ANNALES SCIENTIFIQUES DE L'É.N.S.

HENRI CARTAN

# Théorie de Galois pour les corps non commutatifs

*Annales scientifiques de l'É.N.S. 3^e série*, tome 64 (1947), p. 59-77

<http://www.numdam.org/item?id=ASENS_1947_3_64__59_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1947, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

# THÉORIE DE GALOIS

POUR

# LES CORPS NON COMMUTATIFS

PAR M. HENRI CARTAN.

Nous nous proposons de généraliser aux corps non commutatifs ce qu'on appelle aujourd'hui la *théorie de Galois* des corps *commutatifs*, c'est-à-dire l'étude des relations entre certains *sous-corps* d'un corps donné K, et certains *groupes d'automorphismes* du corps K. Notre théorie contient en particulier les théorèmes de Skolem-Nœther (1) relatifs aux automorphismes intérieurs d'un corps de rang fini sur son centre, théorèmes qui constituent ce que E. Nœther (2) appelait précisément la « théorie de Galois » des corps non commutatifs (*voir* ci-après, § 9). Mais notre actuelle théorie est plus compréhensive, car elle englobe également les résultats de Jacobson (3) relatifs aux groupes d'automorphismes *extérieurs* d'un corps (commutatif ou non), résultats qui contiennent eux-mêmes comme cas particuliers ceux de la théorie de Galois pour un corps commutatif, sous la forme que leur ont donnée Artin et Baer.

Ainsi les deux théories connues, celles de Skolem-Nœther, et celle de Galois-Artin-Jacobson, apparaissent comme les deux pôles d'une théorie unitaire, celle qui fait l'objet du présent article.

1. *Notions générales sur les corps.* — Nous ne revenons pas sur la notion de *corps* (4). Un *isomorphisme* d'un corps K sur un corps K′ est une application

(1) *Voir* DEURING, *Algebren* (*Ergebnisse*, IV, 1, 1935), p. 42-44. *Voir* aussi VAN DEN WAERDEN, *Moderne Algebra*, II, 2e édition, p. 202-204.

(2) E. NOETHER, *Nichtkommutative Algebra* (*Math. Zeits.*, 37, 1933, p. 514-541).

(3) *Ann. of Math.*, 41, 1940, p. 1-7.

(4) Nous adoptons la terminologie de N. BOURBAKI [*Algèbre*, Chap. I (*Actual. scient. et ind.*, fasc. 934; Paris, Hermann, 1942)]. Un *corps* (c'est-à-dire un anneau dont l'ensemble des éléments $\neq 0$ forme un groupe pour la multiplication) n'est donc pas nécessairement supposé commutatif.

biunivoque $f$ de K sur K′ telle que l'on ait, pour tout $x$ et tout $y$ de K,

$$f(x-y)=f(x)-f(y), \qquad f(xy)=f(x)f(y),$$

d'où résulte

$$f(0)=0, \qquad f(1)=1, \qquad f(x^{-1})=[f(x)]^{-1}.$$

En particulier, un *automorphisme* d'un corps K est un isomorphisme de K sur K.

La donnée d'un *sous-corps* L d'un corps K définit sur K deux structures d'*espace vectoriel* (5) par rapport au corps L : une structure d'espace vectoriel *à gauche*, pour laquelle le « produit » d'un élément $x$ de K et d'un « scalaire » $\alpha$ de L est l'élément $\alpha x$ de K; une structure d'espace vectoriel *à droite*, pour laquelle le « produit » d'un élément $x$ de K et d'un « scalaire » $\alpha$ de L est l'élément $x\alpha$ de K. On appellera *rang à gauche* de K sur L, la dimension de K comme espace vectoriel à gauche sur L; on définit de même le *rang à droite*. Ces rangs peuvent être infinis, et ils ne sont pas nécessairement égaux. D'une manière générale, soit E une partie quelconque de K; on appellera rang (à gauche) de E sur L la dimension du sous-espace vectoriel (à gauche sur L) engendré par E; on définit de même le rang (à droite) de E sur L.

Si L est le *centre* C de K, c'est-à-dire le sous-corps des éléments qui permutent avec tout élément de K, les deux structures d'espace vectoriel sur C sont identiques; on parlera donc du *rang* (de K, ou d'une partie de K) sur C, sans spécifier s'il s'agit de rang à droite ou de rang à gauche.

Pour qu'un automorphisme $f$ de K soit en même temps un automorphisme pour la structure d'espace vectoriel (à gauche sur un sous-corps L), il faut et il suffit que $f(\alpha x)=\alpha f(x)$ pour tout $\alpha \in L$, ce qui donne $f(\alpha)=\alpha$ pour tout $\alpha \in L$. Autrement dit, il faut et il suffit que tous les éléments de L soient *invariants* par $f$. Les automorphismes qui jouissent de cette propriété forment évidemment un *groupe*, que nous noterons $G_L^K$.

Inversement, soit $\mathcal{G}$ un groupe d'automorphismes du corps K. Les éléments de K invariants par ce groupe (c'est-à-dire invariants par chaque automorphisme du groupe) forment évidemment un *sous-corps* de K. Nous l'appellerons le sous-corps des invariants de $\mathcal{G}$.

Un sous-corps L de K sera dit *galoisien* s'il existe un groupe d'automorphismes $\mathcal{G}$ tel que L soit précisément le sous-corps des invariants de $\mathcal{G}$. Cela revient à dire que L est le sous-corps des invariants du groupe $G_L^K$, qui prend alors le nom de *groupe de Galois* de K relativement à L. La notion de sous-corps galoisien est relative au surcorps K de L; on dit aussi que K est une *extension galoisienne* de L.

Un sous-corps quelconque L de K étant donné, il existe un plus petit sous-

(5) Pour les notions d'algèbre linéaire, *voir* BOURBAKI, *Algèbre*, Chap. II (*Actual. scient. et ind.*, fasc. 1032; Paris, Hermann, 1947).

corps galoisien de K contenant L : c'est le sous-corps des invariants du groupe $G_L^K$. D'autre part, l'intersection d'une famille quelconque de sous-corps galoisiens $L_i$ de K est un sous-corps galoisien de K, car c'est le sous-corps des invariants du groupe engendré par les automorphismes des groupes $G_{L_i}^K$.

Soit K un corps (commutatif ou non) qui soit de *rang fini* (à gauche) sur un sous-corps L. Alors tout *sous-anneau* de K qui contient L est un *sous-corps*; cela résulte du fait général suivant : si un anneau A, sans diviseur de zéro, contient un *corps* L (commutatif ou non) dont l'élément unité est élément unité de A, et si le rang de A (comme espace vectoriel à gauche sur L) est *fini*, alors A est un *corps* ([6]).

Dans la même hypothèse (K de rang fini sur L), tout isomorphisme de K sur un sous-corps de K, qui laisse invariants les éléments de L, est un isomorphisme de K *sur* K, c'est-à-dire un élément du groupe $G_L^K$ ([7]).

2. *Théorie de Galois pour un corps commutatif.* — Nous voulons, dans ce paragraphe, rappeler quelques points essentiels de la théorie de Galois pour corps *commutatifs*, sous la forme donnée par Artin.

Tout d'abord, en adoptant la définition donnée plus haut d'une extension galoisienne, on a le critère classique :

*Pour que* K (commutatif) *soit extension galoisienne de* L, *il faut et il suffit que :* 1° *tout polynome à coefficients dans* L, *irréductible sur* L, *et qui possède au moins une racine dans* K, *se décompose dans* K *en un produit de polynomes du premier degré;* 2° dans le cas où la caractéristique $p$ de K est $\neq 0$, *tout élément de* K *dont la puissance* $p^{\text{ième}}$ *appartient à* L *appartienne lui-même à* L.

Cela étant, on peut établir, indépendamment du critère précédent, les trois théorèmes suivants :

THÉORÈME A. — *Soit* $\mathcal{G}$ *un groupe d'automorphismes d'un corps* (com.) K, *et soit* L *le sous-corps des invariants de* $\mathcal{G}$. *Pour que* K *soit de rang fini sur* L, *il faut et il suffit que* $\mathcal{G}$ *soit fini; s'il en est ainsi, le rang de* K *sur* L *est égal à l'ordre de* $\mathcal{G}$, *et* $\mathcal{G}$ *est le groupe de Galois* $G_L^K$.

---

([6]) Cette proposition est bien connue lorsque L est dans le *centre* de A, c'est-à-dire lorsque A est une *algèbre* sur L. Elle se démontre aussi aisément dans le cas général : désignons par 1 l'élément unité de A, et montrons d'abord que, pour tout $a$ non nul de A, existe un $b \in A$ tel que $ba = 1$. L'application $x \to xa$ de A dans A est *linéaire* (pour la structure d'espace vectoriel à gauche sur K) et *biunivoque* (sinon $a$ serait diviseur de zéro); comme l'espace vectoriel A est de dimension finie, cette application applique A *sur* A, et il existe donc un $b$ tel que $ba = 1$. On a aussi $ab = 1$, car il existe de même un $c$ tel que $cb = 1$, d'où $c = c(ba) = (cb)a = a$. Ainsi, tout élément $\neq 0$ de A possède un inverse. C. Q. F. D.

([7]) En effet, un tel isomorphisme est une application linéaire biunivoque de l'espace vectoriel K (de dimension finie) sur un sous-espace de K, donc sur K tout entier.

THÉORÈME B. — *Soit* K *une extension galoisienne* (commutative) *de* L, *de rang fini sur* L. *Tout sous-corps* H *contenant* L *est sous-corps galoisien de* K. *En outre, il existe une correspondance biunivoque entre les sous-corps* H *tels que* $L \subset H \subset K$, *et les sous-groupes* $\mathfrak{H}$ *du groupe de Galois* $G_L^K$, *telle que chaque sous-corps* H *soit le sous-corps des invariants du groupe* $\mathfrak{H}$ *associé à* H, *et que chaque sous-groupe* $\mathfrak{H}$ *soit le groupe de Galois* K *de relativement au sous-corps* H *associé à* $\mathfrak{H}$.

THÉORÈME C. — *Soit* K *une extension galoisienne* (commutative) *de* L, *de rang fini sur* L. *Pour qu'un sous-corps* H *contenant* L *soit extension galoisienne de* L, *il faut et il suffit que le groupe* $G_H^K$ *soit sous-groupe distingué de* $G_L^K$, *et alors le groupe de Galois* $G_L^H$ *est isomorphe au groupe quotient* $G_L^K/G_H^K$.

Les théorèmes précédents ont été étendus par Jacobson ([3]) au cas où, K n'étant plus supposé commutatif, on envisage un groupe $\mathcal{G}$ qui ne contient, en dehors de l'automorphisme identique, aucun automorphisme *intérieur* (*voir* § 4 ci-dessous); les théorèmes B et C valent alors si l'on suppose que le groupe de Galois $G_L^K$ satisfait à cette condition.

Nous ne rappellerons pas ici les démonstrations des théorèmes précédents, puisqu'ils apparaîtront comme cas particuliers des théorèmes fondamentaux du paragraphe 5, que nous démontrerons aux paragraphes 6, 7 et 8.

3. *Le théorème de Jacobson-Bourbaki.* — Le théorème que nous allons exposer constitue le résultat essentiel d'un travail de Jacobson ([8]), où n'était envisagé que le cas d'un corps K *commutatif*. La présentation actuelle du théorème et son extension au cas d'un corps non commutatif sont dus à N. Bourbaki ([9]). C'est ce théorème qui nous servira de base de départ pour la généralisation des théorèmes A, B, C (§ 2) au cas non commutatif.

Alors que la théorie de Galois proprement dite n'envisage de correspondance qu'entre certains sous-corps de K (les sous-corps *galoisiens* L tels que K soit de rang fini sur L) et les groupes finis d'*automorphismes* de K, on va envisager ici *tous* les sous-corps L tels que K soit de rang fini sur L; de l'autre côté, il faudra remplacer la considération des groupes d'automorphismes par quelque chose de plus compréhensif.

Nous appellerons *endomorphisme* du corps K un endomorphisme de la structure du *groupe additif* de K, c'est-à-dire une application $f$ de K dans K telle que $f(x-y)=f(x)-f(y)$ pour tout $x$ et tout $y$ de K. Sur l'ensemble $\mathfrak{E}(K)$ des endomorphismes de K, nous considérerons les deux structures suivantes : 1° une structure d'*anneau*, la somme $h$ de deux endomorphismes $f$ et $g$ étant définie par $h(x)=f(x)+g(x)$ pour tout $x \in K$, et le produit $p$ de $f$ et $g$ étant défini par $p(x)=f[g(x)]$ pour tout $x \in K$; 2° une structure d'*espace*

([8]) *Amer. Journal*, 66, 1944, p. 1.

([9]) *Voir*, dans le volume de BOURBAKI cité en ([5]), le paragraphe 5.

*vectoriel* (à droite) sur K, la somme de deux éléments de $\mathcal{E}(K)$ étant définie comme plus haut, et le « produit » d'un endomorphisme $f$ par un élément $k \in K$, noté $fk$, étant défini comme l'endomorphisme qui, à $x \in K$, fait correspondre l'élément $f(x)k$ du corps K.

Nous dirons qu'un sous-anneau $\mathfrak{A}$ de $\mathcal{E}(K)$ est *sous-anneau vectoriel* s'il satisfait aux deux conditions suivantes : 1° $\mathfrak{A}$ contient l'endomorphisme *identique* (qui, à chaque $x$ de K, fait correspondre ce même $x$); 2° $\mathfrak{A}$ est sous-espace vectoriel de $\mathcal{E}(K)$ pour la structure d'espace vectoriel (à droite sur K) définie ci-dessus.

Le théorème de Jacobson-Bourbaki peut alors s'énoncer ainsi :

*Il existe une correspondance biunivoque entre les sous-corps* L *de* K *tels que* K *soit de rang fini (à gauche) sur* L, *et les sous-anneaux vectoriels de* $\mathcal{E}(K)$ *qui sont de dimension finie* (comme espaces vectoriels à droite sur K). *Cette correspondance associe à chaque sous-corps* L *le sous-anneau des endomorphismes* $f$ *tels que* $f(\alpha x) = \alpha f(x)$ *pour tout* $x \in K$ *et tout* $\alpha \in L$ (endomorphismes de la structure d'espace vectoriel à gauche sur L); *inversement, elle associe à chaque sous-anneau vectoriel* $\mathfrak{A}$ *le sous-corps des* $\alpha \in K$ *tels que l'on ait* $f(\alpha x) = \alpha f(x)$ *pour tout* $f \in \mathfrak{A}$ *et tout* $x \in K$. *Dans la correspondance précédente, la dimension d'un sous-anneau vectoriel est égale au rang de* K *sur le sous-corps associé au sous-anneau.*

La définition du sous-corps *associé* à un sous-anneau vectoriel $\mathfrak{A}$ a un sens même si $\mathfrak{A}$ n'est pas de dimension finie. Il résulte du théorème précédent le critère que voici : pour que le sous-corps L associé à un sous-anneau vectoriel $\mathfrak{A}$ soit tel que K soit de *rang fini* (à gauche sur L), il faut et il suffit que $\mathfrak{A}$ soit de *dimension finie* (à droite sur K), et alors le rang de K est *égal* à la dimension de $\mathfrak{A}$.

Pour la démonstration du théorème précédent, nous renvoyons au Traité de Bourbaki (9). Elle fait intervenir la notion d'éléments *primordiaux* d'un sous-espace vectoriel d'un espace vectoriel de base $(e_i)$ donnée (finie ou infinie). Tout élément d'un tel espace vectoriel E (à droite sur un corps K) s'écrivant d'une seule manière sous la forme $\sum_i e_i k_i$ (les coefficients $k_i \in K$ étant tous nuls sauf un nombre fini), on désigne, pour chaque élément $x$ de E, par $I(x)$ l'ensemble (fini) des $i$ tels que les coefficients $k_i$ de $x$ soient $\neq 0$; cet ensemble n'est vide que si $x = 0$. Soit alors V un sous-espace vectoriel de E; un élément $x$ de V sera dit *primordial* [sous-entendu : relativement à la base $(e_i)$ de E] si : 1° l'un au moins des coefficients $k_i$ de $x$ est égal à 1 (unité de K); 2° pour tout $y$ de V tel que $I(y) \subset I(x)$, $I(y)$ est vide ou identique à $I(x)$, ce qui entraîne que $y$ a la forme $xk$ (où le coefficient $k \in K$; nous dirons que $y$ est *proportionnel* à $x$). On voit facilement que *tout* élément de V est combinaison linéaire (à coefficients à droite dans K) d'éléments *primordiaux*; autrement dit, le sous-espace vectoriel V est *engendré* par ses éléments primordiaux.

La notion d'élément primordial jouera un rôle essentiel dans les démonstrations des théorèmes fondamentaux (*voir* ci-après, § 6, 7 et 8).

4. *Automorphismes intérieurs d'un corps; groupes achevés.* — Pour pouvoir énoncer simplement nos théorèmes, nous avons encore à préciser certaines notions et notations.

Étant donné un corps K, nous désignerons par $K^*$ le *groupe multiplicatif* des éléments $\neq o$ de K; plus généralement, pour tout sous-corps L de K, $L^*$ désignera le sous-groupe de $K^*$ formé des éléments $\neq o$ de L.

A chaque $k \in K^*$, associons la transformation de K dans K

$$x \to kxk^{-1},$$

transformation que nous noterons $\sigma_k$ [autrement dit, $\sigma_k(x) = kxk^{-1}$]. C'est un automorphisme de K (§ 1). Les automorphismes de la forme $\sigma_k$ s'appellent les *automorphismes intérieurs* de K; ils forment un *groupe* que nous noterons $\Gamma$ (tant qu'il n'y aura pas ambiguïté sur le corps K). L'application $k \to \sigma_k$ de $K^*$ sur $\Gamma$ est une *représentation* du premier groupe sur le second (le composé $\sigma_k \circ \sigma_h$ est égal à $\sigma_{kh}$); les $k$ tels que $\sigma_k$ soit l'automorphisme identique sont les éléments (autres que o) du *centre* C de K, et par suite la représentation précédente définit un *isomorphisme* du groupe quotient $K^*/C^*$ sur le groupe $\Gamma$ des automorphismes intérieurs. Tout ceci est bien classique.

Si $\omega$ est un automorphisme (quelconque) de K, le « transformé » de $\sigma_k$ par $\omega$, c'est-à-dire l'automorphisme composé $\omega \circ \sigma_k \circ \omega^{-1}$, n'est autre que l'automorphisme intérieur $\sigma_h$, avec $h = \omega(k)$. Il en résulte que si $\mathcal{G}$ est un groupe quelconque d'automorphismes de K, le sous-groupe $\mathcal{G} \cap \Gamma$ est sous-groupe *distingué* de $\mathcal{G}$. Désignons par $K(\mathcal{G})$ l'ensemble des $k \in K^*$ tels que $\sigma_k \in \mathcal{G}$; c'est un sous-groupe de $K^*$ qui contient $C^*$, et qui est *invariant* (dans son ensemble) par le groupe $\mathcal{G}$.

Considérons le *sous-corps* engendré par $K(\mathcal{G})$, sous-corps que nous noterons $\widehat{K(\mathcal{G})}$. Lui aussi est *invariant* (dans son ensemble) par $\mathcal{G}$. L'ensemble des automorphismes (de K) de la forme $\sigma_k \circ \omega$, où $\omega$ parcourt $\mathcal{G}$, et $k$ parcourt $\widehat{K(\mathcal{G})}$, constitue donc un *groupe* qui contient $\mathcal{G}$, et que nous noterons $\widehat{\mathcal{G}}$; les groupes quotients $\mathcal{G}/\mathcal{G} \cap \Gamma$ et $\widehat{\mathcal{G}}/\widehat{\mathcal{G}} \cap \Gamma$ sont d'ailleurs isomorphes.

On remarquera que $\widehat{K(\mathcal{G})}$ contient le sous-espace vectoriel (sur C) engendré par $K(\mathcal{G})$; ce sous-espace vectoriel est un *sous-anneau* de K. Lorsque $K(\mathcal{G})$ est de *rang fini* sur C, ce sous-anneau est un *sous-corps* (*cf.* fin du § 1); c'est donc $\widehat{K(\mathcal{G})}$.

Nous dirons qu'un groupe $\mathcal{G}$ d'automorphismes de K est *achevé* si $\widehat{\mathcal{G}} = \mathcal{G}$; autrement dit, si $K(\mathcal{G}) \cup \{o\}$ est un *sous-corps* de K. Dans tous les cas, le groupe $\widehat{\mathcal{G}}$ est achevé; c'est le plus petit groupe achevé contenant $\mathcal{G}$.

Pour tout sous-corps L de K, le groupe $G_L^K$ (défini au paragraphe 1) est *achevé*, car $\sigma_k \in G_L^K$ signifie que $k$ est $\neq 0$ et permute avec tout élément de L; donc $K(\mathcal{G}) \cup \{0\}$ est le *sous-corps* (que nous noterons toujours L') des éléments de K qui permutent avec tout élément de L.

Si l'on part d'un groupe quelconque $\mathcal{G}$, et si L désigne le sous-corps des invariants de $\mathcal{G}$, le groupe *achevé* $G_L^K$ a même sous-corps d'invariants que $\mathcal{G}$, et par suite le plus petit groupe achevé contenant $\mathcal{G}$ a même sous-corps d'invariants que $\mathcal{G}$. Il ne peut donc pas être question, comme dans la théorie de Galois pour corps *commutatifs*, de caractériser un groupe d'automorphismes de K par le sous-corps (galoisien) des invariants de ce groupe. Toutefois, nous allons voir moyennant quelles hypothèses de finitude un groupe *achevé* peut être caractérisé par son sous-corps d'invariants.

5. *Énoncé des théorèmes fondamentaux.*

THÉORÈME 1. — *Soit $\mathcal{G}$ un groupe d'automorphismes d'un corps* K, *et soit* L *le sous-corps des invariants de $\mathcal{G}$. Pour que* K *soit de rang fini (à gauche) sur* L, *il faut et il suffit que :* 1° *le groupe quotient $\mathcal{G}/\mathcal{G} \cap \Gamma$ soit fini;* 2° $K(\mathcal{G})$ *soit de rang fini sur le centre* C *de* K (10). *Dans ces conditions :*

α. *on a la relation*

$$r = nd$$

*entre le rang r de* K *sur* L, *l'ordre n du groupe $\mathcal{G}/\mathcal{G} \cap \Gamma$, et le rang d de* $K(\mathcal{G})$ *sur* C;

β. *le groupe de Galois* $G_L^K$ *n'est autre que le plus petit groupe achevé contenant $\mathcal{G}$; en particulier, si $\mathcal{G}$ est achevé, il est groupe de Galois de* K *sur le sous-corps des invariants de $\mathcal{G}$.*

Ce théorème, qui généralise le théorème A du paragraphe 2, sera démontré plus loin (§ 6). On a bien entendu le même théorème pour le rang *à droite* (de K sur L), et par suite :

COROLLAIRE DU THÉORÈME 1. — *Si* L *est un sous-corps galoisien de* K, *et si le rang (à gauche) de* K *sur* L *est fini et égal à r, le rang (à droite) de* K *sur* L *est fini et égal à r.* On parlera désormais simplement du *rang* (tout court) de K sur un sous-corps *galoisien* de K.

*Remarques.* — 1° Soit L un sous-corps (galoisien ou non) tel que K soit de rang *fini r* (à gauche) sur L. Alors le groupe $G_L^K$ satisfait aux conditions du théorème 1, puisque son sous-corps d'invariants H contient L. Le rang de K sur H est un diviseur du rang de K sur L, et ne lui est égal que si L est sous-

(10) S'il en est ainsi, on vient de voir (§ 4) que le sous-corps $\widehat{K(\mathcal{G})}$ engendré par $K(\mathcal{G})$ est identique au sous-espace vectoriel (sur C) engendré par $K(\mathcal{G})$.

corps *galoisien* de K. Si $n$ désigne l'ordre de $G_L^K/G_L^K \cap \Gamma$, et $d$ le rang de L' sur C, on voit que $nd$ *divise* $r$ et ne peut être *égal* à $r$ que si L est sous-corps galoisien de K.

2° Le cas envisagé par Jacobson ([3]) est celui où $d = 1$. C'est celui qui se présente toujours si K est *commutatif*.

THÉORÈME 2. — *Soit* L *un sous-corps galoisien d'un corps* K, *tel que* K *soit de rang fini sur* L. *Tout sous-corps* H *contenant* L *est sous-corps galoisien de* K, *et tout sous-groupe achevé du groupe de Galois* $G_L^K$ *est groupe de Galois de* K *relativement à un sous-corps contenant* L. *D'une façon précise, il existe une correspondance biunivoque entre les sous-corps* H *tels que* $L \subset H \subset K$, *et les sous-groupes achevés* $\mathfrak{H}$ *de* $G_L^K$, *telle que chaque* H *soit le sous-corps des invariants du groupe* $\mathfrak{H}$ *associé à* H, *et que chaque* $\mathfrak{H}$ *soit le groupe de Galois de* K *relativement au sous-corps* H *associé à* $\mathfrak{H}$.

Ce théorème, qui généralise le théorème B (§ 2), sera démontré au paragraphe 7.

*Remarque.* — La correspondance précédente est évidemment décroissante : si $L \subset H_1 \subset H_2 \subset K$, le sous-groupe $\mathfrak{H}_1$ associé à $H_1$ contient le sous-groupe $\mathfrak{H}_2$ associé à $H_2$. De là résulte : le sous-groupe associé à l'intersection de deux sous-corps est le plus petit groupe achevé contenant les sous-groupes associés à ces sous-corps respectivement; le sous-groupe associé au sous-corps $[H_1, H_2]$ engendré par deux sous-corps $H_1$ et $H_2$ est l'intersection des sous-groupes associés respectivement à $H_1$ et $H_2$.

Si H est un sous-corps tel que $L \subset H \subset K$, le rang de K sur L est égal au produit des rangs de K sur H et de H sur L; tenant compte du théorème 2 et du corollaire du théorème 1, on voit que *si* K *est extension galoisienne de* L, *de rang fini sur* L, *le rang* (*à gauche*) *de* K *sur tout sous-corps* H *contenant* L *est égal au rang* (*à droite*) *de* K *sur ce même sous-corps*.

THÉORÈME 3. — *Soit* K *une extension galoisienne d'un corps* L, *de rang fini sur* L, *et soit* H *un sous-corps de* K *contenant* L (*cf.* théorème 2). On désignera par $G_L^K(H)$ le sous-groupe de $G_L^K$ formé des automorphismes qui laissent H *invariant* (dans son ensemble). *Alors :*

$\alpha$. *si un isomorphisme de* H *sur un sous-corps de* K *laisse invariants les éléments de* L, *il peut se prolonger en un automorphisme de* K;

$\beta$. *en particulier, les automorphismes du groupe* $G_L^H$ *sont induits, sur* H, *par les automorphismes de* $G_L^K(H)$, *et par suite* $G_L^H$ *est isomorphe au quotient du groupe* $G_L^K(H)$ *par son sous-groupe distingué* $G_H^K$;

$\gamma$. *pour que* H *soit extension galoisienne de* L, *il faut et il suffit que* $G_L^K$ *soit le plus petit groupe achevé contenant* $G_L^K(H)$;

$\delta$. *en particulier, si* H *est invariant par tout automorphisme du groupe de Galois* $G_L^K$ [c'est-à-dire si $G_L^K(H) = G_L^K$], H *est extension galoisienne de* L; *pour*

*qu'il en soit ainsi, il faut et il suffit que* $G_H^K$ *soit sous-groupe distingué de* $G_L^K$, *et* $G_L^H$ *est alors isomorphe au quotient* $G_L^K/G_H^K$.

*Remarque.* — Si $\mathcal{G}$ est un sous-groupe *distingué* (non nécessairement achevé) de $G_L^K$, le sous-corps H des invariants de $\mathcal{G}$ est *invariant* par $G_L^K$, et le groupe de Galois $G_L^H$ est isomorphe au quotient de $G_L^K$ par le groupe $\widehat{\mathcal{G}}$.

Le théorème 3 généralise le théorème C (§ 2) et sera démontré au paragraphe 8.

Dès maintenant, nous pouvons tirer une conséquence intéressante de la partie $\alpha$ de ce théorème. Appelons *polynome* en $x$, à coefficients dans le corps L, toute somme finie de termes dont chacun a la forme

$$a\,x\,b\,x\,c\,x\,\ldots\,e\,x\,l,$$

où les éléments $a$, $b$, $c$, ..., $e$, $l$, en nombre fini quelconque, appartiennent à L, et où $x$ est un « variable » qui va prendre ses valeurs dans K. Si l'on fixe $x$ dans K, les polynomes en $x$ sont des éléments de K qui constituent un *sous-anneau* de K contenant L. Donc, dans les hypothèses du théorème 3, ce sous-anneau est un *sous-corps* de K (*cf.* fin du paragraphe 1); c'est évidemment le sous-corps [L, $x$] *engendré par* L *et* $x$. En tant qu'anneau, il est isomorphe au quotient de l'anneau des polynomes à une variable par l'*idéal bilatère* des polynomes qui s'annulent pour l'élément $x$ considéré de K. Cela posé, convenons de dire que deux éléments $x$ et $y$ de K *satisfont aux mêmes relations algébriques à coefficients dans* L s'ils annulent les mêmes polynomes (à une variable) à coefficients dans L; dans ce cas, il existe un isomorphisme évident du sous-corps [L, $x$] sur le sous-corps [L, $y$], par passage au quotient à partir de l'isomorphisme des anneaux de polynomes. D'après le théorème 3, $\alpha$, l'isomorphisme de [L, $x$] sur [L, $y$] se prolonge en un automorphisme de K.

Convenons alors de dire que deux éléments $x$ et $y$ de K sont *conjugués* par rapport à L s'il existe un automorphisme du groupe $G_L^K$ qui transforme $x$ en $y$. Il est évident que deux éléments conjugués satisfont aux mêmes relations algébriques (à coefficients dans L). Mais ce qui précède montre que la réciproque est exacte. Ainsi :

COROLLAIRE DU THÉORÈME 3, $\alpha$. — *Dans les hypothèses du théorème* 3, *une condition nécessaire et suffisante pour que deux éléments de* K *soient conjugués par rapport à* L *est qu'ils satisfassent aux mêmes relations algébriques à coefficients dans* L.

Dans le cas où L est dans le centre de K, cette condition exprime que les deux éléments sont racines d'un même polynome *irréductible* sur L. On retrouve une proposition bien connue, lorsque K est un corps commutatif.

6. *Démonstration du premier théorème fondamental.* — Reportons-nous aux notions exposées au paragraphe 3. Tout automorphisme du corps K est *a fortiori* un endomorphisme du groupe additif de K, c'est-à-dire un élément de $\mathfrak{E}(K)$, espace vectoriel (à droite) sur K. On peut considérer les *combinaisons linéaires* $\sum_i \omega_i k_i$ d'automorphismes $\omega_i$, à coefficients (à droite) dans K; ce sont des endomorphismes de K, et, exceptionnellement, des automorphismes de la structure de corps de K. On a aussi la notion d'automorphismes *linéairement dépendants* (sous-entendu : à droite sur K). Le lemme suivant va nous donner une condition pour la dépendance linéaire des automorphismes de K.

LEMME 1. — *Pour que les automorphismes d'une famille* $(\omega_i)_{i\in I}$ *soient linéairement dépendants, il faut et il suffit qu'il existe une partie finie non vide* J *de l'ensemble d'indices* I, *et, pour chaque* $i\in J$, *un élément* $k_i\in K^*$, *de manière que* $\sum_{i\in J} k_i = 0$, *et* $\omega_i = \sigma_{k_i}\circ\omega$ *pour tout* $i\in J$ ($\omega$ désignant l'un des automorphismes $\omega_i$).

La condition est suffisante, car on a alors, pour tout $x\in K$,

$$\sum_{i\in J}\omega_i(x)k_i = \sum_{i\in J}[k_i\omega(x)k_i^{-1}]k_i = \left(\sum_{i\in J}k_i\right)\omega(x) = 0.$$

Montrons que la condition est nécessaire. Les systèmes $(k_i)$ d'éléments de K tels que les $k_i$ soient tous nuls sauf un nombre fini, et que $\sum_i \omega_i k_i = 0$, forment un sous-espace vectoriel V de l'espace E (vectoriel à droite sur K) de *tous* les systèmes d'éléments de K, nuls sauf un nombre fini. Désignons par $e_i$ le système des $k_j$ tels que $k_j = 0$ pour $j\neq i$ et $k_i = 1$. Les $e_i$ forment une *base* de E. On a alors la notion d'élément primordial de V (*cf.* § 3), c'est-à-dire de *relation primordiale* entre automorphismes $\omega_i$. Cela posé, si les $\omega_i$ sont linéairement dépendants, il existe au moins une relation primordiale entre les $\omega_i$ (car l'espace vectoriel E de toutes les relations est engendré par les relations primordiales). Soit $\sum_i \omega_i k_i = 0$ une telle relation primordiale, et soit J l'ensemble des indices $i$ tels que $k_i\neq 0$. Puisque

$$\sum_{i\in J}\omega_i(x)k_i = 0 \qquad \text{pour tout } x\in K, \tag{1}$$

on a en particulier, pour $x = 1$, $\sum_{i\in J} k_i = 0$. De plus, remplaçons $x$ par $xy$ dans (1); on a, pour tout $y\in K$, la relation

$$\sum_{i\in J}\omega_i(x)\omega_i(y)k_i = 0,$$

et par suite $\sum_{i\in I}\omega_i h_i = 0$, avec $h_i = 0$ pour $i \notin J$ et $h_i = \omega_i(y)k_i$ pour $i \in J$. La relation (1) étant primordiale, il s'ensuit que le système $(h_i)$ est *proportionnel* (avec coefficient à droite) au système $(k_i)$. Le coefficient de proportionnalité est évidemment $\omega(y)$, $\omega$ désignant celui des $\omega_i$ pour lequel $k_i = 1$. On a donc, pour tout $i \in J$,

$$\omega_i(y)k_i = k_i\omega(y) \qquad \text{pour tout } y \in K, \qquad \text{c'est-à-dire } \omega_i = \sigma_{k_i}\circ\omega.$$

Ceci démontre le lemme.

COROLLAIRE. — *Pour que des automorphismes intérieurs $\sigma_{h_i}$ soient linéairement dépendants (à droite sur* K*), il faut et il suffit que les $h_i$ soient linéairement dépendants sur le centre* C. (La même condition exprimera aussi la dépendance linéaire des $\sigma_{h_i}$ *à gauche* sur K.)

En effet, la condition du lemme s'écrit $\sigma_{h_i} = \sigma_{k_i}\circ\sigma_h$, avec $\sum_{i\in J}k_i = 0$.

Abordons maintenant la démonstration du théorème 1. Soit $\mathcal{G}$ un groupe d'automorphismes du corps K. L'ensemble des combinaisons linéaires (à coefficients à droite dans K) d'automorphismes $\omega_i$ de $\mathcal{G}$ constitue un *sous-anneau vectoriel* de $\mathcal{E}(K)$ : le seul point à vérifier est que le composé d'un endomorphisme $\omega_i k_i$ et d'un endomorphisme $\omega_j k_j$ est proportionnel à $\omega_i\circ\omega_j$; or c'est l'endomorphisme $(\omega_i\circ\omega_j)\omega_i(k_j)k_i$. Cherchons à quelle condition ce sous-anneau vectoriel $\mathfrak{A}$ est de *dimension finie* (à droite sur K). Il *faut* d'abord que $K(\mathcal{G})$ soit de *rang fini* sur C : car si $\mathfrak{A}$ est de dimension $r$, il existe au plus $r$ éléments $k_i \in K^*$, linéairement indépendants sur C, tels que $\sigma_{k_i} \in \mathcal{G}$, en vertu du corollaire du lemme 1. Il *faut* en outre que le groupe quotient $\mathcal{G}/\mathcal{G}\cap\Gamma$ soit *fini* : car il existe au plus $r$ éléments $\omega_j$ de $\mathcal{G}$, non congrus modulo $\mathcal{G}\cap\Gamma$, en vertu du lemme 1.

Réciproquement, supposons que $K(\mathcal{G})$ soit de rang fini $d$ sur C, et que $\mathcal{G}/\mathcal{G}\cap\Gamma$ soit d'ordre fini $n$. Prenons $d$ éléments $k_i \in K(\mathcal{G})$, formant une base de $\widehat{K(\mathcal{G})}$ [qui, rappelons-le, est le sous-espace vectoriel sur C, engendré par $K(\mathcal{G})$; *voir* § 4]. Prenons en outre $n$ éléments $\omega_j$ de $\mathcal{G}$, représentant respectivement les classes de $\mathcal{G}$ modulo $\mathcal{G}\cap\Gamma$. Les $\sigma_{k_i}\circ\omega_j$ sont linéairement indépendants (à droite sur K), et engendrent le sous-espace vectorie $\mathfrak{A}$ de $\mathcal{E}(K)$, comme cela résulte du lemme 1. Puisque ces éléments sont en nombre $nd$, on voit que $\mathfrak{A}$ est de dimension finie égale à $nd$.

Ainsi : pour que le sous-anneau vectoriel $\mathfrak{A}$ formé des combinaisons linéaires (à coefficients à droite dans K) d'automorphismes de $\mathcal{G}$ soit de dimension finie, il faut et il suffit que : 1° le groupe quotient $\mathcal{G}/\mathcal{G}\cap\Gamma$ soit fini; 2° $K(\mathcal{G})$ soit de rang fini sur C; et l'on a alors la relation $r = nd$ entre la dimension $r$ de $\mathfrak{A}$, l'ordre $n$ de $\mathcal{G}/\mathcal{G}\cap\Gamma$, et le rang $d$ de $K(\mathcal{G})$ sur C.

A partir de là, on obtient le théorème 1 en utilisant le théorème de Jacobson-Bourbaki (§ 3), suivant lequel la condition pour que $\mathfrak{A}$ soit de dimension finie égale à $r$, est que K soit de rang fini, égal à $r$, sur le sous-corps L des éléments $\alpha$ de K tels que l'on ait

$$(2) \qquad f(\alpha x) = \alpha f(x) \qquad \text{pour tout } f \in \mathfrak{A} \text{ (et tout } x \in K).$$

Or il suffit d'exprimer la relation (2) pour les $f$ d'un système de générateurs de l'espace vectoriel $\mathfrak{A}$, ici pour les automorphismes $\omega$ du groupe $\mathcal{G}$. Le sous-corps L est donc le sous-corps des invariants de $\mathcal{G}$, ce qui démontre le théorème 1, sauf l'assertion $\beta$.

Pour démontrer $\beta$, cherchons les automorphismes du groupe de Galois $G_L^K$; ce sont des endomorphismes $f$ qui satisfont à (2); d'après le théorème de Jacobson-Bourbaki, ils appartiennent précisément à l'anneau $\mathfrak{A}$ ci-dessus, puisque cet anneau vectoriel est associé au sous-corps L. Le lemme 1 prouve alors que ces automorphismes ont la forme $\sigma_k \circ \omega$, où $\omega$ appartient à $\mathcal{G}$, et $k$ est combinaison linéaire (à coefficients dans C) d'éléments de $K(\mathcal{G})$. Autrement dit, les automorphismes de $G_L^K$ sont ceux du groupe $\widehat{\mathcal{G}}$, plus petit groupe achevé contenant $\mathcal{G}$.

*Remarque.* — On voit que lorsque $n$ et $d$ sont *finis*, le groupe $\widehat{\mathcal{G}}$ se compose des automorphismes qui sont combinaisons linéaires (à coefficients dans K) d'automorphismes du groupe $\mathcal{G}$. Les coefficients à gauche donnent les mêmes automorphismes que les coefficients à droite.

7. *Démonstration du deuxième théorème fondamental.*

LEMME 2. — *Si un sous-anneau vectoriel $\mathfrak{A}$ de $\mathfrak{E}(K)$ est engendré* [en tant que sous-espace vectoriel de $\mathfrak{E}(K)$] *par des automorphismes de* K, *tout sous-anneau vectoriel $\mathfrak{B}$ contenu dans $\mathfrak{A}$ est engendré par des automorphismes du corps* K.

En effet, soient $\omega_i$ des *automorphismes* formant une *base* de l'espace vectoriel $\mathfrak{A}$ (à droite sur K). Pour cette base, considérons les éléments *primordiaux* du sous-espace vectoriel $\mathfrak{B}$. Je dis que si un endomorphisme $f = \sum_i \omega_i k_i$ est un élément primordial de $\mathfrak{B}$, $f$ est *proportionnel* à un automorphisme $\varpi$ du corps K; autrement dit, il existe un $h \in K$ tel que $\varpi = fh$. Le lemme en résultera, puisque $\mathfrak{B}$ est engendré par ses éléments primordiaux.

Puisque $f(x) = \sum_i \omega_i(x) k_i$ pour tout $x \in K$, on a, en remplaçant $x$ par $xy$,

$$f(xy) = \sum_i \omega_i(x)\,\omega_i(y)\,k_i.$$

Or, pour chaque $y \in K$, l'endomorphisme $x \to f(xy)$ appartient à $\mathcal{B}$; en effet $\mathcal{B}$ contient l'endomorphisme identique $x \to x$, et est espace vectoriel sur K, donc contient l'endomorphisme $x \to xy$; de plus, $\mathcal{B}$ est un anneau, donc contient le composé de cet endomorphisme et de l'endomorphisme $f$, ce qui prouve l'assertion. Cela étant, l'endomorphisme $x \to f(xy)$, qui appartient à $\mathcal{B}$, est combinaison des $\omega_i$, avec pour coefficients les $\omega_i(y)k_i$. Comme l'élément $f$ de $\mathcal{B}$ a été supposé primordial, les $\omega_i(y)k_i$ sont proportionnels aux $k_i$; le coefficient de proportionnalité (à droite) est $\omega(y)$, en désignant par $\omega$ celui des $\omega_i$ pour lequel $k_i = 1$. Ainsi, on a

$$f(xy) = f(x)\omega(y), \qquad \text{d'où en particulier } f(y) = f(1)\omega(y).$$

$f(1)$ n'est pas nul, sinon $f(y)$ serait nul pour tout $y$, et $f$ ne serait pas un élément primordial de $\mathcal{B}$. Posons alors

$$\varpi(x) = f(x)[f(1)]^{-1};$$

on a $\varpi(x) = f(1)\omega(x)[f(1)]^{-1}$, donc $\varpi$, comme $\omega$, est un *automorphisme*.

C. Q. F. D.

Abordons maintenant la démonstration du théorème 2. Dans les hypothèses de ce théorème, désignons par $\mathcal{A}$ le sous-anneau vectoriel de $\mathcal{E}(K)$ engendré par les automorphismes du groupe $G_L^K$. D'après le théorème de Jacobson-Bourbaki (§ 3), il y a correspondance biunivoque entre les sous-corps H tels que $L \subset H \subset K$, et les sous-anneaux vectoriels contenus dans $\mathcal{A}$. D'après le lemme 2, un tel sous-anneau vectoriel $\mathcal{B}$ est engendré par des *automorphismes* du corps K, et par suite, le sous-corps H associé à $\mathcal{B}$ est le sous-corps des éléments de K invariants par ces automorphismes; H est donc sous-corps *galoisien* de K. En outre, pour qu'un automorphisme appartienne à $\mathcal{B}$, il faut et il suffit qu'il laisse invariants les éléments du sous-corps H associé; donc les automorphismes qui appartiennent à $\mathcal{B}$ sont précisément ceux du groupe de Galois $G_H^K$. Les groupes $G_H^K$ relatifs aux sous-corps H de K contenant L constituent *tous* les sous-groupes *achevés* de $G_L^K$, car si $\mathcal{H}$ est un sous-groupe achevé de $G_L^K$, le sous-corps H des invariants de $\mathcal{H}$ contient L, donc K est de rang fini sur H, et par suite (théor. 1, $\beta$) $\mathcal{H}$ est le groupe de Galois de K relativement à H.

Le théorème 2 est donc entièrement démontré.

8. *Démonstration du troisième théorème fondamental.* — Les parties $\beta$ et $\delta$ du théorème 3 étant des conséquences immédiates des parties $\alpha$ et $\gamma$, nous nous bornerons à démontrer $\alpha$ et $\gamma$.

La démonstration de $\alpha$ est analogue à celle du lemme 1 (§ 6). Plaçons-nous dans les hypothèses du théorème 3. Soit $\omega$ un isomorphisme de H sur un sous-corps de K, qui laisse invariants les éléments du sous-corps L. Si l'on envisage

sur K la structure d'espace vectoriel (à gauche) sur L, $\omega$ est une application *linéaire* du sous-espace vectoriel H dans l'espace K. On peut donc prolonger $\omega$ (de plusieurs manières) en une application linéaire $\bar{\omega}$ de K dans K, c'est-à-dire en un élément du sous-anneau vectoriel $\mathfrak{A}$ que le théorème de Jacobson-Bourbaki associe au sous-corps L. Or on a supposé que K est une extension *galoisienne* de L, de rang fini sur L; donc $\mathfrak{A}$ se compose des combinaisons linéaires (à droite sur K) des automorphismes du groupe de Galois $G_L^K$.

Bref, le prolongement $\bar{\omega}$ de $\omega$ est combinaison linéaire d'automorphismes $\omega_i$ du groupe $G_L^K$; on aura en particulier une relation de la forme

$$\omega(x) = \sum_i \omega_i(x) k_i \qquad \text{pour tout } x \in H.$$

Les éléments 1 et $-k_i$ sont ainsi les coefficients d'une relation linéaire entre $\omega$ et les $\omega_i$ *sur le sous-corps* H; et l'on peut, parmi toutes les relations linéaires de ce type, en choisir une qui soit *primordiale* (au sens du paragraphe 6, démonstration du lemme 1), et telle que le coefficient de $\omega$ soit égal à 1. Une telle relation primordiale s'écrira

$$\omega(x) = \sum_{i \in J} \omega_i(x) k_i \qquad \text{pour } x \in H, \tag{3}$$

les $k_i$ étant $\neq 0$ pour $i \in J$, et déterminés de façon *unique*. Or, si l'on remplace, dans (3), $x$ par $xy$ ($y \in H$), on obtient

$$\omega(x)\omega(y) = \sum_{i \in J} \omega_i(x)\omega_i(y) k_i \qquad \text{pour } x \in H,$$

d'où, en vertu de l'unicité,

$$k_i \omega(y) = \omega_i(y) k_i \qquad \text{pour tout } y \in H.$$

Ceci exprime que $\omega$ est la restriction à H de l'automorphisme de K

$$x \to k_i^{-1} \omega_i(x) k_i,$$

$i$ désignant un élément particulier (d'ailleurs quelconque) de J.

La partie $\alpha$ du théorème 3 étant ainsi démontrée, démontrons $\gamma$. Soit $L_1$ le sous-corps des invariants de $G_L^K(H)$; comme $G_L^K(H) \supset G_H^K$, $L_1$ est contenu dans H. Dire que L est sous-corps galoisien de H, c'est dire que $L_1 = L$, donc (théor. 1, $\beta$) que $G_L^K$ est le plus petit groupe achevé contenant $G_L^K(H)$.

C. Q. F. D.

9. *Application aux théorèmes de Skolem-Nœther* (1). — Soit K un corps de *rang fini sur son centre* C. Appliquons le théorème 1, $\beta$ en prenant pour groupe $\mathcal{G}$ le groupe $\Gamma$ des automorphismes *intérieurs* de K. Le groupe $\Gamma$ étant

évidemment achevé, et le sous-corps L étant ici le centre C, on voit que Γ *est le groupe de Galois de* K *relativement à son centre* C.

Un sous-groupe *achevé* de Γ est formé des $\sigma_k$ relatifs aux $k$ non nuls d'un *sous-corps* contenant C. Le théorème 2 nous dit alors que les sous-corps contenant C se correspondent deux à deux, chacun des deux se composant des éléments de K qui *permutent* avec les éléments de l'autre. Si H est un sous-corps contenant K, et si H′ désigne le sous-corps associé (formé des éléments qui permutent avec ceux de H), le théorème 1, α donne l'égalité $r = d$ entre le rang $r$ de K sur H et le rang $d$ de H′ sur C; c'est dire que *le rang de* K *sur* C *est égal au produit des rangs de* H *sur* C *et de* H′ *sur* C.

Enfin, le théorème 3, α montre que *si un isomorphisme de* H *sur un sous-corps de* K *laisse invariants les éléments de* C, *il est induit* (*sur* H) *par un automorphisme intérieur de* K (dans cet énoncé, H désigne un sous-corps contenant C).

On retrouve ainsi les principaux théorèmes de Skolem et E. Nœther, par une voie différente de celles suivies jusqu'ici. Mais, tandis que les résultats de Skolem-Nœther valent plus généralement pour un *anneau simple* (de rang fini sur son centre) et ses sous-anneaux simples contenant le centre, nous ne les trouvons ici que pour un *corps*. Toutefois J. Dieudonné me fait remarquer qu'un théorème général qu'il a démontré en 1942 (11) permet de déterminer la nature des automorphismes d'un anneau simple (c'est-à-dire d'un anneau de matrices sur un *corps*, au moins dans le cas où l'anneau en question est de rang fini sur son centre), lorsqu'on connaît les automorphismes de ce corps; on retrouverait donc, par cette voie, le théorème de Skolem-Nœther relatif aux automorphismes d'un anneau simple qui laissent invariants les éléments du centre de cet anneau.

*Remarque.* — Soit K un corps dont nous ne supposons même plus qu'il soit de rang fini sur son centre C, et soit H un sous-corps contenant C et de *rang fini d* sur C. Appliquons le théorème 1 au groupe formé des automorphismes intérieurs $\sigma_k$ relatifs aux $k \in$ H. En désignant toujours par H′ le sous-corps des éléments qui permutent avec les éléments de H, on obtient les résultats suivants : 1° *le rang r de* K *sur* H′ *est égal au rang d de* H *sur* C; 2° *le sous-corps des éléments qui permutent avec les éléments de* H′ *n'est autre que* H. Ceci généralise l'un des théorèmes de Skolem-Nœther aux corps de rang infini sur leur centre.

10. *Interprétation de la théorie générale dans le cas d'un corps de rang fini sur son centre.* — Dans tout ce paragraphe, K désigne un corps de rang *fini* sur son centre C.

Soit L un sous-corps *galoisien* de K, tel que K soit de rang fini sur L. Le sous-corps [C, L] engendré par C et L, sous-corps que nous désignerons par H,

(11) *Bull. Soc. Math. de France*, 70, 1942, p. 46-75; *voir* p. 69, théorème 5.

est sous-corps *galoisien* de K, puisqu'il contient L (*cf.* théor. 2) ([12]), et le groupe de Galois $G_H^K$ est l'*intersection* des groupes de Galois de K relativement à C et L respectivement; c'est donc $G_L^K \cap \Gamma$. Ainsi $G_H^K$ *se compose des automorphismes intérieurs qui appartiennent au groupe* $G_L^K$, c'est-à-dire des $\sigma_k$ relatifs aux $k$ non nuls du sous-corps $L' = H'$.

H *est une extension galoisienne de* L, car, C étant invariant (dans son ensemble) par tout automorphisme du corps K, le sous-corps $H = [C, L]$ est invariant (dans son ensemble) par le groupe $G_L^K$. Il en résulte bien que H est extension galoisienne de L (théor. 3, $\delta$). En outre (théor. 3, $\delta$), le groupe de Galois $G_L^H$ est isomorphe au quotient $G_L^K/G_H^K = G_L^K/G_L^K \cap \Gamma$, groupe qui est *fini*. Soit $n$ l'ordre de ce groupe, qui est aussi le *rang* de H sur L (théor. 1, $\alpha$).

L'intersection $C \cap L$ est le sous-corps des invariants du groupe $\mathcal{G}$ engendré par $G_C^K = \Gamma$ et $G_L^K$, groupe qui se compose des automorphismes $\sigma_k \circ \omega$, où $k \in K^*$ et $\omega \in G_L^K$. Ce groupe est évidemment achevé; l'entier $d$ que lui attache le théorème 1 est égal au rang de K sur C, et l'entier $n$ que lui attache le théorème 1 est égal à l'ordre de $G_L^K/G_L^K \cap \Gamma$, c'est-à-dire à l'entier précisément désigné par $n$ auparavant, et égal au rang de H sur L. D'après le théorème 1, $\mathcal{G}$ est le groupe de Galois de K relativement à $C \cap L$, et le rang de K sur $C \cap L$ est égal à $nd$, produit du rang de K sur C et du rang de H sur L; d'où il résulte que *le rang de* C *sur* $C \cap L$ *est égal au rang* $n$ *de* $H = [C, L]$ *sur* L.

D'ailleurs, C *est extension galoisienne de* $C \cap L$, car tout automorphisme du groupe de Galois de K relativement à $C \cap L$ laisse C invariant; il suffit alors d'appliquer le théorème 3, $\delta$. Nous allons voir que *les groupes de Galois* (finis) $G_{C\cap L}^C$ et $G_L^H$ *sont isomorphes*, de sorte que $G_{C\cap L}^C$ (groupe de Galois d'un corps *commutatif*, relativement à un sous-corps galoisien $C \cap L$) est isomorphe à $G_L^K/G_L^K \cap \Gamma$. Nous allons définir un isomorphisme canonique, bien déterminé, de $G_L^H$ sur $G_{C\cap L}^C$. Pour cela, remarquons que tout automorphisme $\varpi$ de C qui laisse invariants les éléments de $C \cap L$ peut se prolonger en un automorphisme du groupe $G_{C\cap L}^K$, d'après le théorème 3, $\alpha$. Mais ce dernier groupe, on l'a vu, se compose des $\sigma_k \circ \omega$ où $k \in K^*$ et $\omega \in G_L^K$. Comme $\sigma_k$ laisse invariants les éléments de C, on voit que $\varpi$ est la restriction (à C) d'un $\omega \in G_L^K$. Un tel $\omega$ laisse invariants les sous-corps C et L, donc laisse invariant le sous-corps $H = [C, L]$. Bref, *tout automorphisme de* $G_{C\cap L}^C$ *est la restriction à* C *d'un automorphisme de* $G_L^H$. Réciproquement, tout automorphisme de $G_L^H$ laisse C invariant, puisqu'il se prolonge en un automorphisme du corps K (théor. 3, $\alpha$), donc sa restriction à C est un automorphisme du groupe $G_{C\cap L}^C$; en outre deux automorphismes distincts de $G_L^H$ induisent sur C deux isomorphismes *distincts* de $G_{C\cap L}^C$, car si un automorphisme du corps H laisse invariants les éléments de L et ceux de C, c'est l'automorphisme identique. En résumé, si à chaque automorphisme du

([12]) Ce résultat vaut même si le rang de K sur C est infini.

groupe $G_L^H$ on fait correspondre sa restriction à C, on obtient une fois et une seule les automorphismes du groupe $G_{C\cap L}^C$. C. Q. F. D.

*Remarque.* — Puisque le rang de H sur L est égal au rang de C sur $C\cap L$, le rang de H sur C est égal au rang de L sur $C\cap L$; ou encore, le rang de $H=[C, L]$ sur $C\cap L$ est égal au *produit* des rangs de C et de L sur $C\cap L$. Ceci exprime que les corps C et L sont « linéairement disjoints », ou encore que [C, L] est isomorphe au *produit tensoriel* de C et L considérés comme *algèbres* sur $C\cap L$ ([13]).

11. *Nouvelle propriété des corps de rang fini sur leur centre.* — Soit K un corps de rang fini sur son centre C. Il peut fort bien exister un sous-corps H contenant C, distinct de K et de C, tel que H soit une *extension galoisienne* de C : il suffit par exemple de prendre pour K le corps des quaternions réels, pour C le sous-corps *réel* de K, et pour H une extension de rang deux de C, isomorphe au corps des nombres complexes. Dans le cas général, le théorème 3, $\gamma$ affirme que si H est une extension galoisienne de C, le sous-corps de K engendré par les $k$ tels que $\sigma_k$ laisse H invariant (dans son ensemble), n'est autre que K lui-même.

Il est naturel de se demander s'il est possible que *tous* les automorphismes intérieurs $\sigma_k$ laissent H invariant (dans son ensemble). Nous allons voir que ce cas ne peut se présenter; d'une façon précise :

THÉORÈME 4. — *Soit* K *un corps de rang fini sur son centre* C. *Si un sous-corps* H, *tel que* $C\subset H\subset K$, *est invariant par tout automorphisme intérieur de* K, *il est identique à* C *ou à* K.

Ce théorème, que je crois nouveau, peut être interprété de la façon suivante, en tenant compte du corollaire du théorème 3 (fin du § 5). D'après ce corollaire, une condition nécessaire et suffisante pour que deux éléments $x$ et $y$ de K puissent être transformés l'un dans l'autre par un automorphisme intérieur de K, est qu'ils soient racines du même polynome *irréductible* (sur C, à coefficients dans C). Le théorème 4 exprime donc que si un polynome irréductible possède au moins une racine qui soit dans K sans être dans C, *l'ensemble des racines de ce polynome engendre, avec* C, *le corps* K *tout entier* (le mot « engendre » s'entendant au sens de la structure de *corps*; autrement dit, le plus petit sous-corps contenant C et les racines du polynome n'est autre que K). D'ailleurs, ce résultat vaut pour un polynome *quelconque* (non nécessairement irréductible) à coefficients dans C : il suffit de le décomposer en facteurs irréductibles.

Nous allons démontrer le théorème 4 en supposant $K\neq C$ (si $K=C$ il est trivial), c'est-à-dire K non commutatif. En particulier, nous pourrons supposer

([13]) *Voir* un volume de BOURBAKI à paraître prochainement : *Algèbre*, Chapitre III (Algèbre multilinéaire); *voir* en particulier § 3, n° 3.

que K *a une infinité d'éléments*, puisqu'on sait que tout corps fini est commutatif.

Puisque H est supposé invariant par tout automorphisme intérieur, c'est-à-dire par tout automorphisme du groupe de Galois $G_C^K$, le théorème 3, $\delta$ prouve que H est une extension *galoisienne* de C, et que le groupe de Galois $G_C^H$ est isomorphe au quotient $G_C^K/G_H^K$. Or $G_C^K$ se compose des $\sigma_k$ tels que $k \in K^*$, et $G_H^K$ des $\sigma_k$ tels que $k \in H'^*$ (On désigne toujours par H' le sous-corps des éléments de K qui permutent avec tout élément de H). Le groupe $G_C^H$ contient le sous-groupe $\mathcal{G}$ des automorphismes intérieurs *du corps* H, c'est-à-dire des automorphismes induits sur L par les $\sigma_k$ tels que $k$ ait la forme $xy$, avec $x \in H'^*$ et $y \in H^*$; de plus, le groupe quotient $G_C^H/\mathcal{G}$ est *fini* (théor. 1). Cela signifie que si l'on désigne par A le sous-groupe de $K^*$ formé des éléments $xy$ (tels que $x \in H'^*$ et $y \in H^*$), le groupe quotient $K^*/A$ est *fini*.

Considérons le sous-corps [H, H'] engendré par H et H'; il contient A, et par suite l'ensemble des éléments $\neq 0$ de ce sous-corps est un *sous-groupe d'indice fini de* $K^*$. Or K est espace vectoriel (à gauche) sur [H, H']; je dis que le *rang* de K sur [H, H'] ne peut pas être strictement plus grand que *un*. En effet, soit $(k_1, \ldots, k_r)$ une *base* de K sur [H, H']; on obtient un représentant de chaque classe de $K^*$ suivant $[H, H']^*$ en prenant les combinaisons $\sum_{i=1}^{r} \alpha_i k_i$ telles que le premier $\alpha_i$ non nul soit égal à 1, les suivants étant des éléments arbitraires de [H, H']. Puisque le nombre de ces représentants est *fini*, le rang $r$ ne peut être $\geq 2$ que si le corps [H, H'] des coefficients est fini. Or ceci est impossible, sinon K, qui est de rang fini sur ce corps, serait lui-même fini, contrairement à l'hypothèse.

Ainsi le rang de K sur [H, H'] est égal à un; autrement dit, [H, H'] est identique à K. Le corps $H \cap H'$, formé des éléments qui permutent avec H' et H respectivement, est donc réduit au centre C. Cela signifie que C *est le centre de* H. Il s'ensuit que tous les automorphismes du groupe $G_C^H$ sont des automorphismes intérieurs *du corps* H. Comme tout automorphisme intérieur de K induit, sur H, un automorphisme du groupe $G_C^H$, on voit que tout $k \in K^*$ a la forme $xy$, où $x \in H'^*$ et $y \in H^*$.

Or soit $(k_i)$ une base de H sur C, et $(h_j)$ une base de H' sur C. Les produits $k_i h_j$ engendrent $[H, H'] = K$, comme espace vectoriel sur C; et comme leur nombre est égal au *rang* de K sur C (§ 9), ils forment une *base* de K sur C. Ceci va nous permettre de montrer que H *ou* H' *est identique à* C, ce qui démontrera évidemment le théorème. En effet, dans le cas contraire, les $k_i$ seraient en nombre au moins égal à deux, ainsi que les $h_j$; considérons l'élément $k_1 h_1 + k_2 h_2$ de $K^*$ : il doit avoir la forme $xy = yx$, où $x \in H'^*$ et $y \in H^*$. Or ceci est impossible, car si $y = \sum_i c_i k_i$ et $x = \sum_j c'_j h_j$ (les $c_i$ et les $c'_j$ étant dans C),

l'identification de $yx$ à $k_1 h_1 + k_2 h_2$ conduit notamment aux relations

$$c_1 c'_1 = c_2 c'_2 = 1, \qquad c_1 c'_2 = c_2 c'_1 = 0,$$

qui sont évidemment contradictoires.

La démonstration du théorème 4 est ainsi terminée.

Le théorème 4 et le théorème 3, $\gamma$ (§ 5) prouvent : si un sous-groupe *distingué* de $K^*$ contient $C^*$ et est $\neq C^*$, le *sous-corps* qu'il engendre n'est autre que K. Il est naturel de se demander si un tel sous-groupe n'est pas nécessairement *identique* à $K^*$; autrement dit, on est conduit au problème, que je n'ai pas su résoudre : si un corps K est de rang fini sur son centre C, peut-on affirmer que le groupe quotient $K^*/C^*$ est *simple*, ou, ce qui revient au même, que le groupe $\Gamma$ des automorphismes intérieurs de K est *simple* ?

*Note rajoutée lors de la correction des épreuves* (novembre 1947). — Depuis que cet article a été écrit (décembre 1946-janvier 1947), j'ai eu connaissance d'un article de Jacobson (*Amer. Journal of Math.*, t. 69, janvier 1947, p. 27-36) où se trouvent démontrés des théorèmes équivalents à mes théorèmes 1 et 2.