Séminaire Dubreil.
Algèbre et théorie
des nombres

Jean Dieudonné

Généralisation de la théorie de Galois

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 7, p. 1-6
<http://www.numdam.org/item?id=SD_1947-1948__1__A7_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1947/48
-:-:-:-

Exposé n° 7

GÉNÉRALISATION DE LA THÉORIE DE GALOIS

par Jean DIEUDONNÉ

(Conférence résumée par Pierre SAMUEL)

La théorie de Galois, qui avait atteint ses résultats essentiels au siècle dernier, et dont l'exposé était pleinement satisfaisant depuis plus de dix ans, a connu ces dernières années un nouveau bourgeonnement.

Il est dû principalement aux idées développées dans l'enseignement d'Emil ARTIN : la théorie classique "montait" d'un corps à ses extensions ; une des idées principales d'ARTIN est de "descendre" d'un corps à ses sous-corps.

Quatre résultats principaux marquent la théorie de Galois descendante :

1° Le théorème de réciprocité : Si Γ est un groupe fini d'automorphismes d'un corps K, et L le corps des invariants de Γ, alors le groupe de tous les L-automorphismes de K (automorphismes laissant invariant L) est exactement Γ.

2° La relation ordre-degré $(K : L)$ = ordre de Γ.

3° Le théorème des corps intermédiaires ; Si $L \subset E \subset K$, K est galoisien sur E, c'est-à-dire que E est le corps des invariants du groupe de tous les E-automorphismes de K.

4° Le théorème de prolongement des isomorphismes : Si φ est un L-isomorphisme d'un corps intermédiaire E sur un corps intermédiaire E', φ se prolonge en un L-automorphisme de K.

L'outil principal d'ARTIN (qui se trouve d'ailleurs dans DEDEKIND) est le théorème d'indépendance linéaire des automorphismes :

si $\psi_1(x), \ldots, \psi_k(x)$ sont des automorphismes distincts de K sur L :

$$\left[\sum \lambda_i \cdot \psi_i(x) = 0 \text{ , } \lambda_i \in K \text{ , tout } x \longrightarrow \lambda_i = 0\right] .$$

1. Théories de JACOBSON, KALOUJNINE, H. CARTAN.

La première extension de la théorie de Galois est due à KALOUJNINE et à JACOBSON (voir notamment l'exposé 6 de L. KALOUJNINE).

Au lieu des L-automorphismes de K , JACOBSON considère les endomorphismes de K , sous sa structure d'espace vectoriel sur L (nous noterons K_L cet espace vectoriel). Ces endomorphismes forment un anneau $\mathcal{L}(K_L)$, qui contient notamment les combinaisons linéaires (à coefficients dans K) des L-automorphismes de K :

$$a(x) = \sum \lambda_i . \psi_i(x) \ , \quad x \in K \ , \quad \lambda_i \in K \ , \quad \text{(sommation en } i) \ .$$

Afin de ne pas faire jouer un rôle particulier à un sous-corps L , parmi tous les sous-corps de K , il est commode de considérer l'anneau $\mathcal{E}(K)$ de tous les endomorphismes de K , considéré comme groupe additif ; cet anneau contient tous les $\mathcal{L}(K_L)$.

Les "homothéties" :

$$x \longrightarrow \lambda x \quad (\lambda \in K)$$

constituent un sous-corps de $\mathcal{E}(K)$, qu'on peut identifier à K .

JACOBSON considère alors les sous-anneaux M de $\mathcal{E}(K)$, qui contiennent ces homothéties.

A un tel sous-anneau M , on fait correspondre le sous-corps L des homothéties (de K) , qui sont permutables avec tout élément u de M :

$$u(\lambda x) = \lambda . u(x) \ .$$

On voit facilement que tout élément v de $\mathcal{E}(K)$, qui est permutable avec tous les éléments de M , ne peut qu'être une homothétie. Il en résulte que L est le commutant de M dans $\mathcal{E}(K)$.

Dans cette théorie subsistent les propriétés 1 et 2, ci-dessus, que l'on peut appeler "prégaloisiens" :

1° Si M est de rang fini sur K , on a $M = \mathcal{L}(K_L)$;

2° Si L est fini sous K , on a $[\ (K_L) : K] = (K : L)$

Les sous-corps galoisiens L de K , sont caractérisés par le fait que $\mathcal{L}(K_L)$ est engendré linéairement, sur K , par des automorphismes du corps K .

H. CARTAN et JACOBSON sont passés de là au cas d'un corps K, non commutatif. Il faut alors considérer K_L comme espace vectoriel à droite sur L, et M comme espace vectoriel à gauche sur K (identifié avec le corps des homothéties à gauche de K). Les résultats prégaloisiens restent toujours valables.

2. Principe de la théorie de DIEUDONNÉ.

DIEUDONNÉ a étendu la théorie aux anneaux simples. Pour simplifier, on se bornera aux anneaux d'ARTIN simples : c'est-à-dire aux anneaux satisfaisant à la condition minimale pour leurs idéaux à gauche et ne possédant pas d'idéal bilatère non trivial. Un tel anneau peut être considéré comme un anneau d'endomorphismes d'un espace vectoriel, E, à gauche, et de dimension finie sur un corps (gauche) K.

Dans la théorie de Kaloujnine-Jacobson, le corps K intervient dans trois rôles différents :

- comme groupe additif,
- comme domaine d'opérateurs à gauche sur ce groupe,
- comme domaine d'opérateurs à droite.

Dans la théorie actuelle, ces rôles sont remplis par des éléments différents :

E est un groupe abélien (additif) ; le corps K et l'anneau A en sont des ensembles d'opérateurs, à gauche, permutables entre eux.

Pour retrouver la théorie de Cartan-Jacobson, il faut supposer : $E = K$; $K = K$, mais A = le corps opposé (ou symétrique) de K.

3. Propriétés prégaloisiennes.

Nous considérerons donc un groupe abélien (additif) E et l'anneau $\mathfrak{R}$ de tous ses endomorphismes, un sous-corps K de $\mathfrak{R}$, tel que E soit un espace vectoriel E_K, de dimension finie n, sur K, le commutant A de K : c'est alors l'anneau des endomorphismes de l'espace vectoriel E_K, donc un sous-anneau simple de $\mathfrak{R}$.

On démontre facilement que K est le commutant de A et que leur intersection est leur centre commun. La théorie prégaloisienne revient alors essentiellement à la commutation de Schur.

1° Si B est un sous-anneau simple de $\mathfrak{R}$, (de même élément unité), le commutant C de B est un anneau simple, et B est le commutant de C (on suppose ici que E est un B-module de longueur finie).

2° Pour les relations entre deux degrés, il faut d'abord définir deux entiers

caractérisant la position d'un sous-anneau simple A' dans un anneau simple, A. Nous utiliserons à cet effet des idéaux d'un côté, par exemple à gauche.

(a). Soit Z' un idéal minimal de A' ; AZ' est un idéal de A, somme directe de i idéaux minimaux de A. Le nombre entier i, qui ne dépend ni de Z', ni du mode de décomposition de AZ', est appelé l'indice (à gauche) de A' dans A.

(b). Un idéal minimal Z de A est un A'-module de longueur finie, somme directe de h A'-modules simples (donc isomorphes). Le nombre entier h, qui ne dépend ni du choix de Z, ni du mode de décomposition en somme directe, est appelé la hauteur (à gauche) de A sur A'.

Le produit ih, (considéré déjà par ARTIN-WHAPLES), est appelé de degré de A sur A' ; c'est le nombre de A'-modules simples dont A est somme directe.

Les longueurs m et m', de A et A' sont reliées par $m = m'i$. Si A est un corps $m' = 1$, $m = i$, et h est la dimension sur A' d'un idéal minimal de A.

Ceci posé si B et B' sont les commutants de A et A' $(B' \subset B)$; la propriété 2 devient :

indice de A' dans A = hauteur de B' sur B ;
hauteur de A sur A' = indice de B dans B'.

4. Propriétés galoisiennes.

Un automorphisme ψ, d'un corps K, est tel que :

$$\psi(\lambda x) = \psi(\lambda).\psi(x) = \lambda^{\psi}\ \psi(x) ;$$

c'est donc un endomorphisme semi-linéaire, ou semi-endomorphisme, de K, considéré comme espace vectoriel, à gauche, sur lui-même.

A étant l'anneau simple commutant de K, nous dirons que B, sous-anneau simple de A, est galoisien, si son commutant est engendré par des semi-endomorphismes de E.

Nous dirons que deux semi-endomorphismes de E :

$$u(\lambda x) = \lambda^{\psi} u(x) , \quad u'(x) = \lambda^{\psi'} u'(x) ,$$

sont de même classe, si les automorphismes ψ et ψ' de K correspondants, ne diffèrent que par un automorphisme intérieur de K :

$$\lambda^{\psi'} = \alpha . \lambda^{\psi} . \alpha^{-1} \quad (\alpha \in K) .$$

C'est là une relation d'équivalence (ou d'égalité, ou de congruence) ; la classe unité est celle des semi-endomorphismes relatifs aux automorphismes intérieurs (si α est dans K, αu et u sont de même classe).

Le théorème de Dedekind est alors généralisé par le lemme :

(a). Si des semi-endomorphismes de E sont de même classe et s'ils sont linéairement indépendants sur le centre I de K, ils sont linéairement indépendants sur K.

(b). Si F est un sous-espace vectoriel de E sur K engendré par des semi-endomorphismes, F est somme directe de sous-espaces F_Θ ; les F_Θ étant engendrés par les semi-endomorphismes de même classe Θ.

On en déduit la conséquence :

K et A sont linéairement disjoints sur leur centre commun I ; ils engendrent donc un anneau isomorphe à leur produit tensoriel $A \otimes K$ (sur I) ; ce produit est engendré par les semi-endomorphismes de la classe unité.

Nous supposerons désormais que :

K est de degré fini sur I, et que A est de degré fini sur B, et que le commutant C de B est engendré par des semi-endomorphismes de E.

C'est une question non résolue que de savoir si cette deuxième condition est toujours remplie.

Elle l'est dans le cas <u>intérieur</u>, caractérisé par le fait que B contient I ; alors :

$$C \subset K \otimes A \quad \text{et} \quad C = K \otimes D ,$$

D étant le commutant de B, dans A.

Elle l'est aussi dans le cas opposé au cas intérieur, où

$$C \cap (K \otimes A) = K \ ;$$

on dit alors que B est un <u>sous-anneau galoisien extérieur de</u> A.

Si ces conditions sont remplies nous dirons que B est <u>un sous-anneau fortement galoisien de</u> A.

S'il en est ainsi, le commutant C de B est somme directe de C_i ; chacun d'eux étant engendré par des semi-endomorphismes de même classe, de E ; ils ont

tous même dimension d sur K, qui est égale à celle de :

$$C_0 = C \cap (K \otimes A) \ .$$

La dimension de C sur K est donc nd, où n est l'ordre du groupe g, des classes d'automorphismes de K, relativement aux générateurs des C_i : $nd = (C : K)$ est égal au degré de A sur B.

$B \cap I$ est un sous-corps galoisien de I, de groupe isomorphe à g, B et I sont linéairement disjoints sur $B \cap I$, et engendrent par conséquent $B \otimes I$; lequel est un anneau simple qui admet C_0 comme commutant.

Enfin si $B \otimes I$ est simple, B est un sous-anneau fortement galoisien extérieur de $B \otimes I$, et il y a correspondance biunivoque entre les sous-anneaux simples B' $(B \subset B' \subset B \otimes I)$ et les sous-groupes g' de g.