Séminaire Henri Cartan

J. Lafon

Anneaux de fractions. Éléments entiers. Théorèmes de Krull

Séminaire Henri Cartan, tome 8 (1955-1956), exp. n° 1, p. 1-12

<http://www.numdam.org/item?id=SHC_1955-1956__8__A1_0>

Séminaire E.N.S., 1955-56
(H. CARTAN et C. CHEVALLEY)

ANNEAUX DE FRACTIONS.
ÉLÉMENTS ENTIERS. THÉORÈMES DE KRULL.

(Exposé de J. LAFON, 7.11.1955)

Conventions et notations. - Dans cet exposé et les suivants, on fera les conventions suivantes (sauf mention expresse du contraire) : on appelle anneau un anneau commutatif à élément unité $1 \neq 0$; on appelle sous-anneau d'un anneau A un anneau B contenu dans A et ayant même élément unité que A ; on appelle homomorphisme d'anneaux un homomorphisme $f : A \to B$ qui respecte l'addition et la multiplication, et satisfait à $f(1) = 1$. Si A est un anneau, tous les A-modules considérés seront unitaires (c'est-à-dire $1.x = x$ pour tout x du module).

Le mot "corps" désignera un corps commutatif.

Les idéaux d'un anneau seront notés par des minuscules soulignées : $\underline{m}$, $\underline{p}$, etc.

Rappelons que si $\underline{m}$ est un idéal d'un anneau A, l'anneau $A/\underline{m}$ est un corps si et seulement si $\underline{m}$ est un idéal maximal (on appelle ainsi tout idéal distinct de A, et maximal dans l'ensemble des idéaux $\neq A$). L'anneau $A/\underline{m}$ est un anneau d'intégrité (i.e : sans autre diviseur de 0 que 0 lui-même), si et seulement si l'idéal $\underline{m}$ est premier. Tout idéal $\neq A$ est contenu dans un idéal maximal ; tout anneau d'intégrité se plonge dans un corps.

1.- Anneaux de fractions.

Soit A un sous-anneau d'un corps K, et soit S une partie non vide de A, multiplicativement stable, et ne contenant pas 0. L'ensemble AS^{-1} des éléments as^{-1} (où $a \in A$ et $s \in S$) est un sous-anneau de K. On le note A_S, et on l'appelle l'anneau des fractions de A (relativement à S). Si $S = A - \{0\}$, l'anneau A_S n'est autre que le corps des fractions de A.

Proposition 1.- (a) L'application $\underline{m}' \to \underline{m}' \cap A$ est une injection de l'ensemble des idéaux de A_S dans l'ensemble des idéaux de A ; si $\underline{m} = \underline{m}' \cap A$, on a $\underline{m}' = \underline{m}S^{-1}$ (idéal engendré par $\underline{m}$ dans A_S).

(b) L'application $\underline{p}' \to \underline{p}' \cap A$ est une bijection de l'ensemble des

idéaux premiers de A_S sur l'ensemble des idéaux premiers de A qui ne rencontrent pas S .

(c) Si $\underline{p}'$ est un idéal premier de A_S , et $\underline{p} = \underline{p}' \cap A$, l'homomorphisme canonique $\varphi : A \to A/\underline{p}$ se prolonge d'une seule manière en un homomorphisme $A_S \to (A/\underline{p})_{\varphi(S)}$, lequel induit un isomorphisme

$$A_S/\underline{p}' \approx (A/\underline{p})_{\varphi(S)} .$$

Démonstration : (a) résulte de l'égalité $\underline{m}' = (\underline{m}' \cap A)S^{-1}$, valable pour tout idéal $\underline{m}'$ de A_S .

(b) Si $\underline{p}'$ est un idéal premier de A_S , $\underline{p} = \underline{p}' \cap A$ est évidemment un idéal premier de A qui ne rencontre pas S , puisque $\underline{p}' \neq A_S$. L'assertion (b) résulte alors de l'égalité $\underline{p} = (\underline{p}S^{-1}) \cap A$, valable pour tout idéal premier $\underline{p}$ de A , tel que $\underline{p} \cap S = \emptyset$.

(c) φ se prolonge d'une seule manière en un homomorphisme d'anneaux $\bar{\varphi} : A_S \to (A/\underline{p})_{\varphi(S)}$, défini par $\bar{\varphi}(as^{-1}) = \varphi(a)(\varphi(s))^{-1}$. Il est clair que $\bar{\varphi}$ est surjectif ; le noyau de $\bar{\varphi}$ se compose des éléments as^{-1} tels que $\varphi(a) = 0$, donc ce noyau est $\underline{p}S^{-1} = \underline{p}'$.

Proposition 2.- Soit B un anneau tel que $A \subset B \subset A_S$. Si $\underline{p}'$ est un idéal premier de A_S , et $\underline{p} = \underline{p}' \cap A$, $\underline{q} = \underline{p}' \cap B$, on a

$$A_{A-\underline{p}} = B_{B-\underline{q}} .$$

Démonstration : observons d'abord que $A - \underline{p}$, $B - \underline{q}$ et $A_S - \underline{p}'$ sont multiplicativement stables. On a évidemment $A_{A-\underline{p}} \subset B_{B-\underline{q}} \subset (A_S)_{A_S-\underline{p}'}$. Montrons que $(A_S)_{A_S-\underline{p}'} \subset A_{A-\underline{p}}$; tout élément de $(A_S)_{A_S-\underline{p}'}$ s'écrit $(as^{-1})(a's'^{-1})^{-1}$, avec $a \in A$, $s \in S$, $a' \in A-\underline{p}$, $s' \in S$; il est égal à $(as')(a's)^{-1}$, avec $as' \in A$, $a's \in A-\underline{p}$.

2.- Anneau local d'un idéal premier.

Définition : on appelle anneau local un anneau A tel que la somme de deux éléments non-inversibles de A soit non-inversible. Les éléments non-inversibles de A forment alors un idéal $\underline{m}(A)$, distinct de A , et qui contient tout idéal distinct de A ; $\underline{m}(A)$ est donc l'unique idéal maximal de A .

Réciproquement, si un anneau A possède un seul idéal maximal, cet idéal contient tous les éléments non-inversibles, et A est donc un anneau local.

Proposition 3.- Soit A un sous-anneau d'un corps, et soit $\underline{p}$ un idéal premier de A. Si $S = A - \underline{p}$, l'anneau A_S est un anneau local, dont l'idéal maximal est l'idéal $\underline{p}A_S$ engendré par $\underline{p}$.

Démonstration : pour que as^{-1} $(s \notin \underline{p})$ ait un inverse de la forme $a's'^{-1}$ $(s' \notin \underline{p})$, il faut et il suffit que $a \notin \underline{p}$; les éléments non inversibles de A_S sont donc ceux de la forme as^{-1}, avec $a \in \underline{p}$.

Notation : lorsque $S = A - \underline{p}$ ($\underline{p}$ étant un idéal premier de A), on utilisera désormais la notation $A_{\underline{p}}$ pour désigner l'anneau A_S. Ainsi, $A_{\underline{p}}$ est un anneau local dont l'idéal maximal est $\underline{p}A_{\underline{p}}$.

Avec cette notation, la proposition 1, (c) entraîne :

Proposition 4.- Soient $\underline{p}$ et $\underline{q}$ deux idéaux premiers de A, tels que $\underline{q} \supset \underline{p}$. On a

$$(2) \qquad A_{\underline{q}}/\underline{p}A_{\underline{q}} \approx (A/\underline{p})_{\underline{q}/\underline{p}} .$$

(En effet, si $S = A - \underline{q}$, $\underline{p}' = \underline{p}S^{-1}$ n'est autre que $\underline{p}A_{\underline{q}}$, et $\varphi(S)$ est le complémentaire, dans l'anneau $A/\underline{p}$, de l'idéal premier $\underline{q}/\underline{p}$).

D'autre part, la proposition 2, où l'on prend $S = A - \underline{p}$, donne :

Proposition 2 bis.- Soit $\underline{p}$ un idéal premier de A, et soit B un anneau tel que $A \subset B \subset A_{\underline{p}}$. Si $\underline{q} = (\underline{p}A_{\underline{p}}) \cap B$, on a

$$A_{\underline{p}} = B_{\underline{q}} .$$

3.- Eléments entiers sur un anneau.

Soit A un anneau, et soit x un élément d'un anneau B tel que A soit sous-anneau de B. Les conditions suivantes sont équivalentes :

(E) il existe un sous-anneau B' de B, contenant A et x, qui est un A-module de type fini ;

(E') x est zéro d'un polynome unitaire à coefficients dans A ;

(E") le sous-anneau $A[x]$ engendré par A et x est un A-module de type fini.

Démonstration : supposons (E) satisfaite, et soit (y_i) un système fini

d'éléments, contenant 1, et engendrant B' comme A-module. On a $xy_i = \sum_j a_{ij}y_j$, avec $a_{ij} \in A$; d'où, en notant I la matrice-unité de degré n égal au nombre des y_i :

$$y_i \cdot \det(xI - (a_{ij})) = 0 \quad \text{pour tout } i ,$$

et comme l'un des y_i est 1 , on trouve $\det(xI - (a_{ij})) = 0$. Donc (E') est satisfaite.

Si (E') est satisfaite, on a $x^n + a_1x^{n-1} + \ldots + a_n = 0$, $a_i \in A$ $(1 \leqslant i \leqslant n)$. Alors l'anneau $A[x]$ est le A-module engendré par $1 , x , \ldots , x^{n-1}$; il est de type fini.

Enfin, (E") entraîne trivialement (E) , ce qui achève la démonstration.

Définition : un élément $x \in B$ est dit entier sur le sous-anneau A de B , s'il satisfait aux conditions équivalentes (E) , (E') , (E") . On dit qu'un anneau B est entier sur un sous-anneau A , si tout $x \in B$ est entier sur A .

Si des $x_i \in B$ $(0 \leqslant i \leqslant n)$ sont entiers sur A , le sous-anneau $A[x_1 , \ldots , x_n]$ qu'ils engendrent avec A est un A-module de type fini (récurrence sur n), donc est entier sur A ; en particulier, la somme et le produit de deux éléments entiers sur A sont des éléments entiers sur A . L'ensemble des éléments de B entiers sur A est donc un sous-anneau de B (contenant A), et appelé l'anneau dérivé de A dans B .

Transitivité : soient des anneaux $A \subset B \subset C$; si B est entier sur A , et C entier sur B , alors C est entier sur A . En effet : soit $x \in C$; x annule un polynome unitaire dont les coefficients appartiennent à B ; ces coefficients engendrent avec A un sous-anneau B' qui est un A-module de type fini ; alors $B'[x]$ est un A-module de type fini, et par suite x est entier sur A .

Soient des anneaux $A \subset B$; soit A' l'anneau dérivé de A dans B . Tout élément de B , entier sur A' , est entier sur A (d'après ce qui précède), donc appartient à A' ; ainsi l'anneau dérivé de A' dans B est A' lui-même. On dit qu'un sous-anneau A de B est intégralement fermé dans B s'il est identique à l'anneau dérivé de A dans B ; on voit que, dans tous les cas, l'anneau dérivé A' de A dans B est intégralement fermé dans B ; c'est le plus petit anneau intégralement fermé (dans B) et contenant A .

Pour cette raison, A' s'appelle aussi la fermeture intégrale de A dans B.

Un anneau d'intégrité A est dit intégralement clos s'il est intégralement fermé dans son corps des fractions. On appelle anneau normal tout anneau d'intégrité intégralement clos.

Soit φ un homomorphisme d'anneaux $B \longrightarrow B'$; si B est entier sur un sous-anneau A, il est clair que l'anneau $\varphi(B)$ est entier sur $\varphi(A)$.

Proposition 5.- Soit A un sous-anneau d'un corps K, et soit S une partie non vide de A, multiplicativement stable et ne contenant pas 0. Si A' désigne la fermeture intégrale de A dans K, $(A')_S$ est la fermeture intégrale de A_S dans K.

En effet, pour qu'un $x \in K$ soit racine d'un polynome unitaire à coefficients dans A_S, il faut et il suffit qu'il existe un $s \in S$ tel que sx soit racine d'un polynome unitaire à coefficients dans A.

4.- Entiers et anneaux de valuation.

Dans ce qui suit, nous noterons $\underline{r}(A)$ le radical d'un anneau A (voir l'Appendice). Si A est un anneau local, $\underline{r}(A)$ n'est autre que l'unique idéal maximal de A.

Proposition 6.- Soient x un élément et A un sous-anneau d'un anneau B ; soit $A[x]$ le sous-anneau de B engendré par x et A. Si l'idéal de $A[x]$ engendré par $\underline{r}(A)$ contient 1, alors x possède un inverse x^{-1} dans $A[x]$, et x^{-1} est entier sur A.

On a en effet $1 = a + bx$, où $a \in \underline{r}(A)$ et $b \in A[x]$; or $1-a$ possède un inverse $a' \in A$, d'où $1 = (a'b)x$; ceci prouve l'existence de $x^{-1} = a'b$. On a $x^{-1} = \sum_{0 \leq i < n} a_i x^i$, d'où $x^{-n} = \sum_{0 \leq i < n} a_i x^{-(n-1-i)}$, et par suite x^{-1} est entier sur A.

Proposition 7.- Soit B un anneau, entier sur un sous-anneau A. Alors $\underline{r}(A) \subset \underline{r}(B)$.

Démonstration : on doit montrer que si on a des $a_i \in \underline{r}(A)$ et $b_i \in B$, en nombre fini, alors $1 + \sum_i a_i b_i$ est inversible dans B ; il suffit de montrer que cet élément est inversible dans le sous-anneau B' engendré par A et les b_i, et B' est un A-module de type fini. On est donc ramené au cas où B est un A-module de type fini, ce qu'on suppose désormais. Soit

$\mathfrak{m}$ l'idéal de B engendré par $\mathfrak{r}(A)$; d'après la caractérisation du radical $\mathfrak{r}(B)$ (condition (ii) de l'Appendice), il suffit de prouver que, pour un B-module de type fini M , la relation $\mathfrak{m}M = M$ entraîne $M = 0$. Or $\mathfrak{m}M$ n'est autre que $\mathfrak{r}(A)M$, M étant cette fois considéré comme A-module ; M est un A-module de type fini, et puisque $\mathfrak{r}(A)M = M$, on a bien $M = 0$. Ceci achève la démonstration.

Corollaire : si $x \in B$ est entier sur A , l'idéal engendré par $\mathfrak{r}(A)$ dans l'anneau $A[x]$ ne contient pas 1 .

Relation de domination : soient A et B des anneaux locaux, A étant un sous-anneau de B ; les idéaux maximaux $\mathfrak{m}(A)$ et $\mathfrak{m}(B)$ satisfont évidemment à $\mathfrak{m}(B) \cap A \subset \mathfrak{m}(A)$. On dit que B domine A si l'une des conditions suivantes (évidemment équivalentes) est remplie :

(D) $\mathfrak{m}(B) \cap A = \mathfrak{m}(A)$;

(D') $\mathfrak{m}(A) \subset \mathfrak{m}(B)$;

(D") 1 n'appartient pas à l'idéal de B engendré par $\mathfrak{m}(A)$.

On notera que la condition (D") est vérifiée si B est entier sur A (cf. proposition 7).

Soit K un corps. L'ensemble des sous-anneaux locaux de K , ordonné par la relation de domination, est inductif : si $(A_i)_{i \in I}$ est une famille de sous-anneaux locaux de K , totalement ordonnée pour la relation de domination, alors la réunion A des A_i est un anneau local qui domine les A_i et dont l'idéal maximal $\mathfrak{m}(A)$ est la réunion des $\mathfrak{m}(A_i)$. La démonstration est laissée au lecteur.

D'après le théorème de Zorn : si A est un sous-anneau local d'un corps K , il existe un sous-anneau local B de K qui domine A et est maximal pour la relation de domination (dans l'ensemble des sous-anneaux locaux de K).

Théorème 1.- Pour qu'un sous-anneau d'un corps K soit un anneau local, maximal pour la relation de domination, il faut et il suffit que les relations $x \in K$, $x \notin A$ entraînent $x^{-1} \in A$.

Pour établir ce théorème, nous aurons besoin d'un lemme :

Lemme 1.- Soit A un sous-anneau local du corps K . Pour que A soit maximal pour la relation de domination, il faut et il suffit que, pour tout sous-anneau B de K , contenant A et $\neq A$, 1 appartienne à l'idéal engendré par $\mathfrak{m}(A)$ dans B .

En effet, la condition est trivialement suffisante ; elle est nécessaire, sinon il existerait un idéal premier $\underline{p}$ de B tel que $\underline{m}(A) \subset \underline{p}$, et l'anneau local $B_{\underline{p}}$ dominerait A et serait distinct de A.

Démonstration du théorème 1 : la condition est nécessaire. Soit A un anneau local, maximal pour la relation de domination, et soit $x \in K$ tel que $x \notin A$; alors l'anneau $A[x]$ est distinct de A, donc (lemme 1) 1 appartient à l'idéal de $A[x]$ engendré par $\underline{m}(A)$; d'après la proposition 6, x^{-1} est entier sur A. Appliquons le corollaire de la proposition 7, en y remplaçant x par x^{-1} : on voit que l'idéal de $A[x^{-1}]$ engendré par $\underline{m}(A)$ ne contient pas 1, et ceci, en vertu du lemme 1, implique $A[x^{-1}] = A$, c'est-à-dire $x^{-1} \in A$.

La condition est suffisante : si elle est satisfaite, A est un anneau local, car si a et a' sont des éléments non nuls de A, et non inversibles dans A, l'un des éléments a/a' et a'/a est dans A (par exemple $a' = a''a$, avec $a'' \in A$), et alors $a + a' = (1+a'')a$ n'est pas inversible dans A. Il reste à montrer que A satisfait au critère du lemme 1 : soit donc $A \subset B \subset K$, $A \neq B$; prenons $x \in B$ tel que $x \notin A$; alors $x^{-1} \in A$, et par suite $x^{-1} \in \underline{m}(A)$; alors $1 = xx^{-1}$ appartient à l'idéal de B engendré par $\underline{m}(A)$.

Définition : un sous-anneau A du corps K qui est tel que, pour tout $x \in K$, on ait $x \in A$ ou $x^{-1} \in A$, est appelé anneau de valuation du corps K.

Théorème 2.- Soit A un sous-anneau d'un corps K. Pour que $x \in K$ soit entier sur A, il faut et il suffit que x appartienne à tous les anneaux de valuation de K contenant A (autrement dit, la fermeture intégrale de A dans K est l'intersection des anneaux de valuation de K contenant A).

Avant de démontrer ce théorème, établissons un lemme :

Lemme 2.- Soit un sous-anneau B du corps K, et soit $\underline{i}$ un idéal de B, $\underline{i} \neq B$. Alors il existe un anneau de valuation C de K, contenant B, et tel que l'idéal $\underline{m}(C)$ contienne $\underline{i}$; si de plus $\underline{i}$ est premier, on peut choisir C de manière que $\underline{m}(C) \cap B = \underline{i}$.

En effet, soit $\underline{p}$ un idéal premier de B contenant $\underline{i}$; alors $B_{\underline{p}}$ est un anneau local contenant B, et son idéal maximal est $\underline{p}B_{\underline{p}}$. Il existe un sous-anneau local C de K, qui domine $B_{\underline{p}}$ et est maximal pour la relation

de domination. C est donc un anneau de valuation de K (théorème 1), et on a $\underline{m}(C) \cap B = (\underline{m}(C) \cap B_{\underline{p}}) \cap B = (\underline{p}B_{\underline{p}}) \cap B = \underline{p} \supset \underline{i}$.

Démonstration du théorème 2 : la condition est nécessaire. Soit $x \in K$, entier sur A, et soit B un anneau de valuation de K contenant A. Il est clair que x est entier sur B. Appliquons le corollaire de la proposition 7, en y remplaçant B par K, et A par B : l'idéal engendré par $\underline{m}(B)$ dans l'anneau $B[x]$ ne contient pas 1 ; d'après le critère de maximalité du lemme 1, ceci entraîne $B[x] = B$, c'est-à-dire $x \in B$.

La condition est suffisante : $x \in K$, $x \neq 0$, et soit B l'anneau $A[x^{-1}]$. Dire que x n'est pas entier sur A revient à dire $x \notin B$. Donc l'idéal $\underline{i}$ engendré par x^{-1} dans B est $\neq B$; d'après le lemme 2, il existe un anneau de valuation C contenant B, et tel que $x^{-1} \in \underline{m}(C)$. Cela signifie que x^{-1} n'est pas inversible dans C, donc $x \notin C$.

5.- Relèvement des idéaux premiers : théorèmes de Krull.

Théorème 3.- Soit A un sous-anneau d'un anneau d'intégrité A', A' étant entier sur A.

(a) pour tout idéal premier $\underline{p}$ de A, il existe un idéal premier $\underline{p}'$ de A' tel que $\underline{p}' \cap A = \underline{p}$;

(b) la relation $\underline{m}' \cap A = 0$ ($\underline{m}'$: idéal de A') entraîne $\underline{m}' = 0$.

Démonstration : soit $\underline{p}$ un idéal premier de A, et soit K le corps des fractions de A' ; d'après le lemme 2 (paragraphe 4), il existe un anneau de valuation V de K, contenant A, et tel que $\underline{m}(V) \cap A = \underline{p}$. D'après le théorème 2, A' est contenu dans V ; alors $\underline{p}' = \underline{m}(V) \cap A'$ est un idéal premier de A', et $\underline{p}' \cap A = \underline{p}$. Ceci prouve l'assertion (a).

Démontrons (b). Supposons qu'il existe $x \in \underline{m}'$ tel que $x \neq 0$; soit n le plus petit entier > 0 tel que l'on ait une relation de la forme $x^n = \sum_{0 \leq i < n} a_i x^i$, $a_i \in A$. Alors $a_0 \in \underline{m} \cap A$, donc $a_0 = 0$, ce qui exige $n > 1$, et entraîne $x^{n-1} = \sum_{0 \leq i < n} a_i x^{i-1}$, contrairement à l'hypothèse faite sur n.

Corollaire 1.- Soit A un sous-anneau d'un anneau d'intégrité A', A' étant entier sur A. Soient $\underline{q}'$ un idéal premier de A', et $\underline{q} = \underline{q}' \cap A$. Alors :

(a) pour tout idéal premier $\underline{p}$ de A tel que $\underline{p} \supset \underline{q}$, il existe un

idéal premier p' de A' tel que $p' \supset q'$ et $p' \cap A = p$;

(b) si m' est un idéal de A' contenant q' et tel que $m' \cap A = q$, on a $m' = q'$.

(On se ramène au théorème 3 , en considérant les anneaux quotients A/q et A'/q') .

Corollaire 2.- Soit A un sous-anneau d'un anneau d'intégrité A', A' étant entier sur A . Alors tout homomorphisme de A dans un corps Q peut se prolonger en un homomorphisme de A' dans un surcorps de Q .

En effet, soit p le noyau de l'homomorphisme $f : A \to Q$; soit p' un idéal premier de A' tel que $p' \cap A = p$. Alors le corps A/p se plonge dans le corps A'/p' , et f définit un plongement de A/p dans Q . On peut alors plonger A'/p' et Q dans un même corps K , de manière que ces deux plongements coïncident sur A/p (Bourbaki, Alg., Chapitre V, paragraphe 4, proposition 2).

Revenons au corollaire 1 ; si p est un idéal premier de A contenu dans q , il n'existe pas, en général, d'idéal premier p' de A' , contenu dans q' , et tel que $p' \cap A = p$. Cependant :

Théorème 4.- Soient A' un anneau d'intégrité, et A un sous-anneau de A' . Supposons que A soit intégralement clos, et A' entier sur A . Soient p et q des idéaux premiers de A , tels que $p \subset q$, et soit q' un idéal premier de A' tel que $q' \cap A = q$. Alors il existe un idéal premier p' de A' , tel que $p' \subset q'$ et $p' \cap A = p$.

Démonstration : soient Q le corps des fractions de A , et Q' le corps des fractions de A' ; alors Q' est une extension algébrique de Q . Il existe un corps L , extension algébrique de Q' (donc de Q), normale sur Q (i.e : si un polynome irréductible à coefficients dans Q a une racine dans L , il se décompose dans L en facteurs du premier degré). Soit B la fermeture intégrale de A dans L ; alors $B \supset A'$. D'après le théorème 3 , il existe un idéal premier m de B tel que $m \cap A' = q'$; tout revient à trouver un idéal premier n de B tel que $n \subset m$ et $n \cap A = p$, car alors $p' = n \cap A'$ possèdera toutes les propriétés requises.

On est donc ramené à prouver le théorème en remplaçant A' par B et q' par m . Dans ce but, on démontrera un lemme :

Lemme 3.- Soit L une extension algébrique normale d'un corps Q . Soit A un sous-anneau de Q , intégralement fermé dans Q ; soit B la fermeture

intégrale de A dans L. Si deux idéaux premiers $\mathfrak{m}$ et $\mathfrak{m}_1$ de B sont tels que $\mathfrak{m} \cap A = \mathfrak{m}_1 \cap A$, ils sont transformés l'un de l'autre par une transformation du groupe de Galois G de L sur Q (G est le groupe des Q-automorphismes de L).

Montrons d'abord comment le théorème 4 résultera du lemme. L'idéal premier $\mathfrak{m}$ de B étant choisi de manière que $\mathfrak{m} \cap A = \mathfrak{q}$, soit $\mathfrak{n}_1$ un idéal premier de B tel que $\mathfrak{n}_1 \cap A = \mathfrak{p} \subset \mathfrak{q}$, puis soit $\mathfrak{m}_1$ un idéal premier de B tel que $\mathfrak{m}_1 \supset \mathfrak{n}_1$ et $\mathfrak{m}_1 \cap A = \mathfrak{q}$ (corollaire 1 du théorème 3). D'après le lemme, il existe $s \in G$ tel que $\mathfrak{m} = s(\mathfrak{m}_1)$; alors $\mathfrak{n} = s(\mathfrak{n}_1)$ est contenu dans $\mathfrak{m}$, et $\mathfrak{n} \cap A = \mathfrak{p}$.

Tout revient donc à prouver le lemme 3 , ce qu'on va faire maintenant. Soit $\bar{Q}$ la plus grande extension radicielle de Q contenue dans L (en caractéristique 0 , $\bar{Q} = Q$; en caractéristique $p \neq 0$, $\bar{Q}$ se compose des $x \in L$ tels qu'il existe un entier f avec $x^{p^f} \in Q$) . Soit $\bar{A}$ la fermeture intégrale de A dans $\bar{Q}$. Tout idéal premier $\mathfrak{q}$ de A est l'interaction avec A d'un unique idéal premier de $\bar{A}$, à savoir l'ensemble des $x \in L$ tels qu'il existe un entier f avec $x^{p^f} \in \mathfrak{q}$. Le corps L est une extension galoisienne de $\bar{Q}$, et G est le groupe de Galois de L sur $\bar{Q}$. Il suffit donc de prouver le lemme en remplaçant Q par $\bar{Q}$, et A par $\bar{A}$.

Revenant aux notations du lemme 3 , nous supposons désormais que L est une extension galoisienne de Q . Nous voulons montrer que si $\mathfrak{m}$ et $\mathfrak{m}_1$ sont des idéaux premiers de B tels que $\mathfrak{m} \cap A = \mathfrak{m}_1 \cap A$, on a $\mathfrak{m}_1 = s(\mathfrak{m})$ pour un $s \in G$. Il suffit de montrer :

(1) il existe $s \in G$ tel que $\mathfrak{m}_1 \subset s(\mathfrak{m})$.

(cf. la partie (b) du corollaire 1 du théorème 3). On va d'abord prouver (1) dans le cas où le groupe G est fini. Raisonnons par l'absurde : supposons que $\mathfrak{m}_1$ ne soit contenu dans aucun des $s(\mathfrak{m})$, et notons $s_1(\mathfrak{m})$,..., $s_k(\mathfrak{m})$ l'ensemble de tous les idéaux distincts de la forme $s(\mathfrak{m})$. Pour chaque i $(1 \leq i \leq k)$, soit $x_i \in \mathfrak{m}_1$ tel que $x_i \notin s_i(\mathfrak{m})$; pour $i \neq j$, soit $y_{ij} \in s_j(\mathfrak{m})$ tel que $y_{ij} \notin s_i(\mathfrak{m})$. Soient $z_i = x_i \cdot \prod_{j \neq i} y_{ij}$ et $z = \sum_i z_i$. Alors $z \in \mathfrak{m}_1$ et z n'appartient à aucun des $s_i(\mathfrak{m})$. Pour tout $s \in G$, on a donc $sz \notin \mathfrak{m}$; alors $u = \prod_{s \in G} sz$ appartient à $\mathfrak{m}_1$ et non à $\mathfrak{m}$. Comme u est invariant par G , on a $u \in Q$; or u est entier sur A , donc $u \in A$, et par suite $u \in \mathfrak{m}_1 \cap A = \mathfrak{m} \cap A$, ce qui est absurde puisque $u \notin \mathfrak{m}$.

Prouvons enfin l'assertion (1) dans le cas général où le groupe de Galois G est infini. Munissons G de la topologie classique (cf. Bourbaki, Alg., Chapitre V, Appendice II) qui en fait un groupe compact. L est réunion d'une famille filtrante d'extensions galoisiennes L_i de Q, de degré fini ; soit E_i l'ensemble des $s \in G$ tels que $s^{-1}(\underline{m}_1 \cap L_i) \subset \underline{m}$. L'ensemble E_i est fermé, et il n'est pas vide d'après ce qui précède. Comme les E_i forment une famille filtrante décroissante, leur intersection n'est pas vide ; si s appartient à cette intersection, on a $s^{-1}(\underline{m}_1) \subset \underline{m}$. Ceci achève la démonstration.

APPENDICE : Sur le radical d'un anneau.

Soit A un anneau (non nécessairement commutatif) ayant un élément unité $1 \neq 0$. Pour un idéal à gauche $\underline{i}$ de A, les propriétés suivantes sont équivalentes :

(i) pour tout $a \in \underline{i}$, $1 + a$ est inversible à gauche ;

(ii) pour tout A-module à gauche (unitaire) M, de type fini, la relation $\underline{i}M = M$ entraîne $M = 0$;

(iii) $\underline{i}$ est contenu dans tout idéal à gauche maximal.

Démonstration : (i) entraîne (ii). Soit en effet M un A-module à gauche, $\neq 0$, de type fini, et soit (x_i) un système minimal de générateurs de M $(1 \leqslant i \leqslant n)$; l'hypothèse $\underline{i}M = M$ entraîne $x_1 = \sum_i a_i x_i$, avec $a_i \in \underline{i}$, donc $(1-a_1)x_1$ est combinaison linéaire des x_i $(i \geqslant 2)$, et comme $1 - a_1$ est inversible à gauche d'après (i), x_1 est combinaison linéaire des x_i $(i \geqslant 2)$, ce qui contredit la minimalité du système de générateurs de M.

(ii) entraîne (iii) : soit $\underline{j}$ un idéal à gauche maximal, et considérons le A-module à gauche (monogène) $M = A/\underline{j}$; tout sous-module de M est égal à M ou à 0 ; d'après (ii), $\underline{i}M \neq M$, donc $\underline{i}M = 0$, c'est-à-dire $\underline{i} \subset \underline{j}$.

(iii) entraîne (i) : soit $a \in \underline{i}$; si $1 + a$ n'était pas inversible à gauche, $1 + a$ engendrerait un idéal à gauche $\neq A$, donc contenu dans un idéal maximal $\underline{j}$; alors $1+a \in \underline{j}$, donc $a \notin \underline{j}$, contrairement à l'hypothèse (iii).

Il y a un plus grand idéal à gauche satisfaisant aux conditions équivalentes (i), (ii), (iii) : c'est l'intersection des idéaux à gauche maximaux. On l'appelle le radical (à gauche) de A, et on le note $\underline{r}(A)$. L'idéal bilatère engendré par $\underline{r}(A)$ satisfait évidemment à (ii), donc c'est $\underline{r}(A)$.

Ainsi le radical (à gauche) est un idéal bilatère.

Observons maintenant que la propriété (i) , pour un idéal à gauche $\underline{i}$, entraîne que $1 + a$ est inversible (à gauche et à droite) pour tout $a \in \underline{i}$. En effet, soit $x \in A$ tel que $x(1+a) = 1$; alors $x-1 \in \underline{i}$, donc $x = 1 + (x-1)$ possède un inverse à gauche, qui est nécessairement égal à $1 + a$; ainsi x est inverse à droite et à gauche de $1 + a$.

De ceci il résulte que le radical $\underline{r}(A)$ est le plus grand idéal bilatère $\underline{i}$ tel que $1+a$ soit inversible pour tout $a \in \underline{i}$. Le "radical à droite" est donc le même que le "radical à gauche".