

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

MICHEL LAZARD

Théorie de Galois : extensions séparables normales des corps commutatifs

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 3, p. 1-11

http://www.numdam.org/item?id=SD_1947-1948__1__A3_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1947-1948, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » 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/>

-:-:-

Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1947/48

Exposé n° 3

-:-:-

THÉORIE DE GALOIS :
EXTENSIONS SÉPARABLES NORMALES DES CORPS COMMUTATIFS

par Michel LAZARD

1. Vocabulaire et notations.

Il ne s'agira que de corps commutatifs L , H , K , ...

$L|K$ est une extension de K (ou un corps relativement à K) si L contient K ($L \supset K$), ou, plus exactement si L contient un sous-corps K' isomorphe à K . L'extension est engendrée par une famille d'éléments α_i si :

$$(\alpha_i \in L'|K, \text{ pour tout } i) \longrightarrow L' \supset L.$$

$(L : K)$ degré de l'extension = dimension (finie ou infinie) de $L|K$, considéré comme espace vectoriel sur K .

Si $L \supset H \supset K$:

$$(L : K) \text{ fini} \iff ((L : H) \text{ et } (H : K) \text{ finis})$$

$$(L : K) = (L : H) \times (H : K).$$

α élément de $L|K$ est algébrique sur K , s'il est zéro d'un polynôme $f(x)$, à coefficients dans K .

$f(x)$ peut être supposé irréductible et normé (commençant par x^n). Il est alors unique, et peut être appelé le polynôme fondamental de α .

L'extension $L|K$ est algébrique si tous ses éléments sont algébriques. Si $(L : K)$ est fini, l'extension est algébrique.

2. Extension algébrique simple.

On désigne par $K(x)$ le domaine d'intégrité formé par les polynômes en x , à coefficients dans K . Tout idéal de $K(x)$ est principal : c'est l'ensemble des multiples d'un polynôme normé, appelé base (de cet idéal).

$L|K$, désigné par $K(\alpha)$, est une extension simple (algébrique) si elle est

engendrée par un seul élément α , algébrique sur K , de polynôme fondamental $f(x)$.

$L|K$ est isomorphe au corps-quotient $K(x)|f(x)$ du domaine d'intégrité $K(x)$ par l'idéal de base $f(x)$; c'est-à-dire à l'ensemble des polynômes en x , à coefficients dans K , définis, mod $f(x)$;

$$[h(x) \equiv h'(x) \pmod{f(x)}] \iff h(x) - h'(x) = f(x) \cdot Q(x)$$

L'irréductibilité de $f(x)$ entraîne l'existence des inverses.

Un polynôme $f(x)$, irréductible et normé dans K , définit une extension, isomorphe à l'extension simple $K(\alpha)$, engendré par un zéro α , quelconque de $f(x)$; elle est appelée le corps de rupture, ou de dislocation de $f(x)$ (qui admet un zéro dans ce corps). Ce corps reste isomorphe à lui-même quand on remplace K par un corps K' isomorphe, et $f(x)$ par son image, ou son homologue, $f'(x)$ dans K' .

3. Extension normale.

On démontre que : pour qu'une extension $L|K$ soit finie ($(L : K)$ fini), il faut et il suffit qu'elle soit engendrée par une famille finie d'éléments : $L|K = K(\alpha_1, \dots, \alpha_n)$.

Une famille quelconque d'éléments, algébriques sur K , engendre une extension algébrique sur K . La puissance d'une extension algébrique sur K est au plus égale :

- 1° au dénombrable, si K est fini ;
- 2° à la puissance de K , si K est infini.

Le corps de décomposition sur K , d'une famille (finie ou infinie) de polynômes $f_i(x)$ est l'extension $L_0|K$ (définie à un isomorphisme près) :

- 1° engendrée par des zéros des polynômes $f_i(x)$;
- 2° dans laquelle tout polynôme $f_i(x)$ est décomposable en facteurs linéaires.

On démontre l'existence de ce corps par l'application du théorème de Zorn à la famille $\mathcal{L}$ des extensions $L|K$, $L'|K$, ..., engendrées par des zéros des polynômes $f_i(x)$, ordonnée par inclusion :

$$L|K \leq L'|K \iff L' \supset L.$$

Toute sous famille de $\mathcal{L}$, totalement ordonnée, à une borne supérieure qui est

sa réunion, et $\mathcal{L}$ a un élément maximal $L_0|K$.

Dans cette extension $L_0|K$, tout $f_i(x)$ se décompose en facteurs linéaires. En outre elle est unique, à un isomorphisme près.

La démonstration se simplifie si la famille des polynômes $f_i(x)$ est un système fini.

Pour une famille de polynômes $f_i(x)$ (qu'on peut supposer irréductibles et normés) dans K , il existe un corps de décomposition $L_0|K$, défini à un isomorphisme près. Il est manifestement corps de décomposition dans toute sous-extension $H|K$ ($L_0 \supset H \supset K$).

Sa définition peut être exprimée, avec un abus de langage, en disant qu'elle est engendrée par "tous" les zéros des polynômes $f_i(x)$.

Un corps de décomposition est encore appelé une extension normale (du corps K). Une extension normale $L_0|K$, considérée, indépendamment de sa construction, peut être caractérisée par l'une des propriétés suivantes (faciles à justifier) :

1° Tout isomorphisme de $L_0|K$, dans une sur-extension $M|K$, ($M \supset L_0 \supset K$), qui laisse invariants les éléments de K , est un automorphisme.

2° Tout polynôme irréductible sur K , qui possède un zéro dans L_0 est décomposable, dans $L_0|K$, en facteurs linéaires.

On appelle conjugués par rapport au corps K :

- des éléments d'une extension algébrique $L|K$, qui sont zéros d'un même polynôme irréductible sur K ;

- des extensions qui se déduisent les unes des autres par des isomorphismes, (dans une sur-extension commune) qui laissent invariants les éléments de K .

Avec cette notation, les propriétés caractéristiques précédentes d'une extension normale $L_0|K$ deviennent les suivantes :

1° elle coïncide globalement avec tous ses conjugués :

2° elle contient tous les conjugués de ses éléments par rapport à K (dans une sur-extension quelconque).

Cas particuliers - Une extension normale de degré fini est corps de décomposition d'un polynôme $P(x)$ sur K .

Il suffit de considérer une famille finie d'éléments engendrant l'extension et de faire le produit $P(x)$ de leurs polynômes fondamentaux.

Si la famille des $f_i(x)$ est l'ensemble de tous les polynômes sur K , l'extension $L_0|K$ est algébriquement fermée : les seuls polynômes irréductibles y sont les binômes du premier degré (tout polynôme y est décomposable en facteurs linéaires).

4. Isomorphismes des extensions finies séparables.

Pour étudier une extension algébrique $L|K$, nous formerons la famille des polynômes $f_i(x)$, irréductibles dans K , et ayant un zéro dans L , puis le corps de décomposition $L_0|K$ de cette famille. Nous appellerons isomorphismes de $L|K$, les isomorphismes dans $L_0|K$, qui laissent invariants les éléments de K .

$L_0|K$ est la plus petite sur-extension normale de $L|K$: elle est contenue dans toute autre $M|K$ et les isomorphismes de $L|K$ (dans $L_0|K$) sont des isomorphismes dans $M|K$.

Pour une extension simple $L|K = K(\alpha)$, tout isomorphisme applique α sur un zéro $\alpha^{(i)}$ de son polynôme fondamental (égal à α , si l'automorphisme est identique).

Le nombre d'isomorphismes distincts de $L|K$ est donc égal au nombre de zéros distincts du polynôme fondamental $f(x)$ de α . Si ce nombre est égal au degré de $f(x)$ et par suite au degré de l'extension, on dit que α (ou l'extension $K(\alpha)$) est séparable sur K .

Si α n'est pas séparable, ou est inséparable, le polynôme $f(x)$, irréductible dans K , possède, dans $L_0|K$ des zéros multiples. La dérivée $f'(x)$, annulée par ces zéros ne peut qu'être identiquement nulle.

Ceci ne se produit que si la caractéristique du corps K est un nombre premier p , non nul et si $f(x)$ est fonction de x^p seul :

$$f(x) = g(x^p) \longrightarrow f'(x) = pg'(x^p) \cdot x^{p-1} = 0.$$

Un corps est parfait si toutes ses extensions simples sont séparables ; il en est ainsi pour :

- les corps de caractéristique nulle ;
- les corps de caractéristique p , qui contiennent la racine p -ième de chacun de leurs éléments.

Un champ de Galois est notamment un corps parfait.

Une extension $L|K$ est séparable si tous ses éléments sont séparables. Si elle

est finie, il suffit pour cela que ses éléments générateurs soient séparables.

On démontre (parfois sous le nom de théorème de Galois) qu'une extension de degré fini, séparable, est isomorphe à une extension simple.

On construit pour cela, au moyen des éléments générateurs α_i , en nombre fini, un élément :

$$\omega = \sum u_i \cdot \alpha_i \quad (u_i \text{ dans } K),$$

appelé "résolvante de Galois", tel que tous ses "conjugués" soient distincts. L'extension est isomorphe à $K(\omega)$.

L'étude des automorphismes d'une extension finie séparable est ainsi ramenée à celle d'une extension simple.

5. Extension galoisienne.

Nous considérerons, dans ce qui suit, des extensions $L|K$, normales, de K (en supprimant l'indice 0).

Les isomorphismes d'une telle extension (laissant invariants les éléments de K) sont des automorphismes ; ils constituent un groupe, qui est appelé le groupe de Galois de $L|K$ et que nous noterons $G_{L|K}$.

1° A chaque corps P , sur-corps de K et sous-corps de L :

$$K \subset P \subset L,$$

nous associons l'ensemble des automorphismes ψ' (de $L|K$, éléments de $G_{L|K}$) qui laissent invariant tout élément α de P . C'est manifestement le groupe de Galois $G_{L|P}$ de l'extension $L|P$; il est contenu dans $G_{L|K}$:

$$1 \subset G_{L|P} \subset G_{L|K} ;$$

sa définition peut être exprimée par l'équivalence :

$$\psi' \in G_{L|P} \iff (\alpha \in P \longrightarrow \alpha \cdot \psi' = \alpha) .$$

2° A chaque sous-groupe Δ du groupe de Galois $G_{L|K}$:

$$1 \subset \Delta \subset G_{L|K}$$

nous associons l'ensemble des éléments α' de L laissés invariants par tout automorphisme ψ , élément de Δ . C'est manifestement un corps, sur-corps de K et sous-corps de L , nous l'appellerons corps des invariants de Δ , et nous le désignerons par $k(\Delta)$:

$$K \subset k(\Delta) \subset L ;$$

sa définition peut être exprimée par l'équivalence :

$$\alpha' \in k(\Delta) \iff (\varphi \in \Delta \longrightarrow \alpha' \cdot \varphi = \alpha') .$$

Les cas limites triviaux sont :

$$1 : \text{ pour } P = L, \quad G_{L|L} = 1 \quad (\text{pour } P = K, \quad G_{L|K})$$

$$2 : \text{ pour } \Delta = 1, \quad k(1) = L \quad (\text{pour } \Delta = G_{L|K}, \quad k(L|K) = K) .$$

Cette association conserve les inclusions en les renversant :

$$P \subset P' \longrightarrow G_{L|P} \supset G_{L|P'} ; \quad \Delta \subset \Delta' \longrightarrow k(\Delta) \supset k(\Delta') .$$

On peut itérer ces associations et construire, à partir d'un sous-corps P , ou d'un sous-groupe Δ un :

sous-corps $\bar{P} =$ corps des invariants du groupe de Galois de $L|P$;

sous-groupe $\bar{\Delta} =$ groupe de Galois de l'extension $L|k(\Delta)$.

Il résulte immédiatement des définitions, les inclusions :

$$P \subset k(G_{L|P}) = \bar{P}, \quad \Delta \subset G_{L|k(\Delta)} = \bar{\Delta} .$$

Il suffit d'associer l'implication gauche.droite de la 1re équivalence, (après permutation des antécédentes), avec l'implication droite.gauche de la 2e équivalence ;

$$\alpha \in P \longrightarrow (\varphi' \in G_{L|P} \longrightarrow \alpha \cdot \varphi' = \alpha) \longrightarrow \alpha \in k(G_{L|P})$$

et, corrélativement :

$$\varphi \in \Delta \longrightarrow (\alpha' \in k(\Delta) \longrightarrow \alpha' \cdot \varphi = \alpha') \longrightarrow \varphi \in G_{L|P}$$

En rapprochant les inclusions, on constate l'égalité des itérées (entre elles)

$$G_{L|P} = G_{L|\bar{P}} \quad \text{et} \quad \bar{\bar{P}} = \bar{P}, \quad k(\Delta) = k(\bar{\Delta}) \quad \text{et} \quad \bar{\bar{\Delta}} = \bar{\Delta} .$$

Ceci résulte des inclusions inverses :

$$P \subset \bar{P} \longrightarrow G_{L|\bar{P}} \subset G_{L|P} ; \quad G_{L|P} \subset \overline{G_{L|P}} = G_{L|k(G_{L|P})} = G_{L|\bar{P}}$$

$$\Delta \subset \bar{\Delta} \longrightarrow k(\bar{\Delta}) \subset k(\Delta) ; \quad k(\Delta) \subset \overline{k(\Delta)} = k(G_{L|k(\Delta)}) = k(\bar{\Delta})$$

Une extension (normale) $L|K$ est galoisienne, lorsque les inclusions inverses

sont aussi vraies (pour tout P et tout Δ , ce qui entraîne leur égalité avec les itérés) :

$$P = k(G_{L|P}) = \bar{P}, \quad \Delta = G_{L|k(\Delta)} = \bar{\Delta}.$$

Dans une extension galoisienne :

1° tout sous corps P (de L) est corps des invariants d'un sous-groupe qui est le groupe de Galois de la sous-extension $L|P$;

2° tout sous groupe Δ (de $G_{L|K}$) est groupe de Galois d'une sous-extension qui est celle de L , relativement au corps $k(\Delta)$ des invariants de Δ .

Les deux associations sont biunivoques et équivalentes.

Une extension normale, séparable et finie est galoisienne.

Nous examinerons successivement les extensions séparables qui ne vérifient que la propriété 1, puis la condition supplémentaire de degré fini, qui entraîne la propriété 2.

6. Extension séparable.

Si l'extension (normale) $L|K$ est séparable, la propriété 1 est vraie : la correspondance $P \longleftrightarrow G_{L|P}$ est biunivoque, mais elle n'a lieu, a priori, qu'entre les sous-corps P de L et certains sous-groupes de $G_{L|K}$, que nous appellerons sous-groupes fermés.

En partant d'un sous-corps P de L , formons le groupe $G_{L|P}$ des automorphismes qui laissent tout élément de P invariant. Pour montrer que réciproquement tout élément invariant pour les automorphismes de ce groupe est dans P , on raisonne par l'absurde (ou par contraposition).

Si un élément β n'est pas dans P , comme il est séparable, tous ses conjugués dans $L|P$ sont distincts : donc il existe au moins un élément de $G_{L|P}$ qui, le transformant en l'un de ses conjugués, ne le laisse pas invariant.

Nous reviendrons ci-dessous sur l'étude de la correspondance des sous-corps et des sous-groupes fermés.

7. Extension séparable finie.

Si l'extension normale séparable $L|K$ est en outre finie (ou de degré fini), la propriété 2 est aussi vraie : tout sous-groupe de $G_{L|K}$ est fermé. L'association a lieu entre sous-groupe et sous-corps.

L'extension (normale) $L|K$ étant séparable et finie, de degré n est simple, c'est-à-dire engendré par un seul élément α , zéro d'une équation de degré n , dans K , irréductible.

Appelons r l'ordre du groupe Δ , il est diviseur de n qui est égal à l'ordre de $G_{L|K}$.

α est, dans $L|k(\Delta)$, zéro d'un polynôme (normé), $g_1(x)$, irréductible, de degré r' , égal à $(L : k(\Delta))$ et à l'ordre de $\bar{\Delta}$, de sorte que $r \leq r'$.

Formons le polynôme :

$$g(x) = \prod (x - \alpha.\varphi), \quad \varphi \in \Delta;$$

il est de degré r et reste invariant pour tout automorphisme φ de Δ (qui permute seulement ses zéros). Ses coefficients sont donc dans $k(\Delta)$ et il est divisible par $g_1(x)$, polynôme irréductible, avec qui il a un zéro commun. Il en résulte que r' ne peut être supérieur à r et que cette divisibilité est une égalité. Le groupe Δ , inclus dans $\bar{\Delta}$ et de même ordre, lui est égal.

De cette démonstration on déduit encore les égalités :

$$r = \text{ordre de } \Delta = (L : k(\Delta));$$

$$n : r = \text{index de } \Delta \text{ (dans } G_{L|K}) = (k(\Delta) : K).$$

8. Sous-extensions normales.

Nous étudions, dans une extension normale séparable $L|K$, (non nécessairement finie), les sous-corps P (ou sous-extensions $P|K$) et les sous-groupes fermés associés $\bar{\Delta} = G_{L|P}$. Les P et les $\bar{\Delta}$ forment deux treillis entre lesquels existe une correspondance biunivoque, qui conserve l'inclusion, en la renversant.

En particulier : l'intersection de deux sous-groupes fermés est un sous-groupe fermé qui correspond à la sous-extension engendrée par les sous-extensions primitives (réunion complétée).

Les isomorphes, ou conjuguées, d'une sous-extension $P|K$, dans $L|K$, correspondent biunivoquement aux classes (d'un côté convenable) de $G_{L|K}$, relativement au sous-groupe fermé $G_{L|P}$.

Ceci résulte des égalités évidentes :

$$\left. \begin{array}{l} \varphi \in G_{L|K} \\ \psi \in G_{L|P} \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} P.\psi = P \\ P.(\psi \times \varphi) = P.\varphi \end{array} \right. \quad \text{ou : } P.(G_{L|P} \times \varphi) = P.\varphi .$$

(Les classes sont à droite parce qu'on a noté le produit des isomorphismes ; l'ordre de l'écriture étant celui de la succession.

Les groupes fermés correspondant à deux sous-extensions conjuguées sont transmués par l'isomorphisme de conjugaison :

$$G_{L|P}.\psi = \psi^{-1} \times G_{L|P} \times \psi$$

Car :

$$P.\varphi = P \iff (P.\psi).(\psi^{-1} \times \varphi \times \psi) = P.\psi .$$

De ces propriétés on déduit celles des sous-extensions normales (égales à toutes leurs conjuguées).

Pour qu'une sous-extension soit normale, il faut et il suffit que le sous-groupe fermé, associé, soit invariant, ou distingué (égal à tous ses transmués).

Le groupe de Galois de $P|K$ (pour une sous-extension normale) est homomorphe au groupe de Galois de l'extension normale $L|K$; son élément neutre étant l'image des éléments de $G_{L|P}$; de sorte qu'il est isomorphe au groupe quotient : $G_{L|K}|G_{L|P}$.

Les automorphismes de $G_{L|K}$ conservent P dans son ensemble donc sont des automorphismes (non nécessairement différents) de $P|K$. Le groupe $G_{P|K}$ est donc homomorphe à $G_{L|K}$ (le produit étant conservé). Les éléments de $G_{L|K}$ à qui correspond l'élément neutre de $G_{P|K}$ sont ceux qui laissent invariant tout élément de P , donc ceux de $G_{L|P}$.

Si $L|P$ est de degré fini, ce degré est égal à l'ordre du groupe quotient $G_{L|K}|G_{L|P}$ isomorphe à $G_{P|K}$.

9. Caractéristique des groupes fermés.

Pour que, dans une extension normale séparable, non nécessairement finie, $L|K$, un sous-groupe Δ du groupe de Galois $G_{L|K}$, soit fermé, il faut et il suffit que, pour tout isomorphisme ψ , non contenu dans Δ , on puisse former une extension normale, de degré fini $F|K$ ($K \subset F \subset L$), telle que la classe

du groupe quotient $G_{L|K}|G_{L|F}$ qui contient ψ ne contienne aucun élément de Δ :

$\psi \notin \Delta \longrightarrow \text{ext } F, F|K \text{ normale et finie et } [G_{L|F} \times \psi, \Delta] \text{ vide.}$

Condition nécessaire. - Si Δ est fermé, il est égal à $G_{L|k(\Delta)}$. Si ψ n'est pas dans Δ , il existe α

$$\alpha \in k(\Delta) \text{ et } \alpha.\psi \neq \alpha.$$

Formons alors la plus petite sur-extension normale $F|K$, contenant α (et $k(\Delta)$) et son groupe associé $G_{L|F}$:

$$\varphi \in G_{L|F} \longrightarrow \alpha.\varphi = \alpha \longrightarrow \alpha.(\varphi \times \psi) \neq \alpha \longrightarrow \varphi \times \psi \notin \Delta.$$

Ceci montre notamment que la condition est vérifiée pour tout sous-groupe dans une extension normale (séparable) finie.

Condition suffisante. - Je raisonne par l'absurde en supposant $\Delta \neq \bar{\Delta}$; il existe au moins un automorphisme ψ , contenu dans $\bar{\Delta}$ et non dans Δ .

Je prends une sous-extension normale quelconque, de degré fini $F|K$ ($L \supset F \supset K$) et le groupe quotient de degré fini

$$G_{L|K}|G_{L|F} \text{ isomorphe à } G_{F|K}$$

J'y considère la classe $\psi' = G_{L|F} \times \psi$, qui contient ψ et le sous-groupe Δ' formé par les classes qui contiennent un élément de Δ (au moins). Le corps d'invariants de ce sous-groupe est l'intersection $[F, k(\Delta)]$ (contenu dans $F|K$) puisque tout élément doit en être invariant, à la fois pour $G_{L|F}$ et pour Δ .

Mais $\psi \in \bar{\Delta}$ laisse invariant tout élément de $k(\Delta)$, la classe ψ' laisse donc invariante cette intersection. Comme il s'agit d'une extension normale, séparable et finie, le sous-groupe Δ' (du groupe quotient) est fermé et ψ' lui appartient (propriété 2).

Donc la classe $\psi' = G_{L|F} \times \psi$ a au moins un élément commun avec Δ , ce qui est contraire à l'hypothèse.

Cette condition peut être interprétée par une condition topologique dans une certaine famille des sous-groupes. Elle permet alors de démontrer que si l'extension n'est pas finie, il y a des sous-groupes non fermés et l'extension n'est pas galoisienne.

Notes. - La dernière démonstration, basée sur des considérations de topologie

est de KRULL [1] .

M. LAZARD a démontré en même temps que le produit de deux sous-groupes fermés permutables est un sous-groupe fermé, ce qui lui a permis d'établir une propriété (évidente dans le cas d'une extension finie) appelée théorème des irrationalités naturelles :

pour étudier les groupes de Galois des corps de décomposition d'une famille de polynômes $f_i(x)$, sur une extension $H|K$ de K , il suffit de considérer les sous-extensions $H'|K$, du corps de décomposition $L_0|K$ des polynômes $f_i(x)$ sur K .

Les notations ont été préconisées par M. KRASNER ; il n'est peut-être pas inutile de les résumer :

Une extension, notée $L|K$, est un corps L , considéré relativement à un corps (de base) K , donc sous-corps de L .

Une sous-extension $P|K$, d'une extension $L|K$, est définie par un sous-corps P de L , considéré relativement au même corps (de base) K .

Une extension $L|K$ est encore extension relativement à une sous-extension $P|K$, ou plus simplement au corps P , elle est notée $L|P$ (abréviation de $L|K|P|K$).

Le groupe de Galois d'une extension $L|K$, noté $G_{L|K}$, n'a été défini que pour une extension normale ; il est associé à K , dont il laisse les éléments invariants.

Une extension normale $L|K$ reste normale relativement à une sous-extension $P|K$: l'extension $L|P$ est normale, et elle a un groupe de Galois, qui est associé à P (ou $P|K$) dont il laisse les éléments invariants ; il est noté $G_{L|P}$ (il est sous-groupe de $G_{L|K}$).

Si $P|K$ est elle-même normale, elle a un groupe de Galois qui est noté $G_{P|K}$; il est isomorphe au groupe quotient $G_{L|K}/G_{L|P}$ ($G_{L|P}$ étant sous-groupe invariant).

BIBLIOGRAPHIE

- [1] KRULL (Wolfgang). - Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Annalen, t. 100, 1928, p. 687-698.