de la décomposition, les idempotents sont également déterminés de manière unique ; ainsi, $e^{(i)} = e^S$. Puisque Z est un corps de scindage, et donc la représentation $ez = e\zeta$ est déjà médiatisée, e est déjà dans Z_Z et donc $e^{(i)}$ est dans $Z_{\mathsf{Z}^{(i)}}$.

Si Z est spécifiquement galoisien, alors la partie du théorème fondamental de la théorie de Galois relative aux sous-groupes s'ensuit directement ; en effet, si $\mathfrak{H}$ est un sous-groupe du groupe galoisien $\mathfrak{G}$, alors – du fait de la détermination unique des composantes d'une somme directe – l'élément $\sum e^H$ avec H dans $\mathfrak{H}$ admet toutes les substitutions de $\mathfrak{H}$, mais aucune autre. Puisque le groupe $\mathfrak{G}$ a été défini pour Z, il s'agit de la théorie galoisienne de Z ; grâce à l'isomorphisme, la théorie de Z est ainsi complète.

8.4. Lien des idempotents avec les bases complémentaires.

On ne suppose pas nécessairement que Z soit galoisien.

Théorème : Si $a_1, \ldots, a_n$ est une base de Z sur P, alors l'idempotent $e = a_1\beta_1 + \ldots + a_n\beta_n$ est posé – c'est-à-dire $e^S = a_1\beta_1^S + \ldots + a_n\beta_n^S$ – alors $\beta_1^S, \ldots, \beta_n^S$ représente l'image de la base complémentaire $b_1, \ldots, b_n$ par $a_1, \ldots, a_n$ dans l'application médiée par e^S.

Dans l'application $e^S z = e^S \zeta^S$ médiée par $e^S a_i = e^S \alpha_i^S$, puisque $e^S \cdot e^S = e^S$ et $e^S \cdot e^R = 0 (S \neq R)$, les affectations suivantes sont vérifiées : $e^S \to 1; e^R \to 0$. Par conséquent :

$$1 = \alpha_1^S\beta_1^S + \ldots + \alpha_n^S\beta_n^S \quad 0 = \alpha_1^S\beta_1^R + \ldots + \alpha_n^S\beta_n^R \qquad (S \neq R),$$

ou écrite sous forme de matrices, l'équation définissant les bases complémentaires

$$\begin{pmatrix} \alpha_1 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots \\ \alpha_1^S & \ldots & \alpha_n^S \\ \ldots & \ldots & \ldots \end{pmatrix} \begin{pmatrix} \beta_1 & \ldots & \beta_1^R & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \beta_n & \ldots & \beta_n^R & \ldots \end{pmatrix} = E.$$

La transition vers la définition de trace découle du fait que pour $a_i = \sum_S e^S \alpha_i^S$ et $b_i = \sum_S e^S \beta_i^S$ la relation matricielle, après avoir interverti les matrices, devient [8]

$$\mathrm{Sp}(a_i b_i) = 1 \; ; \qquad \mathrm{Sp}(a_i b_k) = 0 \quad \text{pour } i \neq k.$$

Les a_i et b_i appartiennent à Z, puisqu'ils admettent toutes les substitutions S (Théorème de Lesson § 3.3) [9].

La contraréciprocité des bases complémentaires découle du fait que les idempotents e^S sont des invariants de Z, quelle que soit la base sous-jacente. Autrement dit, tous les $a_1\beta_1^S + \ldots + a_n\beta_n^S$ se transforment en eux-mêmes lors du passage à une autre base $\overline{a}_1, \ldots, \overline{a}_n$ de Z. Z/P.

9. Corps de décomposition et corps de décomposition de systèmes arbitraires.

9.1. Définitions et réduction au cas simple.

Les définitions données au § 8 correspondent dans le cas général à

8. Cf. *Representation Theory* § 25.

9. Les relations entre bases complémentaires et idempotents apparaissent pour la première fois chez Dedekind, dans son ouvrage "Sur la théorie des quantités complexes formées à partir d'unités principales" (cf. vol. II des Œuvres complètes, p. 4-5).

Définitions : Soit S un hypercomplexe sur P. Un corps d'extension (commutatif) Λ de P est appelé corps de scindage de S si S_Λ se décompose en facteurs de composition absolument simples pour une série de composition d'idéaux unilatéraux ; autrement dit, si toutes les représentations irréductibles de S dans Λ sont déjà absolument irréductibles. Un corps d'extension T de P est appelé corps de scindage si S_T scinde au moins un facteur de composition absolument simple, c'est-à-dire si au moins une représentation irréductible dans T est déjà absolument irréductible.

Ces définitions contiennent manifestement celles données dans le § 8 pour les algèbres commutatives et dans le § 7 pour les algèbres simples ; notamment pour ces dernières du fait que A_Λ est alors complètement réductible par toute extension commutative du centre, et que donc les facteurs de composition et les composantes de la décomposition en somme directe coïncident. Cependant, seuls les anneaux de matrices complets sur le centre produisent des composantes absolument simples, et donc également des représentations absolument irréductibles. De plus, puisque A_Λ est simple à deux côtés, c'est-à-dire qu'il se décompose en composantes isomorphes à des opérateurs, l'extraction d'une composante absolument simple conduit à la décomposition complète : le corps de décomposition et le corps de scindage de décomposition coïncident.

Les faits suivants découlent directement des définitions :

Les corps de décomposition de S sont donnés comme unions des corps de décomposition des représentations irréductibles dans P ; le corps de décomposition de S est tout corps de décomposition d'une représentation irréductible dans P.

Comme les systèmes simples correspondent biunivoquement au radical et aux représentations irréductibles dans P, il suffit de considérer les systèmes simples. Les résultats seront obtenus en combinant les résultats du § 7 et ceux du § 8.

9.2. Corps de décomposition et corps de décomposition plus simples.

Cas des systèmes. Nous considérons d'abord le cas d'un système simple A à centre séparable Z sur P. À partir des § 8.1 et § 8.3, nous obtenons :

La décomposition bilatérale de A_Ω, correspondant à la décomposition en somme directe de Z_Ω (où Ω désigne un corps de décomposition de Z), donne n composantes conjuguées $e^{(i)}A$ de A isomorphes à A. Ces composantes deviennent des algèbres simples sur leur centre $e^{(i)}\,\mathsf{Z}^{(i)} = e^{(i)}Z$. Les substitutions S sont définies comme opérateurs sur A_Z en stipulant qu'elles induisent l'identité sur A (Voir § 8.3).

Puisque, d'après le § 8.3, les idempotents sont conjugués, il en va de même pour les composantes $e^{(i)}A$ par définition des substitutions de A. Comme A est simple des deux côtés, $e^{(i)}A$ est isomorphe à A par l'anneau. Cela signifie que $e^{(i)}A = e^{(i)}A_{\mathsf{Z}^{(i)}}$ car $e^{(i)}Z = e^{(i)}\,\mathsf{Z}^{(i)} = e^{i)}Z_{\mathsf{Z}^{(i)}}$; ainsi, le centre coïncide avec le domaine des coefficients.

Composantes autour des algèbres normales. Les résultats du § 7.2 impliquent maintenant que :

Si A est un système simple sur P avec un centre séparable Z sur P, alors A_Ω est également complètement réductible sans radical ; Ω peut désigner n'importe quel corps d'extension fini ou infini.

Puisque, d'après le § 7.2, $e^{(i)}A_{\mathsf{Z}^{(i)}}$ reste simplement inchangé par toute extension de coefficients, c'est-à-dire sans radical. Ainsi, il en va de même pour la somme directe ; cependant, celle-ci est A_Ω ou provient — si Ω n'est pas un corps de décomposition de Z — de A_Ω par extension de coefficients. De plus, du § 7.2, découle la :

Caractérisation des corps de détachement et des corps de désintégration : Si A est une algèbre à division de centre séparable Z, alors les plongements irréductibles des corps de décomposition sont donnés par tous les sous-corps commutatifs maximaux de A_r entourant Z, et seulement ceux-ci ; les corps de décomposition sont tous les corps d'union d'un corps de décomposition avec un corps de décomposition du centre, en particulier avec le corps de Galois appartenant au centre, et seulement ceux-ci. Un corps de décomposition minimal peut être un corps de décomposition même si son centre n'est pas galoisien.

Pour qu'un corps de décomposition contienne un corps isomorphe à Z, l'énoncé d'immersion concernant les corps de décomposition découle des faits précédents et du § 7.2. De plus, un corps de décomposition contient nécessairement un corps de décomposition Ω sur Z. Tout corps de décomposition sur Ω est également un corps de décomposition, puisque ses composantes $e^{(i)}A_\Omega$ sont simples et ont un centre isomorphe à Ω. Si Z est galoisien, alors les corps de décomposition minimaux et les corps de décomposition coïncident. Mais même dans le cas non galoisien, contrairement au cas commutatif, il peut exister des corps de décomposition minimaux qui sont aussi des corps de décomposition, c'est-à-dire dès qu'un tel corps de décomposition minimal contient le corps de Galois appartenant à Z [*Exemple* : le corps des quaternions dont le centre est isomorphe à $\mathsf{P}\left(\sqrt[3]{2}\right)$, le corps des nombres rationnels P ; le corps de Galois appartenant à $\mathsf{P}\left(\sqrt[3]{2}\right)$ est un corps de décomposition minimal et un corps de décomposition].

Si le centre est inséparable, alors Z_Ω et donc A_Ω forment un système muni d'un radical. Soit $\mathfrak{C}$ le radical de Z_Ω et $\mathfrak{c}$ l'idéal d'extension dans A_Ω. Alors $Z_\Omega/\mathfrak{C}$ admet une décomposition en somme directe de composantes conjuguées, par analogie exacte avec le § 8.2 ; ceci induit, comme précédemment, la décomposition en somme directe de $A_\Omega/\mathfrak{c}$, de sorte que les composantes $\overline{e}^{(i)}A$ sont isomorphes à A de centre $\overline{e}^{(i)}\,\mathsf{Z}^{(i)}$. Ainsi, les théorèmes sur les corps de décomposition et de division restent valides. De plus, l'énumération des rangs montre que les facteurs de composition correspondant à une série de composition de $\mathfrak{C}$ deviennent des opérateurs *isomorphes* à $A_\Omega/\mathfrak{c}$, et non seulement *homomorphes*.

Exprimé pour les représentations irréductibles, cela se traduit par le résumé suivant : si une représentation irréductible d'un système hypercomplexe existe dans P, alors cette représentation devient absolument complètement réductible si et seulement si le centre correspondant est séparable sur P. Dans tous les cas, les corps de scindage et de décomposition de la représentation peuvent être caractérisés en les plongeant dans le système simple correspondant, comme indiqué précédemment. En particulier, le degré le plus adverse d'un corps de décomposition est égal au produit du degré du centre et de l'indice de la classe d'algèbre correspondante sur le centre, et le degré de chaque corps de décomposition est un multiple de ce produit. La représentation se scinde, au sens des séries

de composition, en autant de classes de représentations absolument irréductibles, différentes mais conjuguées, en autant de classes, donc, que le degré du plus grand corps séparable contenu dans le centre. Chaque classe apparaît autant de fois que le produit de l'indice et du degré du centre après cette extension séparable.

Pour un corps de base parfait, où il n'existe que des corps d'extension séparables, nous revenons ainsi aux résultats connus de I. Schur ; avec l'ajout de la caractérisation d'immersion, que l'on trouve déjà dans R. Brauer.