RÉDACTION N° 109

COTE : NBR 019

TITRE : LIVRE II
CHAPITRE V. CORPS COMMUTATIFS (ÉTAT 4)

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 85

NOMBRE DE FEUILLES : 85

L I V R E II

CHAPITRE V

CORPS COMMUTATIFS (Etat 4)

Sommaire

.....

4 - Existence des corps algébriquement clos.

5 - Unicité de la clôture algébrique - Prolongement des isomorphismes.

§ 7 - Isomorphismes. Dérivations - Séparabilité.

1 - Isomorphismes relatifs à un sous-corps. Eléments conjugués.

2 - Eléments p-radiciels.

3 - Indépendance linéaire des isomorphismes.

4 - Extensions séparables.

5 - Extensions algébriques séparables.

6 - Eléments algébriques séparables.

7 - Eléments séparables d'une extension algébrique.

8 - Bases de transcendance séparantes.

9 - Dérivations dans les corps.

§ 8 - Théorie de Galois.

1 - Extensions galoisiennes. Extensions normales.

2 - Fonctions symétriques des racines d'un polynome. Norme et trace.

3 - La théorie de Galois.

4 - Sous-corps conjugués. Sous-corps galoisiens.

5 - Le théorème de la base normale.

6 - Extensions normales non séparables.

§ 9 - Exemples : Racines de l'unité, corps finis, extensions cycliques.

1 - Racines de l'unité.

2 - Corps des racines de l'unité.

3 - Corps finis

4 - Extensions cycliques.

Appendice - Extensions galoisiennes de degré infini.

Commentaires : Sans commentaires !

LIVRE II

CHAPITRE V

CORPS COMMUTATIFS (Etat 4).

Sauf mention expresse du contraire, tous les corps considérés dans ce chapitre seront tacitement supposés être commutatifs.

§ 1. Corps premiers - Caractéristique.

1)- Corps premiers.

On sait (chap.I, § 9, n° 2) que l'intersection d'une famille quelconque de sous-corps d'un corps K (commutatif ou non) est un sous-corps de K ; en particulier l'intersection P de tous les sous-corps de K est le plus petit sous-corps de K . C'est le sous-corps engendré par l'élément unité. Définition 1 - On dit qu'un corps est premier s'il ne contient pas de sous-corps distinct de lui-même.

Tout corps K (commutatif ou non) contient un corps premier P et un seul, engendré par l'élément unité e . Pour déterminer la structure de P nous allons d'abord déterminer celle du sous-anneau A de K engendré par e . A est l'ensemble des éléments n.e , où $n \in \mathbb{Z}$; et l'application $n \to n.e$ est une représentation de l'anneau $\mathbb{Z}$ des entiers rationnels sur A (chap.I, § 8, n° 6). L'ensemble des entiers $n \in \mathbb{Z}$ tels que $n.e = 0$ est un idéal (p) de $\mathbb{Z}$, où $p \geqslant 0$ est la caractéristique (chap.I, § 8, n° 8) du corps K ; et A est isomorphe à l'anneau $\mathbb{Z}/(p)$. Deux cas peuvent se présenter :

1) $p=0$; A est alors isomorphe à $\mathbb{Z}$; P contient le corps des fractions de A , qui est isomorphe au corps Q des nombres rationnels ; comme P est un corps premier, il est identique au corps des fractions de A , donc est isomorphe à Q .

2) $p > 0$. Comme A est contenu dans un corps, il ne peut contenir de diviseurs de 0 ; donc $\mathbb{Z}/(p)$ ne peut contenir de diviseurs de 0 , ce qui implique que $p = mn$ $(m > 0 , n > 0)$ entraîne $m = p$ ou $n = p$, et par suite p est un nombre premier (chap.I, § 8, n° 7). Mais, pour tout nombre premier p , $\mathbb{Z}/(p)$ est un corps ; et par suite P est identique à A et isomorphe à $\mathbb{Z}/(p)$. En résumé :

Théorème 1 - Le caractéristique d'un corps K (commutatif ou non) est égale à zéro ou à un nombre premier. Si K est de caractéristique 0 , le sous-corps premier de K est isomorphe au corps Q des nombres rationnels. Si K est de caractéristique $p > 0$, le sous-corps premier de K est isomorphe au corps $\mathbb{Z}/(p)$ des entiers mod.p . Il existe des corps de toutes caractéristiques.

On remarquera que la détermination de la caractéristique d'un corps K ne fait intervenir que l'élément unité de K .

2)- Exposant caractéristique - Corps parfaits.

Etant donné un corps K de caractéristique p , nous appellerons exposant caractéristique de K le nombre p si $p > 0$, et le nombre 1 si $p = 0$.

Proposition 1 - Si p est l'exposant caractéristique d'un corps K , l'application $x \to x^p$ est un isomorphisme de K sur un de ses sous-corps (que l'on note K^p lorsque aucune confusion n'est à craindre).

Il est clair que $(xy)^p = x^p y^p$. Nous allons montrer que $(x+y)^p = x^p + y^p$ C'est évident si $p = 1$. Si $p > 1$, on sait que $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$, où $\binom{p}{0} = \binom{p}{p} = 1$. Il ne nous reste donc plus qu'à montrer que, lorsque $1 < k < p$, $\binom{p}{k} e = 0$. Or on a $k! \binom{p}{k} = p(p-1)\dots(p-k+1)$, donc $(k! e)\left(\binom{p}{k} e\right) = p(p-1)\dots(p-k+1)e = 0$; comme $k!s = \prod_{h=1}^{k} hs$ et que $hs \neq 0$ pour $1 < h < p$, on a $k!s \neq 0$, donc $\binom{p}{k} e = 0$. L'application $x \to x^p$ est donc une représentation de K dans lui-même ; comme elle n'est pas nulle c'est un isomorphisme de K sur un de ses sous-corps (chap.I, § 9, th.1).

Corollaire - Pour tout entier $f \geqslant 0$, l'application $x \to x^{p^f}$ est un isomorphisme de K sur un de ses sous-corps (que l'on note K^{p^f} lorsqu'aucune confusion n'est à craindre).

En effet $x \to x^{p^f}$ s'obtient en itérant f fois l'isomorphisme $x \to x^p$.

Quels que soient les entiers f et $n \geqslant 0$ on a donc dans K :

$$(1) \qquad \Big(\sum_{i=1}^{n} x_i\Big)^{p^f} = \sum_{i=1}^{n} x_i^{p^f}$$

Définition 2.- On dit qu'un corps K est parfait si l'application $x \to x^p$ est un automorphisme de K, p étant l'exposant caractéristique de K. K est dit imparfait s'il n'est pas parfait.

Tout corps de caractéristique 0 est parfait car $x \to x^p$ est alors l'application identique. Tout corps fini est parfait car une application biunivoque d'un ensemble fini dans lui-même applique cet ensemble sur lui-même. Dans un corps parfait K, pour tout $y \in K$, il existe $x \in K$ tel que $x^p = y$; autrement dit tout élément d'un corps parfait a une racine p-ième dans ce corps. D'après $(x-x')^p = x^p - x'^p$ cette racine p-ème est unique.

Proposition 2. Soit K un corps parfait d'exposant caractéristique p $f = \sum_{k=1}^{n} a_k X^{kp}$ un polynome de $K[X]$ dont tous les termes ayant un degré non multiple de p sont nuls ; il existe alors un polynome et un seul $g \in K[X]$ tel que $f = g^p$.

En effet, K étant parfait, il existe, pour tout indice k, $\beta_k \in K$ tel que $\beta_k^p = a_k$; si l'on pose $g = \sum_{k=1}^{n} \beta_k X^k$, on a $g^p = f$ d'après la formule (1). L'unicité de g est conséquence immédiate de $(g-g')^p = g^p - g'^p$.

§ 2 - Extensions.

Soit K un corps, L un corps contenant K ; l'élément unité de K est identique à celui de L (car $e^2 = e$ entraîne $e = 1$ si $e \neq 0$). Donc L peut être muni d'une structure d'algèbre sur K (chap. II, § 7, n° 1). Nous dirons que L, muni de cette structure d'algèbre sur K, est une extension de K.

Lorsque, désormais, nous emploierons le mot extension c'est à la structure d'algèbre de L sur K que nous référerons. Lorsque seule la structure de corps de L sera en jeu, nous emploierons le mot surcorps.

De nombreuses propriétés des extensions de K seront valables pour les algèbres sur K ayant un élément unité.

1)- La structure linéaire d'une extension.

Une extension E d'un corps K étant une algèbre sur K, est par suite un espace vectoriel sur K, dont la dimension est appelée le degré (ou le rang) de E sur K (ou encore le degré de l'extension E, lorsque aucune confusion n'est à craindre), et est notée $[E:K]$ lorsqu'elle est finie ; le nombre $[E:K]$ n'est donc défini que dans ce cas.
Le cor. de la prop.1 (chap.II, § 5) entraîne en particulier que :

Théorème 1 - Si E est une extension de K, F une extension de E, et si deux des nombres $[E:K]$, $[F:E]$, $[F:K]$ sont définis, il en est de même du troisième, et on a :

$$(1) \qquad [F:K] = [E:K].[F:E]$$

Corollaire 1 - Si F est une extension de degré fini de K, le degré $[E:K]$ de toute extension E de K, telle que $E \subset F$, est un diviseur de $[F:K]$.

Corollaire 2 - Si $K \subset E \subset F$ et si $[F:K]$ est fini, la relation $[E:K] = [F:K]$ est équivalente à $E = F$ et la relation $[F:E] = [F:K]$ est équivalente à $F = K$.

La première partie est une propriété évidente des espaces vectoriels. La seconde se déduit du fait qu'une extension de degré 1 d'un corps K est identique à K.

Proposition 1 - Soit A une algèbre sur K , ayant un élément unité, et de degré fini ; si $a \in A$ n'est pas diviseur de zéro à gauche (resp. à droite) dans A , a admet un inverse à droite (resp. à gauche) dans A .

En effet l'application $x \to ax$ est un endomorphisme biunivoque de la structure d'espace vectoriel de A ; c'est donc un automorphisme de $b \in A$ tel que $1 = ab$.

Corollaire - Tout anneau d'intégrité A contenant un corps K , et fini sur K , est un surcorps de K .

En effet, l'élément unité e de K , qui satisfait à $e^2 = e$, est élément unité de A , car, de $ex = e^2x$, on déduit $x = ex$.

2) - Adjonction.

Soit E une extension d'un corps K . Etant donnée une famille quelconque $X = (x_\iota)_{(\iota \in I)}$ d'éléments de E , on sait (chap.IV, § ,) qu'on désigne par $K(x_\iota)_{\iota \in I}$ (ou $K(X)$, ou encore $K(x_1,\dots,x_n)$ lorsque I est l'intervalle $[1,n]$ de N) le plus petit sous-corps de E contenant K et les éléments (x_ι) ; nous dirons que $K(x_\iota)_{\iota \in I}$ est obtenu par adjonction à K des éléments de la famille $(x_\iota)_{\iota \in I}$, et que la famille $(x_\iota)_{\iota \in I}$ est un système de générateurs de $K(x)_I$ sur (ou par rapport à) K . On sait que $K(x_\iota)_{\iota \in I}$ ne dépend que de l'ensemble A des éléments de la famille (x_ι) ; on le désigne encore par $K(A)$.

Proposition 2 - Si M et N sont deux parties quelconques de E , on a $K(M \cup N) = K(M)(N) = K(N)(M)$.

En effet, $K(M \cup N)$ contient $K(M)$ et N , donc $K(M)(N)$; et comme c'est le plus petit sous-corps de E contenant $K \cup M \cup N$, il est égal à $K(M)(N)$.

Remarque.- Si P est le sous corps premier de E (§ 1), pour toute partie A de E , $P(A)$ est le plus petit sous-corps de E contenant A . En particulier, si K est un sous-corps de E , on a $P(K) = K$ et

$K(A)=P(K\cup A)$. Si K et K' sont deux sous-corps de E , on a donc $P(K\cup K')= K(K')=K'(K)$; ce corps est le plus petit sous-corps de E contenant K et K' , ou encore la borne supérieure de K et K' dans l'ensemble des sous-corps de E , ordonné par inclusion ; on note quelquefois, par abus de langage, ce corps par KK' .

Proposition 3 - Soit ξ un ensemble de sous-corps de E , filtrant pour la relation $\subset$. Le réunion des corps de ξ est un corps L .

En effet, si x et y sont deux éléments de L , il existe deux corps R et S de ξ tels que $x\in R$, $y\in S$; soit T un corps de ξ contenant R et S ; alors $x\in T$, $y\in T$, donc aussi $x+y$, xy et x^{-1} (si $x\neq 0$) appartiennent à T , donc à L .

Corollaire - Le corps K(A) obtenu par adjonction à K d'une partie quelconque A de E , est la réunion des corps K(F) où F parcourt l'ensemble des parties finies de A .

En effet l'ensemble des corps K(F) est filtrant pour la relation $\subset$ en vertu de la prop.2 . La réunion L de ces corps est donc un corps, contenant $K\cup A$ et contenu dans K(A) ; c'est donc K(A) .

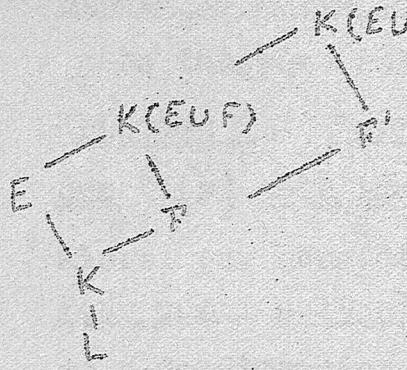
Définition 1 - On dit qu'une extension E d'un corps K est de type fini si elle possède un système de générateurs fini. Elle est dite monogène si elle possède un système de générateurs réduit à un seul élément.

Le corollaire de la prop.3 montre donc que toute extension E d'un corps K est réunion des extensions de type fini contenues dans E .

Il est clair que toute extension E de K de degré fini est aussi de type fini, puisqu'une base de E (considéré comme espace vectoriel sur K) est aussi un système de générateurs de E sur K ; nous verrons plus tard que la réciproque est inexacte.

3)- Diagrammes de Hasse.

Pour aider le lecteur à se représenter une situation où interviennent plusieurs corps, nous nous servirons souvent de diagrammes du type ci-contre (appelés "diagrammes de Hasse"). Un trait rectiligne entre deux lettres (désignant des corps) signifie que le corps dont la lettre est plus basse est un sous-corps de celui dont la lettre est plus haute. Par exemple on a ici : $L \subset K \subset F \subset F' \subset K(E \cup F')$, et : $L \subset K \subset E \subset K(E \cup F) \subset K(E \cup F')$.



§ 3. Extensions algébriques.

1)- Eléments algébriques.

Soient K un corps, L une extension de K, x un élément de L. Nous nous proposons d'étudier l'anneau $K[x]$ (chap.IV, § 2). C'est un anneau commutatif isomorphe à $K[X]/\mathfrak{a}$, $\mathfrak{a}$ étant l'idéal des relations algébriques satisfaites par x, sur K ou encore le module des relations linéaires entre les monômes $(x^n)_{n \in \mathbb{N}}$ (chap.IV, § 2, n°1). Nous voyons donc que deux cas se peuvent présenter, suivant que $\mathfrak{a}$ est ou non réduit à $\{0\}$.

Définition 1 - Un élément x d'une extension L d'un corps K est dit transcendant sur K si les monômes $(x^n)_{n \in \mathbb{N}}$ sont linéairement indépendants sur K ; x est dit algébrique sur K dans le cas contraire.

Les mêmes définitions s'étendent au cas où x est un élément d'une algèbre sur K, ayant un élément unité.

Lorsque $\mathfrak{a} \neq \{0\}$, on sait (chap.IV, § ,) que $\mathfrak{a}$ est un idéal principal (f) et que, si f est de degré n, les classes (mod.f) des x^t $(0 \leqslant t < n)$ forment une base de $K[X]/(f)$ sur K. Puisque l'anneau $K[X]/(f)$ est d'intégrité et est fini sur K, c'est un corps (§ 2, cor. de la prop.1) ;

donc c'est le corps $K(x)$, et (f) est un idéal maximal, et f est un polynome irréductible.

Définition 2 - Si x est algébrique sur K, l'entier $n = [K(x):K]$ est appelé le degré de x sur K.

Le théorème suivant est alors évident :

Théorème 1 - Pour que x soit transcendant sur K, il faut et il suffit que $K[x]$ soit isomorphe à l'anneau de polynomes $K[X]$ (on appelle alors, par abus de langage, les éléments de $K[x]$ des polynomes en x). Pour que x soit algébrique sur K, il faut et il suffit que $K[x]$ soit de dimension (linéaire) finie sur K ; si alors x est de degré n sur K, il existe un polynome $f \in K[X]$ et un seul, de degré n, tel que $f(x) = 0$, et que le coefficient de x dans f soit égal à 1 ; ce polynome, appelé polynome minimal de x sur K, est irréductible ; l'ensemble des polynomes g tels que $g(x)=0$ est l'idéal principal, et maximal (f) ; on a $K(x) = K[x]$; $K(x)$ est isomorphe au corps quotient $K[X]/(f)$, et a l'ensemble $\{x^t\}$ $(1 \leqslant t \leqslant n-1)$ pour base sur K.

Remarque - Si $f = X^n - \sum_{i=0}^{n-1} a_i X^i$ est le polynome minimal de x sur K, on a : $x^{-1} = -\sum_{i=0}^{n-2} a_0^{-1} a_{i+1} x^i + a_0^{-1} x^{n-1}$ (puisque f est irréductible on a $a_0 \neq 0$).

Proposition 1 - Soit x un élément, algébrique sur K, d'un surcorps E de K ; pour tout corps F tel que $K \subset F \subset E$, x est algébrique sur F, et son degré sur F est au plus égal à son degré sur K.

En effet, soit le polynome minimal de x sur K ; puisque $f(x)=0$, f appartient à l'idéal des relations algébriques satisfaites par x sur F, ce qui, compte tenu du th.1, démontre la proposition.

Exemples - * 1) Dans le corps des nombres complexes Ω, le nombre i est algébrique et de degré 2 sur le corps premier Q ; en effet, si $f = X^2+1$, on a $f(i)=0$, et il est clair que $i \notin Q$.

Le corps $Q(i)$ est donc une extension de degré 2 de Q ; il est formé des nombres $a + bi$, où a et b parcourent Q.

2) Soit K un corps, F le corps $K(X)$ des fractions rationnelles à une indéterminée sur K . Soit E le sous-corps $K(X^3)$ de F ; on a $F = E(X)$, et X est algébrique sur E puisqu'il est racine du polynome $Y^3 - X^3$ de l'anneau de polynomes $E[Y]$; ce polynome est irréductible car, dans le cas contraire, il aurait un facteur du premier degré, et il y aurait deux polynomes non nuls u et v de $K[X]$ tels que $u(X^3) = Xv(X^3)$, ce qui est absurde car, si m et n sont les degrés de u et v , cela implique $3m = 3n+1$. F est donc de degré 3 sur E , et a $\{1, X, X^2\}$ pour base.

2)- Extensions algébriques.

Définition 3 - On dit qu'une extension E d'un corps K est algébrique (ou que le surcorps E est algébrique sur K, ou encore, par pléonasme, que l'extension E est algébrique sur K) si tout élément de E est algébrique sur K . Une extension E de K , qui n'est pas algébrique, est dite transcendante.

Proposition 2 - Pour qu'une extension E de K soit algébrique, il faut et il suffit que tout anneau A tel que $K \subset A \subset E$ soit un corps.

En effet si E est algébrique sur K , tout $x \in A$ est algébrique sur K ; alors $K(x) = K[x]$ (th.2), donc $K(x) \subset A$, $x^{-1} \in A$, et A est un corps. Si au contraire E est transcendant sur K , il contient x transcendant sur K , et l'anneau de polynomes $K[x]$ n'est pas un corps, car x^{-1} devrait être un polynome de degré -1 .

Proposition 3 - Toute extension de degré fini n , E de K est algébrique ; et le degré sur K de tout $x \in E$ divise n .

En effet, pour tout $x \in E$, $[K(x):K]$ divise n (§ 2, cor.1 du th.1) ; c'est donc un entier fini, ce qui montre que x est algébrique sur K .

La réciproque de la prop.3 est inexacte : nous donnerons plus tard (§ 6,n°3) des exemples d'extensions algébriques de degré infini.

Proposition 4 - Soit $E = K(a_1 \ldots a_m)$ une extension de K telle que les a_i soient algébriques sur K ; soit n_1 le degré de a_1 sur K, n_i $(2 \leqslant i \leqslant m)$ le degré de a_i sur $K(a_1, \ldots, a_{i-1})$; les éléments $a_1^{\nu_1} a_2^{\nu_2} \ldots a_m^{\nu_m}$ $(0 \leqslant \nu_i \leqslant n_i - 1)$ forment une base de E sur K ; E est donc algébrique de degré $n_1 \ldots n_m$ sur K.

La première partie résulte immédiatement du th.1 et de la prop.1 § 5, chap.II, appliqués inductivement. La seconde partie est alors conséquence immédiate de la prop.3.

Remarque.- L'idéal $\mathfrak{a}$ des relations algébriques entre les a_i est maximal, et E est isomorphe à $K[X_1, \ldots, X_m]/\mathfrak{a}$; car $E = K[a_1, \ldots, a_m]$ (cf.chap.IV, § 2,n°2).

Proposition 5 - Soit A une partie, composée d'éléments algébriques sur K, d'une extension E de K ; alors $K(A)$ est algébrique sur K.

En effet tout $x \in K(A)$ appartient à $K(F)$ où F est une partie finie de A (cor. de la prop.3, § 2) ; or $K(F)$ est algébrique sur K (prop.4) ; donc x est algébrique sur K.

Proposition 6 - Soit φ un isomorphisme d'un corps K sur un corps K' et E une extension algébrique de K ; il existe une extension algébrique E' de E et un isomorphisme φ' de E sur E' prolongeant φ.

Soit en effet $A = (x_\lambda)_{\lambda \in \Lambda}$ une famille d'éléments de E tels que $E = K[A]$ (par exemple une base linéaire de E sur K). Alors (chap.IV, § 2,n°1) E est isomorphe à $K[X_\lambda]_{\lambda \in \Lambda}/\mathfrak{a}$, où $\mathfrak{a}$ est l'idéal des relations algébriques entre les x_λ. Si $\mathfrak{a}'$ est l'idéal de $K'[X_\lambda]_{\lambda \in \Lambda}$ obtenu en appliquant φ à tous les coefficients des polynomes de $\mathfrak{a}$, il est clair que nous pourrons prendre $E' = K'[X_\lambda]_{\lambda \in \Lambda}/\mathfrak{a}'$.

3)- Transitivité des extensions algébriques. Extensions algébriquement fermées.

Proposition 7 - Soient E et F deux surcorps de K tels que $K \subset E \subset F$. Pour que F soit algébrique sur K, il faut et il suffit que E soit algébrique sur K et F algébrique sur E.

La nécessité est évidente (prop.1). Montrons maintenant que la condition est suffisante ; soit x un élément quelconque de F ; il est algébrique sur E, et soit $g \in E[X]$ son polynome minimal sur E ; si A est l'ensemble (fini) des coefficients de g, x est algébrique sur K(A) (th.1) ; or K(A) est de degré fini sur K (prop.4) ; donc $K(A \cup \{x\})$ est de degré fini sur K (§ 2, th.1), et x est algébrique sur K (prop.3).

Définition 4.- On dit qu'un sous-corps K d'un corps E est algébriquement fermé dans E (ou que E est une extension algébriquement fermée de K), si tout élément de E, algébrique sur K, appartient à K.

Autrement dit, K est la seule extension algébrique de K contenue dans E, K est algébriquement fermé dans lui-même. Nous étudierons plus tard (§ 6) les corps algébriquement fermés dans toute extension.

Proposition 8 - Soit E une extension d'un corps K ; l'ensemble L des éléments de E qui sont algébriques sur K est un corps, algébriquement fermé dans E, qu'on appelle la fermeture algébrique de K dans E.

En effet (prop.5) le corps K(L) est algébrique sur K, donc $K(L) \subset L$, et par suite K(L)=L, et L est un corps. Si, d'autre part, $x \in E$ est algébrique sur L, il l'est aussi sur K (prop.7), donc il appartient à L.

§ 4.- Extensions transcendantes.

1)- Familles algébriquement libres. Extensions transcendantes pures.

Nous avons défini au § précédent la notion d'élément transcendant sur un corps K ; x est dit transcendant sur K si les monômes $\{x^n\}$ $(n \in \mathbb{N})$ sont linéairement indépendants sur K. Nous allons généraliser cette définition:

Définition 1 - Dans une extension E d'un corps K, on dit qu'une famille $(x_\lambda)_{\lambda \in \Lambda}$ d'éléments de E est algébriquement libre sur K, si les monômes par rapport aux éléments de la famille sont linéairement indépendants sur K.

Remarque - Toute famille algébriquement libre sur K est a fortiori formée d'éléments linéairement indépendants sur K ; ou encore c'est une famille libre de E pour sa structure d'espace vectoriel sur K. Mais la réciproque est inexacte comme le montre l'exemple de la base linéaire d'une extension algébrique de K. Pour éviter toute confusion, nous emploierons (et avons déjà employé) le mot linéairement libre pour désigner une famille d'éléments de E qui est libre pour la structure d'espace vectoriel de E sur K.

Lorsqu'une famille $(x_\lambda)_{\lambda \in \Lambda}$ n'est pas algébriquement libre, on dit qu'elle est algébriquement liée sur K.

Puisque la sous-famille $(x_\lambda)_{\lambda \in \Lambda}$ est linéairement libre, deux de ses éléments dont les indices sont distincts, sont eux-mêmes distincts (chap.II, §1, n°6). On dira qu'une partie S de E est une partie algébriquement libre (ou un système algébriquement libre) de E sur K, si la famille définie par l'application biunivoque de S sur elle-même est algébriquement libre (auquel cas toute famille définie par une application biunivoque d'un ensemble d'indices sur S est aussi une famille algébriquement libre). Les éléments d'une partie algébriquement libre de E sont encore dits algébriquement indépendants. Si une partie de E n'est pas algébriquement libre, on dit qu'elle est algébriquement liée (ou est un système algébriquement lié) sur K, et que ses éléments sont algébriquement dépendants sur K.

Puisque l'indépendance linéaire est une propriété de caractère fini (chap.II, §1, n°6), l'indépendance algébrique est aussi une propriété de caractère fini (Ens. R, §7, n° 1).

La partie vide de E est algébriquement libre. Dire qu'une partie $\{x\}$ réduite à un élément est algébriquement libre sur K, signifie que x est transcendant sur K ; tout élément d'une partie algébriquement libre de E est transcendant sur K.

La caractérisation suivante est évidente :

Proposition 1 - Pour qu'une famille $(x_\lambda)_{\lambda \in \Lambda}$ d'éléments d'une extension E d'un corps K soit algébriquement libre sur K, il faut et il suffit que la relation $f((x_\lambda))=0$, où f est un polynome de l'anneau $K[X_\lambda]_{\lambda \in \Lambda}$, entraîne $f = 0$.

Cela signifie aussi que l'idéal des relations algébriques entre les x_λ dans $K[X_\lambda]_{\lambda \in \Lambda}$ (chap.IV, § , n°) se réduit à (0). Donc l'anneau $K[(x_\lambda)]$ est isomorphe à l'anneau de polynomes $K[X_\lambda]_{\lambda \in \Lambda}$ (ses éléments seront, par abus de langage appelés polynomes), et son corps des quotients $K(x_\lambda)_{\lambda \in \Lambda}$ est isomorphe au corps des fractions rationnels $K(X_\lambda)_{\lambda \in \Lambda}$.

Posons alors la définition suivante :

Définition 2 - Une extension E d'un corps K est dite transcendante pure si elle est isomorphe à un corps de fractions rationnelles sur K.

Il revient au même de dire qu'il existe une partie algébriquement libre A de E telle que E $\simeq$ K(A).

Nous verrons plus tard, comme conséquence d'une propriété plus générale (§ 5, cor. de la prop.5) que K est algébriquement fermé dans toute extension transcendante pure. Mais la réciproque n'est pas vraie : si K est algébriquement fermé dans E, E n'est pas nécessairement une extension transcendante pure de K. (cf.exerc.2).

2)- Bases de transcendance.

Proposition 2 - Soit E une extension d'un corps K , M et N deux parties de E . Les propriétés suivantes sont équivalentes :

a) $M \cup N$ est algébriquement libre sur K , et $M \cap N = \emptyset$.

b) M est algébriquement libre sur K , et N est algébriquement libre sur $K(M)$.

c) N est algébriquement libre sur K , et M est algébriquement libre sur $K(N)$.

Il suffit évidemment de montrer que a) et b) sont équivalentes.

1°) a) entraîne b). Remarquons que $K[M]$, $K[N]$ et $K[M \cup N]$ sont alors isomorphes à des anneaux de polynomes et que l'on a $K[M \cup N] = K[M][N] = K[N][M]$ (chap.IV, § 1, n°). Les monômes par rapport aux éléments de N , qui forment une base de $K[M][N]$ sur $K[M]$, sont donc linéairement indépendants sur le corps des quotients $K(M)$ (chap.III, § 2, prop.5) .

2°) b) entraîne a). Remarquons qu'alors $K[M]$ et $K[M][N]$ sont isomorphes à des anneaux de polynomes sur K et $K[N]$ respectivement ; on a $K[M][N] = K[M \cup N]$, ce qui montre que $M \cap N = \emptyset$ et que $M \cup N$ est algébriquement libre sur K .

Corollaire - Soit E une extension d'un corps K, x un élément de E , et B une partie de E telle que $x \notin B$. Pour que $B \cup \{x\}$ soit algébriquement libre sur K , il faut et il suffit que B soit algébriquement libre sur K , et x transcendant sur $K(B)$.

On prend en effet $N = B$, $M = \{x\}$.

Proposition 3 - Toute partie A d'une extension E d'un corps K , qui est algébriquement libre sur K , reste algébriquement libre sur toute extension algébrique K' de K contenue dans E .

En effet, si A n'était pas algébriquement libre sur K' , il existerait, d'après le cor. de la prop.2, un élément $x \in A$ algébrique sur $K'(B)$

B désignant $A \cap \complement \{x\}$; or $K'(B) = K(B)(K')$ est algébrique sur $K(B)$ (§ 3, prop.7), donc x est algébrique sur K(B) (§ 3, prop.7), ce qui est contraire au fait que $A = B \cup \{x\}$ est algébriquement libre sur K, d'après le cor. de la prop. 2 .

Définition 3 - On dit qu'une partie B d'une extension E d'un corps K est une base de transcendance de E (sur K), si B est algébriquement libre sur K , et si E est algébrique sur K(B) .

On déduit alors immédiatement du cor. de la prop.3 la :

Proposition 4 - Pour que $B \subset E$ soit base de transcendance de l'extension E d'un corps K , il faut et il suffit que B soit un élément maximal dans l'ensemble (ordonné par inclusion) des parties de E algébriquement libres sur K .

Théorème 1 (Steinitz) - Toute extension E d'un corps K admet une base de transcendance. En d'autres termes toute extension d'un corps K est une extension algébrique d'une extension transcendante pure de K .

Ce théorème est conséquence du théorème plus précis suivant (si l'on prend $L = \emptyset$, $S = E$).

Théorème 2 - Soit E une extension d'un corps K, S une partie de E telle que E soit algébrique sur K(S), et L une partie algébriquement libre (sur K) de E contenue dans S ; il existe alors une base de transcendance B de E telle que $L \subset B \subset S$.

L'ensemble $\mathcal{F}$ des parties algébriquement libres de S contenant L est un ensemble de caractère fini (Ens. R., § 7, n°11) ; il est donc inductif (Ens. R., § 7, n°9) si on l'ordonne par inclusion, et admet donc d'après le th. de Zorn un élément maximal B . D'après le cor. de la prop.2, tout élément $x \in S$ est algébrique sur K(B) . Donc K(S) est algébrique sur K(B) (§ 3, prop.5) ; et E , étant algébrique sur K(S), est algébrique sur K(B) (§ 3, prop.7) ; donc B est une base de transcendance de E .

Corollaire ("théorème d'échange")- Soit E une extension de K, T une partie de E telle que E soit algébrique sur K(T), L une partie algébriquement libre (sur K) de E ; il existe une partie T' de T telle que $L \cup T'$ soit une base de transcendance de E .

On prend en effet $L = L$, $S = L \cup T$.

Remarque - Une extension algébrique F d'une extension transcendante pure E de K peut fort bien être transcendante pure sur K même si $F \neq E$ (cf. § 3, n°1, exemple 2). Ceci montre que l'extension algébrique citée dans le th.1 dépend de la base de transcendance choisie, et n'est nullement bien déterminée, même à un isomorphisme près.

3) - Degré de transcendance d'une extension.

Théorème 3 - Deux bases de transcendance B et C d'une même extension E de K sont équipotentes.

Nous distinguerons deux cas suivant que B est un ensemble fini ou infini.

a) B fini - Soit n le nombre d'éléments de B . Nous procèderons par récurrence sur n , la propriété étant évidente pour n=0 . Soit x un élément de C tel que $x \notin B$. Par le théorème d'échange nous trouvons une partie B' de B telle que $B' \cup \{x\}$ soit une base de transcendance de E ; il est clair que B' a au plus n-1 éléments ; B' et $C' = C \cap \{x\}$ sont des bases de transcendance de E sur K(x) . D'après la récurrence C' a au plus n-1 éléments, donc C a au plus n éléments. Il suffit alors d'échanger les rôles de B et de C pour voir qu'ils ont le même nombre d'éléments.

b) B infini - Il nous suffit de montrer que C a une puissance au moins égale à celle de B . Tout $x \in C$ est algébrique sur K(B) ;

dans les expressions des coefficients du polynome minimal de x sur $K(B)$ figurent seulement un nombre fini d'éléments de B ; soit F_x la partie finie de B constituée par ces éléments, et soit $F = \bigcup_{x \in C} F_x$. Tout $x \in C$ est algèbrique sur $K(F)$, donc $K(C)$, et par conséquent E sont algèbriques sur $K(F)$ (§ 3, prop. 5 et 7). Puisque $F \subset B$, F est identique à B (déf. 3). La puissance de B est donc au plus égale à celle de l'ensemble somme (Ens. R., § 4, n° 5) de la famille (F_x), qui est lui-même équipotent à une partie de l'ensemble produit $C \times N$; or $C \times N$ est équipotent à C (Ens. R, § 7, n° 7) puisque C est infini d'après a) ; donc B est équipotent à une partie de C .

Définition 4 - Soit E une extension d'un corps K , admettant une base de transcendance finie. Le nombre d'éléments d'une quelconque des bases de transcendance de E est appelé le degré de transcendance ou la dimension algèbrique de E (sur K), et noté $\dim_K E$.

$\dim_K E = 0$ caractérise les extensions algèbriques de K . Lorsque E admet une base de transcendance infinie, on dit que son degré de transcendance (ou sa dimension algèbrique) (sur K) est infini. Lorsque E et F sont deux extensions quelconques de K , on dira que le degré de transcendance de E est inférieur ou au plus égal (resp. égal, strictement inférieur) à celui de F , si la puissance d'une quelconque des bases de E est inférieure ou au plus égale (resp. égale, strictement inférieure) à celle d'une des bases de F .

D'après le th.2, toute extension de type fini de K a un degré de transcendance fini sur K .

2 On aura soin de ne pas confondre le degré de transcendance (ou dimension algèbrique) de E sur K , avec le degré (ou dimension linéaire) de E sur K , qui est toujours infini si $\dim_K E \neq 0$ (§ 3, th.1) .

Théorème 4 - Soit E une extension de K, F une extension de E . Si deux des nombres $\dim_K E$, $\dim_K F$, $\dim_E F$ sont définis, il en est de même du troisième et on a :

(1) $$\dim_K F = \dim_K E \cdot \dim_E F .$$

D'après la déf.4, ce théorème résultera de la proposition plus précise suivante :

Proposition 5.- Soit E une extension de K, F une extension de E . Si M est une base de transcendance de E sur K , et N une base de transcendance de F sur E , on a $M \cap N = \emptyset$, et $M \cup N$ est une base de transcendance de F sur K .

En effet N est une base de transcendance de F sur K(M) (prop.4). La prop.5 résulte donc de la prop.2, en tenant compte du fait que F est algèbrique sur K(M)(N) .

§ 5 - Extensions composées.

Soit K un corps, Ω un surcorps de K . Nous nous proposons d'étudier les extensions de K contenues dans Ω . Si E et F sont deux telles extensions, le corps $E(F) = F(E) = K(E \cup F)$ n'est autre que la borne supérieure de E et F dans l'ensemble des sous-corps de Ω , ordonné par inclusion ; on dit encore (par abus de langage) que ce corps est l'extension de K composée des extensions E et F .

On aura soin de ne pas confondre cette notion avec celle de composé direct de deux anneaux (chap.I, § 8, n° 11).

Si G est un corps tel que $K \subset G \subset E$, on a $K(E \cup F) = G(E \cup F) = G(F)(E)$; autrement dit $K(E \cup F)$, considéré comme extension de G , est composé des extensions G(F) et E .

1)- Corps linéairement disjoints.

Proposition 1 - Soient E et F deux extensions de K contenues dans A (resp. B) un sous-anneau de E (resp.F) contenant K , et admettant E (resp. F) pour corps des quotients.

a) Si C est le plus petit sous-anneau de Ω contenant $A \cup B$, le corps composé $K(E \cup F)$ est le corps des quotients de C .

b) Si (b_μ) est une base linéaire de B sur K , l'anneau C est identique à l'ensemble des combinaisons linéaires $\sum_\mu a_\mu b_\mu$ où $a_\mu \in A$; il est isomorphe à un anneau quotient du produit tensoriel $A \otimes B$ des algèbres A et B sur K .

c) Pour que E et F soient linéairement disjoints sur K , il faut et il suffit que A et B soient linéairement disjoints sur K .

a) est évidente. Puisque le produit de deux éléments de la base (b_μ) est une combinaison linéaire des b_μ à coefficients dans K , l'ensemble des combinaisons linéaires $\sum_\mu a_\mu b_\mu$, à coefficients $a_\mu \in A$ est un anneau ; comme il contient B , donc K , il contient aussi A et par filtre C ; étant évidemment contenu dans C , il lui est identique ; le reste de b) résulte immédiatement du n°3, § 3,chap.III . Enfin, si E et F sont linéairement disjoints sur K, (chap.III,§ 3,n°3) il en est de même évidemment de A et B ; si, réciproquement, A et B sont linéairement disjoints sur K,A et F le sont aussi car, si une famille d'éléments de Ω est libre sur B , elle est libre sur son corps des quotients F (chap.III, § 2,prop.5) ; le même raisonnement prouve ensuite que E et F sont linéairement disjoints sur K , ce qui achève la démonstration.

Proposition 2 - Soit E une extension quelconque de K , F une extension algébrique de K . L'anneau C engendré par E et F est un corps, identique à E(F) , et algébrique sur E ; si, le nombre $[F:K]$ est défini, il en est de même de $[E(F):K]$ et on a $[E(F):E] \leq [F:K]$; pour que l'on ait

$[E(F):E] = [F:K]$ il faut et il suffit que E et F soient linéairement disjoints sur K .

E(F) est algèbrique sur E (§ 3, prop.2 et 5), donc son sous-anneau C est un corps (§ 3, prop.2), évidemment identique à E(F). Puisqu'une base de F sur K est un système de générateurs de C sur F (prop.1, b)), l'inégalité est démontrée. Le reste se déduit immédiatement du th.4, § 3, chap.III.

Corollaire - Si E et F sont deux extensions algébriques de K , le corps composé K(E ∪ F) est algèbrique sur K . On a $[K(E \cup F):K] \leq [E:K][F:K]$ lorsque le second membre est défini. Enfin, lorsque les nombres $[E:K]$ et $[F:K]$ sont définis, la relation $[K(E \cup F):K] = [E:K][F:K]$ est nécessaire et suffisante pour que E et F soient linéairement disjoints sur K .

Comme $K(E \cup F) = E(F)$ est algèbrique sur E , et E algèbrique sur K, K(E F) est algèbrique sur K (§ 3, prop.7). Le reste se déduit immédiatement de la formule (1), th.1, § 2, et de la prop.2 .

2)- Corps algébriquement disjoints.

Définition 1 - Deux extensions E et F de K sont dites algébriquement disjointes (sur K) si, quelles que soient les parties A (resp. B) de E (resp. F), algébriquement libres sur K , on a $A \cap B = \emptyset$, et $A \cup B$ est algébriquement libre sur K .

Il est clair que, comme la disjonction linéaire, la disjonction algèbrique est une propriété de caractère fini, c'est-à-dire que E et F sont algébriquement disjointes sur K , si et seulement si, pour tout couple E', F' d'extensions de type fini de K , contenues respectivement dans E et F , E' et F' sont algébriquement disjointes sur K . Remarquons aussi que, si E est algèbrique sur K , E et F sont algébriquement disjointes quel que soit F .

Proposition 3 - Soient E et F deux extensions de K . Une condition nécessaire et suffisante pour que E et F soient algébriquement disjointes, est qu'il existe une base de transcendance C de E qui soit algébriquement libre sur F . Toute partie de E (resp. F), algébriquement libre sur K reste alors algébriquement libre sur F (resp.E) et $E \cap F$ est algébrique sur K .

Si E et F sont algébriquement disjointes et si C (resp.D) est une base de transcendance de E (resp.F), C est algébriquement libre sur K(D) (§ 4,prop.2), donc aussi sur F qui est algébrique sur K(D) (§ 4,prop.3). Si réciproquement C est algébriquement libre sur F , et si A est une partie de F algébriquement libre sur K, C étant a fortiori algébriquement libre sur K(A), on a $B \cap C = \emptyset$ et $B \cup C$ est algébriquement libre sur K , et B est algébriquement libre sur K(C) (§ 4,prop.2) donc sur E qui est algébrique sur K(C) ; si on prend en particulier pour B une base de transcendance de F , on voit, en permutant les roles de E et F , que toute partie A de E , algébriquement libre sur K est aussi algébriquement libre sur F ; appliquant la prop.2, § 4, à A et B on voit que E et F sont algébriquement disjointes. Enfin si un élément de $E \cap F$ était transcendant sur K , il formerait une partie de E algébriquement libre sur K mais non sur F .

Corollaire 1 - Si E et F sont algébriquement disjointe sur K , les fermetures algébriques E' et F' de E et F dans Ω sont algébriquement disjointes sur K .

En effet une base de transcendance B de E sur K est aussi base de transcendance de E' sur K ; comme E est algébriquement libre sur F , elle l'est aussi sur F' (§ 4,prop.3) .

Corollaire 2 - Si $\dim_K F$ est finie, on a $\dim_E E(F) \leqslant \dim_K F$; pour que E et F soient algébriquement disjointes sur K, il faut et il suffit que l'on ait $\dim_E E(F) = \dim_K F$.

Soit en effet C une base de transcendance de F sur K ; $E(F) = E(C)(F)$ est algébrique sur $E(C)$ puisque F est algébrique sur $K(C)$, donc E contient une base de transcendance de $E(F)$ sur E (§ 4, th.2) ; et, pour que E et F soient algébriquement disjoints sur K, il faut et il suffit que C soit une base de transcendance de $E(F)$ sur E.

Corollaire 3 - Si les dimensions algébriques de E et F sur K sont finies on a :

$$\dim_K K(E \cup F) \leqslant \dim_K E + \dim_K F . \tag{2}$$

Pour que E et F soient algébriquement disjoints sur K, il faut et il suffit que l'on ait :

$$\dim_K K(E \cup F) = \dim_K E + \dim_K F .$$

C'est en effet une conséquence immédiate du cor.2 et de la formule (1) du § 4.

3)- Critère de disjonction linéaire.

Les notions d'extensions algébriquement disjointes et d'extensions linéairement disjointes ont des rapports fort étroits. En effet, si B et C sont des bases de transcendance de E et F sur K, dire que $B \cap C = \emptyset$ et que $B \cup C$ est algébriquement libre sur K, signifie, comme on le voit aussitôt, que les algèbres de polynomes $K[B]$ et $K[C]$ sont linéairement disjointes sur K, ou encore (prop.1) que les extensions transcendantes pures $K(B)$ et $K(C)$ sont linéairement disjointes.

Il est donc clair que, si E et F sont linéairement disjointes, elles sont aussi algébriquement disjointes ; mais la réciproque n'est pas vraie, comme le montre le cas où E et F sont identiques à une même extension algébrique de K.

D'autre part, si E et F sont linéairement disjointes sur K , la prop.1 montre que le produit tensoriel $E \otimes F$ (relatif à K) est un anneau d'intégrité (dont le corps des quotients est isomorphe à $K(E \cup F)$) ; mais ici encore cette condition nécessaire n'est pas suffisante comme le montre le cas où E et F sont identiques à une même extension transcendante pure $K(x)$ de K .

Mais en combinant la propriété "$E \otimes F$ est un anneau d'intégrité" (qui ne dépend que des extensions E et F prises isolément) et la propriété de disjonction algèbrique (qui indique la "position relative" de E et F dans le corps Ω), on obtient le critère suivant :

Proposition 4 - Pour que deux extensions E et F de K soient linéairement disjointes, il faut et il suffit que le produit tensoriel $E \otimes F$ (relatif à K) soit un anneau d'intégrité, et que E et F soient algèbriquement disjointes. Le corps composé $K(E \cup F)$ est alors isomorphe au corps des quotients de l'anneau d'intégrité $E \otimes F$.

Nous venons de voir que ces conditions sont nécessaires. On sait (prop.1) que, si C est le sous anneau engendré par $E \cup F$, il existe une représentation φ de l'anneau $M = E \otimes F$ sur C , définie par $\varphi(x \otimes y) = xy$; pour prouver que les conditions sont suffisantes il nous suffira de montrer que φ est un isomorphisme.

Soit A (resp.B) une base de transcendance de E (resp. F) ; comme E et F sont algèbriquement disjointes, $K(A)$ et $K(B)$ sont linéairement disjointes, et par suite l'application φ , restreinte au sous-anneau $N = K(A) \otimes K(B)$ est un isomorphisme de N dans C . Le corps des quotients P de M est une extension algèbrique du corps des quotients $Q \subset P$ de N ; en effet tout élément $x \otimes 1$ $(x \in E)$ (resp. $1 \otimes y$, $y \in F$) est algèbrique sur $K(A) \otimes \{1\}$ (resp. $\{1\} \otimes K(B)$), donc a fortiori sur Q ;

comme tout élément de M est somme de produits d'éléments de cette forme, il est algèbrique sur Q , et par suite aussi tout élément de P . Soit alors z un élément de M tel que $\varphi(z)=0$; par réduction à un même dénominateur des coefficients de son polynome minimal sur Q , on peut écrire $\sum_{i=0}^{n} v_i z^{n-i} = 0$, où $v_i \in M$; de $\varphi(z)=0$, on déduit donc $\varphi(v_n)=0$, donc $v_n=0$ puisque, sur M, φ est un isomorphisme ; le polynome minimal de z , n'ayant pas de terme constant, se réduit donc à X , ce qui prouve que $z=0$, et achève la démonstration.

Corollaire - Soient E et F deux extensions linéairement disjointes de K, σ et τ deux endomorphismes de Ω relatifs à K ; si $\sigma(E)$ et $\tau(F)$ sont algèbriquement disjointes, elles sont linéairement disjointes, et il existe un endomorphisme φ de Ω relatif à K , qui coïncide avec σ sur E et avec τ sur F .

En effet $\sigma(E) \otimes \tau(F)$ est isomorphe à $E \otimes F$, et est donc un anneau d'intégrité ; la prop.4 montre alors que $\sigma(E)$ et $\tau(F)$ sont linéairement disjointes. L'existence de φ résulte alors de la prop. , § ch.III.

Proposition 5 - Toute extension transcendante pure E de K est linéairement disjointe de toute extension F dont elle est algèbriquement disjointe.

Soit $E = K(B)$, B étant algèbriquement libre. D'après la prop.1 il s'agit de montrer que F et $K(B)$ sont linéairement disjoints sur K . Or B étant algèbriquement libre sur F , les monômes par rapport aux éléments de B sont linéairement indépendants sur F ; comme ils forment une base de $K[B]$ sur K , $K[B]$ et F sont linéairement disjoints sur K .

Corollaire 1 - Toute extension transcendante pure est linéairement disjointe de toute extension algébrique de K .

Corollaire 2 - K est algèbriquement fermé dans toute extension transcendante pure E de K .

En effet l'intersection de E avec toute extension algébrique de K se réduit à K d'après le cor.1 .

§ 6.- Théorèmes d'existence.

1)- Le théorème d'immersion.

Soit K un corps, E_λ ($\lambda \in \Lambda$) une famille quelconque d'extensions de K . Nous nous proposons de plonger tous les corps E_λ dans un même corps E . En termes plus précis il s'agit de trouver une extension E de K et des isomorphismes u_λ de E_λ dans E tels que $u_\lambda(a) = a$ pour tout $a \in K$. Nous pourrons évidemment remplacer alors E par le sous-corps de E engendré par les $u_\lambda(E_\lambda)$. Alors l'ensemble composé de E et des isomorphismes u est appelé une extension composée des extensions E_λ .

Remarques - 1) Les extensions composées rencontrées au § précédent rentrent dans le définition donnée ci-dessus, les isomorphismes u étant alors les applications canoniques des sous-corps de Ω dans Ω.

2) Il ne faudrait pas croire qu'une extension composée soit déterminée de façon unique (à un isomorphisme près) par les extensions E . Ainsi, si X_1 et X_2 sont transcendants sur K les corps de fractions rationnelles $K(X,Y)$ et $K(Z)$ sont des extensions composées de $K(X_1)$ et $K(X_2)$, les isomorphismes étant définis par $u_1(X_1) = X$, $u_2(X_2) = Y$ dans le premier cas, par $u'_1(X_1) = u'_2(X_2) = Z$ dans le second.

Théorème 1 - *Soit* K un corps, E_λ ($\lambda \in \Lambda$) *une famille d'extensions de* K . *Il existe une extension* E *de* K *et des isomorphismes* u_λ *des* E_λ *dans* E *tels que* $u_\lambda(a) = a$ *pour tout* $a \in K$, *et que* E *soit engendré par les* $u_\lambda(E_\lambda)$.

Considérons en effet le produit tensoriel $A = \bigotimes_\lambda E_\lambda$ des E_λ considérés comme algèbres sur K (chap.III, §). A est un anneau commutatif ayant un élément unité, et contenant des sous-corps E'_λ ,

ayant même élément unité que A, et isomorphes aux E_λ par des isomorphismes τ_λ. Nous prendrons un idéal maximal $\mathfrak{a}$ de A (chap.I, § 8, th.1). L'anneau quotient $A/\mathfrak{a}$ est un corps (chap.1, § 9,). Puisque l'élément unité de E'_λ coïncide avec celui de A, on a $E'_\lambda \cap \mathfrak{a} = (0)$, et l'homomorphisme canonique φ de A sur $A/\mathfrak{a}$ applique isomorphiquement E'_λ sur son image. Comme les E'_λ engendrent A, les $\varphi(E'_\lambda)$ engendrent $A/\mathfrak{a}$. Nous pourrons donc prendre $E = A/\mathfrak{a}$ et $u_\lambda = \varphi \circ \tau_\lambda$.

Nous identifierons souvent E_λ avec l'extension isomorphe $u_\lambda(E_\lambda)$, et considérerons les surcorps E_λ comme plongés dans un même corps.

2)- Corps de décomposition d'une équation algébrique.

Proposition 1 - Etant donné un polynome f non constant à une indéterminée sur un corps K, il existe une extension algébrique E de K et un élément $x \in E$ tels que $f(x) = 0$.

Autrement dit f, considéré comme élément de $E[X]$, est divisible par $X-x$.

Soit en effet g un facteur irréductible de f dans $K[X]$. L'idéal (g) est maximal (chap.IV, § ,). Si, dans le corps $K[X]/(g)$, on désigne par x la classe de X mod.g, on a $g(x) = 0$, donc $f(x)=0$.

Proposition 2 - Etant donné un polynome non constant f de $K[X]$, il existe une extension algébrique F de K telle que f, considéré comme élément de $F[X]$, se décompose en un produit de polynomes du premier degré.

Soit en effet n le degré de f. Pour toute extension algébrique E de K nous noterons f_E le polynome de $E[X]$ obtenu comme quotient de f par le produit des facteurs du premier degré de f dans $E[X]$; soit n_E le degré de f_E. Si g est un facteur irréductible de f_E dans $E[X]$, et si $E' = E[X]/(g)$, $f_{E'}$ est un diviseur de f_E distinct de f_E (prop.1), et ainsi $n_{E'} < n_E$. Puisque $n_E < n$, nous arriverons, au bout de $n-1$

opérations au plus, à une extension algébrique (§ 2,prop.7) F de K telle que $n_p = 0$.

Le corps F est appelé un corps de décomposition du polynome f ; f a n racines dans F ; le corps engendré sur K par ces n racines s'appelle corps des racines de f ; c'est une extension algébrique de K .

3)- Propriétés des corps algébriquement clos.

Proposition 3 - Pour un corps K les quatre propriétés suivantes sont équivalentes :

(AC) Tout polynome non constant de $K[X]$ se décompose en un produit de polynomes du premier degré (dans $K[X]$).

(AC') Tout polynome non constant de $K[X]$ a au moins une racine dans K .

(AC") Tout polynome irréductible de $K[X]$ est du premier degré.

(AC"') Une extension algébrique quelconque de K est identique à K .

(AC"') peut aussi s'énoncer : K est algébriquement fermé dans toute extension.

Montrons d'abord que les propriétés (AC), (AC') et (AC") sont équivalentes. Il est clair que (AC) entraîne (AC") ; (AC") entraîne (AC') car tout polynome non constant de $K[X]$ est divisible par un polynome irréductible, qui, étant du premier degré, admet une racine dans K ; enfin (AC') entraîne (AC) car on déduit de (AC'), par récurrence sur n, que tout polynome de degré n est produit de n polynomes du premier degré (chap.IV, § ,).

Reste à voir que les propriétés (AC') et (AC"') sont équivalentes. Si (AC") est vraie, un élément algébrique sur K est nécessairement de degré 1 sur K (§ 3,th.1), donc appartient à K , ce qui établit (AC"'). Réciproquement, si K a la propriété (AC"') et si f est un polynome irréductible de $K[X]$, le corps $K[X]/(f)$, algébrique sur K , doit être isomorphe à K ; ceci implique que f est de degré 1 et que K a la propriété (AC") .

Définition 1 - On dit qu'un corps est algébriquement clos s'il possède les quatre propriétés (AC), (AC'), (AC"), (AC"').

On se gardera bien de confondre les notions de corps algébriquement clos et de corps algébriquement fermé dans une extension donnée (§ 3, déf. 4).

On déduit de la prop.3 les corollaires suivants :

Corollaire 1 - Si K est un sous-corps du corps algébriquement clos E, la fermeture algébrique F de K dans E est un corps algébriquement clos.

En effet tout polynome de $F[X]$ a une racine dans E ; celle-ci, étant algébrique sur F, l'est aussi sur K (§ 3, prop.7), et par suite appartient à F.

Corollaire 2 - Si E est une extension algébrique de K telle que tout polynome non constant de $K[X]$ se décompose en un produit de polynomes du premier degré dans $E[X]$, alors E est un corps algébriquement clos.

Remarquons que ce cor. est une propriété plus forte que (AC).

En effet soit L une extension algébrique de E et x un élément de L ; étant algébrique sur E, x est algébrique sur K (§ 3, prop.7) ; soit $f \in K[X]$ un polynome tel que $f(x)=0$; d'après l'hypothèse, $f(X) = a \prod_{i=1}^{n} (X-x_i)$ ($a \in K$, $x_i \in E$). Donc $\prod_{i=1}^{n} (x-x_i)=0$, et $x = x_i$ pour certain indice i ; ainsi $x \in E$, et E est algébriquement clos d'après (AC"').

Corollaire 3 - Un corps algébriquement clos K est parfait.

Soit en effet p l'exposant caractéristique de K (§ 1, n°2) ; pour tout $x \in K$ l'équation $X^p - x = 0$ a une racine y dans K, et $y^p = x$.

Exemples - * 1) Le corps C des nombres complexes est algébriquement clos (cf. Top. Gén., chap. VIII, § 1)*.

2) Un corps fini n'est jamais algébriquement clos ; en effet, si $(x_i)_{1 \leq i \leq n}$ est la suite formée de ses éléments, le polynome $f = 1 + \prod_{i=1}^{n} (X-x_i)$ de $K[X]$ ne peut avoir aucune racine dans K.

4)- Existence des corps algébriquement clos.

Nous allons maintenant montrer qu'il existe des corps algébriquement clos ; de façon précise :

Théorème 2 (Steinitz) - Etant donné un corps K , il existe une extension algébrique de K qui est un corps algébriquement clos.

En effet, pour tout polynome $f \in K[X]$, soit D_f un corps de décomposition de f qui soit algébrique sur K (prop.2). Nous plongeons toutes les extensions D_f de K dans une même extension E (th.1) ; E , étant engendré sur K par les extensions algébriques D_f , est algébrique sur K; et le cor.2 de la prop.3 montre que E est algébriquement clos.

Remarque - En particulier tout corps fini admet une extension algébrique algébriquement close E . E est un corps infini ($n^0$3) ; c'est donc une extension algébrique de degré infini de K (car toute extension de degré fini de K est un corps fini).

Une extension algébrique algébriquement close de K s'appelle une clôture algébrique de K .

5)- Unicité de la clôture algébrique. Prolongement des isomorphismes.

Proposition 4 - Soit M une extension algébrique d'un corps L, N une clôture algébrique de L . Il existe un isomorphisme φ de M dans N tel que $\varphi(a) = a$ pour tout $a \in L$.

Au moyen du th.1 nous pouvons construire un corps E contenant N et un isomorphisme φ de M dans E tel que $\varphi(a) = a$ pour tout $a \in L$. E étant engendré par $\varphi(M)$ et N est algébrique sur L , donc sur N ; donc $E = N$ (prop.3) .

Si M est aussi une clôture algébrique de L , il en est de même de $\varphi(M)$; on a donc aussi $\varphi(M) = N$, et

Théorème 3 (Steinitz) - Deux clôtures algébriques d'un corps L sont isomorphes.

Nous allons maintenant montrer, de façon plus générale, que toute extension algébriquement close E d'un corps K a la propriété de contenir (à un isomorphisme près) toute extension de K dont le degré de transcendance est au plus égal à celui de E ; de façon précise :

Théorème 4 (Steinitz) - Soit γ un isomorphisme d'un corps K' sur un corps K . Soient E une extension algébriquement close de K, F' une extension de K' dont le degré de transcendance soit au plus égal, à celui de E. Dans ces conditions il existe un isomorphisme de F' dans E qui prolonge γ.

Soit $(a'_\lambda)_{\lambda \in \Lambda}$ une base de transcendance (§ 4, n°2) de F' . Nous prenons dans E une famille algébriquement libre $(a_\lambda)_{\lambda \in \Lambda}$ équipotente à Λ . Soit $L' = K'((a'_\lambda))$, $L = K((a_\lambda))$. En remplaçant, dans chaque fraction rationnelle $u((a'_\lambda)) \in L'$, les a'_λ par les a_λ et chaque coefficient $c' \in K'$ par $\gamma(c') \in K$, on obtient un isomorphisme de L' sur L, qui prolonge γ et que nous noterons encore γ par abus de langage. F' est alors une extension algébrique de L' . Soit M la fermeture algébrique de L dans E ; M est un corps algébriquement clos (cor.1 de la prop.3). La prop.6, § 3, nous fournit une extension algébrique F de L et un isomorphisme de F' sur F , prolongeant γ , et que nous noterons encore γ . D'après la prop.4 il existe un isomorphisme φ de F dans M tel que $\varphi(a) = a$ pour tout $a \in L$. Il est clair que l'isomorphisme $\varphi \circ \gamma$ de F' dans M , donc dans E , répond aux conditions requises.

Corollaire - Deux extensions algébriquement closes E et E' d'un corps K , de même degré de transcendance, sont isomorphes.

En effet, si M et M' sont des bases de transcendance de E et E' , elles sont équipotentes, et K(M) et K(M') sont isomorphes. Nous sommes donc ramenés au cas traité au th.3 .

Nous dirons qu'une extension Ω de K est une extension universelle pour une famille $(E_\lambda)_{\lambda \in \Lambda}$ d'extensions de K, si, pour tout $\lambda \in \Lambda$, il existe un isomorphisme u_λ de E_λ dans Ω laissant K invariant. La prop.4 montre que la cloture algèbrique de K est extension universelle pour la famille des extensions algèbriques de K. Le th.4 montre que la cloture algèbrique de l'extension transcendante pure $K((X_n))$ $(n \in \mathbb{N})$ est extension universelle pour la famille des extensions de K dont les bases de transcendance sont finies ou dénombrables, et a fortiori pour la famille des extensions de type fini de K.

§ 7 - Isomorphismes. Dérivations. Séparabilité.

1)- Isomorphismes relatifs à un sous-corps. Eléments conjugués.

Définition 1 - Soit K un corps, E et F deux extensions de K. On dit qu'un isomorphisme de E dans F est un isomorphisme relatif à K, ou un K-isomorphisme, s'il laisse invariant tout élément de K.

Remarquons qu'un K-isomorphisme est un isomorphisme pour les structures d'extension de E et F (§ 2, n° 1). Si F = E nous parlerons de K-endomorphismes de E.

Il est clair que, si f est un isomorphisme quelconque de E dans un corps F contenant E, l'ensemble des éléments de E invariante par f est un sous corps K de E ; f peut donc être considéré comme un K-isomorphisme de E. En particulier le seul isomorphisme du corps premier P de F dans F est l'automorphisme identique de P.

Rappelons (§ 6, n° 1) que, étant donnée une famille (E_λ) d'extensions d'un corps K, on peut les plonger dans une même extension Ω de K. Donc, sauf mention expresse du contraire, les corps que nous considérerons dans le reste de ce chapitre seront des extensions d'un même corps K, toutes contenues dans une même extension algébriquement close Ω de K. Pour tout tel corps E nous désignerons par E

sa fermeture algébrique dans Ω (§ , n°3) ; $\mathbb{E}$ est un corps algébriquement clos (§ 6, cor.1 de la prop.3) .

On déduit immédiatement du th.4, § 6, et du th.4, § 4 , la :

Proposition 1 - Si le degré de transcendance de $\mathbb{E}$ sur K est strictement inférieur, ou encore fini et inférieur ou au plus égal, à celui de Ω sur K , tout K-isomorphisme de $\mathbb{E}$ dans Ω se prolonge en un K-endomorphisme de Ω .

Si nous prenons Ω de degré de transcendance infini sur K , la prop.1 s'appliquera donc à toutes les extensions $\mathbb{E}$ de degré de transcendance fini sur K .

Si x est transcendant (resp. algébrique), sur K , tout K-endomorphisme de Ω transforme x en un élément transcendant (resp. algébrique) sur K . Nous allons, étant donnés deux éléments x et y de Ω , étudier à quelles conditions un K-endomorphisme de Ω applique x sur y . Il est clair que x et y doivent être tous deux transcendants, ou tous deux algébriques sur K .

Si x et y sont tous deux transcendants sur K , les corps $K(x)$ et $K(y)$, isomorphes au corps des fractions rationnelles $K(X)$, sont K-isomorphes. Et, d'après la prop.1, ce K-isomorphisme se prolonge en un K-endomorphisme de Ω . Remarquons que, puisqu'on peut prendre pour y tout élément de $K(x)$ non dans K (§ 5, cor.2 de la prop.5), et en particulier $y = x^2$, il existe une infinité d'éléments distincts de Ω qui peuvent être transformés de x par un K-endomorphisme de Ω .

Dans le cas où x est algébrique, nous poserons la définition suivante:

Définition 2 - Deux éléments x et y de Ω , algébriques sur K , sont dits conjugués par rapport à K , s'il existe un K-endomorphisme de Ω appliquant x sur y .

Nous allons voir qu'un élément $x \in \Omega$, algébrique sur K n'a qu'un nombre fini de conjugués. Ceci résultera de la proposition plus précise suivante :

Proposition 2 - Pour que x et y soient conjugués par rapport à K , il faut et il suffit qu'ils aient même polynome minimal f sur K .

Si x et y ont même polynome minimal f sur K , les corps K(x) et K(y) K-isomorphes au corps $K[X]/(f)$ (§ 3,th.1), sont K-isomorphes ; et on déduit aussitôt de la prop.1 que x et y sont conjugués sur K . Si inversement, x et y sont conjugués par rapport à K , et si f et g sont leurs polynomes minimaux sur K , on déduit de $f(x)=0$ et $g(y)=0$, que l'on a $f(y)=0$ et $g(x)=0$; donc (§ 3,th.1) f est un multiple de g , et g un multiple de f ; ce qui prouve que $f = g$ car ils ont, par définition même coefficient dominant égal à 1 .

2)- Eléments p-radiciels.

Les résultats des § 2,4,5,6,7 sont vrais, mais trivialement vrais, lorsque K est un corps d'exposant caractéristique $p = 1$.

Définition 3 - Un élément x est dit p-radiciel sur K , s'il est invariant par tout K-endomorphisme de Ω .

Il est clair que les éléments p-radiciels sur K forment un sous-corps de Ω contenant K ; ce sous corps est le corps des invariants pour la famille $\mathcal{E}$ de tous les K-endomorphismes de Ω (sous-corps de Ω attaché à $\mathcal{E}$ (chap.II, § 5,n°6)). Si x est p-radiciel sur K , il est p-radiciel sur tout surcorps E de K contenu dans Ω . Nous allons maintenant caractériser ces éléments p-radiciels :

Proposition 3 - Soit p l'exposant caractéristique de Ω (§ 1,n°2). Pour que $x \in \Omega$ soit p-radiciel sur K , il faut et il suffit qu'il existe un entier $m \geqslant 0$ tel que $x^{p^m} \in K$; si e est le plus petit de ces entiers, le polynome minimal de x sur K est $X^{p^e} - x$.

La condition est suffisante, car, si σ est un K-endomorphisme de Ω et si $y = \sigma(x)$, on a $y^{p^m} = \sigma(x^{p^m}) = x^{p^m}$; donc (formule (1), § 1) on a $(y-x)^{p^m} = 0$ et $y=x$. Soit réciproquement $x \in \Omega$ et p-radiciel sur K ; si x était transcendant sur K, un K-endomorphisme de Ω le transformerait en $x^2 \neq x$, donc x est algébrique sur K ; soit donc f son polynome minimal et n son degré ; d'après la prop. 2, f ne peut avoir d'autre racine que x, donc $f = (X-x)^n$. Si $n > 1$, x est aussi racine de $f' = n(X-x)^{n-1}$, comme $f' \in K[X]$ et que f est polynome minimal de x, ceci implique que Ω est d'exposant caractéristique $p > 1$ et que n est un multiple de p. Soit p^e la plus haute puissance de p divisant n ; alors $n = n'p^e$, avec $n' \not\equiv 0 \pmod{p}$. On peut alors écrire $f = (X^{p^e} - x^{p^e})^{n'}$; dans f le coefficient de $X^{p^e(n'-1)}$ est $-n'x^{p^e}$; comme $f \in K[X]$ et que n' n'est pas multiple de p, ceci implique $x^{p^e} \in K$; autrement dit x est racine de $X^{p^e} - x^{p^e}$ qui appartient à $K[X]$; donc $n = p^e$, $n'=1$ et $f = X^{p^e} - x^{p^e}$. Puisque f est minimal, on a $x^{p^h} \notin K$ pour tout $h < e$.

Le corps des éléments p-radiciels est donc (ce qui explique son nom), l'ensemble des racines de tous les polynomes $X^{p^e} - a$, où $a \in K$, et où e parcourt l'ensemble des entiers ≥ 0. Un tel polynome (irréductible ou non) n'admet qu'une seule racine dans Ω (car, si $y^{p^e} = z^{p^e}$, on a $(y-z)^{p^e} = 0$, et $y = z$) ; nous désignerons cette racine par $a^{p^{-e}}$ (ou a^{1/p^e}).

Proposition 4 - L'application $a \longrightarrow a^{p^{-e}}$ est un isomorphisme de K sur un sous-corps de Ω contenant K.

En effet, si $x = a^{p^{-e}}$ et $y = b^{p^{-e}}$ $(a \in K, b \in K)$, on a $x^{p^e} = a$, $y^{p^e} = b$, donc $(x+y)^{p^e} = a+b$; il en résulte, par définition, que $x+y = (a+b)^{p^{-e}}$; on vérifie de même que $xy = (ab)^{p^{-e}}$.

Nous désignerons par $K^{p^{-e}}$ l'image de K par l'isomorphisme $a \to a^{p^{-e}}$; c'est une extension algébrique de K , en général de degré infini ; pour $e \leqslant f$, on a $K^{p^{-e}} \subset K^{p^{-f}}$. Le sous-corps de Ω formé des éléments p-radiciels sur K est la réunion des corps $K^{p^{-e}}$ où e parcourt l'ensemble des entiers naturels ; nous le désignerons par $K^{p^{-\infty}}$; c'est une extension algébrique de K .

Proposition 5 - Le corps $K^{p^{-\infty}}$ est le plus petit sous-corps parfait de Ω contenant K (§ 1, n° 2).

En effet l'isomorphisme $x \to x^p$ applique $K^{p^{-e}}$ sur $K^{p^{-e+1}}$, et est donc un automorphisme de $K^{p^{-\infty}}$. Inversement, si P est un sous-corps parfait de Ω contenant K , il contient toutes les racines p-ièmes des éléments de K , quel que soit l'entier naturel e ; donc il contient K.

Corollaire - Pour que les seuls éléments de Ω , p-radiciels sur K , soient les éléments de K , il faut et il suffit que K soit parfait.

Remarque - Si K est imparfait, les corps $K^{p^{-e}}$ sont tous distincts, car alors $K^p \neq K$, et l'isomorphisme $x \to x^{p^{-e}}$ de K sur $K^{p^{-e}}$ applique K^p sur K^{p-e+1} . Le corps $K^{p^{-\infty}}$ est donc toujours une extension de degré infini de K si K est imparfait.

Exemple - Soit K_0 un corps de caractéristique $p > 0$, et $K = K_0(X)$ le corps des fractions rationnelles à une indéterminée sur K_0 . K est imparfait car, dans K , X ne peut être égal à la puissance p-ième d'une fraction rationnelle $f(X)/g(X)$; en effet on aurait $(f(X))^p = X(g(X))^p$, le premier membre ayant un degré multiple de p , et le second un degré non multiple de p .

Définition 4 - On dit qu'une extension E de K est p-radicielle (sur K) si tous ses éléments sont p-radiciels sur K .

Les extensions p-radicielles de K sont donc les extensions de K contenues dans $K^{p^{-\infty}}$; elles sont algébriques sur K . Si A est un ensemble d'éléments radiciels sur K, K(A) est une extension p-radicielle de K .

Proposition 6 - Le degré d'une extension p-radicielle E de degré fini de K est une puissance de p .

Soit $E = K(e_1,\dots,e_n)$; chaque e_i étant p-radiciel sur $K(e_1,\dots,e_{i-1})$ $[K(e_1,\dots e_i):K(e_1,\dots,e_{i-1})]$ est une puissance de p (prop.3) ; la proposition résulte alors de la prop.5, § 3 .

3)- Indépendance linéaire des isomorphismes.

Les k-endomorphismes de Ω (endomorphismes de la structure d'extension de Ω) sont en particulier des endomorphismes de Ω considéré comme espace vectoriel sur K ; afin d'éviter toute confusion nous désignerons par Ω_K l'espace vectoriel sur K sous jacent de Ω , et nous parlerons d'endomorphismes de Ω_K . Les K-endomorphismes de Ω appartiennent donc à l'anneau $\mathcal{L}(\Omega_K)$.

Or $\mathcal{L}(\Omega_K)$ (chap.II, § 5, n°6) est muni d'une structure d'espace vectoriel sur Ω , le produit au d'un élément $a \in \Omega$ et d'un endomorphisme $u \in \mathcal{L}(\Omega_K)$ étant l'endomorphisme $x \longrightarrow au(x)$, produit de u par l'homothétie $y \longrightarrow ay$. Lorsque nous parlerons de combinaisons linéaires, à coefficients dans Ω , d'endomorphismes de Ω_K , et en particulier de K-endomorphismes de Ω , c'est de cette structure d'espace vectoriel qu'il s'agira ; ce sera un endomorphisme de Ω_K de la forme $x \longrightarrow \sum_i a_i u_i(x)$ $(a_i \in \Omega)$. Dire que les u_i sont linéairement indépendants signifie donc que, pour toute famille (a_i) d'éléments de Ω non tous nuls, mais nuls sauf un nombre fini d'entre eux, il existe $x \in \Omega$ tel que $\sum_i a_i u_i(x) \neq 0$.

Soit maintenant V un sous-espace vectoriel de Ω . La restriction à V d'un endomorphisme $u \in \mathcal{L}(\Omega_K)$ est une application linéaire de V dans Ω , c'est-à-dire un élément de $\mathcal{L}(V, \Omega_K)$. Or $\mathcal{L}(V, \Omega_K)$ a une structure d'espace vectoriel sur Ω (induite par la structure d'espace vectoriel produit de Ω^V). Nous dirons que les u_i ($u_i \in \mathcal{L}(\Omega_K)$) sont <u>linéairement indépendants dans</u> V, si leurs restrictions à V sont linéairement indépendantes pour la structure d'espace vectoriel sur Ω de $\mathcal{L}(V, \Omega_K)$; il revient au même de dire que, pour toute famille (a_i) d'éléments de Ω non tous nuls, mais nuls sauf un nombre fini d'entre eux, il existe $x \in V$ tel que $\sum_i a_i u_i(x) \neq 0$. Nous noterons $\mathcal{A}_V$ l'ensemble des applications K-linéaires de V dans Ω_K , induites sur V par des combinaisons linéaires de K-endomorphismes de Ω ; $\mathcal{A}_V$ est un sous-espace vectoriel de $\mathcal{L}(V, \Omega_K)$. Nous nous proposons d'étudier le rang de $\mathcal{A}_V$ sur Ω , et la manière dont $\mathcal{A}_V$ est engendré par les restrictions à V des K-endomorphismes de Ω .

<u>Théorème 1</u> (Dedekind) - <u>Soit</u> $(u_i)(i \in I)$ <u>une famille de</u> K-<u>endomorphismes de</u> Ω , <u>et soit</u> E <u>un sous-corps de</u> Ω <u>contenant</u> K . <u>Si les restrictions des</u> u_i <u>à</u> E <u>sont des</u> K-<u>endomorphismes de</u> E <u>dans</u> Ω <u>distincts deux à deux, les</u> u_i <u>sont linéairement indépendants dans</u> E .

Si les restrictions v_i des u_i à E étaient linéairement dépendantes sur Ω , il existerait entre elles une <u>relation primordiale</u> (chap.II, §5,n°4) $\sum_i \mu_i v_i = 0$. On aurait donc $\sum_i \mu_i v_i(x) = 0$ pour tout $x \in E$. Or si $x \in E$ et $y \in E$, on a $xy \in E$ car E est un corps ; on a donc :

$$\sum_i \mu_i v_i(yx) = 0 . \qquad (1)$$

Mais, puisque les v_i sont des isomorphismes de E :

$$\sum_i \mu_i v_i(y) v_i(x) = 0 . \qquad (2)$$

Ainsi les $v_i(y)$ sont coefficients d'une relation linéaire entre les v_i ; comme $\sum_i \mu_i v_i = 0$ est une relation primordiale, il existe, pour tout $y \in E$, un élément $\varphi(y)$ tel que, pour tout $i \in I$, on ait :

$$(3) \qquad \mu_i v_i(y) = \mu_i \varphi(y) \ ;$$

(chap.II, § 5, prop.2). Donc, si α et β sont deux indices distincts de I tels que $\mu_\alpha \neq 0$ et $\mu_\beta \neq 0$, on a $v_\alpha(y) = v_\beta(y)$ pour tout $y \in E$, contrairement à l'hypothèse. Il existe donc un seul indice $\lambda \in I$ tel que $\mu_\lambda \neq 0$; alors on a $u_\lambda = 0$, ce qui est absurde.

Remarque - Le même raisonnement s'applique, plus généralement, au cas où les u_i sont des représentations d'un monoïde multiplicatif E dans le groupe multiplicatif du corps Ω ; dans l'espace vectoriel Ω^E des applications de E dans Ω, les u_i sont linéairement indépendantes si elles sont distinctes deux à deux.

Après cette propriété d'indépendance linéaire dans l'espace $\mathcal{L}(V, \Omega_K)$ (dans le cas où V est un corps), nous allons maintenant étudier la situation dans $\mathcal{L}(V, \Omega_K)$ du sous-espace $\mathcal{A}_V$ engendré par les restrictions à V des K-endomorphismes de Ω. Si u est de la forme $\sum_i a_i \sigma_i$ ($a_i \in \Omega$, σ_i étant un K-endomorphisme de Ω), il est clair que u est induite sur V par une application $K^{p^{-\infty}}$-linéaire dans $\Omega_{K^{p^{-\infty}}}$, de l'espace vectoriel $\overline{V}$ sur $K^{p^{-\infty}}$ engendré par V. Nous allons montrer que, réciproquement, toute application K-linéaire u de V dans Ω_K qui se prolonge en une application $K^{p^{-\infty}}$-linéaire de V, est de la forme $\sum_i a_i \sigma_i$. Ceci résultera de la proposition plus générale suivante :

Proposition 7 - Soit $\mathcal{E}$ un ensemble d'endomorphismes d'un corps L, contenant l'endomorphisme identique, et tel que, si $\sigma \in \mathcal{E}$ et $\tau \in \mathcal{E}$, alors $\sigma \circ \tau \in \mathcal{E}$. Soit N le corps des invariants de $\mathcal{E}$ et $V \subset L$

un espace vectoriel sur $\mathbb{M}$. Dans ces conditions $\mathcal{L}(V, L_{\mathbb{M}})$ est identique à l'ensemble $\mathcal{A}$ des applications induites sur V par les combinaisons linéaires (à coefficients dans L) d'éléments de $\mathcal{E}$.

Soit $(a_\lambda)_{\lambda \in \Lambda}$ une base de V sur $\mathbb{M}$. Pour tout $u \in \mathcal{A}$ considérons l'élément $(u(a_\lambda))$ de l'espace vectoriel L^Λ sur L ; ces éléments forment un sous-espace W de L. Supposons que $\mathcal{A} \neq \mathcal{L}(V, L_{\mathbb{M}})$; cela signifie que $W \neq L^\Lambda$. Pour tout $\sigma \in \mathcal{E}$, soit $\overline{\sigma}$ l'application de L^Λ dans lui-même définie par $\overline{\sigma}((x_\lambda)) = (\sigma(x_\lambda))$; pour tout $u \in \mathcal{A}$ on a $\overline{\sigma}((u(a_\lambda))) = (\sigma(u(a_\lambda)))$, et comme $\sigma \circ u$ appartient à $\mathcal{A}$, on voit que $\overline{\sigma}(W) \subset W$. Par suite le sous-corps de L attaché à W (pour la base canonique de L^Λ) est contenu dans $\mathbb{M}$ (chap.II, § 5, prop.10). Il en résulte que (chap.II, § 5, th.2) il existe un système d'équations de W à coefficients dans $\mathbb{M}$. Puisque $W \neq L^\Lambda$, il existera une famille (b_λ) d'éléments de $\mathbb{M}$, non tous nuls, mais nuls sauf un nombre fini d'entre eux, tels que $\sum_\lambda b_\lambda u(a_\lambda) = 0$ pour tout $u \in \mathcal{A}$; prenant pour u l'endomorphisme identique de L, on en déduit $\sum_\lambda b_\lambda a_\lambda = 0$, contrairement au fait que les a_λ forment une base de V sur $\mathbb{M}$.

Corollaire 1 - Si V est de dimension finie n sur $\mathbb{M}$, le rang dans $\mathcal{L}(V, L_{\mathbb{M}})$ de l'ensemble des restrictions à V d'éléments de $\mathcal{E}$ est égal à n.

En effet ce rang est égal à la dimension de $\mathcal{A} = \mathcal{L}(V, L_{\mathbb{M}})$ sur L, qui est égale à $[V:\mathbb{M}] = n$ (chap.II, § 2, cor.1 de la prop.3).

Corollaire 2 - Soit $V \subset \Omega$ un espace vectoriel de dimension finie sur K. Le rang dans $\mathcal{L}(V, \Omega_K)$ de l'ensemble des restrictions à V des K-endomorphismes de Ω est égal au rang de V sur $K^{p^{-\infty}}$.

Ceci résulte immédiatement du fait que $K^{p^{-\infty}}$ est le corps des invariants de l'ensemble $\mathcal{E}$ de tous les K-endomorphismes de Ω ($n^o 2$).

Remarques - 1) Nous verrons au § suivant que le cor.1 de la prop.7 a pour conséquence immédiate le théorème fondamental de la théorie de Galois.

2) Si V est un sous-espace vectoriel de dimension n de Ω_K, tout ensemble de K-endomorphismes de Ω linéairement indépendants dans V a au plus n élément (th.1).

4)- Extensions séparables.

Nous venons de trouver une borne supérieure du nombre des K-endomorphismes de Ω linéairement indépendants dans un sous-espace V de dimension finie de Ω_K. Mais cette borne supérieure peut ne pas être atteinte, comme le montre le cas où $V \subset K^{p^{-\infty}}$.

Définition 5 - On dit qu'une extension E de K, contenue dans Ω, est séparable (sur K) si, pour tout sous-espace V de Ω_K, contenu dans E et de dimension finie n, il existe n K-endomorphismes de Ω linéairement indépendants dans V.

Il revient au même de dire que, étant donnés n éléments (a_i) de E linéairement indépendants sur K, il existe n K-endomorphismes u_i $(1 \leqslant i \leqslant n)$ de Ω, tels que le système d'équations

$$\sum_i \xi_i u_i(a_j) = 0$$

n'ait que la solution $\xi_i = 0$ dans Ω ; c'est-à-dire que le déterminant $\det(u_i(a_j))$ ne soit pas nul.

La notion de séparabilité est de caractère fini ; pour que E soit séparable sur K, il faut et il suffit que toute extension de type fini de K contenue dans E soit séparable. Il est clair que, si E est séparable sur K, toute extension de K contenue dans E est séparable.

Dire que E est séparable veut dire (cor.2 de la prop.7) que, pour tout sous-espace de dimension finie V de Ω contenu dans E, le rang de V

sur K est égal au rang de V sur $K^{p^{-\infty}}$; autrement dit, toute famille d'éléments de E qui est linéairement libre sur K , le reste sur $K^{p^{-\infty}}$.

Donc :

Proposition 8 - Pour qu'une extension $E \subset \Omega$ soit séparable sur K , il faut et il suffit que E et $K^{p^{-\infty}}$ soient des extensions de K linéairement disjointes.

Corollaire 1 - Toute extension d'un corps parfait K est séparable.

En effet $K^{p^{-\infty}} = K$.

Corollaire 2 - Toute extension transcendante pure d'un corps quelconque K est séparable.

Ceci résulte immédiatement du cor.1 de la prop.5, § 5 .

Corollaire 3 - L'intersection d'une extension séparable et d'une extension p-radicielle de K (contenues dans Ω) est identique à K .

C'est une conséquence du cor. de la prop.5, chap.III, § 2 .

On notera que l'intersection d'une extension E de K avec K peut se réduire à K sans que E soit séparable.

Théorème 2 (Critère de Mac-Lane) - Pour qu'une extension E d'un corps K d'exposant caractéristique p , soit séparable, il faut et il suffit que, pour toute famille finie (a_i) $(1 \leqslant i \leqslant n)$ d'éléments de E , linéairement libre sur K , la famille (a_i^p) soit linéairement libre sur K .

En effet, dire que (a_i^p) n'est pas linéairement libre sur K , équivaut à dire qu'il existe des éléments $b_i \in K$ non tous nuls tels que $\sum_i b_i a_i^p = 0$. Si $c_i = b_i^{p^{-1}}$, ceci s'écrit $\sum_i c_i^p a_i^p = 0$, ou encore $(\S\ 1, n^o 1)$ $\sum_i c_i a_i = 0$, avec les $c_i \in K^{p^{-\infty}}$ non tous nuls ; donc cela veut dire que la famille (a_i) n'est pas linéairement libre sur $K^{p^{-1}}$, et a fortiori sur $K^{p^{-\infty}}$. Réciproquement montrons que, si (a_i^p) est libre sur K, E est linéairement disjointe de $K^{p^{-\infty}}$; en effet de

$\sum a_1 a_1 = 0$, $(a_1 \in K^{p^{-\infty}})$, on déduit, pour un entier f assez grand, que $a_1^{p^f} \in K$, et $\sum_\iota a_1^{p^f} a_1^{p^f} = 0$; puisque, par itération la famille $(a_1^{p^f})$ est libre sur K , ceci implique $a_1 = 0$.

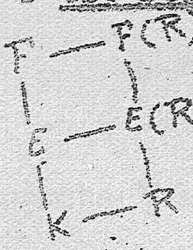
Remarques - 1) La démonstration du th.2 montre que, pour que E soit séparable, il suffit qu'elle soit linéairement disjointe de $K^{p^{-1}}$.

2) La définition de la séparabilité paraît dépendre du corps algébriquement clos Ω dans lequel E est plongée ; le th.2 montre qu'il n'en est rien.

Corollaire - Pour qu'une extension E de K soit séparable, il suffit qu'il existe une base (a_λ) de E sur K telle que la famille (a_λ) soit linéairement libre sur K .

En effet ceci signifie que la famille (a_λ) est libre sur $K^{p^{-1}}$, donc que E est linéairement disjointe de $K^{p^{-1}}$ (th.1, § 3, chap.III).

Proposition 9 - Si E est séparable sur K et F séparable sur E , alors F est séparable sur K .



Il nous suffira de montrer que F est linéairement disjointe de toute extension p-radicielle de degré fini R de K . Or on a (§ 5, prop.2) $[R:K] = [E(R):E]$, et puisque $E(R)$ est extension p-radicielle de E , $[E(R):E] = [F(R):F]$; donc $[R:K] = [F(R):F]$ ce qui prouve (§ 5, prop.2) que F est linéairement disjointe de R .

On notera par contre que, si F est séparable sur K et E une extension de K contenue dans F, F n'est pas nécessairement séparable sur E (sans quoi, comme les corps premiers sont parfaits, il n'y aurait que des extensions séparables !). Nous verrons cependant, au § suivant, que F est séparable sur E lorsque E est algébrique sur K .

5)- Extensions algébriques séparables.

De la prop.1 nous déduisons aussitôt que, si E est une extension algébrique de K contenue dans Ω, tout K-isomorphisme de E dans Ω peut être prolongé en un K-automorphisme de Ω. Si, de plus, E est de degré fini sur K, nous déduisons du th.1 et du cor.2 de la prop.7, le :

Proposition 10 - Si $E \subset \Omega$ est une extension algébrique de degré fini sur K, le nombre des K-isomorphismes de E dans Ω est fini et égal au rang de E sur $K^{p^{-\infty}}$.

Définition 6 - Lorsqu'une extension algébrique $E \subset \Omega$ de K est telle que le nombre des K-isomorphismes de E dans Ω soit fini, ce nombre est appelé facteur séparable du degré de E sur K, et se note $[E:K]_s$.

La raison de cette dénomination apparaîtra plus loin. $[E:K]_s$ est égal au rang de E sur $K^{p^{-\infty}}$; il en résulte immédiatement la :

Proposition 11 - Pour qu'une extension algébrique de degré fini E de K soit séparable, il faut et il suffit que l'on ait $[E:K]_s = [E:K]$.

Remarquons aussi que $[E:K]_s = 1$ caractérise les extensions p-radicielles.

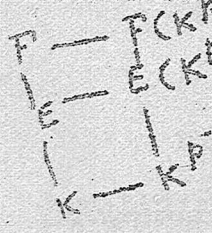
Si E et F sont deux extensions de K (contenues dans Ω), l'espace vectoriel engendré par E sur F (ensemble des $\sum_i e_i f_i$, $e_i \in E$ $f_i \in F$) est identique au sous-anneau de Ω engendré par E et F. Lorsque l'une des deux extensions E,F est algébrique, cet espace vectoriel est identique au corps E(F) (§ 5, prop.1 et 2). Dans le cas où E est algébrique et de degré fini sur K on a donc : $[E:K]_s = [E(K^{p^{-\infty}}):K^{p^{-\infty}}]$. Mais, si $F = E^{p^{-\infty}}$, tout K-isomorphisme de E dans Ω s'étend d'une seule manière à F ; donc $[F:K]_s = [E:K]_s$, ou encore, puisque $F(K^{p^{-\infty}}) = F$, $F = E(K^{p^{-\infty}})$.

Proposition 12 - Si E est algébrique sur K, on a $E^{p^{-\infty}} = E(K^{p^{-\infty}})$, et donc $[E:K]_s = [E^{p^{-\infty}} : K^{p^{-\infty}}]$.

En effet nous venons de le démontrer quand E est de degré fini sur K . Le cas général s'en déduit en considérant E comme réunion d'extensions de degré fini de K .

Corollaire 1 - Toute extension algébrique d'un corps parfait est un corps parfait.

Corollaire 2 - Soit F une extension séparable quelconque de K, E une extension algébrique de K contenue dans F . Alors F est séparable sur E .



Il s'agit de montrer que F et $E^{p^{-\infty}} = E(K^{p^{-\infty}})$ sont linéairement disjointes sur E . Soit (f_λ) une famille d'éléments de F linéairement libre sur E . Supposons que l'on ait, avec $a_\lambda \in E(K^{p^{-\infty}})$, $\sum a_\lambda f_\lambda = 0$; soit (e_i) une base de E sur K ; on peut écrire, puisque $E(K^{p^{-\infty}}) = E\left[K^{p^{-\infty}}\right]$, $a_\lambda = \sum_i e_i x_{i\lambda}$, avec $x_{i\lambda} \in K^{p^{-\infty}}$. On a donc $\sum_{i,\lambda} e_i f_\lambda x_{i\lambda} = 0$; mais la famille $(e_i f_\lambda)$ est linéairement libre sur K , donc sur $K^{p^{-\infty}}$ puisque F est séparable sur K ; donc $x_{i\lambda} = 0$, et a

Corollaire 3 - Soit F une extension algébrique de E, E , F une extension (algébrique) de K ; si deux des trois nombres $\left[E:K\right]_s$, $\left[F:K\right]_s$, $\left[F:E\right]_s$ sont définis, il en est de même du troisième et on a :

$$\left[F:K\right]_s = \left[F:E\right]_s \cdot \left[E:K\right]_s .$$

En effet ces trois nombres sont respectivement égaux à $\left[E^{p^{-\infty}} : K^{p^{-\infty}}\right]$, $\left[F^{p^{-\infty}} : K^{p^{-\infty}}\right]$ et $\left[F^{p^{-\infty}} : E^{p^{-\infty}}\right]$.

Proposition 13 - Si E est une extension algébrique séparable de K , on a $K(E^p) = E$. Réciproquement, si E est une extension algébrique de degré fini de K , telle que $K(E^p) = E$, E est séparable.

En effet considérons d'abord le cas où E est de degré fini n sur K ; soit (a_i) $(1 \leqslant i \leqslant n)$ une base de E sur K ; puisque $a_j^p a_k^p$ est combinaison linéaire des a_i^p avec coefficients dans K ($1, n^0 1$), l'espace vectoriel V engendré sur K par les a_i^p est un sous-anneau de E , donc un

un sous-corps de E (§ 3, prop.2) ; comme il contient E^p , c'est le corps $K(E^p)$. Donc dire que $K(E^p)=E$, équivaut à dire que les a_i^p forment une base de E sur K , c'est-à-dire qu'ils sont linéairement indépendants, ou encore, d'après le critère de Mac-Lane (th.2) et son cor., que E est séparable sur K . Si maintenant E est une extension algébrique séparable de degré infini de K, E est réunion d'extensions F de degré fini ; on a, pour chacune, $K(F^p)=F$; donc $K(E^p)=E$.

Lorsque E est algébrique de degré infini sur K , la condition $K(E^p)=E$ n'est pas suffisante pour que E soit séparable ; par exemple $E^{p^{-\infty}}$ vérifie cette condition

Corollaire - Soit E une extension algébrique séparable de K ; si (a_i) est une base de E sur K , (a_i^p) est aussi une base de E sur K .

En effet la famille (a_i^p) est linéairement libre sur K (th.2) ; d'autre part le raisonnement de la prop.13 montre que l'espace vectoriel engendré par les a_i^p sur K est $K(E^p)$, c'est à dire E .

Proposition 14 (théorème de "l'élément primitif") - Soit E une extension algébrique, séparable, de degré fini d'un corps infini K ; il existe $x \in E$ tel que $E = K(x)$: E est une extension monogène de K .

Soit $n = [E:K]$; il existe n K-isomorphismes distincts $(\sigma_i)(1 \leqslant i \leqslant n)$ de E dans Ω (prop.11). L'ensemble V_{ij} des éléments $y \in E$ tels que $\sigma_i(y) = \sigma_j(y)$ $(i \neq j)$ est un sous-corps de E contenant K , donc un sous-espace vectoriel de E ; les V_{ij} sont, par définition, distincts de E ; donc (chap.IV, § 2, th.2), puisque K est infini, il existe $x \in E$ tel que $x \notin V_{ij}$ pour tout couple (i,j) ; cela signifie que les $\sigma_i(x)$ sont tous distincts. Donc x a n conjugués distincts sur K , et son polynome minimal est de degré n (prop.2) ; donc $[K(x):K] = n = [E:K]$, et $E = K(x)$.

Nous verrons (§ 9) que la prop.14 est encore vraie si K est un corps fini.

6)- Eléments algèbriques séparables.

Définition 7 - On dit qu'un élément $x \in \Omega$, algèbrique sur K , est séparable sur K , si l'extension K(x) est séparable sur K .

Proposition 15 - Pour qu'un élément $x \in \Omega$, algèbrique et de degré n sur K , soit séparable sur K , il faut et il suffit qu'il ait n conjugués distincts sur K (ou, ce qui revient au même, que toutes les racines de son polynome minimal sur K soient simples).

Cette proposition est une conséquence immédiate de la prop.2, de la déf.7 et de la prop.11, puisqu'un K-isomorphisme de K(x) est déterminé par sa valeur pour l'élément x , et que $\left[K(x):K\right] = n$.

Corollaire 1 - Si un polynome $f \in K[X]$ n'a que des racines simples dans Ω , ces racines sont séparables sur K .

En effet tout facteur irréductible de f n'a que des racines simples.

Remarque - Un élément $x \in \Omega$ n'est donc non séparable sur K , que si K est de caractéristique $p > 0$, et si le polynome minimal $f \in K[X]$ de x sur K ne possède de termes non nuls que de degré multiple de p .

On déduit en particulier du cor.1 :

Corollaire 2 - Si x est algèbrique séparable sur K , il est séparable sur tout surcorps F de K contenu dans Ω .

Proposition 16 - Pour qu'un élément $x \in \Omega$, algèbrique sur K , soit séparable sur K , il faut et il suffit que $K(x^p) = K(x)$.

En effet, si $E = K(x)$, on a $E^p = K^p(x^p)$, donc $K(E^p) = K(x^p)$, et la proposition résulte de la prop.13 .

Proposition 17 - Si A est une partie de Ω formée d'éléments algèbriques séparables sur K, K(A) est une extension algèbrique séparable de K .

La séparabilité étant une propriété de caractère fini, il nous suffit de montrer que K(A) est séparable lorsque A est finie. Soit n le nombre

d'éléments de A ; nous allons procéder par récurrence sur n ; c'est évident pour $n=1$ (déf.7) ; si $K(A)=K(a_1,..,a_n)$, $K(A)$ est séparable sur $E = K(a_1,...,a_{n-1})$ (cor.2 de la prop.15) ; or E est séparable sur K par hypothèse inductive ; donc K(A) est séparable sur K (prop.9).

Corollaire - Pour qu'une extension algébrique E de K soit séparable il faut et il suffit que tous les éléments de E soient séparables sur K.

Proposition 18 - Pour tout élément $x \in \Omega$, algébrique sur K , il existe un entier $m \geqslant 0$ tel que x^{p^m} soit séparable sur K .

En effet, pour tout entier $m \geqslant 0$, on a $K \subset K(x^{p^{m+1}}) \subset K(x^{p^m}) \subset K(x)$; donc $\left[K(x^{p^m}):K\right]$ est fini et décroissant en fonction de m ; il existe donc m tel que $K(x^{p^{m+1}}) = K(x^{p^m})$, c'est à dire que x^{p^m} est séparable sur K (prop.16).

7)- Eléments séparables d'une extension algébrique.

Soit E une extension algébrique de K ; l'ensemble E_0 des éléments de E qui sont séparables sur K est une extension de K (prop.17). E est une extension p-radicielle de E_0 (prop.18) ; puisque tout K-isomorphisme de E_0 se prolonge d'une seule manière à E , on a $\left[E:K\right]_s = \left[E_0:K\right]_s = \left[E_0:K\right]$ (déf.5). Donc :

Proposition 19 - Dans une extension algébrique E de K, l'ensemble E_0 des éléments de E séparables sur K est une extension séparable de K ; E est p-radiciel sur E_0 ; si l'un des deux nombres $\left[E:K\right]_s$, $\left[E_0:K\right]$ est défini, il en est de même de l'autre et on a $\left[E:K\right]_s = \left[E_0:K\right]$.

Corollaire - $\left[E:K\right]_s$ est un diviseur de $\left[E:K\right]$.

Ainsi est justifié le nom "facteur séparable du degré" donné à $\left[E:K\right]_s$. Le quotient $\left[E:K\right]/\left[E:K\right]_s$ est appelé facteur inséparable du degré ; on en la note $\left[E:K\right]_i$; il jouit évidemment de la même propriété de multiplicativité que $\left[E:K\right]$ et $\left[E:K\right]_s$ (th.1, § 2 et cor.) de la prop. 12).

8)- Bases de transcendance séparantes.

Définition 8 - On dit qu'une base de transcendance B de l'extension E de K est séparante, si E est une extension séparable de K(B).

D'après le cor.2 de la prop.8 et la prop.9, toute extension E de K, qui admet une base de transcendance séparante, est séparable. Mais toute base de transcendance de E n'est pas nécessairement séparante.

Ainsi la base de transcendance $\{X^p\}$ de l'extension transcendante pure K(X).

Et d'autre part il existe des extensions séparables qui n'admettent aucune base de transcendance séparante.

Par exemple soit x un élément de Ω transcendant sur K ; soit E l'extension de K engendrée par les éléments $x^{p^{-n}}$, $n \geqslant 0$. E est séparable, car, si on pose $E_n = K(x^{p^{-n}})$, toute extension de type fini de K contenue dans E est contenue dans une E_n qui est une extension transcendante pure de K, donc séparable. Mais, pour toute base de transcendance $\{y\}$ de E, K(y) est contenu dans une E_n, sur laquelle E est p-radicielle.

On a toutefois la proposition suivante :

Proposition 20 - Soit E une extension séparable de type fini de K. De toute partie finie F de E telle que E = K(F), on peut extraire une base de transcendance séparante de E.

Nous procéderons par récurrence sur le degré de transcendance (fini) d de E, la proposition étant triviale pour d=0. Soit B une base de transcendance quelconque de E contenue dans F. Si on a $K(E^p)=E$, on a a fortiori $K(B)(E^p)=E$, et E est algébrique séparable sur K(B) (prop.13) ; ainsi B est base de transcendance séparante de E. Supposons donc que $K(E^p) \neq E$ (ce qui est d'ailleurs toujours le cas si $d \geqslant 1$; cf. exerc.), et prenons $x \in F$, $x \notin K(E^p)$; x est transcendant sur K.

sans quoi il serait algébrique séparable sur K , et on aurait $x \in K(x^p) \subset K(E^p)$ (prop.16). Nous allons montrer que E est une extension séparable de K(x) .

Soit donc (u_i) $(1 \leqslant i \leqslant n)$ une famille d'éléments de E linéairement libre sur K(x) ; si les u_i^p étaient linéairement dépendants sur K(x), il existerait (chap.III, § 2, prop.5) n polynomes $f_i \in K[x]$ non tous nuls et tels que $\sum_i f_i(x) u_i^p = 0$. Par division euclidienne des exposants par p, les f_i s'écrivant $f_i(x) = \sum_{j=0}^{p-1} h_{ij}(x^p) x^j$, où les coefficients des h_{ij} sont dans K . On a alors $\sum_{j=0}^{p-1} \left(\sum_i h_{ij}(x^p) y_i^p \right) x^j = 0$. Ceci est une équation de degré $< p$ satisfaite par x sur $K(E^p)$; mais comme $x \notin K(E^p)$ et $x^p \in K(E^p)$, x est de degré p sur $K(E^p)$, et on doit avoir $\sum_i h_{ij}(x^p) u_i^p = 0$ pour $0 \leqslant j \leqslant p-1$. Ces quantités sont des combinaisons linéaires, à coefficients dans K des $(x^n u_i)^p$; les $x^n u_i$ étant linéairement indépendants sur K , les $(x^n u_i)^p$ le sont aussi puisque E est séparable sur K . Donc les coefficients des h_{ij} sont nuls et on a $f_i(x)=0$, contrairement à l'hypothèse.

Cela étant, E est une extension séparable de type fini et de degré de transcendance d-1 de K(x) ; on a $E=K(x)(F)$, et, d'après l'hypothèse inductive, nous pouvons extraire de F une base de transcendance séparante C de E sur K(x) ; l'ensemble $B = C \cup \{ x \}$ est alors base de transcendance séparante de E sur K .

Remarque - La prop.20 et le théorème de l'élément primitif (prop.14) montrent que toute extension séparable, de type fini et de degré de transcendance d de K , peut s'écrire K(F), où F est une partie de cette extension, contenant d+1 éléments.

9)- Dérivations dans les corps.

Nous avons défini au chap.IV, 4, la notion de dérivation d'un anneau A . Nous étudierons ici le problème suivant : étant donnés une dérivation D

d'un corps $K \subset \Omega$, et un surcorps $E \subset \Omega$ de K, peut on prolonger D en une dérivation $\overline{D}$ de E ? Lorsque la dérivation D donnée est nulle, $\overline{D}$ sera une dérivation de E considéré comme algèbre sur K (chap.IV, § 4, n°3) ; conformément aux définitions (§ 2, n°1) nous dirons alors que $\overline{D}$ est une dérivation de l'extension E de K.

Toute dérivation D d'une corps K est une dérivation de E considéré comme extension de son corps premier P, car $D(1)=0$ et $D(n.1)=0$;

Si D est une dérivation d'un corps K, on sait (chap.IV, § 4) que D peut se prolonger à tout anneau $K[X_i]_{i \in I}$ de polynomes sur K de la manière suivante : on applique la dérivation D à chaque coefficient du polynome f ; soit f^D le polynome obtenu. Ceci dit nous allons établir une condition de prolongement de D :

Proposition 21 - Soit D une dérivation d'un corps K, $E = K(x_i)_{i \in I}$ un surcorps de K contenu dans Ω, $\mathcal{A}$ l'idéal des relations algèbriques entre les x_i dans $K[X_i]_{i \in I}$ (ensemble des polynomes f tels que $f((x_i))=0$), (u_i) une famille d'éléments de E. Pour qu'il existe une dérivation $\overline{D}$ de E, prolongeant D, et telle que $\overline{D}x_i = u_i$ pour tout i, il faut et il suffit que, pour tout $f \in \mathcal{A}$, l'on ait :

$$(R) \qquad f^D((x_i)) + \sum_i \frac{\partial f}{\partial X_i} u_i = 0$$

La dérivation $\overline{D}$ satisfaisant aux conditions précédentes est alors unique.

La condition (R) est nécessaire car, pour tout $g \in K[X_i]$, on a, d'après les règles de calcul des dérivations :

$$(S) \qquad \overline{D}(g((x_i))) = g^D((x_i)) + \sum_i \frac{\partial g}{\partial X_i} u_i .$$

Inversement, si la condition (R) est vérifiée, et si g et h sont deux polynomes tels que $g((x_i))=h((x_i))$, les seconds membres de (S), ont la même valeur pour g et h car $g-h \in \mathcal{A}$; nous avons donc défini une application de $K[X_i]$ dans lui-même, qui est manifestement une dérivation $\overline{D}$; il suffit alors de prolonger celle-ci au corps des quotients E,

ce qui est possible, et de façon unique (chap.IV, § 4, prop.10) ;

Corollaire 1 - Pour que la condition (R) soit satisfaite pour tout $f \in \mathfrak{a}$, il suffit qu'elle le soit pour les polynomes f_λ d'une base de $\mathfrak{a}$.

En effet tout $f \in \mathfrak{a}$ s'écrit $f = \sum_\lambda \varphi_\lambda f_\lambda$; on a donc $f^D = \sum_\lambda \varphi_\lambda^D f_\lambda + \sum_\lambda \varphi_\lambda f_\lambda^D$ et de même $\frac{\partial f}{\partial x_1} = \sum_\lambda \frac{\partial \varphi_\lambda}{\partial x_1} f_\lambda + \sum_\lambda \varphi_\lambda \frac{\partial f_\lambda}{\partial x_1}$; comme on a $f_\lambda((x_1)) = 0$ par hypothèse, il vient

$$f^D((x_i)) + \sum_i \frac{\partial f}{\partial x_1} u_1 = \sum_\lambda \varphi_\lambda((x_1)).(f^D((x_1)) + \sum_i \frac{\partial f_\lambda}{\partial x_1} u_1) ;$$

d'où le corollaire.

Corollaire 2 - Pour qu'il existe une dérivation $\overline{D}$ de l'extension E de K telle que $\overline{D}x_1 = u_1$, il faut et il suffit que l'on ait, pour tout $f \in \mathfrak{a}$, on ait $\sum_i \frac{\partial f}{\partial x_1} u_1 = 0$.

Appliquons maintenant le critère de la prop.21 à divers types de surcorps E de K :

1) Si $E = K((x_1))$, (x_1) étant algébriquement libre, $\mathfrak{a} = (0)$, et la dérivation D de K se prolonge en une dérivation $\overline{D}$ de E.

2) E est algébrique séparable sur K. Si E est de degré fini sur K, on peut écrire $E = K(x)$ (prop.14) ; si f est le polynome minimal de x sur K, $\mathfrak{a} = (f)$, et (prop.21) on doit avoir $f^D(x) + f'(x)\overline{D}x = 0$. Puisque x est séparable sur K, $f'(x) \neq 0$; donc $\overline{D}x$ est déterminé de façon unique et, s'il a cette valeur, D se prolonge en $\overline{D}$ (cor.1 de la prop.21). Si maintenant E est de degré infini sur K, on prolongera D à tout sous-corps de E de degré fini sur K par le procédé que l'on vient d'indiquer ; d'après l'unicité ces prolongements coïncident là où plusieurs d'entre eux sont définis ; enfin l'application D ainsi obtenue est une dérivation car, si x et y sont deux éléments quelconques de E, $K(x,y)$ est de degré fini sur K, et on a, dans ce corps, $D(x+y) = Dx + Dy$ et $D(xy) = xDy + yDx$. Donc :

Proposition 22 - Toute dérivation D d'un corps K se prolonge, et de façon unique, en une dérivation d'un surcorps algébrique séparable sur

3) E est p-radiciel de degré fini (>1) sur K. Supposons d'abord que $E = K(x)$, et soit $f = X^{p^e} - a$ le polynome minimal de x sur K ; pour que D se prolonge à E, il faut que $f^D(x) + f'(x)\,Dx = 0$, donc $f^D(x) = 0$ puisque $f' = 0$; ainsi le prolongement de D ne sera pas toujours possible. Mais si on prend pour D la dérivation nulle, la condition du cor.2 de la prop.21 sera satisfaite quel que soit Dx. Dans le cas où E n'est pas monogène, il existe un système de générateurs (x_i) $(1 \leqslant i \leqslant n)$ de E sur K tel que $x_n \notin K(x_1, \ldots, x_{n-1}) = L$; on prendra alors la dérivation nulle sur L, que l'on pourra prolonger de façon non triviale à K ; donc :

Proposition 23 - Toute extension p-radicielle de degré fini > 1 d'un corps K admet une dérivation non nulle.

Théorème 3 - Pour qu'une extension de type fini E d'un corps K n'admette que la dérivation nulle, il faut et il suffit qu'elle soit algébrique et séparable.

La suffisance est évidente (prop.22). Soit réciproquement $E = K(x_1, \ldots, x_n)$, et posons $E_0 = K$, $E_i = K(x_1, \ldots, x_i)$ pour tout i $(1 \leqslant i \leqslant n)$. Soit h le plus petit des entiers i tels que $E = E_n$ soit algébrique et séparable sur E_h ; si $h > 0$, $E_h = E_{h-1}(x_h)$ n'est pas algébrique séparable sur E_{h-1} (prop.9). Si x_h est transcendant sur E_{h-1}, il existe une dérivation non nulle de E_h prolongeant la dérivation nulle de E_{h-1}. Si x_h est algébrique sur E_{h-1}, soit F la plus grande extension séparable de E_{h-1} contenue dans E_h (prop.19) ; alors $E_h \neq F$ et E_h est p-radiciel sur F ; donc on peut prolonger à E, de façon non triviale, la dérivation nulle de F (prop.23). On a donc dans les deux cas une dérivation non nulle de l'extension E_h de E, que l'on peut prolonger à E_n (prop.22).

Si E n'est pas une extension de type fini de K , il peut se faire que la seule dérivation de E soit nulle, sans que E soit séparable ; par exemple, si $p > 1$ et si K est imparfait, on peut prendre $E = K^{p^{-\infty}}$; pour tout $x \in E$ il existe $y \in E$ tel que $x = y^p$, donc $Dx = py^{p-1}Dy = 0$, et toute dérivation du corps E est nulle.

Corollaire - Soient f_i $(1 \leqslant i \leqslant n)$ n polynomes de $K[X_1,\dots,X_n]$, x_i $(1 \leqslant i \leqslant n)$ n éléments de Ω tels que $f_i(x_1,\dots,x_n)=0$ pour tout i . Si le déterminant $\det\left(\frac{\partial f_i}{\partial x_j}\right)$ n'est pas nul, l'extension $E=K(x_1,\dots,x_n)$ est algèbrique et séparable.

Soit D une dérivation de l'extension E ; on déduit de $f_i(x_1,\dots,x_n)=0$ que l'on a $\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j} Dx_j = 0$ pour tout i ; d'où, en vertu de l'hypothèse, $Dx_j = 0$ pour tout j ; donc D est nulle.

Les dérivations d'une extension E de K sont des applications K-linéaires particulières de E dans Ω ; il est immédiat qu'elles forment un sous espace vectoriel (sur Ω) de Ω^E ; on déduit du th.3 que :

Proposition 24 - Soit E une extension séparable et de type fini d'un corps K ; si r est la dimension algébrique de E , l'espace des dérivations de E est de dimension linéaire r sur Ω .

Au moyen d'une base de transcendance séparante (prop.20) (x_i) $(1 \leqslant i \leqslant r)$ de E, on est ramené (prop.22) à étudier l'espace des dérivations de l'extension transcendante pure $K(x_1,\dots,x_r)$. Ses dérivations $D_i = \frac{\partial}{\partial x_i}$ sont linéairement indépendantes sur Ω , car, pour tout indice j , on a $D_i x_j = 0$ pour $i \neq j$, et $D_j x_j = 1$; d'une relation $\sum_{i=1}^{r} \lambda_i D_i = 0$, on tire donc $\lambda_j = 0$ pour tout j . Si d'autre part D est une dérivation quelconque de cette extension, et si $Dx_i = a_i$ pour $1 \leqslant i \leqslant r$, posons $D' = D - \sum_{i=1}^{r} a_i D_i$, D' est une dérivation de l'extension, et on a $D'x_i = 0$ pour tout i ; d'où $D' = 0$, ce qui achève la démonstration.

§ 8 - Théorie de Galois.

Nous allons, dans ce § , étudier les K-endomorphismes d'extensions algèbriques de K .

Proposition 1 - Si E est une extension algèbrique de K , tout K-endomorphisme u de E est un automorphisme.

Il s'agit de montrer que $u(E)=E$. Pour tout $x \in E$, soit F_x l'ensemble des conjugués de x sur K qui appartiennent à E ; F_x est un ensemble fini pour tout x , et E est la réunion des F_x lorsque x parcourt E . Pour tout $y \in F_x$, $u(y)$ est conjugué de y donc de x ; donc $u(F_x) \subset F_x$, et puisque F_x est fini et u biunivoque, $u(F_x) = F_x$. Donc $u(E) = E$.

1)- Extensions galoisiennes. Extensions normales.

Définition 1 - Une extension E de K est dite galoisienne, si elle est algèbrique et si K est le corps des invariants de l'ensemble des K-automorphismes de E . L'ensemble des K-automorphismes de E est un groupe, qu'on appelle dans ce cas le groupe de Galois de E (sur K).

Si E est une extension algèbrique quelconque de K , et si F ($K \subset F \subset E$) est le corps des invariants de l'ensemble des K-automorphismes de E , ces applications sont des F-automorphismes, et E est une extension galoisienne de F ;

Proposition 2 - Pour qu'une extension algèbrique E de K soit galoisienne, il faut et il suffit que, pour tout $x \in E$, le polynome minimal f de x sur K ait toutes ses racines simples et contenues dans E (ou encore, se décompose en facteurs distincts du premier degré dans E X) .

Soient (x_i) $(1 \leqslant i \leqslant n)$ les conjugués distincts de x contenus dans E ; les coefficients du polynome $g(X) = \prod_{i=1}^{n} (X-x_i)$ sont invariants par tout K-automorphisme de E , et appartiennent donc à K si E est galoisienne ; on a donc $f = g$, ce qui montre la nécessité. Soit, réciproquement, u un K-isomorphisme de E dans Ω ; pour tout $x \in E$, $u(x)$ est un conjugué de x sur K , donc $u(x) \in E$ (§ 7, prop.2), et par filtre $u(E) \subset E$ et $u(E) = E$.

(prop.1) ; puisque E ne contient, par hypothèse, d'autres éléments p-radiciels sur K que ceux de K , il existe, pour tout $x \in E$, $x \notin K$, un K-automorphisme u de E tel que $u(x) \neq x$; ceci montre que E est une extension galoisienne de K .

La condition de la prop.2 se décompose en deux :

1) Tout élément $x \in E$ étant séparable sur K (§ 7,prop.15), E est séparable sur K (§ 7,prop.17).

2) Tout polynome irréductible de $K[X]$ ayant une racine dans E a toutes ses racines dans E . Nous dirons qu'une extension algébrique E de K ayant cette propriété est une extension normale de K . Donc :

Théorème 1 - Pour qu'une extension algébrique soit galoisienne, il faut et il suffit qu'elle soit normale et séparable.

Remarque - La seconde partie de la démonstration de la prop.2 montre que, pour qu'une extension normale soit séparable, il suffit qu'elle ne contienne d'autres éléments p-radiciels sur K que ceux de K .

Proposition 3 - Soit E une extension algébrique de K . Les propriétés suivantes sont équivalentes :

1) E est une extension normale de K .

2) Tout K-isomorphisme de E dans Ω est un K-automorphisme de E .

3) E est invariant par tout K-endomorphisme de Ω .

En effet la normalité de E veut dire que, avec tout x , E contient tous les conjugués de x (§ 7,prop.2), et la proposition résulte de la définition des éléments conjugués (§ 7,déf.1).

Corollaire - Soit N une extension normale de K, E une extension de K contenue dans N . Tout K-isomorphisme u de E dans Ω peut se prolonger en un K-automorphisme de N .

En effet u peut se prolonger en un K-endomorphisme de Ω (§ 7,prop.1).

Proposition 4 - Soit (N_i) une famille d'extensions normales d'un corps K, contenues dans Ω ; l'intersection $\bigcap_i N_i$ et le corps composé $K(\bigcup_i N_i)$ sont des extensions normales de K.

En effet, pour tout K-endomorphisme f de Ω, on a $f(N_i) = N_i$ pour tout i ; donc, si $N = \bigcap_i N_i$, on a $f(N) \subset N_i$ pour tout i, donc $f(N) \subset N$, et N est normale sur K. D'autre part, si $M = K(\bigcup_i N_i)$, $f(M)$ est engendré par les $f(N_i) = N_i$, donc est identique à M.

De la prop.4 on déduit en particulier que, si E est une extension algébrique quelconque de K, il existe une plus petite extension normale N de K contenant E, l'intersection des extensions normales de K contenant E (il en existe, Ω par exemple) ; nous dirons que N est l'extension normale de K engendrée par E.

Proposition 5 - Soit A un ensemble d'éléments de Ω, algébriques sur K et soit B l'ensemble des conjugués les éléments de A dans Ω. Le corps $K(B)$ est l'extension normale de K engendrée par $K(A)$.

En effet toute extension normale de K contenant A doit contenir B ; d'autre part $K(B)$ est normale sur K car, pour tout K-endomorphisme u de Ω, on a $u(B) \subset B$, donc $u(K(B)) \subset K(B)$.

Corollaire 1 - Si E est une extension algébrique de degré fini de K, l'extension normale N engendrée par E est de degré fini. Si E est séparable, N est galoisienne.

On a en effet $E \subset K(A)$, où A est un ensemble fini ; donc l'ensemble B des conjugués est fini. Si les éléments de A sont séparables sur K, les éléments de B le sont aussi, et $N = K(B)$ est séparable sur K (§7, prop.17).

Corollaire 2 - Si (f_i) est une famille de polynomes de $K[X]$, et A l'ensemble de leurs racines dans Ω, $K(A)$ est une extension normale de K.

En effet l'ensemble des conjugués d'éléments de A est identique à A .

En particulier le <u>corps des racines</u> ($\S 6, n^0 2$) d'un polynome $f \in K[X]$ est normal sur K .

On notera qu'en général, même si f est irréductible dans $K[X]$, le corps $K(x_1)$ obtenu par adjonction à K d'<u>une</u> racine de f dans Ω, n'est pas identique au corps des racines de f . Lorsque f est irréductible dans $K[X]$, et que $K(x_1)$ est identique au corps des racines de f , alors $K(x_1)=K(x_j)$ pour toute racine x_j de f , puisque $K(x_j)$ est transformé de $K(x_1)$ par un K-endomorphisme de Ω ; on dit dans ce cas que $f(X)=0$ est une <u>équation normale</u> ; si en outre les racines de f sont séparables sur K , on dit que f est une <u>équation galoisienne</u>.

2)- <u>Fonctions symétriques des racines d'un polynome</u>. <u>Norme et trace</u>.

Soit K un corps, $E = K(X_1,\dots,X_n)$ le corps des fractions rationnelles à n indéterminées sur K . Nous pouvons écrire $f(Z) = Z^n + \sum_{j=1}^{n} (-1)^j s_j Z^{n-j}$ où $s_j(X_1,\dots,X_n) = \sum_{i_1<i_2<\dots<i_j} X_{i_1},\dots,X_{i_j}$. Le polynome s_j est appelé la <u>fonction symétrique élémentaire</u> de degré j des n indéterminées $X_1..X_n$; on a $s_1 = X_1+\dots+X_n$, $s_n = X_1\dots X_n$. Soit $E = K(s_1,\dots,s_n)$; le polynome $f(Z)$ appartient à $E[Z]$. Donc E est le corps des racines de f sur E , et par conséquent E est une extension normale de E . Puisque les racines X_j de f sont simples, E est une extension <u>galoisienne</u> finie de E .

Toute permutation σ des X engendre un automorphisme de E ; il est clair que les s_j , et donc E , sont invariants par cet automorphisme. Réciproquement tout E-automorphisme de E ne peut que permuter les X_j , et est déterminé par son effet sur eux . Donc le groupe de Galois Γ de E , E est isomorphe au <u>groupe symétrique</u> $\mathcal{S}_n$. Puisque $\mathcal{S}_n$ opère transitivement sur les X_j , ils sont deux à deux conjugués sur E , donc f est <u>irréductible</u> dans $E[Z]$.

D'autre part, puisque E est algébrique sur E , les n fonctions symétri-

D'autre part, puisque M est algébrique sur E, les n fonctions symétriques s_j forment un système algébriquement libre sur K (§ 4, th.4).

Enfin, si nous appelons <u>fonction symétrique</u> des X_i, une fraction rationnelle g des X_i qui reste invariante pour toute permutation des X_i, g appartient à E (déf.1) ; g s'exprime donc sous la forme $g(X_1,\dots,X_n) = \varphi(s_1,\dots,s_n)$, φ étant une fraction rationnelle de n indéterminées ; puisque les s_j sont algébriquement indépendantes, φ est déterminé de façon unique. En résumé :

<u>Proposition 6</u> - <u>Soient</u> K <u>un corps</u>, S_k $(1 \leqslant k \leqslant n)$ n <u>indéterminées</u>. <u>Sur le corps</u> $E = K(S_1,\dots,S_n)$ <u>le polynome</u> $f(Z) = Z^n + \sum_{k=1}^{n} (-1)^k S_k Z^{n-k}$ <u>est irréductible et séparable ; son corps des racines</u> M <u>est une extension transcendante pure</u> $K(X_1,\dots,X_n)$ <u>de</u> K ; <u>c'est une extension galoisienne de</u> E <u>dont le groupe de Galois est isomorphe au groupe symétrique</u> $\mathfrak{S}_n$. <u>Les</u> S_k <u>sont les fonctions symétriques élémentaires des</u> X_i, <u>et toute fonction symétrique des</u> X_i <u>s'exprime rationnellement et de façon unique en fonction des</u> S_k.

<u>Formules de Newton</u>.

Soit $P_a = \sum_{i=1}^{n} (X_i)^a$ la <u>somme des puissances</u> a-ièmes des X_i ; P_a est une fonction symétrique des X_i, que nous nous proposons d'exprimer en fonction des S_j. Considérons le polynome $f(Z) = Z^n - \sum_{j=1}^{n} (-1)^j S_j Z^{n-j} = Z^n - \sum_{j=1}^{n} U_j Z^{n-j}$, en posant $U_j = (-1)^{j+1} S_j$. Nous allons calculer $f'(Z)/f(Z)$ de deux façons différentes dans le <u>corps des séries formelles</u> $M((T))$ à une indéterminée T sur M, en posant $1/Z = T$.

1) Puisque $f(Z) = \prod_{i=1}^{n} (Z - X_i)$, on a $f'(Z)/f(Z) = \sum_{i=1}^{n} 1/(Z-X_i)$; or $\frac{1}{Z-X_i} = \frac{T}{1-X_i T} = T \sum_{a=0}^{\infty} (X_i T)^a$. On a donc :

(1) $f'(Z)/f(Z) = nT + \sum_{a=1}^{\infty} P_a T^{a+1}$.

2) D'autre part $f'(Z) = nZ^{n-1} - \sum_{j=1}^{n} (n-j)U_j Z^{n-j-1} = nZf(Z) + \sum_{j=1}^{n} jU_j Z^{n-j-1}$

On a donc $f'(Z)/f(Z) = nT + \sum_{j=1}^{n} jU_j T^{j+1} \Big/ 1 - \sum_{j=1}^{n} U_j T^j =$

$= nT + T^2 \left(\sum_{j=1}^{n} jU_j T^{j-1} \right) \left(\sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} U_j T^j \right)^i \right)$

Soit $g(T) = \sum_{j=1}^{n} U_j T^j$; on peut alors écrire :

$$f'(Z)/f(Z) = nT + T^2 g'(T) \left(\sum_{i=1}^{\infty} (g(T))^i \right)$$

En caractéristique zéro chaque terme $g'(T)(g(T))^r$ est la dérivée de $\frac{1}{r+1}(g(T))^{r+1}$. On a donc :

(2) $$f'(Z)/f(Z) = nT + T^2 \sum_{i=1}^{\infty} \frac{1}{r} \frac{d}{dT} \left(\sum_{j=1}^{n} U_j T^j \right)^r .$$

Le terme en T^{a+1} a donc un coefficient de la forme

$$\sum_{a_1+2a_2+\ldots+na_n = a} A_{a_1 \ldots a_n} U_1^{a_1} \ldots U_n^{a_n} .$$

Le terme $A_{a_1 \ldots a_n} U_1^{a_1} \ldots U_n^{a_n}$ de ce coefficient ne peut provenir que de la $(a_1+\ldots+a_n)$-ième puissance de $\sum_{j=1}^{n} U_j T_j$. Donc :

(3) $$A_{a_1 \ldots a_n} = \frac{a}{a_1+\ldots+a_n} \frac{(a_1+\ldots+a_n)!}{(a_1)! \ldots (a_n)!} = \frac{(a_1+\ldots+a_{n-1})!\, a}{(a_1)! \ldots (a_n)!}$$

3) En comparant les coefficients de T^{a+1} dans (1) et dans (2), nous voyons que :

(4) $$P_a = \sum_{a_1+2a_2\ldots+na_n=a} A_{a_1 \ldots a_n} U_1^{a_1} \ldots U_n^{a_n} .$$

où $U_j = (-1)^{j+1} S_j$, et où les A sont donnés par la formule (3) . Les formules (4) sont appelées "formules de Newton" . Comme ce sont des formules à coefficients entiers, le fait d'être valables en caractéristique zéro les rend valables en caractéristique quelconque (Chap.IV, § , n°). On déduit de la prop.6 que, si K est un corps quelconque, f un polynome quelconque de $K[Z]$, et $a_1 \ldots a_n$ ses racines dans $K(f(Z) = \prod_{i=1}^{n} (Z-a_i)$ dans $K[Z]$), toute fonction symétrique des a_i , à coefficients dans K , est un élément de K .

Parmi les fonctions symétriques des racines d'une équation, la somme et le produit des racines jouent un rôle particulièrement important. Si x est une racine d'une équation irréductible et séparable, et si (σ_i) $(1 \leqslant i \leqslant n)$ sont les K-isomorphismes distincts de $K(x)$ dans Ω, ces quantités sont respectivement égales à :

$$\sigma_1(x) + \sigma_2(x) + \ldots + \sigma_n(x) \quad \text{et} \quad \sigma_1(x)\sigma_2(x)\ldots\sigma_n(x) .$$

Il est un peu plus commode de se placer une fois pour toutes dans une même extension séparable et de degré fini de K, et de poser la définition suivante :

Définition 2 - Soit E une extension algébrique, séparable et de degré fini n sur K ; soient σ_i $(1 \leqslant i \leqslant n)$ les n K-isomorphismes distincts de E. Pour tout $x \in E$ on appelle norme et trace de x relatives à E et K, et on note $N_{E|K}(x)$ et $Tr_{E|K}(x)$ (ou simplement $N_E(x)$, $Tr_E(x)$, et même $N(x)$, $Tr(x)$ si aucune confusion n'en peut résulter) les éléments : $N_{E|K}(x) = \sigma_1(x).\sigma_2(x)\ldots\sigma_n(x)$, $Tr_{E|K}(x) = \sigma_1(x) + \ldots + \sigma_n(x)$.

Il résulte immédiatement de cette définition que les éléments $N_{E|K}(x)$ et $Tr_{E|K}(x)$ appartiennent à K (car l'extension normale Ω engendrée par E est galoisienne, et tout automorphisme de celle-ci permute les $\sigma_i(x)$), et que les applications $x \to Tr_{E|K}(x)$ et $x \to N_{E|K}(x)$ sont des représentations du groupe additif de E dans celui de K et du groupe multiplicatif E^* de E dans celui de K.

Remarque - Lorsque E est galoisienne, les σ_i sont les éléments du groupe de Galois Γ de E, et on peut considérer l'application $x \to Tr(x)$ comme produite par l'opérateur $\sigma_1 + \ldots + \sigma_n$ de l'algèbre A du groupe Γ par rapport à l'anneau $\mathbb{Z}$ des entiers rationnels ; de façon générale, pour tout $\sum_{i=1}^{n} h_i\sigma_i = \lambda \in A$ et tout $x \in E$, on pose $\lambda.x = \sum_{i=1}^{n} h_i\sigma_i(x)$; cette loi externe définit (avec l'addition dans E) une structure de A-module à gauche sur E.

Lorsque l'on considère les questions multiplicatives, on écrit x^σ de préférence à $\sigma(x)$ pour $\sigma \in \Gamma$; pour tout élément $\lambda = \sum_{i=1}^{m} h_i \sigma_i$ de Δ et tout $x \in E$, on pose : $x^\lambda = \prod_{i=1}^{m} (x^{\sigma_i})^{h_i} = \prod_{i=1}^{m} (x^{h_i})^{\sigma_i}$; alors $N(x) = x^\lambda$ avec $\lambda = \sigma_1 + \ldots + \sigma_n$. Avec cette convention la loi de groupe multiplicatif de E^*, et la loi externe $(\lambda, x) \longrightarrow x^\lambda$, définissent sur E^* une structure de Δ-module à gauche.

Proposition 7 - Soit E une extension séparable de degré fini n sur K ; si F est une extension séparable de degré fini m de E, on a pour tout $x \in F$:

$$N_{F|K}(x) = N_{E|K}(N_{F|E}(x))$$
$$Tr_{F|K}(x) = Tr_{E|K}(Tr_{F|E}(x))$$

En effet, si σ_i $(1 \leqslant i \leqslant n)$ sont les K-isomorphismes de E (prolongés en des automorphismes de K) et τ_j $(1 \leqslant j \leqslant m)$ les E-isomorphismes de F les $\sigma_i \tau_j$ sont mn K-isomorphismes distincts de F. On a donc, pour tout $x \in F$: $Tr_{F|K}(x) = \sum_{i=1}^{n} (\sum_{j=1}^{m} \sigma_i(\tau_j(x))) = \sum_{i=1}^{n} \sigma_i(\sum_{j=1}^{m} \tau_j(x)) = \sum_{i=1}^{n} \sigma_i (Tr_{F|E}(x)) = Tr_{E|K}(Tr_{F|E}(x))$, puisque $Tr_{F|E}(x) \in E$. Démonstration analogue pour les normes.

Corollaire 1 - Pour tout élément $x \in E$, on a :

$$N_{F|K}(x) = (N_{E|K}(x))^m \quad \text{et} \quad Tr_{F|K}(x) = m.Tr_{E|K}(x).$$

Corollaire 2 - Soient E une extension séparable de degré n de K, et x un élément de E de degré m et de polynome minimal $f(z)$ sur K. Si $f(z) = z^m + \sum_{k=1}^{m} a_k z^{m-k}$, on a $N_{E|K}(x) = ((-1)^m a_m)^{n/m}$; $Tr_{E|K}(x) = -\frac{n}{m} a_1$.

Ceci résulte du cor.1 appliqué à $K(x)$ et E.

Au chap.VII, nous retrouverons les notions de trace et de norme comme cas particuliers de notions plus générales s'appliquant à toute algèbre de rang fini sur un corps (en particulier à une extension non séparable).

La trace d'une matrice M (chap.III, § 4, n°5) est la somme des racines de l'équation caractéristique (cf. chap.VI) de M, qui s'écrit $\det(M-ZI) = 0$, I étant la matrice unité.

5)- La théorie de Galois.

Soit N une extension galoisienne d'un corps K, Γ son groupe de Galois. Nous allons, dans ce n° , étudier les corps E intermédiaires entre K et N ($K \subset E \subset N$) ; lorsque nous parlerons de sous-corps (dans ce n° et le suivant), c'est de ces derniers qu'il s'agira.

Remarquons d'abord que N est normal sur tout sous corps E, puisque tout E-endomorphisme de Ω est a fortiori un K-endomorphisme (prop.3) ; d'autre part N est séparable sur E (§ 7, cor.2 de la prop.12) ; donc N est galoisien sur tout sous corps (th.1).

Etant donné un sous-corps E, nous noterons $g(E)$ et appellerons sous-groupe associé de E, l'ensemble des automorphismes de Ω laissant invariant tout élément de E. Etant donné un sous-groupe $\Delta \subset \Gamma$, nous noterons $k(\Delta)$ et appellerons sous-corps associé à Δ, le corps des invariants de Δ. Il est clair que les applications $E \to g(E)$ et $\Delta \to k(\Delta)$ sont décroissantes pour les relations d'inclusion dans les ensembles $\mathcal{G}$ et $\mathcal{K}$ des sous-groupes de Γ et des sous-corps de N. Plus généralement le groupe associé au corps composé $k(\bigcup_i E_i)$ est l'intersection des groupes associés aux E_i ; et le sous-corps associé au sous-groupe engendré par une famille (Δ_i) est l'intersection des sous-corps associés aux Δ_i.

Soit E un sous-corps de N. Puisque N est galoisien sur E, on a :

$$k(g(E)) = E \qquad (1)$$

Il est donc naturel de se demander à quelles conditions g et k établissent une correspondance biunivoque entre $\mathcal{G}$ et $\mathcal{K}$; il faut et il suffit pour cela (Mus.R., § 2, n°12) que $k \circ g$ et $g \circ k$ soient les applications

identiques de g et de $\mathcal{K}$ sur eux-mêmes ; ceci est vrai pour $k \circ g$ d'après (1). D'autre part tout élément de Δ laissent, par définition, tout élément de $k(\Delta)$ invariant, on a :

$$g(k(\Delta)) \supset \Delta \qquad (2)$$

Il nous reste donc à obtenir une condition pour que $g(k(\Delta)) = \Delta$ pour tout sous-groupe $\Delta \subset \Gamma$. Pour cela nous allons démontrer d'abord la proposition suivante :

Proposition 8 (Lemme d'Artin") - Soit L un corps, Δ un groupe d'automorphismes de L,K le corps des invariants de Δ . Pour que soit fini il faut et il suffit que Δ soit d'ordre fini ; et alors $[L:K]$ est égal à l'ordre de Δ .

D'après le théorème de Dedekind (§ 7,th.1), les automorphismes de Δ sont linéairement indépendants dans I ; d'autre part (§ 7,prop.7) ils engendrent linéairement sur L l'espace vectoriel $\mathcal{L}(L,L_K)$; puisque le rang de $\mathcal{L}(L,L_K)$ sur L est fini avec $[L:K]$, et égal dans ce cas à $[L:K]$, la proposition est démontrée.

Corollaire - Soit N une extension galoisienne de K , et Γ son groupe de Galois ; on a $g(k(\Delta)) = \Delta$ pour tout sous groupe fini Δ de Γ .

Soit n l'ordre de Δ ; on a $[N:k(\Delta)] = n$ (prop.8). Mais $k(\Delta)$ est aussi le corps des invariants de $g(k(\Delta))$, donc l'ordre de $g(k(\Delta))$ est aussi égal à n ; et l'inclusion (2) démontre le cor.

L'égalité $g(k(\Delta)) = \Delta$ n'est pas toujours vraie pour des sous-groupes infinis $\Delta \subset \Gamma$. Nous verrons, dans l'appendice, comment on peut caractériser, par l'emploi de la Topologie, les sous-groupes Δ tels que $g(k(\Delta)) = \Delta$.

Nous pouvons maintenant résumer les résultats obtenus :

Théorème 2 (théorème fondamental des extensions galoisiennes) - Soit $\mathbb{N}$ une extension galoisienne finie d'un corps $\mathbb{K}$, Γ son groupe de Galois ; soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbb{N}$ contenant $\mathbb{K}$, $\mathcal{G}$ l'ensemble des sous-groupes de Γ ; pour tout sous-groupe $\Delta \in \mathcal{G}$, soit $k(\Delta)$ son corps des invariants (sous-corps associé à Δ), et pour tout sous-corps $\mathbb{E} \in \mathcal{K}$ soit $g(\mathbb{E})$ le sous-groupe de Γ formé des automorphismes laissant tout élément de $\mathbb{E}$ invariant (sous-groupe associé à $\mathbb{E}$). Alors g et k sont deux applications bijectives décroissantes réciproques de $\mathcal{K}$ sur $\mathcal{G}$ et de $\mathcal{G}$ sur $\mathcal{K}$ respectivement. Pour tout $\mathbb{E} \in \mathcal{K}$, l'ordre de $g(\mathbb{E})$ est égal à $[\mathbb{N}:\mathbb{E}]$, et l'indice $(\Gamma : g(\mathbb{E}))$ est égal au degré $[\mathbb{E}:\mathbb{K}]$.

Le dernier point résulte de la formule $[\mathbb{N}:\mathbb{K}] = [\mathbb{N}:\mathbb{E}][\mathbb{E}:\mathbb{K}]$.

Corollaire 1 - Pour que les sous-corps $\mathbb{E}_1$ et $\mathbb{E}_2$ soient linéairement disjoints sur $\mathbb{K}$, il faut et il suffit que l'on ait :

$$(\Gamma : (g(\mathbb{E}_1) \cap g(\mathbb{E}_2))) = (\Gamma : g(\mathbb{E}_1))(\Gamma : g(\mathbb{E}_2)).$$

En effet $\mathbb{E} = \mathbb{K}(\mathbb{E}_1 \cup \mathbb{E}_2)$ est le sous-corps associé à $g(\mathbb{E}_1) \cap g(\mathbb{E}_2)$ et la relation annoncée équivaut donc à $[\mathbb{E}:\mathbb{K}] = [\mathbb{E}_1:\mathbb{K}][\mathbb{E}_2:\mathbb{K}]$, ce qui est un critère de disjonction linéaire (§ 5, cor. de la prop. 2).

Corollaire 2 - Si $\mathbb{E}$ est une extension algébrique séparable de degré fini de $\mathbb{K}$, il n'existe qu'un nombre fini de corps $\mathbb{F}$ tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$.

En effet l'extension normale $\mathbb{N}$ de $\mathbb{K}$ engendrée par $\mathbb{E}$ est galoisienne et finie (cor. 1 de la prop. 5) ; donc il résulte du th. 2 qu'il n'y a qu'un nombre fini de corps entre $\mathbb{K}$ et $\mathbb{N}$, et a fortiori entre $\mathbb{K}$ et $\mathbb{E}$.

Remarque - Nous pouvons compléter la prop. 6 relative aux fonctions symétriques par la relation

$$[\mathbb{K}(X_1, \ldots, X_n) : \mathbb{K}(s_1, \ldots, s_n)] = n!$$

puisque $n!$ est l'ordre du groupe symétrique $\mathfrak{S}_n$.

4)- Sous-corps conjugués. Sous-corps galoisiens.

Soit N une extension galoisienne d'un corps K, Γ son groupe de Galois, E un sous-corps de N contenant K, et σ un K-automorphisme de N; $\sigma(E)$ est un sous-corps de N que l'on appelle un corps conjugué de E.

Proposition 9 - Soit σ un K-automorphisme de N; pour tout sous-corps E de N et tout sous-groupe Δ de Γ, on a :

$$(3) \qquad g(\sigma(E)) = \sigma g(E)\, \sigma^{-1}.$$

$$(4) \qquad k(\sigma \Delta \sigma^{-1}) = \sigma(k(\Delta)).$$

En effet les propositions suivantes sont équivalentes : $\tau \in g(\sigma(E))$; $\tau\sigma(x) = \sigma(x)$ pour tout $x \in E$; $\sigma^{-1}\tau\sigma(x) = x$ pour tout $x \in E$; $\sigma^{-1}\tau\sigma \in g(E)$ $\tau \in \sigma g(E)\sigma^{-1}$; ceci démontre (3). Pour démontrer (4) il suffit de constater l'équivalence de : $x \in \sigma(k(\Delta))$; $\sigma^{-1}(x) \in k(\Delta)$; $\tau\sigma^{-1}(x) = \sigma^{-1}(x)$ pour tout $\tau \in \Delta$; $\sigma\tau\sigma^{-1}(x) = x$ pour tout $\tau \in \Delta$; $x \in k(\sigma \Delta \sigma^{-1})$.

Remarquons que tout sous-corps E, normal sur K, est galoisien sur K (§ 7, n° 4) ; les sous-corps galoisiens E sont donc caractérisés par $\sigma(E)=E$ pour tout $\sigma \in \Gamma$, c'est à dire, d'après (3), par le fait que $g(E)$ est un sous-groupe distingué de Γ ; (4) montre que, si Δ est distingué, $k(\Delta)$ est galoisien, et réciproquement. Si E est galoisien sur K, tout automorphisme $\sigma \in \Gamma$ induit sur E un automorphisme σ_E ; puisque tout K-automorphisme de E se prolonge à Ω (§ 7, prop. 1), donc à N, l'application $\sigma \longrightarrow \sigma_E$ est un homomorphisme de Γ sur le groupe de Galois de E sur K ; σ_E est l'automorphisme identique si, et seulement si, $\sigma \in g(E)$. Donc :

Proposition 10 - Une condition nécessaire et suffisante pour que E (resp. $k(\Delta)$) soit galoisien sur K, est que $g(E)$ (resp. Δ) soit un sous-groupe distingué de Γ ; le groupe de Galois de E sur K est alors isomorphe à $\Gamma/g(E)$.

Appelons <u>abélienne</u> une extension galoisienne de K dont le groupe de galois est abélien ; on a :

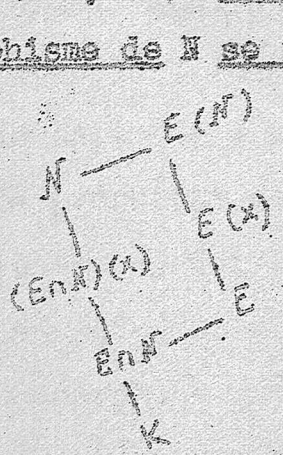
<u>Corollaire 1</u> - <u>Si</u> N <u>est une extension abélienne d'un corps</u> K , <u>tout sous-corps de</u> N <u>est abélien sur</u> K .

On dit qu'une équation irréductible $f \in K[X]$ est abélienne, si le corps des racines de f est abélien sur K . On notera que, dans ce cas, f est une équation galoisienne, car le corps $K(x_1)$ (x_1 étant une racine quelconque de f) est identique à ses conjugués sur K .

<u>Corollaire 2</u> - <u>Soit</u> N <u>une extension galoisienne de degré fini de</u> K , <u>si son groupe de Galois</u> Γ <u>est produit direct de deux de ses sous-groupes</u> Δ_1 <u>et</u> Δ_2 , <u>les sous-corps</u> $K(\Delta_1)$ <u>et</u> $k(\Delta_2)$ <u>sont deux extensions galoisiennes de</u> K , <u>linéairement disjointes, et</u> N <u>est leur extension composée</u> (isomorphe à leur produit tensoriel).

Δ_1 et Δ_2 étant distingués dans Γ , $k(\Delta_1)$ et $k(\Delta_2)$ sont galoisiens sur K . Le reste résulte de $\Delta_1 \cap \Delta_2 = \{e\}$ au moyen de (1), du cor.1 du th.2, et du fait que l'ordre de Γ est égal au produit des ordres de Δ_1 et Δ_2 .

<u>Théorème 3</u> - <u>Soit</u> N <u>une extension galoisienne de</u> K, E <u>une extension quelconque de</u> K . <u>Les corps</u> E <u>et</u> N <u>sont linéairement disjoints sur</u> $E \cap N$, E(N) <u>est une extension galoisienne de</u> E , <u>et tout</u> $(E \cap N)$-<u>automorphisme de</u> N <u>se prolonge d'une seule manière en un</u> E-<u>automorphisme de</u> E(N).



On peut évidemment se borner au cas où $E \cap N = K$, ce que nous supposerons dans la suite de la démonstration. Tout E-isomorphisme de E(N) dans Ω induit sur N un K-automorphisme, donc laisse E(N) globalement invariant ; tout élément de N étant algébrique séparable sur K , donc sur E

(§ 7, prop.15), E(M) est algébrique séparable sur M (§ 7, prop.17) ; donc E(M) est une extension galoisienne de E . La propriété de prolongement des automorphismes résultera du cor. de la prop.4, § 5, lorsque nous aurons démontré la propriété de disjonction linéaire (l'unicité du prolongement étant évidente).

Pour démontrer que E et F sont linéairement disjoints sur K , il suffit de montrer que E est linéairement disjoint de tout sous-corps M de F , contenant K , et fini sur K . Or, d'après le th. de l'élément primitif (prop.14, § 7), nous pouvons écrire $M = K(x)$. Soient x_i ($1 \leqslant i \leqslant n$) les conjugués de x sur E ; puisque x est séparable sur E , son polynome minimal sur E est $f(X) = \prod_{i=1}^{n} (X - x_i)$; or les x_i, étant des conjugués de x sur K , appartiennent à F ; donc les coefficients de f appartiennent à $E \cap F = K$. Puisque f divise le polynome minimal de x sur E , il lui est identique, et on a $[E(x):E] = [K(x):K]$, ce qui démontre que E et $K(x)$ sont linéairement disjoints sur K (cor. de la prop.2, § 5)

(Corollaire - Soient M et N deux extensions galoisiennes de K telles que $M \cap N = K$. Alors M et N sont linéairement disjointes, $K(M \cup N)$ est une extension galoisienne de K dont le groupe de Galois est isomorphe au produit direct $\Gamma_1 \times \Gamma_2$ des groupes de Galois de M et N .

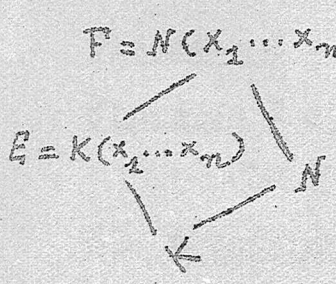
Tout K-endomorphisme de Ω, laissant M et N globalement invariant laisse $K(M \cup N)$ globalement invariant, donc $K(M \cup N)$ est normal sur K (prop.3) ; la séparabilité de $K(M \cup N)$ sur K se déduit immédiatement de celle de M et N (prop.17, § 7) ; donc $K(M \cup N)$ est galoisien sur K . La propriété de disjonction linéaire est une conséquence immédiate du th.3 . Soit Γ le groupe de Galois de $K(M \cup N)$ sur K ; les sous-groupes $g(M)$ et $g(N)$ sont distingués (prop.10), et Γ_1 (resp. Γ_2) est isomorphe à $\Gamma / g(M)$ (resp. $\Gamma / g(N)$) ; si $\sigma \in g(M) \cap g(N)$, σ laisse $K(M \cup N)$ invariant, et est par conséquent l'automorphisme identique ;

le sous groupe engendré par $g(M)$ et $g(N)$ a $M \cap N = K$ pour sous corps associé (relation (1),n°3), et c'est donc Γ . Donc (chap.I, § 6, prop.7) Γ est produit direct de $g(M)$ et $g(N)$. Donc $g(M)$ est isomorphe à $\Gamma / g(N)$, et $g(N)$ à $\Gamma / g(M)$; et par conséquent Γ est isomorphe à $\Gamma_1 \times \Gamma_2$.

5)- Le théorème de la base normale.

Soit N une extension galoisienne, de degré fini n, de K . Nous dirons qu'une base (θ_i) $(1 \leqslant i \leqslant n)$ de N sur K est normale si elle se compose d'un élément θ et de tous ses conjugués. Soit (a_i) $(1 \leqslant i \leqslant n)$ une base quelconque de N sur K , et (σ_i) $(1 \leqslant i \leqslant n)$ les K-automorphismes de N ; on peut écrire $\sigma_i(a_j) = \sum_{k=1}^{n} \gamma_{ijk} a_k$ $(\gamma_{ijk} \in K)$. Pour que les conjugués de $\theta = \sum_{j=1}^{n} \lambda_j a_j$ $(\lambda_j \in K)$ forment une base de N sur K , il faut et il suffit qu'ils soient linéairement indépendants sur K ; puisque $\sigma_i(\theta) = \sum_{j,k} \lambda_j \gamma_{ijk} a_k$, cela veut dire que le déterminant de la matrice des $\mu_{ik} = \sum_j \lambda_j \gamma_{ijk}$ est différent de 0 . Puisque les γ_{ijk} sont donnés, il s'agira de choisir convenablement les λ_j dans K . Nous remarquons d'abord que le déterminant envisagé est un polynome $P(\lambda_1,\ldots,\lambda_n)$ à coefficients dans K ; prenons n indéterminées $X_1,\ldots,X_n$ et considérons le polynome $P(X_1,\ldots,X_n)$; si nous démontrons que $P(X_1,\ldots,X_n) \neq 0$, et si nous supposons que K est infini, nous pourrons trouver $\lambda_1,\ldots,\lambda_n$ dans K tels que $P(\lambda_1,\ldots,\lambda_n) \neq 0$ (chap.IV, § , th.), et par conséquent les conjugués de $\theta = \sum_{j=1}^{n} \lambda_j a_j$ formeront une base normale de N sur K .

Nous avons donc à interpréter $P(X_1,\ldots,X_n)$. Considérons les corps $E = K(X_1,\ldots,X_n)$ et $F = N(X_1,\ldots,X_n)$; E et N sont linéairement disjoints sur K (§ 5,prop.5), donc F est une extension galoisienne de E (th.3), ayant $\{a_1,\ldots,a_n\}$ pour base sur E , et tout automorphisme σ



se prolonge de façon unique en un E-automorphisme de F que nous noterons encore σ . D'après l'analyse précédente la condition $P(X_1,\dots,X_n)\neq 0$ signifie que les conjugués de l'élément $Y_\varepsilon = \sum_{i=1}^{n} a_i X_i$ sont <u>linéairement indépendants</u> sur E .

Ces conjugués sont $Y_\sigma = \sum_{i=1}^{n} \sigma(a_i)X_i$. Puisque le déterminant $\det(\sigma(a_i))$ $(1\leqslant i\leqslant n,\ \sigma\in\Gamma)$ n'est pas nul (§ 7, n°4), les X_i sont des combinaisons linéaires à coefficients dans N des Y_σ (*) ; donc les Y_σ sont <u>algébriquement indépendants</u> sur N , car ils sont en nombre n (§ 4, th. 5). Supposons que les Y_σ ne soient pas linéairement indépendants sur E ; il existe alors n polynomes non tous nuls $u_\sigma \in K[X_1,\dots X_n]$ (chap. III, § 2, prop. 5) tels que $\sum_{\sigma\in\Gamma} u_\sigma(X_1,\dots,X_n)Y_\sigma = 0$. Si nous remplaçons les X_i par leurs expressions en fonction des Y_σ , nous obtenons $\sum_\sigma v_\sigma((Y_\tau))Y_\sigma = 0$ (1), où les v_σ sont des polynomes.

Soit r le plus grand des degrés des polynomes v_σ par rapport à Y_ε (ε : automorphisme identique) et soit π un élément de Γ tel que v_π soit non nul et de degré r par rapport à Y_ε . Nous aurions, dans (1), un terme isolé en Y_ε^{r+1} si nous avions $\pi = \tau$. Afin d'obtenir, en général un tel terme, nous allons <u>appliquer l'automorphisme</u> π^{-1} <u>à la relation</u> (1) ; il vient, puisque $\pi^{-1}(u_\sigma) = u_\sigma$ $(u_\sigma \in K[X_1,\dots,X_n])$ $\sum_\sigma u_\sigma Y_{\pi^{-1}\sigma} = 0$, ou encore $\sum_\sigma u_{\pi\sigma} Y_\sigma = \sum_\sigma v_{\pi\sigma}((Y_\tau))Y_\sigma = 0$. Le terme en $v_\pi((Y_\tau))Y_\varepsilon$ contient un terme $Y_\varepsilon^{r+1} w_\pi$, où w_π est un polynome non nul ne contenant pas Y_ε , terme qui est le seul en Y_ε^{r+1} dans $\sum_\sigma v_{\pi\sigma}Y_\sigma$; on devrait donc avoir $w_\pi = 0$, ce qui est absurde. Donc les Y_σ sont linéairement indépendants sur $E(X_1,\dots,X_n)$. Par conséquent :

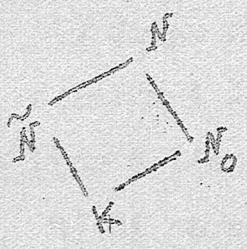
(*) Le lecteur qui a l'esprit tourné vers la géométrie remarquera que nous opèrons un <u>changement linéaire de variables</u> en exprimant les X_i en fonction des Y_σ .

Théorème 4 - *Si K est un corps infini, toute extension galoisienne finie de K admet une base normale.*

Le th.4 est encore vrai lorsque le corps K est fini (cf. § 9, exerc.)

6)- *Extensions normales non séparables.*

Soit N une extension normale de K, $\widetilde{N}$ le corps des invariants du groupe des automorphismes de N, et N_0 la plus grande extension séparable de K contenue dans N (§ 7, n°7).



Puisque tout élément de Ω, qui n'est pas p-radiciel sur K, peut être transformé en un élément distinct par un K-endomorphisme de $\widetilde{N} = N \cap K^{p^{-\infty}}$, et $\widetilde{N}$ est p-*radicielle* sur K. D'autre part N est *galoisienne* sur $\widetilde{N}$ par définition.

Si $x \in N$ est séparable sur K, tout conjugué de x est aussi séparable sur K, donc appartient à N_0 ; ceci montre (prop.5) que N_0 est *normale*, et donc *galoisienne* sur K. N est p-radicielle sur N_0 ; et tout K-automorphisme de N_0 se prolonge de façon unique en un K-automorphisme de N.

N_0 et $\widetilde{N}$ sont *linéairement disjointes* sur K par définition de la séparabilité.

Montrons enfin que $\widetilde{N}$ et N_0 *engendrent* N ; en d'autres termes $N = K(\widetilde{N} \cup N_0) = \widetilde{N}(N_0)$. Soit en effet $x \in N$, et soit M une extension normale contenant x, contenue dans N, et de degré fini sur K (par exemple l'extension normale engendrée par x (cor.1 de la prop.5)) ; on a $N_0 \supset M_0$, $\widetilde{N} \supset \widetilde{M}$; pour montrer que $x \in K(N_0 \cup \widetilde{N})$, il nous suffira donc de montrer que $x \in K(M_0 \cup \widetilde{M})$; or, d'après la propriété de prolongement des automorphismes, les groupes de Galois de M sur $\widetilde{M}$ et de M_0 sur K sont isomorphes ; on a donc $[M_0 : K] = [M : \widetilde{M}]$ (Prop.8), ce qui montre que $M = K(M_0 \cup \widetilde{M})$ (§ 5, cor. de la prop.2).

§ 9 - Exemples : Racines de l'unité, Corps finis, Extensions cycliques.

Nous utiliserons, dans ce §, certains résultats élémentaires de Théorie des Nombres, qui trouveront leur place naturelle au chap. VI. Ces résultats sont les suivants (pour les définitions, voir chap.I, § 8, n° 5, 6 et 7) :

1) Si un nombre entier divise un produit de deux facteurs, et s'il est premier à l'un, il divise l'autre (deux nombres entiers sont dits premiers l'un à l'autre si leur p.g.c.d. est 1).

2) Si un entier a est premier à tout entier (b_i) $(1 \leqslant i \leqslant n)$, il est premier à leur produit.

3) Tout entier est égal à un produit $p_1^{\nu_1} \ldots p_s^{\nu_s}$ de nombres premiers.

4) Toute puissance p^ν d'un nombre premier est première à tout produit de nombres premiers distincts de p.

5) Si $a = p_1^{\lambda_1} \ldots p_s^{\lambda_s}$ et $b = p_1^{\mu_1} \ldots p_s^{\mu_s}$, les p_i étant premiers, le p.p.c.m. de a et de b est $c = \prod_{i=1}^{s} p_i^{\max(\lambda_i, \mu_i)} = \prod_{i=1}^{s} p^{\nu_i}$.

Pour le lecteur qui ne voudrait pas se reporter au chap.VI ou qui craindrait un cercle vicieux, voici les démonstrations succintes de ces propriétés :

1) Si pgcd.$(a,b)=1$, on a pgcd.$(ac,bc)=c$; donc si a divise bc il divise c, puisqu'il divise ac. 2) Si a est premier à b_1, il existe des entiers m_i et n_i tels que $n_i b_i = 1 + m_i a$; par multiplication $\prod_{i=1}^{s} n_i \prod_{i=1}^{s} b_i$ est de la forme $1 + ma$, donc $\prod_{i=1}^{s} b_i$ est premier à a. 3) se démontre par récurrence sur a, en remarquant que tout diviseur minimal > 1 d'un entier est premier. 4) se déduit de 2) par récurrence sur ν, en remarquant que deux nombres premiers distincts sont premiers entre eux. 5) Il est clair que c est un multiple de a et de b et que tout multiple m de a et de b est multiple de $p_i^{\nu_i}$; on montre alors, par récurrence sur s, que m est un

multiple de $\prod_{i=1}^{s} p_i^{\nu_i}$: en effet m est un multiple de $e = p_s^{\nu_s}$ et de $f = \prod_{i=1}^{s-1} p_i^{\nu_i}$ qui sont premiers entre eux ; on a ainsi $m = ee' = ff'$; mais, d'après 1), f' est multiple de e , donc m est multiple de ef .

1)- Racines de l'unité.

Définition 1 - On dit qu'un élément x d'un corps K est une racine de l'unité, s'il existe un entier $n \geqslant 0$ tel que $x^n = 1$; pour tout entier n tel que $x^n=1$ on dit que x est racine n-ième de l'unité.

Il revient au même de dire que les racines de l'unité sont les éléments d'ordre fini du groupe multiplicatif K^* des éléments non nuls de K . Les racines de l'unité, et les racines n-ièmes de l'unité forment évidemment des sous-groupes de K^*. Etant donné une racine de l'unité x , l'ensemble (non réduit à $\{0\}$) des entiers n tels que $x^n=1$ est un idéal de Z , c'est-à-dire l'ensemble des multiples d'un entier $m > 0$; m est, conformément à la terminologie de la théorie des groupes (chap.I, § 6, n°7) appelé l'ordre de x .

Si p est la caractéristique de K, et si $x \in K$ est une racine de l'unité, son ordre n'est pas un multiple de p (c'est-à-dire est premier à p) ; en effet on tirerait de $x^{mp} = (x^m)^p = 1$, que l'on a $x^m = 1$ avec $m < mp$.

Les racines n-ièmes de l'unité sont les racines du polynome X^n-1 ; elles sont donc algèbriques sur le corps premier P ; il nous suffira donc de considèrer tous les corps envisagés dans ce n° comme contenus dans la cloture algèbrique $\overline{P}$ de P ; comme celle-ci est unique à une isomorphie près, ceci ne restreindra pas la généralité des résultats obtenus. Lorsque n est premier à p, la dérivée nX^{n-1} de X^n-1 n'a pas de racine commune avec X^n-1 ; il y a donc exactement n racines n-ièmes distinctes de l'unité dans $\overline{P}$. Comme P est parfait (§ 1, et cor.1 de la prop.8 a Z/(n) ; les racines de l'unité sont séparables sur P .

a un diviseur

Nous allons d'abord étudier la structure du groupe des racines n-ièmes de l'unité dans P .

Théorème 1 - Si n est premier à la caractéristique p de P , les racines n-ièmes de l'unité dans P forment un groupe cyclique à n éléments.

Lemme - Si un groupe abélien G contient deux éléments α et β d'ordre a et b , il contient un élément ayant pour ordre le ppcm de a et b .

Soient $a = p_1^{\lambda_1} \dots p_m^{\lambda_m}$, $b = p_1^{\mu_1} \dots p_m^{\mu_m}$ des expressions de a et b en produits de nombres premiers, certains exposants λ ou μ pouvant être nuls ; si $\nu_i = \max(\lambda_i, \mu_i)$ le ppcm. de a et b est $p_1^{\nu_1} \dots p_m^{\nu_m}$; puisque $p_i^{\nu_i}$ divise a ou b, soit par exemple $p^{\nu_i} c = a$, G contient un élément d'ordre $p_i^{\nu_i}$ qui est a^c . Comme $p_i^{\nu_i}$ est premier à $\prod_{j \neq i} p_j^{\nu_j}$, il nous suffira, pour montrer par récurrence qu'il existe dans G un élément d'ordre $\prod_i p_i^{\nu_i}$, de prouver que, si γ et δ sont des éléments de G d'ordres premiers entre eux c et d , il existe dans G un élément d'ordre cd ; en effet on a $(\gamma\delta)^{cd} = 1$; et si $(\gamma\delta)^n = 1$, on a $\delta^{nc} = 1$, donc $nc = kd$; comme c et d sont premiers entre eux, n est multiple de d ; de même n est multiple de c ; donc n est multiple de cd .

Soit maintenant G le groupe des racines n-ièmes de l'unité dans P , et soit m le plus grand des ordres des éléments de G ; si q est l'ordre d'un élément de G , on a, d'après le lemme, ppcm.$(m,q) = m$, donc q divise m . D'autre part m divise n ; mais, comme il y a exactement n racines n-ièmes et m racines m-ièmes de l'unité dans P , ceci implique $m = n$. Si a est un élément d'ordre m dans G , le sous-groupe cyclique engendré par a aura n éléments, et sera donc identique à G .

Remarques - 1) Une racine n-ième de l'unité dont l'ordre est n s'appelle racine primitive n-ième de l'unité. Ce sont donc les générateurs du groupe cyclique G ; celui-ci est isomorphe à $\mathbb{Z}/(n)$; or la classe $m \pmod{n}$ d'un entier m qui a avec n un diviseur

commun $d > 1$, est telle que $(n/d)m=0$ dans $Z/(n)$; donc les générateurs du groupe cyclique $Z/(n)$ ne peuvent être que des classes (mod.n) d'entiers premiers à n ; or celles-ci sont d'ordre n dans $Z/(n)$ d'après la propriété 1). Si nous désignons donc par $\varphi(n)$ le nombre des entiers m $(1 \leqslant m \leqslant n)$ premiers à n (l'indicateur d'Euler de n), il existe $\varphi(n)$ racines primitives n-ièmes de l'unité dans P. Comme l'ordre de toute racine n-ième de l'unité est un diviseur d de n et qu'il existe des racines primitives d-ièmes pour tout d (th.1) on a :

$$n = \sum_{n \equiv 0 \ (d)} \varphi(d)$$

2) Cherchons maintenant la structure du groupe G_p de toutes les racines de l'unité dans un corps F de caractéristique p . Soit $\lambda(n)$ le produit des n premiers nombres >0 premiers à p ; considérons les groupes H_n des racines $\lambda(n)$-ièmes de l'unité ; on a $H_{n+1} \supset H_n$, $G_p = \bigcup_n H_n$. Nous construisons, par récurrence sur n , une suite (a_n) de générateurs des H_n telle $a_n = (a_{n+1})^{\nu(n+1)}$ où $\nu(n+1) = \dfrac{\lambda(n+1)}{\lambda(n)}$ est le (n+1)-ième nombre premier à p . Soit S_p le sous-groupe du groupe additif de Q composé des nombres rationnels pouvant se mettre sous la forme r/s avec $s \not\equiv 0$ (mod.p) . Tout élément x de S_p peut se mettre sous la forme $r/\lambda(n)$ pour certain n ; faisons lui correspondre l'élément $(a_n)^r$ de G ; cet élément ne dépend pas de la forme $r/\lambda(n)$ de x d'après la convention $a_n = (a_{n+1})^{\nu(n+1)}$; nous avons ainsi défini une application φ de S_p dans G_p . φ est évidemment un homomorphisme, et applique S_p sur G_p puisque $G_p = \bigcup_{n=0}^{\infty} H_n$. Si $\varphi(r/\lambda(n))=1$, cela veut dire que $(a_n)^r=1$, donc que r est un multiple de $\lambda(n)$. Donc G_p est isomorphe à S_p/Z .

2)- Corps des racines n-ièmes de l'unité.

Soit $K \subset \Omega$ un corps de caractéristique p et P le corps premier de K. On appelle corps des racines n-ièmes de l'unité sur K, et on note $R_n(K)$, le corps obtenu en adjoignant à K toutes les racines n-ièmes de l'unité dans Ω. $R_n(K)$ est une extension galoisienne de K ; en effet, si $n=mp^h$ $(m \not\equiv 0\ (p))$, c'est le corps des racines de l'équation séparable $X^n-1=0$ (cor.1 et 2 de la prop.5, §8). Si ζ est une racine primitive n-ième de l'unité, toute autre racine n-ième de l'unité est une puissance de ζ ; donc $R_n(K)=K(\zeta)$ pour toute racine primitive n-ième de l'unité ζ. Soit Γ le groupe de Galois de $R_n(K)$ sur K. Deux automorphismes appartenant à Γ coïncident s'ils coïncident pour ζ ; tout $\sigma \in \Gamma$ doit transformer ζ en une racine primitive n-ième de l'unité, donc $\sigma(\zeta)=\zeta^{r(\sigma)}$; pour toute autre racine n-ième $\xi=\zeta^a$, on a $\sigma(\xi)=\zeta^{ar(\sigma)}=\xi^{r(\sigma)}$. L'entier $r(\sigma)$ est bien déterminé mod.n, et est premier à n puisque $\zeta^{r(\sigma)}$ est primitive ; puisque $\sigma\tau(\zeta)=\sigma(\zeta^{r(\tau)})=\zeta^{r(\sigma)r(\tau)}$, on a $r(\sigma\tau)=r(\sigma)r(\tau)$; donc l'application $\sigma \to r(\sigma)$ est un isomorphisme de Γ dans le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/(n)$. En résumé :

Proposition 1 - Soit K un corps de caractéristique p et n un entier premier à p ; le corps $R_n(K)$ des racines n-ièmes de l'unité sur K est une extension abélienne de K, dont le groupe de Galois est isomorphe à un sous-groupe du groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/(n)$.

On en déduit que $\left[R_n(K):K\right]$ est un diviseur de $\varphi(n)$. On notera aussi que $R_n(K)=K(R_n(P))$, donc le groupe de Galois de $R_n(K)$ sur K est isomorphe à celui de $R_n(P)$ sur $K \cap R_n(P)$ (§8, th.3), c'est-à-dire à un sous-groupe du groupe de Galois Γ_0 de $R_n(P)$ sur P.

On verra en exercice que, si $p=0$, Γ_o est isomorphe au groupe multiplicatif des éléments inversibles de $\mathbb{Z}/(n)$, et a par conséquent $\varphi(n)$ éléments. Mais ce résultat n'est plus vrai si $p > 0$.

3) Corps finis.

Nous allons étudier les corps finis commutatifs ; nous verrons en effet au chap.VII que tout corps fini est commutatif.

Un corps fini K ne peut contenir de sous-corps isomorphe au corps infini $\mathbb{Q}$; il est donc de caractéristique $p > 0$. Etant une extension du corps premier $\mathbb{F}_p$ (isomorphe à $\mathbb{Z}/(p)$), c'est un espace vectoriel sur $\mathbb{F}_p$; donc K a $p^n = q$ éléments.

Le groupe multiplicatif K^* des éléments non nuls de K ayant q-1 éléments, on a $x^{q-1}=1$ pour tout $x \in K^*$, donc $x^q - x = 0$ pour tout $x \in K$; le polynome $f(X)=X^q-X$, ayant -1 pour dérivée, a ses q racines distinctes ; donc K est à la fois le corps des racines et l'ensemble des racines de X^q-X dans Ω. Ceci montre à la fois l'existence et l'unicité, pour toute puissance p^n de tout entier premier p, d'un corps ayant p^n éléments ; nous noterons ce corps $\mathbb{F}_{p^n}$. En résumé, tenant compte du th.1 et de la prop.1 :

Théorème 2 - Un corps fini a nécessairement un nombre d'éléments q égal à une puissance p^n d'un nombre premier. Dans la cloture algébrique du corps premier $\mathbb{F}_p$ (isomorphe à $\mathbb{Z}/(p)$) il existe, pour tout $n > 0$, un corps $\mathbb{F}_{p^n}$ et un seul ayant $q = p^n$ éléments. $\mathbb{F}_{p^n}$ est le corps des invariants de l'automorphisme $x \to x^q$. C'est le corps et l'ensemble des racines de l'équation $X^q - X = 0$ sur $\mathbb{F}_p$. Le groupe multiplicatif $\mathbb{F}_q^*$ des éléments non nuls de $\mathbb{F}_q$ est un groupe cyclique à q-1 éléments ; si ζ est un générateur de ce groupe, on a $\mathbb{F}_q = \mathbb{F}_p(\zeta)$. $\mathbb{F}_q$ est une extension abélienne de $\mathbb{F}_p$, dont le groupe de Galois Γ est le groupe cyclique à n éléments engendré par l'automorphisme $\sigma : x \to x^p$.

Remarque - Le théorème de l'élément primitif (§ 7, prop. 14) est encore vrai pour les corps finis ; si en effet le corps F_q est une extension du corps K, et si ζ est une racine primitive $(q-1)$-ième de l'unité, tous les éléments de F_q en sont des puissances, et on a donc $F = K(\zeta)$.

4)- Extensions cycliques.

Définition 1 - On dit qu'une extension $E \subset \Omega$ d'un corps K est cyclique, si elle est galoisienne, et si son groupe de Galois est cyclique.

Si donc E est de degré n sur K, son groupe de Galois est isomorphe à $\mathbb{Z}/(n)$; comme tous les sous-groupes et groupes quotients de $\mathbb{Z}/(n)$ sont cycliques, pour tout sous-corps F de E tel que $K \subset F \subset E$, F est cyclique sur K (§ 8, prop. 10), et E sur F (§ 8, th. 2).

Dans une extension cyclique E d'un corps K, la norme et la trace d'un élément de E jouissent de la propriété fondamentale suivante :

Théorème 3 ("théorème 90 de Hilbert") - Soit E une extension cyclique d'un corps K, σ un générateur du groupe de Galois (cyclique) de E.

a) Pour qu'un élément $x \in E$ soit tel que $N_{E/K}(x) = 1$, il faut et il suffit qu'il existe $y \in E^*$ tel que $x = y^{1-\sigma}$; en outre tout $y_1 \in E$ tel que $x = y_1^{1-\sigma}$ est de la forme λy, avec $\lambda \in K^*$.

b) Pour qu'un élément $x \in E$ soit tel que $Tr_{E/K}(x) = 0$, il faut et il suffit qu'il existe $z \in E$ tel que $x = z - \sigma(z)$; en outre tout $z_1 \in E$ tel que $x = z_1 - \sigma(z_1)$ est de la forme $z + \lambda$, avec $\lambda \in K$.

a) Soit n le degré de E sur K. Pour un élément quelconque $t \in E$, considérons l'élément :

$$u(t) = t + xt^{\sigma} + x^{1+\sigma}t^{\sigma^2} + x^{1+\sigma+\sigma^2}t^{\sigma^3} + \dots + x^{1+\sigma+\dots+\sigma^{n-2}}t^{\sigma^{n-1}}$$

("résolvante de Lagrange-Hilbert") ; comme les n K-automorphismes distincts σ^k $(0 \leqslant k \leqslant n-1)$ de E sont linéairement indépendants (§ 7, th. 1),

il existe $t_0 \in E$ tel que $y=u(t_0)\neq 0$; or comme $x^{1+\sigma+..+\sigma^{n-1}} = N_{E|K}(x)=1$ par hypothèse, on a :

$$y^\sigma = t^\sigma + x^\sigma t^{\sigma^2} + \dots x^{\sigma+\sigma^2+..+\sigma^{n-2}} t^{\sigma^{n-1}} + tx^{-1}$$

d'où $xy^\sigma = y$, $x = y^{1-\sigma}$. Il est évident, inversement, que si $x=y^{1-\sigma}$, on a $N_{E|K}(x)=1$ (ceci est d'ailleurs vrai dans toute extension). Enfin la relation $y^{1-\sigma} = y_1^{1-\sigma}$ entraîne $y_1 y^{-1} = (y_1 y^{-1})^\sigma$; par suite $y_1 y^{-1}$ est invariant par tous les K-automorphismes de E, donc appartient à K .

b) En raison de l'indépendance linéaire des automorphismes σ^k , il existe $v \in E$ tel que $\mathrm{Tr}_{E|K}(v) = \sum_{k=0}^{n-1} \sigma^k(v) \neq 0$; considérons alors :

$$z = \frac{1}{\mathrm{Tr}_{E|K}(v)} (x\sigma(v)+(x+\sigma(x))\sigma^2(v)+\dots+(x+\sigma(x)+..+\sigma^{n-2}(x))\sigma^{n-1}(v)).$$

Si on a $\mathrm{Tr}_{E|K}(x) = \sum_{k=0}^{n-1} \sigma^k(x) = 0$, il vient :

$$\sigma(z) = \frac{1}{\mathrm{Tr}_{E|K}(v)} (\sigma(x)\,\sigma^2(v) \dots (\sigma(x)+\sigma^2(x)+\dots+\sigma^{n-2}(x))\sigma^{n-1}(v) - xv)$$

D'où $z-\sigma(z)=x$. Il est évident, inversement, que si $x=z-\sigma(z)$, on a $\mathrm{Tr}_{E|K}(x)=0$; enfin la relation $z-\sigma(z)=z_1-\sigma(z_1)$ équivaut à $z_1-z=\sigma(z_1-z)$ par suite z_1-z est invariant par tous les K-automorphismes de E , ce qui signifie que $z_1-z \in K$.

Corollaire (Lagrange) - Si E est une extension cyclique de degré n premier à la caractéristique p de E , d'un corps K contenant toutes les racines n-ièmes de l'unité, il existe un polynome irréductible de $K[X]$, de la forme X^n-a (une "équation binôme"), tel que E soit engendré par une racine quelconque de ce polynome. Si, réciproquement K contient toutes les racines n-ièmes de l'unité, avec n premier à la caractéristique p de K , le corps des racines du polynome X^n-a est, pour tout $a \in K$, une extension cyclique E de K , engendrée par une quelconque des racines de X^n-a ; le degré $d = [E:K]$ est un diviseur de n , égal au plus petit des entiers $r>0$ tels que a^r soit puissance n-ième d'un élément de K .

Soit en effet ζ une racine primitive n-ième de l'unité ; on a $N_{E|K}(\zeta)=\zeta^n=1$, donc il existe $\theta \in E$ tel que $\zeta=\theta^{1-\sigma}$, ou encore $\theta^\sigma=\zeta^{-1}\theta$; on en tire $\theta^{\sigma k}=\zeta^{-k}\theta$, donc les conjugués de θ sont au nombre de n , et par suite $E=K(\theta)$; d'autre part on a $1=\zeta^n=(\theta^n)^{1-\sigma}$, donc $\sigma(\theta^n)=\theta^n$, ce qui veut dire que $\theta^n \in K$.

Si, réciproquement θ est une racine de X^n-a , on a, pour toute autre racine θ' , $(\frac{\theta}{\theta'})^n=1$, d'où $\theta'=\omega\theta$, où ω est une racine n-ième de l'unité, qui appartient par hypothèse à K ; donc $E=K(\theta)$. Comme la dérivée de X^n-a ne s'annule pas pour $x=0$ (sauf si $a=0$, cas trivial), θ n'est pas racine multiple, et E est séparable, donc galoisienne, sur K . Soit Γ son groupe de Galois, et $\sigma \in \Gamma$; comme $E=K(\theta)$, la donnée de $\sigma(\theta)$ détermine θ ; comme $\sigma(\theta)$ est racine de X^n-a , on a $\sigma(\theta)=\zeta_\sigma\theta$, où ζ_σ est une racine n-ième de l'unité bien déterminée par σ . L'application $\sigma \longrightarrow \zeta_\sigma$ est une application biunivoque de Γ dans le groupe multiplicatif G des racines n-ièmes de l'unité ; en outre c'est une <u>représentation</u> de Γ dans G car, si τ est un élément de Γ , on a $\sigma\tau(\theta)=\sigma(\tau(\theta))=\sigma(\zeta_\tau\theta)=\zeta_\tau\sigma(\theta)=\zeta_\tau\zeta_\sigma\theta$, d'où $\zeta_{\sigma\tau}=\zeta_\sigma\zeta_\tau$. On voit donc que Γ est isomorphe à un <u>sous-groupe</u> de G ; comme G est cyclique d'ordre n (th.1), Γ est un groupe cyclique dont l'ordre d divise n . Posons $n=dh$; des relations $\sigma(\theta)=\zeta_\sigma\theta$, on déduit que $N_{E|K}(\theta)=\mu\theta^d$, où $\mu \in K$; d'où $\theta^d=b \in K$. Par suite on a $a=\theta^n=b^h$, d'où $a^d=b^{nh}=(b^h)^n$. S'il existait un nombre $r<d$ tel que $a^r=c^n$, où $c \in K$, on déduirait de la relation $\theta^n=a$, que $\theta^{rn}=c^n$, d'où $\theta^r=\omega c$, ω étant une racine n-ième de l'unité ; θ serait donc racine du polynome $x^r-\omega c$ de $K[X]$, ce qui est contraire au fait que θ est de degré d sur K .

APPENDICE

Extensions galoisiennes de degré infini.

Soit Ω une extension galoisienne d'un corps K, Γ son groupe de Galois ; nous nous proposons de compléter, dans cet Appendice, la théorie de Galois exposée au § 8, en étudiant le cas où Γ est un groupe quelconque, fini ou non. Munissons Ω de la structure uniforme discrète ; Γ est une partie de l'ensemble $\zeta(\Omega,\Omega)$ des applications de Ω dans Ω ; Ω étant complet, $\zeta(\Omega,\Omega)$ est complet pour la structure uniforme de la convergence simple (Top.Gén., chap.X, § 1, prop.) ; les entourages d'un système fondamental de celle-ci se composent des couples (f,g) d'applications de Ω dans Ω tels que $f(x_i)=g(x_i)$ pour un ensemble fini de points donnés $x_i \in \Omega$. Pour la topologie induite sur Γ, les voisinages d'un K-automorphisme σ sont donc les ensembles d'automorphismes τ tels que $\tau(x_i)=\sigma(x_i)$ pour un ensemble fini d'éléments x_i de Ω ; ces éléments x_i engendrent une extension algébrique finie F de K, et on a évidemment $\sigma(x) = \tau(x)$ pour tout $x \in F$; nous noterons $V_F(\sigma)$ ce voisinage de σ. Il est clair que $V_F(\sigma\tau) = \sigma V_F(\tau) = V_{\tau(F)}(\sigma)\tau$. En particulier $V_F(\sigma) = \sigma V_F(\epsilon)$, ϵ désignant l'élément neutre de Γ ; d'après sa définition $V_F(\epsilon)$ est un sous-groupe de Γ, et $\sigma V_F(\epsilon)\sigma^{-1} = V_F(\sigma)\sigma^{-1} = V_{\sigma(F)}(\sigma\sigma^{-1}) = V_{\sigma(F)}(\epsilon)$; si F est le corps composé de F_1 et F_2, on a $V_F(\epsilon) = V_{F_1}(\epsilon) \cap V_{F_2}(\epsilon)$; donc la topologie induite sur Γ par la structure uniforme de la convergence simple est compatible avec la structure de groupe de Γ, la structure uniforme induite étant la structure uniforme droite de Γ (Top. Gén., chap.III, § 2).

La vérification du fait qu'une application f de Ω dans Ω est un K-automorphisme ne faisant intervenir qu'un nombre fini d'éléments, nous en déduisons que Γ est un sous-espace fermé, donc complet, de $\zeta(\Omega,\Omega)$.

F étant une extension algébrique finie de K , il n'existe qu'un nombre fini m de K-isomorphismes $\{\tau_i\}$ de F dans M ; soit $\{\sigma_i\}$ m K-automorphismes de M induisant les τ_i sur F ; pour tout $\sigma \in \Gamma$, la restriction de σ à F est identique à un τ_i ; donc $\sigma_i^{-1}\sigma \in V_F(e)$, et les m classes à droite $\sigma_i V_F(e)$ forment une partition de Γ . Le voisinage $V_F(e)$ étant arbitrairement petit cela prouve que Γ est précompact.

Enfin Γ est totalement discontinu car sa topologie est définie par des sous-groupes. Donc :

Théorème 1 - Le groupe de Galois d'une extension galoisienne quelconque, muni de la topologie de la convergence simple, est un groupe topologique compact et totalement discontinu.

Soit E une extension de K contenue dans M , et $g(E)$ le groupe des automorphismes de M induisant l'automorphisme identique sur E . D'après la définition de la convergence simple, $g(E)$ est un sous-groupe fermé de Γ . Soit maintenant Δ un sous-groupe de Γ ; pour tout $\sigma \in \overline{\Delta}$ et toute extension finie F de K il existe $\tau \in \Delta$ tel que σ et τ coïncident sur F ; ceci caractérise $\overline{\Delta}$, et on peut même se borner aux extensions galoisiennes finies F de K , puisque l'extension galoisienne engendrée par une extension finie est finie (§ 8, cor.1 de la prop.5). Si $\sigma \in g(k(\Delta))$, laisse invariants tous les éléments de $F \cap k(\Delta)$, qui n'est autre que le sous-corps de F laissé invariant par tous les automorphismes appartenant au groupe Δ_F des restrictions à F des éléments de Δ ; donc la restriction $\sigma_F \in \Delta_F$ (§ 8, cor. de la prop.8), et il existe $\tau \in \Delta$ tel que $\sigma_F = \tau_F$; donc $\sigma \in \overline{\Delta}$. Puisque $g(k(\Delta))$ est fermé et contient Δ , on a $g(k(\Delta)) = \overline{\Delta}$. Nous pouvons donc généraliser le théorème fondamental des extensions galoisiennes (§ 8, th.2) :

Théorème 2 - Si N est une extension galoisienne de K, l'application $E \to g(E)$ est une application biunivoque strictement décroissante de l'ensemble $\mathcal{K}$ des sous-corps de N contenant K sur l'ensemble $\mathcal{G}$ des sous-groupes fermés du groupe de Galois Γ de N ; et $\Delta \longrightarrow k(\Delta)$ en est l'application réciproque.

Soit enfin E une extension galoisienne de K contenue dans N, et soit σ_E la restriction à E de $\sigma \in \Gamma$; σ_E est un automorphisme de E (§ 8, prop. 3) ; $\sigma_E \in \Gamma_E$; et tout élément du groupe de Galois Γ_E de E s'obtient de cette façon (§ 7, prop. 1). L'application $\sigma \longrightarrow \sigma_E$ est continue d'après la définition de la topologie de la convergence simple; c'est donc une représentation continue de Γ sur Γ_E ; son noyau est évidemment $g(E)$. Puisque $\Gamma/g(E)$ est compact, il est isomorphe à Γ_E (en tant que groupe topologique). En tenant compte de la prop. 10, § 6, nous en déduisons la :

Proposition 1 - Pour qu'un sous-corps E de N soit galoisien sur K, il faut et il suffit que $g(E)$ soit un sous-groupe distingué fermé de Γ. Alors le groupe de Galois de E est (algébriquement et topologiquement) isomorphe à $\Gamma/g(E)$.
