THEORIE DES CORPS COMMUTATIFS
(REDACTION CHEVALLEY)

Rédaction n° 047

Nombre de pages : 79

Nombre de feuilles : 79

A 47 (2)

THEORIE DES CORPS COMMUTATIFS

(Rédaction Chevalley)

Etat 2

Sommaire

THEORIE DES CORPS COMMUTATIFS

Tous les corps considérés dans ce chapitre seront des corps commutatifs. Nous conviendrons donc, dans ce chapitre, d'entendre par "corps" un corps commutatif.

I. LA CARACTERISTIQUE. CORPS PREMIERS

Nous avons défini la notion de caractéristique d'un anneau quelconque (Alg.I, § 8, n°8).

Théorème 1. La caractéristique d'un corps est ou bien 0 ou bien un nombre premier.

Supposons en effet qu'un corps K soit de caractéristique $p > 0$, et soit e l'élément unité de K. Si $p = qr$ est une décomposition de p en deux facteurs $q > 0$ et $r > 0$, on a $pe = (qe)(re) = 0$, d'où il résulte que l'un des éléments qe, re est 0, donc que l'un des entiers q, r est $\geqslant p$. Comme ils sont tous deux $\leqslant p$, l'un doit être p et l'autre 1, ce qui prouve que p est premier.

Soit K un corps quelconque, et soit e l'élément unité de K. L'image de Z par l'application $n \to ne$ est un sous-anneau P de K. Si K est de caractéristique $p > 0$, P est isomorphe à Z/pZ, qui est lui-même, comme nous le savons, un corps ; P est dans ce cas le plus petit sous-corps de K. Si au contraire K est de caractéristique 0, P est dans ce cas le plus petit sous-corps de K. Si au contraire K est de caractéristique 0, P est isomorphe à Z et K contient le corps des quotients Q de P, qui est isomorphe au corps des rationnels ; Q est dans ce cas le plus petit sous-corps de K. Nous avons donc démontré la

Proposition 1. Parmi tous les sous-corps d'un corps K, il en est un plus petit L. Si K est de caractéristique $p > 0$, L est isomorphe à Z/pZ ; si K est de caractéristique 0, L est isomorphe au corps des nombres rationnels.

Un corps qui ne contient aucun sous-corps différent de lui-même est dit premier.

Proposition 2.- Soit K un corps de caractéristique $p > 0$. L'application $x \to x^p$ est alors un isomorphisme de K sur un sous-corps de K .

Il est évident que $(xy)^p = x^p y^p$. Nous allons montrer que $(x+y)^p = x^p + y^p$. On sait que $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$ et que $\binom{p}{0} = \binom{p}{p} = 1$. Il nous suffira donc de montrer que, si $1 < i < p$, $\binom{p}{i}$ est un multiple de p . Or on a $i!\binom{p}{i} = p(p-1)\ldots(p-i+1)$. Soit e l'élément unité de K ; on a $i!e = \prod_{j=1}^{i} je \neq 0$, mais $p(p-1)\ldots(p-i+1)e = 0$, d'où $\binom{p}{i}e = 0$; ce qui démontre notre assertion. L'application $x \to x^p$ est donc un homomorphisme de la structure d'anneau de K ; puisqu'elle n'applique pas K sur $\{0\}$, c'est un isomorphisme, ce qui démontre la proposition 2 .

Il résulte tout de suite de la proposition 2 que, si x et y sont des éléments d'un corps K de caractéristique $p > 0$, on a aussi $(x-y)^p = x^p - y^p$. D'autre part, procédant par récurrence sur f , on établit facilement que $(x+y)^{p^f} = x^{p^f} + y^{p^f}$. Enfin, on établit par récurrence sur n la formule

$$\left(\sum_{i=1}^{n} x_i\right)^{p^f} = \sum_{i=1}^{n} x_i^{p^f} ,$$

valable pour toute famille finie (x_i) d'éléments de K .

II. EXTENSIONS ALGEBRIQUES.

Définition 1. On entend par extension d'un corps K une paire (K,L) formée de K et d'un corps L contenant K comme sous-corps.

Si (K,L) est une extension d'un corps K , L peut être considéré comme un anneau sur K . Nous avons alors défini (Alg.III, , n°) la notion d'élément de L transcendant par rapport à K .

Définition 2. Soit (K,L) une extension d'un corps K . Un élément de L qui n'est pas transcendant par rapport à K est dit algèbrique par rapport à K , on dit que l'extension (K,L) est algèbrique, ou encore que L est algèbrique par rapport à K .

Soit (K,L) une extension d'un corps K . Pour qu'un élément x de L soit algèbrique par rapport à K , il faut et suffit qu'il existe un polynome $f(X) \neq 0$ en une lettre X à coefficients dans K tel que $f(x)=0$. Il en résulte que x est alors aussi algèbrique par rapport à tout sous-corps de L contenant K . On en déduit que, si (K,L) est une extension algèbrique, et si L' est un sous-corps de L contenant K , les extensions (K, L') et (L',L) sont algèbriques. La réciproque de cette assertion sera démontrée plus loin.

Définition 3.- Une extension (K,L) d'un corps K est dite finie si la structure d'espace vectoriel sur K de L est de dimension finie. Cette dimension s'appelle alors le degré de L par rapport à K et se désigne par $[L : K]$.

Théorème 1. Soit (K,L) une extension d'un corps K , et soit L' un sous-corps de L contenant K . Pour que (K,L) soit finie, il faut et suffit que (K,L') et (L',L) soient toutes deux finies ; s'il en est ainsi, on a $[L : K] = [L : L'][L' : K]$.

Cela résulte immédiatement de la prop. , Alg.II, , n° .

Proposition 1. Toute extension finie est algèbrique.

Soit (K,L) une extension finie de degré n , et soit x un élément de L . Les n+1 éléments 1 (l'élément unité de L),x,..,x^n sont alors linéairement dépendants par rapport à K , ce qui prouve que x est algèbrique par rapport à K .

La réciproque de la proposition 1 est inexacte : il n'est pas vrai que toute extension algèbrique soit finie. Mais nous allons montrer qu'il en est ainsi des extensions qui peuvent être engendrées par un nombre fini d'éléments algèbriques, au sens que nous allons préciser.

Définition 4. Soit (K,L) une extension d'un corps K , et soit A une parti de L . On désigne par $K\langle A\rangle$ l'intersection de tous les sous-corps de L qui contiennent K et A . Si $K\langle A\rangle = L$, on dit que l'extension (K,L) est engendrée par les éléments de A , ou encore que L se déduit de K par adjonction des éléments de A .

Si A ne contient qu'un nombre fini d'éléments $x_1,\ldots,x_n$, $K\langle A\rangle$ se note aussi $K\langle x_1,..,x_n\rangle$.

Proposition 2. Soit (K,L) une extension d'un corps K engendrée par un seul élément x qui est algèbrique par rapport à K . L'extension (K,L) est alors finie ; si n est son degré, les éléments $1,x,\ldots,x^{n-1}$ forment une base de la structure d'espace vectoriel sur K de L . Il existe un polynome f(X) de degré n en une lettre X à coefficients dans K , dans lequel le coefficient de X^n est 1 , qui est tel que $f(x) = 0$; le polynome f est caractérisé d'une manière unique par ces conditions ; si g(X) est un élément de $K[X]$ tel que $g(x) = 0$, g est divisible par f dans $K[X]$.

Parmi tous les polynomes $h \in K[X]$ tels que $h \neq 0$, $h(x) = 0$, choisissons-en un de plus petit degré, et soit n le degré du polynome ainsi obtenu. Divisant le polynome en question par le coefficient de X^n, on obtient un polynome f de degré n tel que $f(x) = 0$ et dans lequel le coefficient de X^n est 1. Formons l'espace vectoriel $M = K + Kx + \ldots + Kx^{n-1}$; il est clair que cet espace vectoriel est de dimension n sur K. Si $f(X) = X^n + \sum_{i=1}^{n} a_i X^{n-i}$, on a $x^n = -\sum_{i=1}^{n} a_i x^{n-i} \in M$, d'où on déduit tout de suite que $xM \subset M$. Procédant par récurrence sur h, on voit que $x^h M \subset M$ pour tout $h > 0$, d'où $MM \subset M$; l'ensemble M est donc ur sous-anneau de L. Soit y un élément $\neq 0$ de M ; l'application $u \to yu$ de M dans lui-même est linéaire et univalente. L'espace vectoriel M étant de dimension finie, on a $yM = M$; en particulier, $1 \in yM$, d'où $y^{-1} \in M$, ce qui prouve que M est un corps. Puisque M contient K et x, on a $M = L$. On voit ainsi que (K,L) est finie et de degré n. Pour démontrer que tout $g \in K[X]$ tel que $g(x) = 0$ est divisible par f dans $K[X]$, nous pouvons nous limiter au cas où $g \neq 0$, et nous procédons alors par récurrence sur le degré p de g. Notre assertion est vraie si $p < n$, car il n'y a alors aucun polynome de degré p dans $K[X]$ admettant x pour zéro. Supposons que $p \geqslant n$ et que notre assertion soit vraie pour les polynomes de degrés $< p$. Soit c le coefficient de X^p dans g ; si on pose $g' = g - cX^{p-n}f$, on a $g'(x) = 0$ et g' est ou bien 0 ou bien de degré $< p$. En tous cas, g' est divisible par f dans $K[X]$, et il en est par suite de même de g. Si g est de degré n, on a $g = cf$, où $c \in K$, et si le coefficient de X^n dans g est 1, $c = 1$, d'où $g = f$, ce qui montre que f est uniquement déterminé par les conditions que nous lui avons imposées.

Définition 5. Les notations étant celles de la prop.2, n est appelé le degré de x par rapport à K, et f est appelé le polynome minimal de x par rapport à K.

Proposition 3. Soit j un isomorphisme d'un corps K sur un corps K'. Soient (K,L) et (K',L') des extensions algébriques de K et de K' respectivement. Supposons que $L = K\langle x\rangle$, $L' = K'\langle x'\rangle$ et que x' soit un zéro du polynome déduit du polynome minimal $f(X)$ de x par rapport à K en appliquant l'opération j aux coefficients de $f(X)$. On peut alors prolonger j par un isomorphisme de L sur L' qui applique x sur x'.

Si $g \in K[X]$, nous désignerons par $j^*(g)$ le polynome déduit de g par application de j aux coefficients de g ; j^* est donc un isomorphisme de $K[X]$ sur $K'[X]$. Il résulte de la prop.2 que tout $y \in L$ peut se mettre sous la forme $y = g(x)$, où $g \in K[X]$. De plus, si $g_1(x) = g_2(x)$, on a $(g_1-g_2)(x) = 0$, d'où $g_1-g_2 = fh$, avec un $h \in K[X]$. On en déduit que $j^*(g_1)-j^*(g_2) = j^*(f)\ j^*(h)$, d'où $(j^*(g_1))(x') = (j^*(g_2))(x')$. On peut donc définir une application J de L dans L' telle que $J(g(x)) = (j^*(g))(x')$ pour tout $g \in K[X]$. Il est clair que J est un homomorphisme et prolonge j ; puisque $L' = K[x']$, on a $J(L) = L'$. Il résulte du th.1, Alg.I, §9, n°3 que J est un isomorphisme de L sur L'. La prop.3 est donc démontrée.

Soit (K,L) une extension d'un corps K, et soient A et B des parties de L. Nous allons montrer que $K\langle A \cup B\rangle = (K\langle A\rangle)\langle B\rangle$. En effet, $(K\langle A\rangle)\langle B\rangle$ est un sous-corps de L qui contient $K\langle A\rangle$ et B, donc aussi K, A et B, d'où $K\langle A\cup B\rangle \subset (K\langle A\rangle)\langle B\rangle$. D'autre part, $K\langle A \cup B\rangle$ contient K et A, donc aussi $K\langle A\rangle$; $K\langle A \cup B\rangle$ contient $K\langle A\rangle$ et B, donc $(K\langle A\rangle)\langle B\rangle \subset K\langle A\cup B\rangle$, ce qui complète la démonstration de notre assertion. On voit de même que $K[A\cup B] = (K[A])[B]$.

Proposition 4.- Soit (K,L) une extension d'un corps K . Supposons que $L = K\langle A\rangle$, où A est une partie de L composée d'éléments qui sont algèbriques par rapport à K . L'extension (K,L) est alors algèbrique, et on a $L = K[A]$. Si A est finie, l'extension (K,L) est finie.

Considérons d'abord le cas où A est finie. Dans ce cas, nous démontrerons par récurrence sur le nombre n d'éléments de A que (K,L) est finie et que $L = K[A]$. C'est évident si $n=0$; si $n=1$, cela résulte de la prop.2 . Supposons que $n>1$ et que notre assertion soit vraie pour les parties composées de n-1 éléments. Ecrivons $A = B \cup \{x\}$, où $x \in A$ et B contient n-1 éléments. On a $K\langle A\rangle = (K\langle B\rangle)\langle x\rangle$; les extensions $(K,K\langle B\rangle)$ et $(K\langle B\rangle , K\langle A\rangle)$ sont finies, d'où il résulte que $(K,K\langle A\rangle)$ est finie. De plus, $K\langle B\rangle = K[B]$, d'où
$K\langle A\rangle = (K\langle B\rangle)[x] = (K[B])[x] = K[A]$.

Passons maintenant au cas général. Il nous suffira évidemment de démontrer le lemme suivant :

Lemme 1. Soit (K,L) une extension d'un corps K . Supposons que $L = K\langle A\rangle$. Le corps L est alors l'union des corps $K\langle F\rangle$, où F décrit les parties finies de A .

Soit en effet L_o l'union des corps $K\langle F\rangle$, et soient x,y des éléments de L_o . Il existe donc des parties finies F et G de A telles que $x \in K\langle F\rangle$, $y \in K\langle G\rangle$; les éléments x,y sont donc tous deux contenus dans $K\langle F \cup G\rangle$; il en est de même de x-y , de xy et (si $y \neq 0$) de y^{-1}. Puisque $K\langle F \cup G\rangle$ est contenu dans L_o , on voit que L_o est un sous-corps de L . Il est clair que L_o contient K et A , d'où $L_o = L$, ce qui démontre le lemme 1 et par suite aussi la prop.4 .

Corollaire.- Soit (K,L) une extension d'un corps K , et soit A l'ensemble des éléments de L qui sont algèbriques par rapport à K . L'ensemble A est alors un sous-corps de L .

En effet, il résulte de la prop.3 que $(K, K\langle A\rangle)$ est algébrique, d'où $K\langle A\rangle \subset A$ et par suite $A = K\langle A\rangle$.

Proposition 5. Soit (K,L) une extension d'un corps K, et soit L' un sous-corps de L contenant K. Pour que (K,L) soit algébrique, il faut et suffit que (K,L') et (L',L) le soient.

Nous avons déjà montré que la condition est nécessaire. Inversement, supposons la satisfaite. Soient x un élément de L et $f(X)$ le polynome minimal de x par rapport à L'. Désignons par A l'ensemble des coefficients de f ; l'extension $(K, K\langle A\rangle)$ est alors finie (prop.4), et x est algébrique par rapport à $K\langle A\rangle$, ce qui montre que $(K\langle A\rangle, K\langle A \cup \{x\}\rangle)$ est finie. Donc $(K, K\langle A \cup \{x\}\rangle)$ est finie, d'où il résulte que x est algébrique par rapport à K.

---

3. CORPS ALGEBRIQUEMENT FERMES.

Définition 1.- Un corps K est dit algèbriquement fermé quand (K,K) est la seule extension algèbrique de K . Une extension (K,L) d'un corps K est dite algèbriquement fermée quand L est algèbriquement fermé.

Théorème 1 (Steinitz).- Tout corps admet une extension algèbrique algèbriquement fermée.

Soit K un corps. Formons l'anneau $K[X]$ des polynomes en une lettre X à coefficients dans K . Nous allons montrer que, si (K,L) est une extension algèbrique de K , L est équipotent à une partie de $K[X]$. A chaque $x \in L$ faisons correspondre le polynome minimal de x par rapport à K que, pour noter sa dépendance de x , nous désignerons par $\varphi(x)$; φ est donc une application de L dans $K[X]$.

Il résulte immédiatement du th. , Alg., , , n° que, pour tout $g \in K[X]$, l'ensemble $\varphi^{-1}(g)$ est fini ; soient $x_{g,1},\ldots,x_{g,\partial(g)}$ les éléments distincts de cet ensemble. Si $\varphi(x) = f$, on a $x = x_{f,i(x)}$ $(1 \leqslant i(x) \leqslant \partial(f))$, et l'application $x \to (i(x), \varphi(x))$ applique L bi-univoquement sur une partie de $\mathbb{N} \times K[X]$, qui est, comme on sait, équipotent à $K[X]$.

Ceci dit, formons ur ensemble E équipotent à l'ensemble des parties de $K[X]$ et contenant K . Désignons par $\mathcal{L}$ l'ensemble des corps dont les éléments appartiennent à E , qui contiennent K comme sous-corps et sont algèbriques par rapport à K . Nous ordonnerons $\mathcal{L}$ par la convention que, si L et L' sont des éléments de $\mathcal{L}$, la relation $L \leqslant L'$ sera vraie si et seulement si L est un sous-corps de L' . L'ensemble ordonné $\mathcal{L}$ ainsi obtenu est inductif. Soit en effet $\mathcal{L}_o$ une partie non vide totalement ordonnée de $\mathcal{L}$, et soit L_o l'union des éléments de $\mathcal{L}_o$. Si x et y sont des éléments de L_o , il existe des éléments L , L' de $\mathcal{L}_o$ tels que $x \in L$, $y \in L'$; si $L \leqslant L'$, x et y sont tous deux dans L' .

De plus, si L' et L" sont deux corps appartenant à $\mathcal{L}_o$ et qui tous deux contiennent x et y , la somme et le produit de x et de y dans L' sont les mêmes que dans L", puisque l'un des corps L' et L" est sous-corps de l'autre. Nous pouvons donc définir une addition et une multiplication dans L_o de telle manière que, si $L \in \mathcal{L}_o$, les restrictions à $L \times L$ de l'addition et de la multiplication dans L_o soient respectivement l'addition et la multiplication dans L . Si on tient compte du fait qu'étant donnés trois éléments de L_o , il existe toujours un $L \in \mathcal{L}_o$ les contenant tous les trois, on voit tout de suite que l'addition et la multiplication ainsi définie confèrent à L_o une structure de corps. Tout $L \in \mathcal{L}_o$ est un sous-corps de L_o ; puisque tout élément de L_o appartient à un $L \in \mathcal{L}_o$, L_o est algèbrique par rapport à K , d'où $L_o \in \mathcal{L}$, ce qui montre que la famille $\mathcal{L}$ est inductive. Cette famille contient donc un élément maximal L_1. Soit (L_1, M) une extension algèbrique quelconque de L_1 . L'extension (K,M) est alors algèbrique, d'où il résulte que le complément R de L_1 par rapport à M est de puissance strictement inférieure à celle de E . Par ailleurs, L_1 est lui-même de puissance strictement inférieure à celle de E , ce qui montre que le complément de L_1 dans E est équipotent à E . Ce complément contient donc un ensemble R_1 équipotent à R . Nous pouvons établir une correspondance bi-univoque entre M et $L_1 \cup R_1$ qui coïncide avec l'identité sur L_1 . Par transport de structure, notre correspondance bi-univoque permet de définir sur $L_1 \cup R_1$ une structure de corps. Soit M_1 le corps ainsi obtenu ; il est clair qu'il existe un isomorphisme de M_1 sur M qui coïncide avec l'identité sur L_1 . On en conclut que M_1 est algèbrique par rapport à K , d'où $M_1 \in \mathcal{L}$, et par suite $M_1 = L_1$, $M = L_1$, puisque L_1 est maximal dans $\mathcal{L}$. On voit donc que L_1 est algèbriquement fermé.

Théorème 2. Une condition nécessaire et suffisante pour qu'un corps K soit algèbriquement fermé est que tout polynome de degré $\geqslant 1$ en une lettre à coefficients dans K se décompose en un produit de polynomes du premier degré à coefficients dans K .

1) La condition est nécessaire. Supposons K algèbriquement fermé, et soit f(X) un polynome de degré $n \geqslant 1$ à coefficients dans K . Nous démontrerons par récurrence sur n que f peut se mettre sous la forme $f = c\prod_{i=1}^{n}(X-x_i)$ avec $c, x_1, .., x_n \in K$. La proposition est évidente si n=1 . Supposons la vraie pour les polynomes de degré n-1 (où $n \geqslant 2$). Il est évident que f n'a pas d'inverse dans $K[X]$. Il en résulte que f est contenu dans au moins un idéal maximal $\mathfrak{p}$ de $K[X]$ (alg.I, § 8, n° 7, th.2). L'anneau $K[X]/\mathfrak{p}$ est un corps (Alg.1, § 9, n°3, th.2). L'homomorphisme canonique de $K[X]$ sur $K[X]/\mathfrak{p}$ n'applique pas K sur $\{0\}$; donc cet homomorphisme induit un isomorphisme de K sur un sous-corps K_1 de $K[X]/\mathfrak{p}$. Si χ est la classe de X-modulo $\mathfrak{p}$, on a $K[X]/\mathfrak{p} = K_1[\chi]$, et $f^*(\chi) = 0$, où f^* est le polynome déduit de f par application de φ à ses coefficients. On voit donc que $K[X]/\mathfrak{p}$ est algèbrique par rapport à K_1 . Soit R_1 le complément de K_1 par rapport à $K[X]/\mathfrak{p}$; formons un ensemble R sans élément commun avec K et équipotent à R_1 . L'application φ peut alors se prolonger par une application bi-univoque φ_1 de $K \cup R$ sur $K[X]/\mathfrak{p}$. Par transport de structure, l'application φ_1 permet de définir sur $K \cup R$ une structure de corps ; soit L le corps ainsi obtenu. Il est clair que L contient K comme sous-corps et est algèbfique par rapport à K . On a donc $L = K$, d'où $K[X]/\mathfrak{p} = K_1$, $\chi \in K_1$. Soit x l'élément de K tel que $\varphi(x) = \chi$. On a donc $f(x)=0$, d'où $f(X) = (X-x)g(X)$, où g est un polynome de degré n-1 à coefficients dans K . Il résulte de notre hypothèse que g est un produit de facteurs

du premier degré à coefficients dans K ; il en est donc de même de f .

2) la condition est suffisante. Supposons la satisfaite, et soit (K,L) une extension algèbrique de K . Soit x un élément quelconque de L et soit f(X) le polynome minimal de x par rapport à K . Du fait que f(X) est un produit de polynomes du premier degré à coefficients dans K , on déduit tout de suite que f peut se mettre sous la forme $c\prod_{i=1}^{n}(X-x_i)$, avec $c,x_1,..,x_n \in K$, $c \neq 0$ (en effet, si $a \neq 0$, $aX+b = a(X-(-a^{-1}b))$). On a donc $\prod_{i=1}^{n}(x-x_i)=0$ et x est égal à l'un des éléments $x_1,\ldots,x_n$. On a donc $L = K$, ce qui montre que K est algèbriquement fermé.

On déduit du th.4 que le corps Q des rationnels n'est pas algèbriquement fermé ; il est en effet clair que X^2+1 n'a aucun zéro dans Q . De même, un corps fini K ne peut être algèbriquement fermé ; soient en effet $x_1,..,x_n$ les éléments distincts de K : le polynome $1 + \prod_{i=1}^{n}(X-x_i)$ ne peut évidemment avoir aucun zéro dans K .

Théorème 5. Soit h un isomorphisme d'un corps K sur un corps K'. Soient (K,L) et (K',L') des extensions de K et de K' respectivement. Si le corps L' est algèbriquement fermé, et si (K,L) est algèbrique, on peut prolonger h par un isomorphisme de L sur un sous-corps de L'.

Soit J l'ensemble des isomorphismes j de sous-corps de L contenant K sur des sous-corps de L' qui coïncident avec h sur K (on a en particulier $h \in J$) . Si $j \in J$, nous désignerons par M_j le sous-corps de L sur lequel j est défini. Nous ordonnerons J par la convention que $j \leqslant j'$ si $M_j \subset M_{j'}$ et j' prolonge j . Nous allons montrer que J , ainsi ordonné, est inductif. Nous avons besoin pour cela du lemme suivant :

Lemme 1. Soit $\mathcal{M}$ une famille non vide de sous-corps d'un corps L . Supposons que $\mathcal{M}$ soit totalement ordonnée par inclusion. L'union M_o des sous-corps appartenant à $\mathcal{M}$ est alors un sous-corps de L , et toute partie finie de M_o est contenue dans un $M \in \mathcal{M}$.

Si $x_1,..,x_n$ sont des éléments de M_o, il existe pour chaque i un $M_i \in \mathcal{M}$ tel que $x_i \in M_i$. La famille finie $(M_1,..,M_n)$ étant totalement ordonnée par inclusion, il existe un i_o tel que $M_i \subset M_{i_o}$ $(1 \leqslant i \leqslant n)$, d'où $x_i \in M_{i_o}$ $(1 \leqslant i \leqslant n)$. Appliquant ceci au cas où $n = 2$, on voit que $x_1 - x_2$, $x_1 x_2$ et (si $x_1 \neq 0$) x_1^{-1} sont dans M_{i_o} , donc dans M_o , ce qui prouve que M_o est un sous-corps de L .

Ceci dit, soit J_o une partie totalement ordonnée non vide de J . La famille $(M_j)_{j \in J_o}$ est totalement ordonnée ; l'union des ensembles de cette famille est donc un sous-corps M_o de L . Si $x \in M_o$ et si j,j' sont des éléments de J_o tels que $x \in M_j$, $x \in M_{j'}$, on a $j(x) = j'(x)$, puisque l'une des applications j,j' est un prolongement de l'autre. Il existe donc une application j_o de M_o dans L' qui prolonge tous les $j \in J_o$. Si x,y sont des éléments de M_o , il y a un $j \in J_o$ tel que $\{x,y\} \in M_j$, d'où $j_o(x+y) = j(x+y) = j(x)+j(y) = j_o(x)+j_o(y)$, et de même $j_o(xy) = j_o(x)\ j_o(y)$. On en conclut que j_o est un isomorphisme de M_o sur un sous-corps de L'. Il est évident que j_o prolonge h , d'où $j_o \in J$, ce qui démontre que l'ensemble J est inductif.

Soit j^* un élément maximal de J . Posons $M = M_{j^*}$, $M' = j^*(M)$. Le théorème 3 sera démontré si nous établissons que $M = L$. Soit x un élément de L ; x est algébrique par rapport à K , donc aussi par rapport à M . Soit f(X) le polynome minimal de x par rapport à M . Si g est un polynome quelconque en une lettre X à coefficients dans M , nous désignerons par $j_1^*(g)$ le polynome déduit de g en appliquant l'opération j^*

à ses coefficients ; j_1^* est donc un isomorphisme de $M[X]$ sur $M'[X]$; posons $f' = j_1^*(f)$. Puisque L' est algèbriquement fermé, f' peut se représenter comme produit de polynomes du premier degré à coefficients dans L', d'où il résulte immédiatement que f' admet au moins un zéro x' dans L'. Il résulte de la prop.3, § 2 qu'il existe un isomorphisme j^{**} de $M\langle x\rangle$ sur $M'\langle x'\rangle$ qui prolonge j^*.

Puisque j^* est maximal dans J, on a $j^{**} = j^*$, d'où $M\langle x\rangle = M$, $x \in M$. Ceci étant vrai pour tout $x \in L$, on a $L = M$ et le th.3 est démontré.

Corollaire 1.- Soient (K,L) et (K,L') des extensions algèbriquement fermées d'un corps K. Soient M un sous-corps de L contenant K et j un isomorphisme de M sur un sous-corps de L' qui coïncide avec l'identité sur K. On peut alors prolonger j par un isomorphisme de L sur L'.

On peut prolonger j par un isomorphisme de L sur un sous-corps L'_1 de L'. Le corps L'_1, étant isomorphe à L, est algèbriquement fermé. D'autre part, puisque $K \subset L'_1$, l'extension (L'_1, L') est algèbrique, d'où $L'_1 = L'$.

Corollaire 2. Soient (K,L) et (K,L') des extensions algèbriques algèbriquement fermées d'un corps K. Il existe alors un isomorphisme de L sur L' qui coïncide avec l'identité sur K.

C'est un cas particulier du corollaire 1.

---

§ 4. EXTENSIONS NORMALES.

Rappelons qu'on appelle automorphisme d'un corps tout isomorphisme de ce corps sur lui-même.

Définition 1.- On appelle automorphisme d'une extension (K,L) d'un corps K tout automorphisme de L qui applique chaque élément de K sur lui-même.

Il est clair que les automorphismes d'une extension forment ungroupe.

Définition 2.- Soit (K,L) une extension d'un corps K , et soient x et x' des éléments de L algébriques par rapport à K . On dit que x et x' sont conjugués par rapport à K , s'ils ont le même polynome minimal par rapport à K .

Proposition 1. Soit (K,L) une extension d'un corps K , et soit x un élément de L algèbrique par rapport à K . Les conjugués de x par rapport à K dans L sont alors tous les zéros dans L du polynome minimal de x par rapport à K .

Soit f(X) le polynome minimal de x par rapport à K . Il est clair que tout conjugué de x est un zéro de f(X). Soit réciproquement x' un zéro de f(X) dans L , et soit f'(X) le polynome minimal de x' par rapport à K . On a donc $f = f'h$, $h \in K[X]$ (prop.2 §2), d'où $f'(x)h(x)=0$. Puisque f est le polynome minimal de x , l'un au moins des polynomes f' ou h est de degré au moins égal au degr! n de f ; comme f' ne peut être de degré 0 , h doit être de degré 0 . Puisque les coefficients de X^n dans f et dans f' sont égaux à 1, on a $f = f'$, ce qui prouve que x' est conjugué de x .

Proposition 2. Soit (K,L) une extension d'un corps K et soit x un élément de L algèbrique par rapport à K . Tout automorphisme de (K,L) change x en l'un de ses conjugués par rapport à K .

Soit $f(X) = X^n + \sum_{i=1}^{n} a_i X^{n-i}$ le polynome minimal de x par rapport à K , et soit σ un automorphisme de (K,L). On a $\sigma(a_i) = a_i$ $(1 \leqslant i \leqslant n)$. Si nous posons $\sigma(x) = x'$, l'égalité $x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$ entraîne $x'^n + \sum_{i=1}^{n} a_i x'^{n-i} = 0$, d'où $f(x')=0$, et la prop.2 résulte alors de la prop.1 .

La réciproque de la prop.2 n'est pas vraie en général : si x et x' sont des éléments de L conjugués par rapport à K , il n'existe pas toujours un automorphisme de (K,L) qui change x en x'. Cependant, nous allons voir que la réciproque est vraie dans le cas des extensions algèbriquement fermées.

Proposition 3. Soit (K,L) une extension algèbriquement fermée d'un corps K , et soient x et x' des éléments de L algèbriques par rapport à K . Pour que x et x' soient conjugués par rapport à K , il faut et suffit qu'il existe un automorphisme de (K,L) qui change x en x'.

Nous savons déjà que la condition est suffisante. Supposons x et x' conjugués par rapport à K . Il résulte de la prop.3, § 2 qu'il existe un isomorphisme σ de $K\langle x\rangle$ sur $K\langle x'\rangle$ qui applique tout élément de K sur lui-même et qui applique x sur x'. Il résulte du corollaire 1 au th.3, § 3 que σ peut se prolonger par un automorphisme de (K,L), ce qui démontre la prop.3 .

Définition 3. Si σ est un automorphisme d'un corps L , on appelle invariant de σ tout élément $x \in L$ tel que $\sigma(x) = x$. Si S est un ensemble d'automorphismes de L , on appelle invariant de S tout élément de L qui est un invariant de tous les éléments de S .

Proposition 4. Soit S un ensemble d'automorphismes d'un corps L . Les invariants de S forment alors un sous-corps de L .

Cela résulte immédiatement des définitions.

Il résulte immédiatement de la prop.4 que tout élément du corps premier contenu dans un corps K en invariant par tout automorphisme de K . En particulier, un corps premier n'admet aucun automorphisme distinct de l'identité. * On verra plus tard qu'il en est de même du corps des nombres réels * .

Supposons que (K,L) soit une extension algèbrique algèbriquement fermée d'un corps K , et soit G le groupe des automorphisme de cette extension. Il résulte de la prop.3 que les invariants de G sont les éléments x de L qui n'admettent pas de conjugués différents d'eux-mêmes. Soit $f(X)$ le polynome minimal d'un tel élément x . Puisque $f(X)$ se décompose en facteurs du premier degré à coefficients dans L , il résulte de la prop.1 que $f(X)$ doit être de la forme $(X-x)^n$, où n est le degré de x par rapport à K . Si $n>1$, x est aussi un zéro de $df/dX = n(X-x)^{n-1}$; si df/dX était $\neq 0$, ce serait un polynome de degré $n-1$ à coefficients dans K et f ne serait pas le polynome minimal de x . Donc $df/dX = 0$, d'où $nX^{n-1}=0$, ce qui implique que K est de caractéristique $p>0$ et que n est multiple de p . Nous allons voir que n doit être une puissance de p . En effet, il est clair que l'on peut mettre n sous la forme $p^a n'$, où n' est un entier non divisible par p . On a alors $f(X) = (Xp^a - x^{p^a})^{n'}$ et le coefficient de $X^{p^a(n'-1)}$ dans f est $-n'x^{p^a}$. Si ε est l'élément unité de K , on a $n'\varepsilon \neq 0$; puisque $-n'x^{p^a} \in K$, on a aussi $x^{p^a} \in K$, d'où $n \leqslant p^a$ et par suite $n = p^a$.

Définition 4. Soit (K,L) une extension d'un corps K . Un élément x de L est dit radiciel par rapport à K si l'une ou l'autre des conditions suivantes est satisfaite : a) $x \in K$; b) K est de caractéristique $p>0$ et il existe un entier $a>0$ tel que $x^{p^a} \in K$. Si tout élément de L est radiciel par rapport à K , on dit que (K,L) est une extension radicielle, ou encore que L est radiciel par rapport à K .

Revenant aux notations utilisées plus haut, nous avons vu que tout invariant de G est radiciel par rapport à K . Inversement, soit x un élément de L qui est radiciel par rapport à K . Si K est de caractéristique 0, x est évidemment un invariant de G . Sinon, soit p la caractéristique de K , et soit a un entier >0 tel que $x^{p^a} = y \in K$. Si $\sigma \in G$, on a $(\sigma(x))^{p^a} = \sigma(y) = y = x^{p^a}$, d'où $(\sigma(x)-x)^{p^a} = 0$ et $\sigma(x)=x$, ce qui montre que x est un invariant de G . Nous avons donc démontré la

Proposition 5. Soit (K,L) une extension algèbrique algèbriquement fermée d'un corps K . Les invariants du groupe des automorphismes de (K,L) sont alors les éléments de L qui sont radiciels par rapport à K .

Définition 6.- Une extension algèbrique (K,M) d'un corps K est dite normale si le polynome minimal par rapport à K d'un élément quelconque de M peut se représenter comme produit de polynomes du premier degré à coefficients dans M .

Il est clair que toute extension algèbrique algèbriquement fermée est normale. De plus, si K est un corps quelconque, l'extension (K,K) ent normale .

Théorème 1. Soient (K,M) une extension normale d'un corps K et soit N un sous-corps de M contenant K . Tout isomorphisme de N sur un sous-corps de M qui coïncide avec l'identité sur K peut se prolonger par un automorphisme de (K,M) . Pour que (K,N) soit normale, il faut et suffit que $\sigma(N)=N$ pour tout automorphisme σ de (K,M).

Soit (M,L) une extension algèbrique algèbriquement fermée de M . Un isomorphisme σ_0 de N sur un sous-corps de M qui coïncide avec l'identité sur K peut se prolonger par un automorphisme σ de (K,L) (corol.1 au th.3, § 3). Soient x un élément de M et f(X) le polynome minimal de x par rapport à K ; on a donc $f(X) = \prod_{i=1}^{n}(X - x_i)$, avec $x_i \in M$ $(1 \leqslant i \leqslant n)$.

Or $\sigma(x)$ est conjugué de x par rapport à K (prop.2), d'où $f(\sigma(x)) = \prod_{i=1}^{n}(\sigma(x)-x_i)=0$, ce qui montre que $\sigma(x)$ est l'un des éléments $x_1,..,x_n$, i.e. que $\sigma(x)\in M$. On a donc $\sigma(M)\subset M$; comme on a aussi $\sigma^{-1}(M)\subset M$, on a $\sigma(M)=M$, et la restriction de σ à M est un automorphisme de (K,M) qui prolonge σ_0. Le raisonnement que nous venons de faire prouve que, si (K,M) est normale, tout automorphisme de (K,L) applique M sur lui-même. Ceci dit, si (K,N) est normale, il est clair en vertu de ce qui précède que tout automorphisme de (K,M) applique N sur lui-même. Inversement, supposons cette dernière condition satisfaite. Utilisant les mêmes notations que plus haut, supposons de plus que $x\in N$. Chaque x_i est un conjugué de x (prop.1), d'où $x_i=\tau_i(x)$, où τ_i est un automorphisme de (K,L) (prop.3). La restriction de τ_i à M est un automorphisme de (K,M), d'où $\tau_i(N)=N$ et $\tau_i(x)\in N$ $(1\leqslant i\leqslant n)$, ce qui montre que (K,N) est normale.

Corollaire 1. Soit (K,L) une extension d'un corps K, et soit $(M_i)_{i\in I}$ une famille de sous-corps de L. Supposons que les corps M_i contiennent tous K, et que les extensions (K,M_i) soient normales. Les extensions $(K, \bigcap_{i\in I} M_i)$ et $(K, K\langle \bigcup_{i\in I} M_i \rangle)$ sont alors normales.

Soit (L, L_1) une extension algèbriquement fermée de L, et soit L_2 le corps formé des éléments de L_1 qui sont algèbriques par rapport à K. Il est clair que $M_i\subset L_2$ pour tout $i\in I$ et que L_2 est algèbriquement fermé.

L'extension (K,L_2) est normale, et tout automorphisme de cette extension transforme chacun des corps M_i en lui-même. Le corollaire découle alors immédiatement du th. 1.

Corollaire 2. Soit (K,N) une extension algèbrique d'un corps K. Il existe alors une extension (N,M) de N qui possède les propriétés suivantes

l'extension (K,M) est normale, et le seul sous-corps M' de M contenant N tel que (K,M') soit normale est M lui-même.

Soit en effet (N,L) une extension algèbrique algèbriquement fermée de N . Il suffit de prendre pour M l'intersection de tous les sous-corps P de L contenant N et tels que (K,P) soit normale.

Définition 7.- Les notations étant les mêmes que dans le corollaire 2 ci-dessus, on dit que (K,M) est une extension normale minima déterminée par N .

Proposition 6. Soient (K,N) une extension algèbrique d'un corps K , (K,M) une extension normale minima déterminée par N et (K,M') une extension normale de K . Supposons qu'il existe un isomorphisme j de N sur un sous-corps de M' qui coïncide avec l'identité sur K . On peut alors prolonger j par un isomorphisme de M sur un sous-corps de M'.

Soient (M,L) et (M',L') des extensions algèbriques algèbriquement fermées de M et de M' respectivement. Il résulte du corol1 au th.3, § 3 que l'on peut prolonger j par un isomorphisme j_1 de L sur L'. Posons $j(N) = N_1$, $j_1(M) = M_1$. Il est clair que (K,M_1) est une extension normale minima déterminée par N_1 , d'où $M_1 \cap M' = M_1$ et $M_1 \subset M'$, ce qui démontre la proposition 6 .

Corollaire. Soit (K,N) une extension algèbrique d'un corps K , et soient (K,M) et (K,M') des extensions normales minima déterminées par N . Il existe alors un isomorphisme de M sur M' qui coïncide avec l'identité sur N .

Cela résulte immédiatement de la prop. 6 .

Proposition 7. Soient (K,M) une extension normale d'un corps K et f(X) un polynome en une lettre X à coefficients dans K . Soit A l'ensemble des zéros de f(X) dans M . L'extension $(K,K\langle A\rangle)$ est alors normale.

Il est clair que tout automorphisme de (K,M) permute entre eux les

les éléments de A ; la proposition 7 découle donc immédiatement du th.1 .

Proposition 8.- Soient (K,N) une extension finie d'un corps K , et (K,M) une extension normale minima déterminée par N . L'extension (K,M) est alors finie.

Il est clair que l'on peut trouver une partie finie B de N telle que $N = K\langle B\rangle$ (par exemple, une base de N par rapport à K). Soit f(X) le produit des polynomes minimaux par rapport à K des éléments de N . Introduisons une extension algèbrique algèbriquement fermée (N,L) de N , et désignons par A l'ensemble des zéros de f(X) dans L . L'extension $(K,K\langle A\rangle)$ est finie (prop.4, § 2) et normale (prop.7). De plus, on a $N \subset K\langle A\rangle$. Donc $K\langle A\rangle$ contient un sous-corps M_1 tel que (K,M_1) soit finie et soit une extension normale minima déterminée par N . La prop.8 découle alors du corollaire à la prop.6 .

Proposition 9. Soit (K,U) une extension d'un corps K , et soient M et N des sous-corps de U contenant K . Si l'extension (K,M) est normale, il en est de même de $(N,N\langle M\rangle)$.

Soit (U,U^*) une extension algèbriquement fermée de U, et soit N^* le corps formé des éléments de U^* qui sont algèbriques par rapport à N ; N^* est évidemment algèbriquement fermé. De même, le corps K^* formé des éléments de N^* qui sont algèbriques par rapport à K est algèbriquement fermé. Si σ est un automorphisme de (N,N^*), σ est aussi un automorphisme de (K,N^*) et on a évidemment $\sigma(K^*) = K^*$. L'extension (K,K^*) étant normale, le th.1 montre que $\sigma(M) = M$, d'où $\sigma(N\langle M\rangle) = N\langle M\rangle$, et la prop.9 résulte de la prop.6 .

Proposition 10.- Soit (K,M) une extension normale d'un corps K . Une condition nécessaire et suffisante pour qu'un élément x de M soit un invariant du groupe des automorphismes de (K,M) est que x soit radiciel par rapport à K .

Soit (M,L) une extension algèbrique algèbriquement fermée de M . Tout automorphisme de (K,M) peut se prolonger par un automorphisme de (K,L) (corol.1 au th.3, § 2) et tout automorphisme de (K,L) induit un automorphisme de (K,M) (th.1). Les invariants du groupe des automorphismes de (K,M) sont donc ceux des invariants du groupe des automorphismes de (K,L) qui sont dans M . La prop.10 résulte alors de la prop.5 .

Proposition 11. Soient M un corps, G un groupe d'automorphismes de M et K le corps des invariants de G . Si l'extension (K,M) est algèbrique, elle est normale. Si x est un élément de M algèbrique et de degré m par rapport à K , le polynome minimal de x par rapport à K admet m zéros distincts dans M , qui sont tous simples.

Soit x un élément de M algèbrique par rapport à K . Si $\sigma \in G$, $\sigma(x)$ est conjugué de x par rapport à K , ce qui montre que l'ensemble des $\sigma(x)$ (pour $\sigma \in G$) est fini. Soient $x_1,..,x_m$ les éléments distincts de cet ensemble, et soit $g(X) = \prod_{i=1}^{m}(X-x_i)$. Si on soumet les coefficient de g à un automorphisme $\sigma \in G$, on obtient un polynome $g' = \prod_{i=1}^{m}(X - \sigma(x_i))$ qui est égal à g parce que σ permute entre eux les éléments $x_1,..,x_m$. On a donc $g \in K[X]$; puisque $g(x) = 0$, g est divisible dans $K[X]$ par le polynome minimal f de x par rapport à K . D'autre part, $x_1,...,x_m$ sont des zéros de f , et par suite f est de degré $\geqslant m$. Le coefficient de X^m dans g étant 1 , on en déduit que $g = f$. On voit donc que, si (K,M) est algèbrique, le polynome minimal par rapport à K de tout élément de M se décompose en facteurs du premier degré dans $M[X]$, ce qui montre que (K,M) est normale. Puisque f, qui est de degré m , admet m zéros distincts, ces zéros sont tous simples.

---

§ 5. LA THEORIE DE GALOIS.

Définition 1. Une extension (K,L) d'un corps K est dite galoisienne si elle satisfait aux conditions suivantes : 1) elle est finie ; 2) tout invariant du groupe de ses automorphismes est dans K . Le groupe des automorphismes de (K,L) s'appelle alors le groupe de Galois de l'extension, ou groupe de Galois de L par rapport à K .

Il résulte immédiatement de la prop.11, § 4 qu'une extension galoisienne est toujours normale. Une condition nécessaire et suffisante pour qu'une extension normale finie (K,L) soit galoisienne est que tout élément de L qui est radiciel par rapport à K soit dans K (prop.10, § 4).

Proposition 1.- Soient L un corps, G un groupe fini d'automorphismes de L et K le corps des invariants de G . L'extension (K,L) est alors galoisienne et son degré est égal à l'ordre de G .

Soient $\sigma_1,\dots,\sigma_n$ les éléments distincts de G , σ_1 représentant l'identité. Soient $a_1,..,a_{n+1}$ n+1 éléments de L . Nous allons montrer que ces éléments sont linéairement dépendants par rapport à K . Introduisons n+1 lettres $X_1,..,X_{n+1}$ et écrivons le système de n équations linéaires

$$(1) \qquad \sum_{i=1}^{n+1} \sigma_j(a_i)X_i = 0 \qquad (1 \leqslant j \leqslant n)$$

Ce système admet au moins une solution non triviale dans L . Parmi toutes les solutions non triviales de (1) nous en choisissons une, soit $(x_1,..,x_{n+1})$, pour laquelle le nombre r des inconnues qui reçoivent la valeur 0 est le plus grand possible. Soit α un indice tel que $x_\alpha \neq 0$; posons $y_i = x_i x_\alpha^{-1}$ $(1 \leqslant i \leqslant n+1)$. Donc $(y_1,..,y_{n+1})$ est une solution de (1) et $y_\alpha = 1$ (l'élément unité de K). Soit σ un élément quelconque de G ; on a $\sum_{i=1}^{n+1} \sigma(y_i)\,\sigma\sigma_j(a_i) = 0$ $(1 \leqslant j \leqslant n)$; or, si j varie de 1 à n , $\sigma\sigma_j$ parcourt l'ensemble G tout entier. Il en résulte que les formules $X_i = \sigma(y_i)$

fournissent encore une solution de (1), et qu'il en est par suite de même des formules $X_i = \sigma(y_i)-y_i$. Or on a $\sigma(y_\alpha)-y_\alpha = 0$ et il y a r indices i différents de α tels que $y_i=\sigma(y_i)=0$. Il y a donc r+1 indices i tels que $\sigma(y_i)-y_i=0$; en vertu de notre choix de r, cela signifie que $\sigma(y_i)=y_i$ $(1\leqslant i\leqslant n+1)$. Ceci étant vrai pour tout $\sigma\in G$, on a $y_i\in K$ $(1\leqslant i\leqslant n+1)$. Or, la première des équations (1) donne $\sum_{i=1}^{n+1} a_i y_i=0$. Notre assertion que $a_1,..,a_{n+1}$ sont linéairement dépendants par rapport à K est donc prouvée. Il en résulte immédiatement que (K,L) est finie et de degré $\leqslant n$. Pour établir que le degré de cette extension est n, nous démontrerons d'abord le lemme suivant :

Lemme 1. Soient L et Ω des corps, et $\sigma_1,..,\sigma_n$ des isomorphismes distincts de L sur des sous-corps de Ω . Si $\omega_1,..,\omega_n$ sont des éléments de Ω tels que $\sum_{j=1}^{n} \omega_j\sigma_j(x) = 0$ pour tout $x\in L$, on a $\omega_1=...=\omega_n = 0$. Les éléments x de L pour lesquels les $\sigma_j(x)$ sont tous égaux entre eux forment un sous-corps K de L ; il est impossible que l'extension (K,L) soit finie et de degré $\leqslant n$.

Nous démontrerons la première assertion par récurrence sur n. Elle est évidente pour n=1 . Supposons la vraie pour tout système de n-1 isomorphismes (où $n>1$). Soient $\omega_1,..,\omega_n$ des éléments de Ω tels que $\sum_{j=1}^{n} \omega_j\sigma_j(x) = 0$ pour tout $x\in L$. On a, pour tout $y\in L$, $\sigma_1(y)\sum_{j=1}^{n} \omega_j\sigma_j(x)=0$ et aussi $\sum_{j=1}^{n} \omega_j\sigma_j(yx) = 0 = \sum_{j=1}^{n} \omega_j\sigma_j(y)\sigma_j(x)$, d'où $\sum_{j=2}^{n} \omega_j(\sigma_j(y)-\sigma_1(y))\sigma_j(x) = 0$. Il en résulte que $\omega_j(\sigma_j(y)-\sigma_1(y))=0$ pour $2\leqslant j\leqslant n$, $y\in L$. Pour chaque $j>1$ il existe un $y\in L$ tel que $\sigma_j(y)\neq\sigma_1(y)$, d'où $\omega_j=0$. Il en résulte immédiatement que $\omega_1=0$. La première assertion est donc démontrée. Il est évident que les éléments x tels que les $\sigma_j(x)$ soient tous égaux entre eux forment un sous-corps K de L . Supposons que (K,L) soit finie et de degré m ; soit alors $(u_1,..,u_m)$ une base de L par rapport à K . Introduisons n lettres

$z_1,..,z_n$ et écrivons le système d'équations linéaires

(2) $\sum_{j=1}^{n} z_j \sigma_j(u_k) = 0 \qquad (1 \leqslant k \leqslant m)$

Tout élément $u \in L$ peut se mettre sous la forme $u = \sum_{k=1}^{m} x_k u_k$, $x_k \in K$ $(1 \leqslant k \leqslant m)$; on en conclut aisément que, si $(z_1,..,z_m)$ est une solution de (2), on a $\sum_{j=1}^{n} z_j \sigma_j(u) = 0$ pour tout $u \in L$, d'où $z_1 = \ldots = z_n = 0$. Il en résulte que $m \geqslant n$; le lemme 1 est donc démontré.

Revenant à la démonstration de la prop.1 et aux notations utilisées plus haut, on voit que tout $x \in L$ pour lequel les $\sigma_j(x)$ sont tous égaux entre eux est un invariant de G . Il résulte donc du lemme 1 que $\left[L : K\right] \geqslant n$. Comme nous savons déjà que $\left[L : K\right] \leqslant n$, la prop.1 est démontrée.

Théorème 1. Soient (K,L) une extension galoisienne d'un corps K et G le groupe de Galois de cette extension. Si M est un sous-corps de L contenant K , l'extension (M,L) est galoisienne. Si M est le corps des invariants d'un sous-~~sarp~~ groupe H de G , H est le groupe de Galois de (M,L).

Soit H_o le groupe des automorphismes de (M,L) ; H_o est donc un sous-groupe de G . Désignons par n l'ordre de G et par m celui de H_o. Tout élément $\sigma \in G$ induit un isomorphisme $\overline{\sigma}$ de M sur un sous-corps de L ; si σ_1 , $\sigma_2 \in G$, une condition nécessaire et suffisante pour que $\overline{\sigma}_1 = \overline{\sigma}_2$ est que $\sigma_1 H_o = \sigma_2 H_o$; puisqu'il y a n/m ensembles distincts de la forme σH_o , on voit qu'il y a au moins n/m isomorphismes distincts de M sur des sous-corps de L qui coïncident avec l'identité sur K , d'où, en vertu du lemme 1 , $\left[M : K\right] \geqslant n/m$. D'autre part, on a $\left[L : K\right] = n$ (prop.1), d'où $\left[L : M\right] \leqslant m$ (th.1, § 2). Soit M' le corps des invariants de H_o ; l'extension (M',L) est donc galoisienne et de degré m (prop.1). D'autre part, il est évident que $M \subset M'$; puisque $\left[L : M\right] \leqslant m$, il résulte tout de suite du th.1, § 2 que $M = M'$. L'extension (M,L) est donc galoisienne, et on a $\left[L : M\right] = m$. Supposons que M soit le corps des invariants

d'un sous-groupe H de G . On a alors $H \subset H_0$; d'autre part, l'ordre de H est égal à $[L : M]$ (prop.1), donc à l'ordre de H_0. Il en résulte que $H = H_0$. Le théorème 1 est donc démontré.

Soit (K,L) une extension galoisienne. Il résulte immédiatement du th.1 qu'il existe une correspondance bi-univoque entre les sous-groupes H de G et les sous-corps M de L contenant K dans laquelle, si H et M se correspondent, M est le corps des invariants de H tandis que H est le groupe de Galois de (M,L). Le théorème suivant donne de nouvelles propriétés de cette correspondance.

Théorème 2. Soient (K,L) une extension galoisienne, G le groupe de Galois de cette extension, H_1 et H_2 des sous-groupes de G et M_1 et M_2 les corps des invariants de H_1 et H_2 respectivement. Dans ces conditions :

1) les conditions $H_1 \subset H_2$ et $M_2 \subset M_1$ sont équivalentes ;

2) le corps des invariants de $H_1 \cap H_2$ est le sous-corps de L engendré par M_1 et M_2 ;

3) le corps des invariants du sous-groupe de G engendré par H_1 et H_2 est $M_1 \cap M_2$.

Si $H_1 \subset H_2$, on a évidemment $M_2 \subset M_1$. Inversement, si $M_2 \subset M_1$, on a $H_1 \subset H_2$ parce que H_1 est le groupe de Galois de (M_1, L) $(i=1,2)$.

Le corps des invariants M'_3 de $H_1 \cap H_2$ contient évidemment M_1 et M_2 donc aussi le corps M_3 engendré par M_1 et M_2 . D'autre part, le groupe de Galois de (M_3, L) est évidemment contenu dans $H_1 \cap H_2$, d'où $M_3 \supset M'_3$. On a donc $M_3 = M'_3$.

Le corps des invariants M_4 du groupe H_4 engendré par H_1 et H_2 est évidemment contenu dans $M_1 \cap M_2$. D'autre part, le groupe de Galois de $(M_1 \cap M_2 , L)$ contient H_1 et H_2, donc aussi H_4 , d'où $M_1 \cap M_2 \subset M_4$.

On a donc $M_1 \cap M_2 = M_4$.

Les assertions 2) et 3) du théorème 2 se généralisent aisément au cas où on considère un ensemble quelconque de sous-groupes de G . Nous laissons au lecteur le soin de faire cette généralisation.

Proposition 2.- Soient (K,L) une extension galoisienne et G son groupe de Galois. Soit M le corps des invariants d'un sous-groupe H de G . Si $\sigma \in G$, le corps des invariants de $\sigma H \sigma^{-1}$ est $\sigma(M)$. Pour que (K,M) soit galoisienne, il faut et suffit que H soit un sous-groupe distingué de G . S'il en est ainsi, le groupe de Galois de (K,M) est isomorphe à G/H .

Si $x \in M$, $\eta \in H$, on a $(\sigma\eta\sigma^{-1})(\sigma(x)) = \sigma(x)$, de sorte que $\sigma(M)$ est contenu dans le corps des invariants de $\sigma H \sigma^{-1}$. Inversement, si un $y \in L$ est tel que $(\sigma\eta\sigma^{-1})(y) = y$ pour tout $\eta \in H$, on a $\eta(\sigma^{-1}(y)) = \sigma^{-1}(y)$, d'où $\sigma^{-1}(y) \in M$, $y \in \sigma(M)$. La première assertion est donc démontrée. La seconde résulte de la première, de la prop.10, §4 et du th.1 . Supposons (K,M) galoisienne. La restriction $\overline{\sigma}$ à M d'un élément $\sigma \in G$ est alors un automorphisme de (K,M) ; l'application $\sigma \to \overline{\sigma}$ est évidemment un homomorphisme de G dans le groupe de Galois $\overline{G}$ de (K,M) . L'ensemble des $\sigma \in G$ qui sont appliqués sur l'identité est le groupe des automorphismes de (M,L) , c'est-à-dire H . D'autre part, tout automorphisme de (K,M) est la restriction à M d'un automorphisme de (K,L) (th.1, §4), ce qui montre que l'homomorphisme $\sigma \to \overline{\sigma}$ applique G sur $\overline{G}$. La dernière assertion résulte donc du th.3, Alg.I, §6, n°4 .

---

§ 6. EXTENSIONS ALGEBRIQUES SEPARABLES.

Soient (K,L) une extension finie d'un corps K et (K,M) une extension normale minima déterminée par L . Nous nous proposons de rechercher à quelle condition l'extension (K,M) sera galoisienne. Il est évidemment nécessaire que tout élément de L qui est radiciel par rapport à K soit dans K ; mais cette condition n'est pas suffisante, comme on peut le montrer par des exemples. Il résulte immédiatement de la prop.11, § 4 qu'il est aussi nécessaire que tout élément de L soit un zéro simple de son polynome minimal par rapport à K . Nous montrerons au cours de ce § que cette condition est aussi suffisante.

Définition 1.- Soit (K,L) une extension d'un corps K . On dit qu'un élément x de L qui est algèbrique par rapport à K est séparable par rapport à K s'il est un zéro simple de son polynome minimal par rapport à K . Si (K,L) est algèbriquement et si tous les éléments de L sont séparables par rapport à K , on dit que (K,L) est séparable, ou que L est séparable par rapport à K .

Remarque. On définira plus loin la notion de séparabilité pour les extensions non-algèbriques.

Proposition 1. Soient (K,L) une extension d'un corps K et x un élément de L qui est zéro d'un polynome g(X) à coefficients dans K , mais qui n'est pas zéro de $dg\,dX$; x est alors séparable par rapport à K .

Soit en effet f le polynome minimal de x par rapport à K ; on a $g = fh$, où h est un polynome à coefficients dans K (prop.2, § 2). Il en résulte que $0 \neq (dg/dX)(x) = (df/dX)(x).h(x)$, d'où $(df/dX)(x) \neq 0$, ce qui montre que x est un zéro simple de f .

Proposition 2.- Soient (K,L) une extension d'un corps K et x un élément de L algèbrique par rapport à K . Si K est de caractéristique 0, x est séparable par rapport à K . Si K est de caractéristique $p>0$, il existe un entier $e \geqslant 0$ qui possède les propriétés suivantes : x^{p^e} est séparable par rapport à K ; pour tout $k>0$, on a $K\langle x^{p^{e+k}}\rangle = K\langle x^{p^e}\rangle$; le degré de l'extension $(K\langle x^{p^e}\rangle, K\langle x\rangle)$ est p^e ; si $g(X)$ est le polynome minimal de x^{p^e} par rapport à K, celui de x est $g(X^{p^e})$. L'entier e est uniquement caractérisé par ces propriétés. Pour que x soit séparable par rapport à K, il faut et suffit que $e = 0$.

Soit $f(X)$ le polynome minimal de x par rapport à K . Si K est de caractéristique 0, df/dX est $\neq 0$ et de degré moindre que f ; donc x n'est pas un zéro de df/dX et est un zéro simple de f . Supposons que K soit de caractéristique $p>0$; soit e le plus grand entier $h \geqslant 0$ tel que $f(X) \in K\left[X^{p^h}\right]$; on peut donc écrire $f(X) = g(X^{p^e})$, où g est un polynome à coefficients dans K qui n'est pas dans $K\left[X^p\right]$. Il résulte immédiatement de cette propriété de g que $dg\,dX = 0$. Soit d le degré de g ; on a $g(x^{p^e})=0$, et par suite g est divisible par le polynome minimal de x^{p^e} ; d'où $\left[K\langle x^{p^e}\rangle : K\right] \leqslant d$ (cf. prop.2, § 2). D'autre part, $X^{p^e}-x^{p^e}$ est divisible dans $(K\langle x^{p^e}\rangle)\left[X\right]$ par le polynome minimal de x par rapport à $K\langle x^{p^e}\rangle$, d'où $\left[K\langle x\rangle : K\langle x^{p^e}\rangle\right] \leqslant p^e$. Le polynome f étant de degré d^{p^e} , on a $d^{p^e} = \left[K\langle x\rangle : K\right] =$ $= \left[K\langle x\rangle : K\langle x^{p^e}\rangle\right] \cdot \left[K\langle x^{p^e}\rangle : K\right]$, d'où $\left[K\langle x\rangle : K\langle x^{p^e}\rangle\right] = p^e$ et $\left[K\langle x^{p^e}\rangle : K\right] = d$. Le coefficient de X^d dans g étant 1, g est le polynome minimal de x^{p^e} par rapport à K ; puisque dg/dX est de degré $< d$ et est $\neq 0$. On a $(dg/dX)(x^{p^e}) \neq 0$, et x^{p^e} est séparable par rapport à K . Posons $y = x^{p^e}$, et formons une extension normale (K,M) de K telle que M contienne L comme sous-corps. On a $g(X) = \prod_{i=1}^{d}(X-y_i)$, où $y_1,\ldots,y_d \in M$ et $y_1 = y$. Il existe pour chaque i $(1 \leqslant i \leqslant d)$

un automorphisme σ_i de (K,M) tel que $\sigma_i(y_1) = y_i$ (prop.3 et th.1, § 4), d'où il résulte que chaque y_i est un zéro simple de g et par suite que $y_i \neq y_j$ pour $i \neq j$. On a donc $y_i^{p^k} - y_j^{p^k} = (y_i - y_j)^{p^k} \neq 0$ pour $i \neq j$, $k \geqslant 0$; il en résulte que y^{p^k} admet d conjugués distincts dans M, d'où (puisque $y^{p^k} \in K\langle y \rangle$), $\left[K\langle y^{p^k}\rangle : K\right] \geqslant d$ et par suite $K\langle y^{p^k}\rangle = K\langle y\rangle$, c'est-à-dire $K\langle x^{p^{e+k}}\rangle = K\langle x^{p^e}\rangle$. L'entier e que nous avons défini possède donc bien les propriétés annoncées. Inversement, si un entier e possède ces propriétés, f(X) peut se mettre sous la forme $g(X^{p^e})$, où g est un polynome à coefficients dans K et le degré de g est égal au degré de x^{p^e} par rapport à K. Si g pouvait s'écrire sous la forme $g_1(X^{p^{e+k}})$, où $k \geqslant 0$ (g_1 étant un polynome à coefficients dans K), g_1 serait de degré plus petit que g et on aurait $g_1(x^{p^{e+k}})=0$, ce qui est impossible puisque $K\langle x^{p^{e+k}}\rangle = K\langle x^{p^e}\rangle$; on voit donc que e est uniquement déterminé par les propriétés que nous lui avons imposées. Si $e = 0$, $x = x^{p^e}$ est séparable par rapport à K ; si $e > 0$, on voit tout de suite que $df/dX = 0$, donc que x n'est pas séparable par rapport à K.

Corollaire. Soit (K,L) une extension d'un corps K de caractéristique $p > 0$. Pour qu'un élément x de L qui est algébrique par rapport à K soit séparable par rapport à K, il faut et suffit que $K\langle x^p\rangle = K\langle x\rangle$.

La condition est évidemment nécessaire en vertu de la prop.2. Inversement, si elle est satisfaite, le degré de x^p par rapport à K est le même que celui de x ; il en résulte que le polynome minimal f(X) de x par rapport à K ne peut pas se mettre sous la forme $h(X^p)$, où h est un polynome à coefficients dans K (on aurait en effet $h(x^p)=0$ et h serait de degré plus petit que f). On voit que dans ce cas le nombre e de la prop.2 est nécessairement 0.

Proposition 3.- *Soit* (K,L) *une extension finie d'un corps* K *de caractéristique* $p>0$. *Pour que cette extension soit séparable, il faut et suffit que* $K\langle L^p\rangle = L$ (*où* L^p *est le corps des* p-*ièmes puissances d'éléments de* L).

Si (K,L) est séparable, on a, pour tout $x\in L$, $K\langle x\rangle = K\langle x^p\rangle \subset K\langle L^p\rangle$ d'où $L = K\langle L^p\rangle$. Inversement, supposons que $K\langle L^p\rangle = L$. Soit x un élément de L ; formons une base $(x_i)_{1\leqslant i\leqslant n}$ de L par rapport à K qui contienne une base $(x_i)_{1\leqslant i\leqslant d}$ de $K\langle x\rangle$ par rapport à K ; on peut de plus supposer que $x_1=1$. On a $x_ix_j = \sum_{k=1}^{n} c_{ijk}x_k$ avec $c_{ijk}\in K$, d'où $x_i^p x_j^p = \sum_{k=1}^{n} c_{ijk}^p x_k^p$, ce qui montre que l'espace vectoriel $O = \sum_{k=1}^{n} Kx_i^p$ est un sous-anneau de L . Puisque $x_1=1$, on a $K\subset O$. Si $y = \sum_{i=1}^{n} a_ix_i \in L$ (avec $a_i\in K$, $1\leqslant i\leqslant n$), on a $y^p = \sum_{i=1}^{n} a_i^p x_i^p \in O$, d'où $L^p\subset O$ et $K[L^p]\subset O$. Or on sait que $L = K\langle L^p\rangle = K[L^p]$ (prop.4, § 2) ; on a donc $O = L$, ce qui montre que $x_1^p,\ldots,x_n^p$ sont linéairement indépendants par rapport à K . Il en est de même de $x_1^p,\ldots,x_d^p$, ce qui montre que l'espace vectoriel $\sum_{i=1}^{d} Kx_i^p$ est de dimension d . Si $1\leqslant i\leqslant d$, on a $x_i\in K\langle x\rangle$, d'où on conclut aisément que $x_i^p\in K\langle x^p\rangle$. On a donc $[K\langle x^p\rangle : K] = d$, d'où $K\langle x^p\rangle = K\langle x\rangle$, ce qui montre que x est séparable par rapport à K .

Proposition 4.- *Soit* (K,L) *une extension algèbrique d'un corps* K . *Supposons que* $L = K\langle A\rangle$, *où* A *est une partie de* L *composée d'éléments séparables par rapport à* K . *L'extension* (K,L) *est alors séparable.*

La proposition est évidente si K est de caractéristique 0 . Supposons K de caractéristique $p>0$. Si $x\in L$, il existe une partie finie $F = \{x_1,\ldots,x_m\}$ de A telle que $x\in K\langle F\rangle$ (lemme 1, § 2). On a $x_i\in K\langle x_i^p\rangle \subset K[F^p]$, d'où $K\langle F\rangle = K[F^p]$. Si nous posons $N = K\langle F\rangle$, on a *a fortiori* $N = K\langle N^p\rangle$. L'extension (K,N), étant finie, est séparable, ce qui prouve que x est séparable par rapport à K .

Corollaire 1.- Soit (K,L) une extension algèbrique d'un corps K . L'ensemble S des éléments de L qui sont séparables par rapport à K est alors un sous-corps de L et l'extension (S,L) est radicielle.

Il résulte de la prop.4 que $K\langle S\rangle \subset S$, donc que S est un corps. Que (S,L) soit radicielle, cela résulte de la prop.2 .

Corollaire 2.- Soient (K,U) une extension d'un corps K , et L et M des sous-corps de U contenant K . Supposons que l'extension (K,L) soit algèbrique et séparable. Il en est alors de même de $(M, M\langle L\rangle)$.

Il résulte en effet immédiatement du corol. à la prop.2 que tout élément de L est séparable par rapport à M .

Nous pouvons maintenant démontrer le résultat annoncé plus haut :

Proposition 5.- Soit (K,L) une extension finie d'un corps K , et soit (K,M) une extension normale minima déterminée par L . Une condition nécessaire et suffisante pour que (K,M) soit galoisienne est que (K,L) soit séparable.

Nous avons déjà observé que la condition est nécessaire. Inversement, supposons-là satisfaite. Soit A l'ensemble de tous les conjugués dans M d'éléments de L . L'ensemble A est transformé en lui-même par tout automorphisme de (K,M) (prop.2, §4), d'où il résulte que $(K, K\langle A\rangle)$ est normale (th.1, §4) et que $K\langle A\rangle = M$. Tout élément de A peut se déduire d'un élément de L par un automorphisme de (K,M) (prop.3, th.1, §4), donc est séparable par rapport à K . Il résulte alors de la prop.5 que (K,M) est séparable. Si $x \in M$, et si K est de caractéristique $p > 0$, on a $K\langle x^p\rangle = K\langle x\rangle$, d'où on déduit par récurrence sur n que $K\langle x^{p^n}\rangle = K\langle x\rangle$ pour tout $n > 0$; si donc x est radiciel par rapport à K , il est dans K . Il en résulte que (K,M) est galoisienne (prop.10, § 4) .

Corollaire 1.- Une condition nécessaire et suffisante pour qu'une extension normale finie soit galoisienne est qu'elle soit séparable.

Corollaire 2.- Soient (K,U) une extension d'un corps K et L et M des sous-corps de U contenant K . Si (K,L) est galoisienne, il en est de même de $(M, M\langle L\rangle)$.

On sait en effet que $(M, M\langle L\rangle)$ est finie (c'est évident), normale (prop.9, §4) et séparable (coroll. 2 à la prop.4) .

Proposition 6. Soient (K,M) une extension normale d'un corps K , L un sous-corps de M contenant K et S le corps formé des éléments de L qui sont séparables par rapport à K . Supposons que (K,S) soit finie et de degré s . Il existe alors exactement s isomorphismes distincts de L sur des sous-corps de M qui coïncident avec l'identité sur K .

Il existe un sous-corps T de M contenant S et tel que l'extension (K,T) soit galoisienne. Soit G le groupe de Galois de cette extension. Si $\sigma \in G$, la restriction $\bar{\sigma}$ de σ à S est un isomorphisme de S sur un sous-corps de M . Inversement, tout isomorphisme η de S sur un sous-corps de M qui coïncide avec l'identité sur K peut se prolonger par un automorphisme η_0 de (K,M) (th.1, §4), et on a $\eta_0(T) = T$ (th.1, §4), ce qui montre que $\eta_0 = \bar{\sigma}$ avec un $\bar{\sigma} \in G$. Soit H le groupe de Galois de (S,T) ; si σ , $\sigma' \in G$, une condition nécessaire et suffisante pour que $\bar{\sigma} = \bar{\sigma}'$ est que $\sigma' H = \sigma H$; le nombre des $\bar{\sigma}$ distincts est donc l'indice de H dans G . Or, l'ordre de G est $[T : K]$, celui de H est $[T : S]$ et on a $[T : K] = [T : S]\,[S : K]$; l'indice de H dans G est donc $[S : K] = s$, ce qui montre qu'il y a exactement s isomorphismes distincts de S sur des sous-corps de M qui coïncident avec l'identité sur K . Chacun de ces isomorphismes peut se prolonger par un isomorphisme de L sur un sous-corps de M (th.1, §4). De plus, si des isomorphismes ζ , ζ' de L sur des sous-corps de M coïncident sur S , ils sont identiques. C'est évident si K est de caractéristique 0 , car alors $S = L$.

si K est de caractéristique $p>0$ et si $x \in L$, il existe un $e \geqslant 0$ tel que $x^{p^e} \in S$ (corol.1 à la prop.4), d'où $(\zeta(x))^{p^e} = \zeta(x^{p^e}) = \zeta'(x^{p^e}) = (\zeta'(x))^{p^e}$ et $(\zeta'(x)-\zeta(x))^{p^e} = (\zeta'(x))^{p^e} - (\zeta(x))^{p^e} = 0$, ce qui démontre notre assertion. La prop.6 est donc démontrée.

Définition 2.- On dit qu'un corps K est parfait si toute extension algèbrique de K est séparable.

Il est clair qu'un corps de caractéristique 0 est parfait. Pour ce qui concerne les corps de caractéristiques $\neq 0$, on a le résultat suivant :

Proposition 7. Pour qu'un corps K de caractéristique $p>0$ soit parfait, il faut et il suffit que $K = K^p$.

Soient x un élément de K et (K,K^*) une extension algèbriquement fermée de K. Il est clair que K^* contient un élément y tel que $y^p = x$. Si K est parfait, $(K,K\langle y\rangle)$ est séparable, et on a $K\langle y^p\rangle = K\langle y\rangle$ (corol. à la prop.2), d'où $y \in K$ et $K^p = K$. Inversement, supposons que $K^p = K$, et soit (K,L) une extension finie de K. Puisque l'application $z \to z^p$ de L sur L^p est un isomorphisme, on a $[L : K] = [L^p : K^p] = [L^p : K]$, d'où $L = L^p$, ce qui prouve que (K,L) est séparable (prop.3). Il résulte de là et de la prop.4 que K est parfait.

Remarque. La démonstration montre de plus que, si (K,M) est une extension finie d'un corps parfait, M est parfait. La conclusion reste évidemment vraie si (K,M) est une extension algèbrique quelconque de K.

---

§ 7. RACINES de l'UNITÉ. CORPS FINIS.

Définition 1.- On dit qu'un élément x d'un corps est une racine de l'unité s'il existe un exposant $n>0$ tel que $x^n = 1$; le plus petit exposant $n>0$ satisfaisant à cette condition est alors appelé l'ordre de x . Si m est un exposant >0 quelconque tel que $x^m = 1$, on dit que x est une racine m-ième de l'unité. Une racine n-ième de l'unité qui est d'ordre n est appelée une racine primitive n-ième de l'unité.

Soit x une racine de l'unité d'ordre n dans un corps K . L'application $h \to x^h$ est un homomorphisme du groupe additif Z dans le groupe multiplicatif K^* des éléments $\neq 0$ de K , et l'image inverse de 1 par rapport à cet homomorphisme est l'ensemble nZ des multiples de n . Le sous-groupe de K engendré par x est donc cyclique d'ordre n . Si K est de caractéristique $p>0$, n n'est pas divisible par p . Supposons en effet $n = pn'$, d'où $(x^{n'})^p = 1 = 1^p$, $(x^{n'}-1)^p = 0$ et $x^{n'}=1$, ce qui est impossible puisque $n'<n$.

Proposition 1.- Soit K un corps algébriquement fermé, et soit n un entier >0 qui n'est pas divisible par la caractéristique de K . Il existe alors dans K une racine primitive n-ième x de l'unité ; x est séparable par rapport à tout sous-corps de K .

Nous procéderons par récurrence sur n . La proposition est évidente si $n=1$. Supposons la vraie pour tous les entiers $<n$ (où $n>1$). Le nombre n est divisible par au moins un nombre premier q, soit $n = qn'$, d'où $n'<n$. Soit y une racine primitive n-ième de l'unité dans K , et soit H le groupe multiplicatif engendré par y . Si q divise n', y n'est la puissance q-ième d'aucun élément de H ; en effet, si $y = y^{aq}$, $aq-1$ est divisible par n' , ce qui est impossible si q divise n'. Si q ne divise pas n', et si u, u' sont des éléments de H tels que $u^q = u'^q$, on a

$(u'u^{-1})^q=1$; l'ordre de $u'u^{-1}$ divise donc q et n', c'est-à-dire est égal à 1 , d'où $u=u'$. On peut donc dire dans tous les cas qu'il existe au plus un $u\in H$ tel que $u^q=y$. Ceci dit, introduisons une lettre X et formons le polynome X^q-y . Puisque K est algèbriquement fermé, ce polynome peut se mettre sous la forme $\prod_{i=1}^{q}(X-x_i)$, avec $x_i \in K$ $(1\leqslant i\leqslant q)$ (th.2, § 3). La dérivée de X^q-y est qX^{q-1} , et on a $qx_i^{q-1}\neq 0$ $(1\leqslant i\leqslant q)$, puisque q n'est pas divisible par la caracéristique de K . Donc chaque x_i est un zéro simple de X^q-y , et par suite on a $x_i\neq x_j$ pour $i\neq j$. Puisque $q>1$, il existe au moins un x_i , soit x, qui n'est pas dans H . Le groupe multiplicatif engendré par x contient H mais est $\neq H$; ce groupe est donc d'ordre $n'q_1$, $q_1>1$. Par ailleurs, x est évidemment une racine n-ième de l'unité, et par suite $n'q_1$ divise $n = n'q$; q étant premier, on a $q_1=q$, ce qui montre que x est une racine primitive n-ième de l'unité. L'élément x est un zéro de X^n-1, mais non de la dérivée nX^{n-1} de X^n-1 (parce que n n'est pas divisible par la caractéristique de K) ; on en conclut que x est séparable par rapport à tout sous-corps de K (prop.1, § 6). La prop.1 est donc démontrée.

Soit (K,L) une extension d'un corps K telle que $L = K\langle x_1,\ldots,x_n\rangle$, où $x_1,..,x_n$ sont tous les zéros du polynome X^n-1 dans quelque extension algèbriquement fermée de K . On dit alors que L <u>résulte de K par adjonction des racines n-ièmes de l'unité</u>. S'il en est ainsi, l'extension (K,L) est galoisienne (prop.7, § 4 et prop.4, § 6). Si K est de caractéristique $p>0$ et si $n=p^h n'$, où n' n'est pas divisible par p , toute racine n-ième de l'unité est aussi une racine n'-ième de l'unité (cf. plus haut). Si K est de caractéristique 0, nous poserons $n'=n$. Il résulte de la prop.1 que l'un des x_i , soit x , est une racine primitive n'-ième de l'unité. Les puissances de x fournissent

alors n' racines n'ièmes distinctes de l'unité ; puisque le polynome $X^{n'}-1$ ne peut avoir plus de n' zéros dans L , tous les x_i sont des puissances de x et $L = K\langle x \rangle$. Soit G le groupe de Galois de l'extension (K,L) ; un élément $\sigma \in G$ est uniquement déterminé quand on connaît son effet sur x ; de plus $\sigma(x)$ doit être l'un des x_i , soit $\sigma(x) = x^s$, où s est un entier, qui est déterminé à un multiple près de n' quand σ est donné. Désignons par $\chi(\sigma)$ la classe de s modulo n'Z ; χ est donc une application bi-univoque de G dans l'anneau $Z/n'Z$. On voit tout de suite que $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ et que l'image par χ de l'identité est l'élément unité de $Z/(n'Z)$. Puisque χ est biunivoque, on voit que G est abélien ; par ailleurs, un élément de $\chi(G)$ admet un inverse dans $Z/(n'Z)$ et est par suite un élément régulier de cet anneau. Nousavons donc démontré les résultats suivants :

Proposition 2.- Soient n un entier >0 et (K,L) une extension obtenue par adjonction à un corps K des racines n-ièmes de l'unité. L'extension (K,L) est alors galoisienne. Si K est de caractéristique 0, posons n'=n ; si K est de caractéristique $p>0$, posons $n = p^h n'$, où n' est un entier non divisible par p . Le groupe de Galois de (K,L) est alors isomorphe à un sous-groupe du groupe multiplicatif des éléments inversibles de l'anneau $Z/n'Z$. Le corps L contient une racine primitive n'-ième de l'unité, soit x ; on a $L = K\langle x \rangle$ et toutes les racines n-ièmes de l'unité contenues dans L sont des puissances de x .

Définition 2.- Soit n un entier >0 ; on désigne par $\varphi(n)$ l'ordre du groupe multiplicatif des éléments inversibles de l'anneau Z/nZ . La fonction φ s'appelle l'indicatrice d'Euler.

On remarquera que tout élément régulier u de l'anneau Z/nZ est inversible. En effet, l'application $v \to uv$ est biunivoque ; l'anneau Z/nZ étant fini, notre application applique cet anneau sur lui-même, ce qui démontre notre assertion.

Soit x une racine primitive n-ième de l'unité dans un corps. Cherchons à quelle condition une racine de l'unité de la forme x^d est encore une racine primitive n-ième de l'unité. En vertu de la prop.2, une condition nécessaire et suffisante pour qu'il en soit ainsi est qu'il existe un entier $e>0$ tel que $(x^d)^e = x$, c'est-à-dire tel que de -1 soit divisible par n. Cela signifie évidemment que la classe de d modulo nZ doit être inversible dans Z/nZ. On a donc le résultat suivant :

Proposition 3.- Soient n un entier >0 et K un corps qui contient une racine primitive n-ième de l'unité. Le nombre des racines primitives n-ièmes de l'unité contenues dans K est alors $\varphi(n)$.

Si x est une racine primitive n-ième de l'unité et si d est un entier >0 qui divise n, on voit facilement que $x^{n/d}$ est une racine primitive d-ième de l'unité. De plus, si y est une puissance quelconque de x, l'ordre de y est un diviseur de n. On déduit facilement de là la formule

$$\sum_{d\in D} \varphi(d) = n$$

où D est l'ensemble des entiers >0 qui divisent n.

Nous allons maintenant étudier les résultats que nous avons obtenus sur les racines de l'unité à l'étude des corps finis. Un corps fini K ne peut contenir aucun corps isomorphe au corps des rationnels ; il est donc de caractéristique $p>0$. Le corps premier K_0 de K est isomorphe à Z/pZ et contient p éléments. L'extension (K_0, K) est évidemment finie ; si n est son degré, la structure d'espace vectoriel sur K_0 de K est isomorphe à celle de $(K_0)^n$, ce qui montre que le nombre d'éléments de K est p^n. Le groupe multiplicatif des éléments $\neq 0$ de K est un groupe fini d'ordre p^n-1 ; c'est donc un groupe de racines de l'unité (Prop.9, §6 - n° 7 - Alg.- Ch.I). Si on pose $d = p^n-1$, l'équation

$X^d - 1 = 0$ a d racines distinctes dans K , ce qui montre que K se déduit de K_o par adjonction des racines d-ièmes de l'unité. Le nombre d n'étant pas divisible par la caractéristique de K , K contient une racine primitive d-ième de l'unité, ce qui montre que le groupe multiplicatif des éléments $\neq 0$ de K est cyclique. L'application $x \to \sigma(x)=x^p$ est un isomorphisme de K sur un sous-corps K' de K ; comme K' contient le même nombre d'éléments que K , on a $K'=K$ et σ est un automorphisme de (K_o,K). Les invariants de σ sont les zéros de X^p-X dans K ; il ne peut y en avoir plus de p , ce qui montre que le corps des invariants de σ est K_o. Il résulte de là et du th.1, § 5 que le groupe de Galois de (K_o,K) est le groupe cyclique engendré par σ ; il est d'ordre n .

. Soient réciproquement K_o un corps isomorphe à Z/pZ et K un corps obtenu par adjonction à K_o des racines (p^n-1)-ièmes de l'unité, où n est un entier >0 . Le corps K est alors obtenu par adjonction à K_o d'un nombre fini d'éléments algèbriques par rapport à K_o ; il est donc fini. Le même raisonnement que plus haut montre que le groupe de Galois de (K_o,K) est engendré par l'opération σ définie par $\sigma(x) = x^p$ $(x \in K)$. De plus, on a $K = K_o\langle u\rangle$, où u est une racine primitive (p^n-1)-ième de l'unité. On a $\sigma^n(u) = u^{p^n} = u$ mais, si $1 < m < n$, $\sigma^m(u)=u^{p^m} \neq u$; on en conclut que σ est d'ordre n et que $[K : K_o]= n$. Nous avons donc démontré les résultats suivants :

Proposition 4.- Soit K_o un corps isomorphe à Z/pZ , où p est un nombre premier, et soit (K_o,K^*) une extension algèbriquement fermée de K_o . Pour tout entier n ≥ 0 le corps K admet un sous-corps K_n et un seul qui est de degré n par rapport à K_o . Le corps K_n contient une racine primitive (p^n-1)-ième de l'unité u_n et on a $K_n = K_o\langle u_n\rangle$.

Le groupe multiplicatif des éléments $\neq 0$ de K_n est le groupe cyclique d'ordre p^n-1 engendré par u_n . L'extension (K_o,K_n) est galoisienne ; son groupe de Galois est cyclique d'ordre n et est engendré par l'automorphisme $x \to x^p$.

Corollaire. Tous les corps finis ayant le même nombre d'éléments sont isomorphes.

Nous sommes maintenant en mesure de démontrer en toute généralité le résultat suivant :

Proposition 5.- Soit (K,L) une extension finie séparable d'un corps K . Il existe alors un élément x de L tel que $L = K\langle x\rangle$.

Si K est fini, il en est de même de L et la proposition 5 résulte immédiatement de la prop.4 . Supposons maintenant que K soit infini. Soit (K,M) une extension normale minima déterminée par L ; on sait donc que (K,M) est galoisienne (prop.5, § 6). Soient $\sigma_1,\ldots,\sigma_n$ les isomorphismes distincts de L sur des sous-corps de M qui coïncident avec l'identité sur K , σ_1 représentant l'identité. On peut trouver une partie finie $F = \{x_1,..,x_r\}$ de L telle que $L = K\langle F\rangle$. Introduisons r lettres $X_1,..,X_r$ et formons le polynome $P = \prod_{i=2}^{n}\left(\sum_{j=1}^{r} X_j(x_j-\sigma_i(x_j))\right)$. Si $i \geqslant 2$, on a $\sigma(x_j) \neq x_j$ pour au moins un indice j ; il en résulte que $P \neq 0$.

Puisque K est infini, on peut trouver des éléments $a_1,\ldots,a_r$ de K tels que $P(a_1,..,a_r) \neq 0$. Posons alors $x = \sum_{j=1}^{r} a_j x_j$; on a donc $\prod_{i=2}^{n}(x - \sigma_i(x)) \neq 0$, ce qui montre que $K\langle x\rangle$ admet au moins n isomorphismes distincts sur des sous-corps de M qui coïncident avec l'identité sur K . Faisant usage de la prop.6, §6, on voit que $[L : K] = n$, $[K\langle x\rangle : K] \geqslant n$, d'où $L = K\langle x\rangle$. (car $K\langle x\rangle \subset L$) .

---

§ 8. EXTENSIONS FINIES CONSIDEREES COMME ALGEBRES.

Si (K,L) est une extension finie d'un corps K , le corps L possède une structure d'algèbre par rapport à K . Nous nous proposons d'étudier les propriétés de L qui sont liées à l'existence de cette structure.

Définition 1.- Soit (K,L) une extension finie d'un corps K . Si $x \in L$, désignons par $\varphi(x)$ l'endomorphisme de la structure d'espace vectoriel sur K de L que la représentation régulière de L (considéré comme algèbre sur K) fait correspondre à x . Le polynome caractéristique de $\varphi(x)$ est alors appelé le polynome caractéristique de x dans l'extension (K,L) . La trace et le déterminant de $\varphi(x)$ sont appelés respectivement trace et norme de x de L à K , et se désignent par $Sp_{L/K}\, x$ et $N_{L/K} x$.

On observera que les quantités ainsi définies dépendent non seulement de x et de K , mais aussi de L .

Si n est le degré de L par rapport à K , le polynome caractéristique de x par rapport à K (écrit avec une lettre X) est un polynome de degré n dans lequel le coefficient de X^n est 1 ; le coefficient de X^{n-1} est $-Sp_{L/K} x$, et le terme constant est $(-1)^n N_{L/K}\, x$. L'application $x \to \varphi(x)$ étant une représentation de la structure d'algèbre de L , on a, pour $x,y \in L$ et $a \in K$,

$$Sp_{L/K}(x+y) = Sp_{L/K} x + Sp_{L/K} y \quad ; \quad Sp_{L/K} ax = a\, Sp_{L/K} x$$
$$N_{L/K}(xy) = N_{L/K} x \cdot N_{L/K} y \quad ; \quad N_{L/K} ax = a^{[L:K]} N_{L/K} x .$$

Proposition 1.- Soient (K,L) une extension finie d'un corps K , M un sous-corps de L contenant K , x un élément de L , G(X) et F(X) les polynomes caractéristiques de x dans les extensions (M,L) et (K,L) respectivement. Introduisons une extension algébriquement fermée (K, Ω) de K , et désignons par $\xi_1, \ldots, \xi_{m^*}$ les isomorphismes distincts de M sur des sous-corps de Ω qui coïncident avec l'identité sur K . Si on pose $m = [M : K]$, m^* divise m et on a

$$F(X) = \left(\prod_{k=1}^{m^*} \left(\zeta_k(G(X)) \right)^{m/m^*}\right.$$

(On désigne par $\zeta_k(G(X))$ le polynome déduit de $G(X)$ en soumettant ses coefficients à l'opération ζ_k).

Le corps L étant considéré comme une algèbre sur K , on peut en déduire par extension du corps de base une algèbre $\mathfrak{L}$ sur Ω ; nous désignerons par j une injection de L dans $\mathfrak{L}$. L'algèbre $\mathfrak{L}$ est un espace vectoriel de dimension finie sur Ω ; on peut la considèrer comme un $\mathfrak{L}$-module, et les sous-modules de cet $\mathfrak{L}$-module sont alors des sous-espaces vectoriels de $\mathfrak{L}$. Il en résulte tout de suite que l'on peut former une suite de Jordan-Holder $M_0 = \{0\} \subset M_1 \subset \ldots \subset M_n = \mathfrak{L}$ dans $\mathfrak{L}$, considéré comme $\mathfrak{L}$-module. Les M_i sont des idéaux de $\mathfrak{L}$, et, si $i > 0$, M_i / M_{i-1} possède une structure de $\mathfrak{L}$-module irréductible. L'algèbre $\mathfrak{L}$ étant commutative et Ω étant algèbriquement fermé, M_i / M_{i-1} est de dimension 1 sur Ω , ce qui montre que n est égal au rang de $\mathfrak{L}$, c'est-à-dire à $[L : K]$. Désignons par ξ_i un élément de M_i non contenu dans M_{i-1} $(1 \leqslant i \leqslant n)$; si $y \in L$, on a

$$j(y)\,\xi_i \equiv \sigma_i(y)\,\xi_i \pmod{M_{i-1}} \qquad (1)$$

où $\sigma_i(y) \in \Omega$. Il est clair que σ_i est un homomorphisme (et par suite un isomorphisme) de L sur un sous-corps de Ω qui coïncide avec l'identité sur K . Le polynome F(X) est évidemment égal au polynome caractéristique de l'endomorphisme $\xi \longrightarrow j(x)\,\xi$ de la structure d'espace vectoriel de $\mathfrak{L}$ sur Ω ; les éléments $\xi_1, \ldots, \xi_n$ forment une base de $\mathfrak{L}$ par rapport à Ω et les formules (1) montrent que la matrice qui représente l'endomorphisme $\xi \longrightarrow j(x)\,\xi$ par rapport à cette base n'a que des zéros au-dessous de la diagonale, tandis que les éléments diagonaux sont $\sigma_1(x), \ldots, (\sigma_n(x)$. On a donc

$$F(X) = \prod_{i=1}^{n} (X - \sigma_i(x))$$

Par restriction du corps de base de Ω à K , on déduit de L une algèbre L_0 sur K qui peut être considérée comme un produit kroneckerien des structures d'algèbres de L et de Ω par rapport à K . Soit τ un automorphisme de Ω qui laisse fixes les éléments de K ; il correspond alors à τ un automorphisme τ^* de L_0 tel que $\tau^*(j(x)) = j(x)$ pour tout $x \in L$ et $\tau^*(\omega) = \tau(\omega)$ pour tout $\omega \in \Omega$. Les ensembles $\tau^*(M_i)$ $(1 \leqslant i \leqslant n)$ sont des idéaux de L_0 , donc aussi de L , et forment une nouvelle suite de Jordan-Hölder de la structure de L-module de L . Par ailleurs, on a

$$j(y)\,\tau^*(\xi_i) \equiv (\tau \circ \sigma_i)(y)\,\tau^*(\xi_i) \pmod{\tau^*(\mathfrak{M}_{i-1})}$$

Faisant usage du théorème de Jordan-Holder, on en déduit que $\tau \circ \sigma_i$ figure autant de fois dans la suite finie $(\sigma_1, .., \sigma_n)$ que σ_i lui-même. Ceci dit, soit σ un isomorphisme quelconque de L sur un sous-corps de Ω qui coïncide avec l'identité sur K ; $\sigma \circ \sigma_1^{-1}$ est alors un isomorphisme de $\sigma_1(L)$ sur un sous-corps de Ω . Comme tel, il peut se prolonger par un automorphisme τ de Ω , et on a $\sigma = \tau \circ \sigma_1$. On voit donc que tous les isomorphismes de L sur des sous-corps de Ω qui coïncident avec l'identité sur K figurent le même nombre de fois dans la suite $(\sigma_1, \ldots, \sigma_n)$. Nous pouvons donc supposer que $\sigma_1, \ldots, \sigma_{n^*}$ sont tous les isomorphismes distincts de L sur des sous-corps de Ω qui coïncident avec l'identité sur K , et on a alors

$$F(X) = \left(\prod_{i=1}^{n^*} (X - \sigma_i(x))\right)^{n/n^*} \tag{2}$$

ce qui démontre la prop.1 dans le cas où $M = L$.

Ceci dit, pour chaque $i (1 \leqslant i \leqslant n)$, la restriction $\bar{\sigma}_i$ de σ_i à M est l'un des isomorphismes ζ_k . Désignons par J_k l'ensemble des i pour lesquels $\bar{\sigma}_i = \zeta_k$; on a

$$F(X) = \prod_{k=1}^{m^*} \left(\prod_{i \in J_k} (X - \sigma_i(x))\right)$$

Il résulte du th.3, § 3 qu'aucun des J_k n'est vide. Choisissons d'une manière quelconque un élément i(k) dans chaque J_k, et posons $L_k = \sigma_{i(k)}(L)$, $M_k = \sigma_{i(k)}(M)$, $x_k = \sigma_{i(k)}(x)$. Si $i \in J_k$, l'application $\sigma_i \circ \sigma_{i(k)}^{-1}$ est un isomorphisme de L_k sur un sous-corps de Ω qui coïncide avec l'identité sur M_k ; inversement, si θ est un isomorphisme de L_k sur un sous-corps de Ω qui coïncide avec l'identité sur M_k, $\theta \circ \sigma_{i(k)}$ figure n/n^* fois dans la suite finie $(\sigma_1,..,\sigma_n)$, et tous les indices i tels que $\sigma_i = \theta \circ \sigma_{i(k)}$ sont dans J_k. On a donc

$$\prod_{x \in J_k} (X - \sigma_i(x)) = \Big(\prod_{\theta \in \Theta_k} (X - \theta(x_k))\Big)^{n/n^*}$$

où Θ_k est l'ensemble des isomorphismes de L_k sur des sous-corps de Ω qui coïncident avec l'identité sur M_k. Puisque $\sigma_{i(k)} \circ \sigma_1^{-1}$ applique L_1 sur L_k et M_1 sur M_k, tous les ensembles Θ_k ont le même nombre d'éléments, soit p^*, et on a $n^* = p^* m^*$. D'autre part, si $m = [M : K]$, $p = [L : M]$, on a $n = pm$, d'où $n/n^* = (p/p^*)(m/m^*)$. Faisant usage de la formule analogue à (2) pour l'extension (M_k, L_k), on voit que $\prod_{\theta \in \Theta_k} (X - \theta(x_k))^{p/p^*}$ est le polynome caractéristique $G_k(X)$ de x_k dans l'extension (M_k, L_k). D'autre part, la considération de l'isomorphisme $\sigma_{i(k)}$ montre que $G_k(X) = \sigma_{i(k)}(G_k(X)) = \zeta_k(G(X))$ (car les coefficients de G sont dans M). La prop.1 est donc démontrée.

Corollaire 1.- Soient (K,L) une extension finie d'un corps K, (K, Ω) une extension algèbriquement fermée de K, $\sigma_1, \ldots, \sigma_{n^*}$ les isomorphismes distincts de L sur des sous-corps de Ω qui coïncident avec l'identité sur K et n le degré de L par rapport à K. On a alors, pour tout $x \in L$,

$$Sp_{L/K}\, x = n/n^* \sum_{i=1}^{n^*} \sigma_i(x) \quad ; \quad N_{L/K}\, x = \Big(\prod_{i=1}^{n^*} \sigma_i(x)\Big)^{n/n^*}$$

Cela résulte immédiatement de la formule (2) si on observe que $-Sp_{L/K}\, x$ est le coefficient de X^{n-1} dans F(X) tandis que $(-1)^n N_{L/K}\, x$ est le terme constant de F(X).

On observera que les formules du corollaire 1 se simplifient dans le cas où (K,L) est séparable, car on sait que, dans ce cas, $n = n^*$ (prop.6, § 6).

Corollaire 2.- Soient (K,L) une extension finie d'un corps K et M un sous-corps de L contenant K . On a alors, pour tout $x \in L$,

$$Sp_{L/K}\, x = Sp_{M/K}\,(Sp_{L/M}\, x)\ ; \quad N_{L/K}\, x = N_{M/K}\,(N_{L/M}\, x)$$

Posons en effet $p = [L:M]$; on a alors

$$G(X) = X^p - (Sp_{L/M}\, x)X^{p-1} + \ldots + (-1)^p N_{L/M}\, x$$

d'où

$$(G(X))^{m/m^*} = X^{pm/m^*} - m/m^*\,(Sp_{L/M}\, x)X^{p\,m/m^*-1} + \ldots + (-1)^{pm/m^*} N_{L/M}\, x$$

et on déduit de la prop.1 que

$$Sp_{L/K}\, x = m/m^* \sum_{k=1}^{m^*} \zeta_k(Sp_{L/M}\, x)\ ; \quad N_{L/K}\, x = \Big(\prod_{k=1}^{m^*} \zeta_k(N_{L/M}\, x)\Big)^{m/m^*}$$

ce qui, compte tenu du corol.1, démontre le corol.2 .

Proposition 2.- Soient (K,L) une extension finie d'un corps K , F(X) le polynome caractéristique d'un élément $x \in L$ dans l'extension (K,L) et f(X) le polynome minimal de x par rapport à K . On a alors $F(X) = (f(X))^e$, où $e = [L : K\langle x\rangle]$.

Appliquons la prop.1 en posant $M = K\langle x\rangle$. Il est évident que G(X) est alors $(X-x)^e$, d'où

$$F(X) = \Big(\Big(\prod_{k=1}^{m^*} (X - \zeta_k(x))^{m/m^*}\Big)^e$$

Or $f^*(X) = \Big(\prod_{k=1}^{m^*} (X - \zeta_k(x))\Big)^{m/m^*}$ est le polynome caractéristique de x dans l'extension (K,M). On peut supposer sans restreindre la généralité que $M \subset \Omega$ on voit alors que f^* est un polynome de degré m à coefficients dans K tel que $f^*(x)=0$ et dans lequel le coefficient de X^m est 1 . Mais ces propriétés caractérisent le polynome minimal de x par rapport à K ; on a donc $f^* = f$, $F = f^e$.

Observons maintenant que, si (K,L) est une extension finie mais non séparable d'un corps K , on a $Sp_{L/K}\, x = 0$ pour tout $x \in L$. Soit en

en effet M le sous-corps de L formé des éléments de L qui sont séparables par rapport à K , et soit (K, Ω) une extension algèbrique algèbriquement fermée de K . On sait (prop.6, § 6) que le nombre n^* des isomorphismes de L sur des sous-corps de Ω qui coïncident avec l'identité sur K est égal à $\left[M : K\right]$. Il en résulte que, si $n = \left[L : K\right]$, n/n^* est égal à $\left[L : M\right]$. Or toute élément de L est radiciel par rapport à M . Notre assertion résultera alors du corol.1 à la prop.1 aussitôt que nous aurons prouvé le

Lemme 1.- Soit (M,L) une extension radicielle finie d'un corps M de caractéristique $p > 0$. Le nombre $\left[L : M\right]$ est alors une puissance de p.

Ecrivons en effet $L = M\langle x_1, .., x_r\rangle$, et posons $L_0 = L$, $L_i = L\langle x_1, .. x_i\rangle$ d'où $L_i = L_{i-1}\langle x_i\rangle$ $(1 \leqslant i \leqslant r)$. Il résulte tout de suite du th.2, § 2 que $\left[L : M\right] = \prod_{i=1}^{r} \left[L_i : L_{i-1}\right]$. On voit donc qu'on peut se borner au cas où $M = L\langle x\rangle$. Dans ce cas, le lemme 1 résulte tout de suite de la prop.2, § 6 .

Si maintenant nous considérons au contraire le cas d'une extension finie séparable (K,L) de degré n d'un corps K , on sait qu'il existe n isomorphismes distincts de L dans un corps algèbriquement fermé Ω contenant K comme sous-corps qui coïncident avec l'identité sur K . Il résulte alors du lemme 1, § 5 et du corol.1 à la prop.1 qu'il existe un élément $x \in L$ tel que $Sp_{L/K}\, x \neq 0$. Nous avons donc démontré la

Proposition 3.- Soit (K,L) une extension finie d'un corps K . Pour qu'il existe un élément $x \in L$ tel que $Sp_{L/K}\, x \neq 0$, il faut et il suffit que (K,L) soit séparable.

Soit (K,L) une extension finie séparable. L'application $(x,y) \longrightarrow Sp_{L/K}\, xy$ est alors une forme bilinéaire symétrique sur $L \times L$. Cette forme bilinéaire n'est pas dégénérée. En effet, soit y un élément

$\neq 0$ de L , et soit x_0 un élément de L tel que $Sp_{L/K} x_0 \neq 0$; on a alors $Sp_{L/K}(x_0 y^{-1})y \neq 0$, ce qui démontre notre assertion. On obtient donc le résultat suivant :

Proposition 4.- Soit (K,L) une extension finie séparable d'un corps K , et soit $(x_1,..,x_n)$ une base de L par rapport à K . La matrice $(Sp_{L/K} x_i x_j)_{1 \leqslant i,j \leqslant n}$ est alors de rang n .

Définition 2.- Les notations étant celles de la prop.4, le déterminant de la matrice $(Sp_{L/K} x_i x_j)_{1 \leqslant i,j \leqslant n}$ est appelé le discriminant de la base $(x_1,...,x_n)$.

On observera qu'il résulte tout de suite de la prop.3 qu'il existe une base $(x'_1,..,x'_n)$ de L par rapport à K telle que $Sp_{L/K} x'_i x'_j = \delta_{ij}$ (le symbole de Kronecker) (cf. Alg.II,...). La considération de cette base permet de donner des formules qui expriment les coefficients $a_1,..,a_n$ de l'expression d'un x donné de L sous forme de combinaison linéaire $x = \sum_{i=1}^{n} a_i x'_i$ de $x'_1,..,x'_n$ à coefficients dans K : on a effet $a_i = Sp_{L/K} x x'_i$.

Il existe une autre méthode pour déterminer les coefficients a_i . Désignons en effet par (L, Ω) une extension algèbriquement fermée de L et par $\sigma_1,..,\sigma_n$ les n isomorphismes de L sur des sous-corps de Ω qui coïncident avec l'identité sur K . Formons la matrice $X = (\sigma_i(x_j))_{1 \leqslant i,j \leqslant n}$; on voit immédiatement que $X.{}^tX$ est la matrice $(Sp_{L/K} x_i x_j)_{1 \leqslant i,j \leqslant n}$, ce qui prouve que X est de rang n . Ceci dit, on a

$$\sigma_i(x) = \sum_{j=1}^{n} a_j \sigma_i(x_j) \qquad (1 \leqslant i \leqslant n)$$

et les quantités $a_1,..,a_n$ peuvent être obtenues en résolvant ce système de n équations linéaires, qui est de rang n , pourvu que les quantités $\sigma_i(x)$ soient connues.

Continuant à désigner par (K,L) une extension finie séparable d'un corps K , nous utiliserons de plus les notations de la démonstration

de la prop.1. Si ξ est un élément quelconque de $\mathcal{L}$, on a $\xi\xi_i \in \mathfrak{M}_i$ $(1 \leqslant i \leqslant n)$, donc σ_i est une application de $\mathcal{L}$ dans Ω. On voit tout de suite que $\tilde{\sigma}_i$ est une représentation sur Ω de la structure d'algèbre de $\mathcal{L}$. De plus, on a $\sigma_i(x) = \tilde{\sigma}_i(j(x))$ pour tout $x \in L$. On sait que tout isomorphisme de L sur un sous-corps de Ω qui coïncide avec l'identité sur K intervient dans la suite finie $(\sigma_1,..,\sigma_n)$; comme il y a n de ces isomorphismes, $\sigma_1,..,\sigma_n$ sont distincts et on déduit du lemme 1, § 5 qu'il ne peut exister aucun système $(\omega_1,..,\omega_n)$ d'éléments non tous nuls de Ω tels que $\sum_{i=1}^{n} \omega_i \tilde{\sigma}_i(\xi) = 0$ pour tout $\xi \in \mathcal{L}$. L'application $\xi \to \tilde{\sigma}(\xi) = (\tilde{\sigma}_1(\xi),..,\tilde{\sigma}_n(\xi))$ de $\mathcal{L}$ dans Ω^n (considéré comme espace vectoriel sur Ω) est linéaire et il résulte de ce que nous venons de dire qu'aucune forme linéaire $\neq 0$ sur Ω^n ne s'annulle identiquement sur $\tilde{\sigma}(\mathcal{L})$. On a donc $\tilde{\sigma}(\mathcal{L}) = \Omega^n$; puisque $\mathcal{L}$ est de dimension n, l'application $\tilde{\sigma}$ est univalente. Désignons par ε_i l'élément de $\mathcal{L}$ défini par les conditions $\tilde{\sigma}_j(\varepsilon_i) = \delta_{ij}$ $(1 \leqslant j \leqslant n)$. Il est clair que ε_i^2 satisfait aux mêmes conditions que ε_i, d'où $\varepsilon_i^2 = \varepsilon_i$. D'autre part, si $i \neq j$, on a $\tilde{\sigma}(\varepsilon_i \varepsilon_j) = 0$, d'où $\varepsilon_i \varepsilon_j = 0$. Si $\xi \in \mathcal{L}$, on a $\xi = \sum_{i=1}^{n} \tilde{\sigma}_i(\xi)\varepsilon_i$, ce qui montre que $\mathcal{L}$ est somme directe des n idéaux $\mathcal{L}\varepsilon_i = \Omega\varepsilon_i$.

Nous avons donc obtenu les résultats suivants :

Proposition 5.- Soient (K,L) une extension finie, séparable et de degré n d'un corps K, (K, Ω) une extension algébriquement fermée de K et $\mathcal{L}$ une algèbre sur Ω qui se déduise de la structure d'algèbre de L par rapport à K par extension de K à Ω du corps de base. On peut alors trouver n éléments $\varepsilon_1,..,\varepsilon_n$ de $\mathcal{L}$ tels que $\varepsilon_i\varepsilon_j = \delta_{ij}$ $(1 \leqslant i,j \leqslant n)$ et que $\mathcal{L}$ soit somme directe des n idéaux $\mathcal{L}\varepsilon_i = \Omega\varepsilon_i$. Soit j l'injection de L dans $\mathcal{L}$; si on pose $j(x) = \sum_{i=1}^{n} \sigma_i(x)\varepsilon_i$, $(x \in L)$, $\sigma_1,...,\sigma_n$ sont tous les isomorphismes de L sur des sous-corps de Ω qui coïncident

avec l'identité sur K .

Supposons maintenant que (K,L) soit galoisienne. Soient alors $\tau_1,\dots,\tau_n$ les éléments du groupe de Galois de (K,L). Il correspond à chaque τ_k un automorphisme τ_k^* de la structure d'algèbre de $\mathcal{L}$ qui est caractérisé par le fait que $j(\tau_k(x)) = \tau_k^*(j(x))$ pour tout $x \in L$. Il est clair que, pour tout $i (1 \leqslant i \leqslant n)$, $\sigma_i \circ \tau_k$ est l'un des isomorphismes $\sigma_1,\dots,\sigma_n$, soit $\sigma_{\varpi(i)}$; ϖ est une permutation de l'ensemble $\{1,\dots,n\}$. On voit tout de suite que $\tilde{\sigma}_i \circ \tau_k^* = \tilde{\sigma}_{\varpi(i)}$; il résulte de là que $\tau_k^*(\varepsilon_{\varpi(i)}) = \varepsilon_i$: chaque τ_k^* permute entre eux les éléments $\varepsilon_1,\dots,\varepsilon_n$. Si i reste fixe, les n éléments $\sigma_i \circ \tau_k$ $(1 \leqslant k \leqslant n)$ sont évidemment distincts, ce qui montre que, pour tout j $(1 \leqslant j \leqslant n)$ il existe un k tel que $\sigma_i \circ \tau_k = \sigma_j$. En d'autres termes, le groupe $\{\tau_1^*,\dots,\tau_n^*\}$ permute transitivement les éléments $\varepsilon_1,\dots,\varepsilon_n$. Ceci dit, nous allons démontrer la

Proposition 6. Soient K un corps qui contient une infinité d'éléments, (K,L) une extension galoisienne de K , et $\tau_1,\dots,\tau_n$ les éléments distincts du groupe de Galois de cette extension. Il existe alors un élément $x \in L$ tel que les éléments $\tau_k(x)$ $(1 \leqslant k \leqslant n)$ forment une base de L par rapport à K .

Formons une base quelconque $\{x_1,\dots,x_n\}$ de L par rapport à K , et posons $\tau_k(x_i) = \sum_{l=1}^{n} a_{ikl} x_l$ $(1 \leqslant i,k \leqslant n)$, où $a_{ikl} \in K$. Les éléments $j(x_1),\dots,j(x_n)$ forment une base de $\mathcal{L}$ par rapport à Ω ; posons $\varepsilon_1 = \sum_{i=1}^{n} y_i j(x_i)$, avec $y_i \in \Omega$ $(1 \leqslant i \leqslant n)$. On a

$$\tau_k^*(\varepsilon_1) = \sum_{i,l=1}^{n} y_i a_{ikl} j(x_l)$$

Or, il résulte de ce que nous avons vu plus haut que les éléments $\tau_k^*(\varepsilon_1)$ sont, à l'ordre près, les éléments $\varepsilon_1,\dots,\varepsilon_n$. Ces derniers étant évidemment linéairement indépendants par rapport à Ω ,

la matrice $(\sum_{i=1}^{n} y_i a_{ikl})_{1 \leqslant k,l \leqslant n}$ est de rang n . Introduisons n lettres $Y_1,\ldots,Y_n$, et désignons par $D(Y_1,..,Y_n)$ le déterminant de la matrice $(\sum_{i=1}^{n} Y_i a_{ikl})_{1 \leqslant k,l \leqslant n}$; D est un polynôme $\neq 0$ à coefficients dans K . Puisque K contient une infinité d'éléments, il existe des éléments $z_1,\ldots,z_n$ de K tels que $D(z_1,\ldots,z_n) \neq 0$; posons $x = \sum_{i=1}^{n} z_i x_i$. On a $\tau_k(x) = \sum_{i,l=1}^{n} z_i a_{ikl} x_l$ $(1 \leqslant k \leqslant n)$; l'inégalité $D(z_1,..,z_n) \neq 0$ montre que $\tau_1(x),\ldots,\tau_n(x)$ sont linéairement indépendants par rapport à K ; ces éléments forment donc une base de L par rapport à K .

Remarque. La conclusion de la prop.6 est encore valable dans le cas où K ne contient qu'un nombre fini d'éléments ; mais nous ne démontrerons ni n'utiliserons ce résultat.

---

§ 9. BASES de TRANSCENDANCE.

Définition 1.- Une extension d'un corps est appelée transcendante quand elle n'est pas algèbrique.

Il en résulte qu'une condition nécessaire et suffisante pour qu'une extension (K,L) d'un corps K soit transcendante est que L contienne un élément qui soit transcendant par rapport à K .

Définition 2.- Soient (K,L) une extension d'un corps K et E une partie de L . On dit que E est algèbriquement libre par rapport à K si les éléments d'une partie finie quelconque de E sont algèbriquement indépendants les uns des autres par rapport à K . S'il n'en est pas ainsi, on dit que E est algèbriquement liée par rapport à K .

La propriété pour une partie de L d'être algèbriquement libre par rapport à K est donc une propriété de caractère fini ; de plus, la partie vide de L possède cette propriété. Il existe donc des parties algèbriquement libres maximales de L .

Définition 3.- Soit (K,L) une extension d'un corps K . Une partie de L est maximale dans l'ensemble des parties algèbriquement libres par rapport à K est appelée une base de transcendance de L par rapport à K .

Proposition 1.- Soit (K,L) une extension d'un corps K , et soient A et B des parties de L qui n'ont pas d'élément commun. Pour que $A \cup B$ soit algèbriquement libre par rapport à K , il faut et suffit que les conditions suivantes soient satisfaites : 1) A est algèbriquement libre par rapport à K ; 2) B est algèbriquement libre par rapport à $K\langle A\rangle$.

1) Montrons d'abord que les conditions sont nécessaires. C'est évident pour la condition 1). Désignons par $x_1,..,x_r$ des éléments distincts de B , et par f un polynome en r lettres $X_1,..,X_r$, à coefficients dans $K\langle A\rangle$ et tel que $f(x_1,..,x_r)=0$. L'ensemble $K\langle A\rangle$ est l'union des

ensembles $K\langle A'\rangle$, où A' parcourt l'ensemble des parties finies de A. Supposant A non vide (sinon, la nécessité de 2) est évidente), on voit qu'il existe un certain nombre d'éléments distincts $y_1,\ldots,y_s$ de A tels que les coefficients de f appartiennent tous à $K\ y_1,\ldots,y_s$. Or, on voit tout de suite que $K\langle y_1,..,y_s\rangle$ est le corps des quotients de $K\left[y_1,..,y_s\right]$; tout coefficient de f peut donc se mettre sous la forme $\varphi(y_1,..,y_s)/\psi(y_1,..,y_s)$, où φ et ψ sont des polynomes en s lettres $Y_1,..,Y_s$ à coefficients dans K et $\psi(y_1,\ldots,y_s)\neq 0$. Soit θ le produit des polynomes ψ relatifs à tous les coefficients de f ; on a alors $f(X_1,..,X_r)\ \theta(y_1,..,y_s) = g(X_1,..,X_r,y_1,..,y_s)$, où g est un polynome en r+s lettres à coefficients dans K. On a $g(x_1,..,x_r,y_1,..,y_s) = 0$; si donc $A\cup B$ est algèbriquement libre par rapport à K, il résulte de $A\cap B = \phi$ que $g=0$, d'où, puisque $\theta \neq 0$, $f = 0$, ce qui prouve que B est algèbriquement libre par rapport à $K\langle A\rangle$.

2) Montrons maintenant que les conditions sont suffisantes. Supposons les en effet satisfaites, et soient $x_1,\ldots,x_r$, $y_1,\ldots,y_s$ des éléments distincts de $A\cup B$, avec $x_i\in B$ $(1\leqslant i\leqslant r)$ et $y_j\in A$ $(1\leqslant j\leqslant s)$. Soit f un polynome en r+s lettres $X_1,..,X_r,Y_1,..,Y_s$ à coefficients dans K tel que $f(x_1,..,x_r,y_1,\ldots,y_s)=0$. Si B est algèbriquement libre par rapport à $K\langle A\rangle$, on a $f(X_1,..,X_r,y_1,..,y_s)=0$ (car les coefficients de ce polynome en $X_1,..,X_r$ sont dans $K\langle A\rangle$). Si on considère f comme un polynome en $X_1,\ldots,X_r$ à coefficients dans $K\left[Y_1,..,Y_s\right]$, chaque coefficient φ de ce polynome a la propriété que $\varphi(y_1,..y_s)=0$. Si donc A est algèbriquement libre par rapport à K, les coefficients de f, considéré comme polynome en $X_1,..,X_r$, sont tous nuls, d'où $f=0$, ce qui prouve que $A\cup B$, est algèbriquement libre par rapport à K.

Corollaire 1.- Soit (K,L) une extension d'un corps K . Pour qu'une partie A de L soit une base de transcendance de L par rapport à K , il faut et suffit que A soit algèbriquement libre par rapport à K et que L soit algèbrique par rapport à $K\langle A\rangle$.

Corollaire 2.- Les notations étant les mêmes que dans la prop.1,supposons de plus que A soit algèbriquement libre par rapport à K . Pour que $A \cup B$, soit une base de transcendance de L par rapport à K , il est alors nécessaire et suffisant que B soit une base de transcendance de L , par rapport à $K\langle A\rangle$.

Propositbon 2.- Soit (K,L) une extension d'un corps K , et soit A une partie de L telle que $L = K\langle A\rangle$. L'ensemble A contient alors une base de transcendance de L par rapport à K .

L'ensemble $\mathcal{F}$ des parties de A qui sont algèbriquement libres par rapport à K est évidemment inductif et non vide ; il contient donc un élément maximal B . En vertu de la prop.1, tout $x \in A$ est algèbrique par rapport à $K\langle B\rangle$. Puisque $L = (K\langle B\rangle)\langle A\rangle$, L est algèbrique par rapport à $K\langle B\rangle$ (prop.4, §2), et la prop.2 résulte du corol.1 à la prop.1 .

Proposition 3 (théorème d'échange). Soient (K,L) une extension d'un corps K , A une partie de L algèbriquement libre par rapport à K et B une base de transcendance de L par rapport à K . Il existe alors une partie C de B telle que $A \cup C$ soit une base de transcendance de L par rapport à K .

Il résulte de la prop.2 que B contient une partie C qui est une base de transcendance de $K\langle A \cup B\rangle = (K\langle A\rangle)\langle B\rangle$ par rapport à $K\langle A\rangle$. En vertu du corol.2 à la prop.1, $A \cup C$ est une base de transcendance de $K\langle A \cup B\rangle$ par rapport à K . De plus, L est algèbrique par rapport à $K\langle A \cup B\rangle$, puisque $K\langle A \cup B\rangle \supset K\langle B\rangle$. On en déduit que $A \cup C$ est une base de transcendance de L pa

est une base de transcendance de L par rapport à K .

Théorème 1. Soit (K,L) une extension d'un corps K . Supposons que L admette une base de transcendance finie par rapport à K . Toutes les bases de transcendance de L par rapport à K sont alors finies et ont le même nombre d'éléments.

Nous démontrerons par récurrence sur n que le théorème est vrai de toutes les extensions (K,L) telles que L ait une base de transcendance B par rapport à K formée de n éléments. C'est évident pour n=0 ; supposons notre assertion vraie pour n-1 (où n est supposé >1). Soit C une base de transcendance quelconque de L par rapport à K . Si $B \subset C$, on a $C = B$. Sinon, B contient un élément x tel que $x \notin C$. Nous supposerons que nous sommes dans ce second cas. Soit B' l'ensemble des éléments de B différents de x ; en vertu du corol.2 à la prop.1, B' est une base de transcendance de L par rapport à $K\langle x\rangle$. Il résulte de la prop.3 que C contient une partie C' telle que $C' \cup \{x\}$ soit une base de transcendance de L par rapport à K , donc que C' soit une base de transcendance de L par rapport à $K\langle x\rangle$. Puisque B' ne contient que n-1 éléments, il en est de même de C'. Soit C'' le complément de C' par rapport à C ; il résulte de la prop.1 que C'' et $\langle x\rangle$ sont des bases de transcendance de L par rapport à $K\langle C'\rangle$. Puisque C' ne contient que n-1 éléments tandis que B en contient n , C'' n'est pas vide ; soit y un élément de C'' . Il résulte de la prop.3 que l'un des ensembles $\{y\}$, $\{x,y\}$ est une base de transcendance de $(K\langle C'\rangle)\langle x,y\rangle$ par rapport à $K\langle C'\rangle$. Puisque y est algèbrique par rapport à $(K\langle C'\rangle)\langle x\rangle$, la seconde possibilité est exclue, et il en résulte que $(K\langle C'\rangle)\langle x,y\rangle$ est algèbrique par rapport à $(K\langle C'\rangle)\langle y\rangle$. Mais L est algèbrique par rapport à $(K\langle C'\rangle)\langle x\rangle$, donc aussi par rapport à $(K\langle C'\rangle)\langle x,y\rangle$ et par rapport à $(K\langle C'\rangle)\langle y\rangle$ (prop.5, § 2).

On en conclut que y est le seul élément de C" , donc que C contient n éléments.

Définition 4.- Soit (K,L) une extension telle que L possède une base de transcendance finie par rapport à K . Le nombre d'éléments d'une quelconque de ces bases de transcendance est alors appelé le degré de transcendance de l'extension (K,L), ou encore le degré de transcendance de L par rapport à K .

Pour exprimer que L possède une base de transcendance finie par rapport à K , on dit aussi que le degré de transcendance de (K,L) (ou de L par rapport à K) est fini.

Théorème 2.- Soient (K,L) et (L,M) des extensions dont les degrés de transcendance sont finis ; soient respectivement d et e les degrés de transcendance de ces extensions. Le degré de transcendance de (K,M) est alors fini et égal à d+e .

Cela résulte immédiatement du corol.2 à la prop.1.

Proposition 4.- Soient (K,U) une extension d'un corps K , L et M des sous-corps de U contenant K et B une base de transcendance de M par rapport à K . Supposons que B soit algèbriquement libre par rapport à L . Alors, toute partie de M qui est algèbriquement libre par rapport à K l'est aussi par rapport à L .

Il suffit de démontrer qu'il en est ainsi pour les parties finies C de M qui sont algèbriquement libres par rapport à K . Les éléments de C étant algèbriques par rapport à $K\langle B\rangle$, il existe une partie finie B_0 de B telle que les éléments de C soient algèbriques pra rapport à $K\langle B_0\rangle$. L'ensemble C est une partie d'une base de transcendance D de $K\langle B_0 \cup C\rangle$ par rapport à K (prop.3) ; puisque B_0 est évidemment une base de transcendance de $K\langle B_0 \cup C\rangle$ par rapport à K , D et B_0 ont le même nombre d'éléments, soit d . Le corps $L\langle B_0 \cup C\rangle$ est algèbrique par rapport à

à $L\langle B_o\rangle$ et à $L\langle D\rangle$; de plus B_o est algèbriquement libre par rapport à L . Le degré de transcendance de $L\langle B_o \cup C\rangle$ par rapport à L est donc d ; puisque D contient une base de transcendance de $L\langle B_o \cup C\rangle$ par rapport à L (cela résulte tout de suite de la prop.2), D doit être lui-même une base de transcendance de $L\langle B_o \cup C\rangle$ par rapport à L , ce qui prouve que C est algèbriquement libre par rapport à L .

Définition 5.- Une extension (K,L) d'un corps K est dite purement transcendante s'il existe une base de transcendance B de L par rapport à K telle que $L = K\langle B\rangle$.

Soient K un corps et $X_1,\ldots,X_n$ n lettres. Il est clair que l'extension $(K,K\langle X_1,\ldots,X_n\rangle)$ (où $K\langle X_1,..,X_n\rangle$ est le corps des fractions rationnelles en $X_1,..,X_n$ à coefficients dans K) est purement transcendante et que son degré de transcendance est n . Réciproquement, on voit facilement que, si (K,L) est une extension purement transcendante de degré de transcendance n , L est isomorphe à $K\langle X_1,\ldots,X_n\rangle$.

---

§ 10. EXTENSIONS COMPOSÉES.

Définition 1.- Soient (K,L) et (K,M) des extensions d'un corps K . On entend par extension composée de ces extensions un triplet $((K,U),\lambda,\mu)$ formé d'une extension (K,U) de K et d'isomorphismes λ et μ de L et M respectivement sur des sous-corps de U qui possèdent les propriétés suivantes : 1) λ et μ coïncident avec l'identité sur K ; 2) on a $U = K\langle\lambda(L) \cup \mu(M)\rangle$.

Soit $((K,U),\lambda,\mu)$ une extension composée de (K,L) et de (K,M). Considérant L et M comme des algèbres sur K , formons d'autre part un produit kroneckerien (P,γ) de ces algèbres. Si nous définissons une application de $L\times M$ dans U par la formule $\gamma'(x,y) = \lambda(x)\mu(y)$, il est clair que γ' est bilinéaire et que $\gamma'(x,y)\gamma'(x',y') = \gamma'(xx',yy')$ (où $x,x' \in L$, $y,y' \in M$). Soit P' l'ensemble des combinaisons linéaires à coefficients dans K d'éléments de $\gamma'(L\times M)$; on sait que P' est un sous-anneau de U , et qu'il existe un homomorphisme φ de P sur P' tel que $\varphi(\gamma(x,y)) = \gamma'(x,y)$ pour tout $(x,y) \in L\times M$. Par ailleurs, P' contient $\lambda(L)$ et $\mu(M)$, ce qui montre que le corps des quotients de P' est U . L'anneau P' est isomorphe à $P/\mathfrak{p}$, où $\mathfrak{p} = \varphi^{-1}(0)$; $\mathfrak{p}$ est un idéal de P qui possède la propriété que $P/\mathfrak{p}$ est un anneau d'intégrité (nous appellerons plus loin premiers de semblables idéaux).

Soit réciproquement $\mathfrak{p}$ un idéal de P tel que $P/\mathfrak{p}$ soit un anneau d'intégrité $\neq \{0\}$. Formons un corps des quotients U_0 de $P/\mathfrak{p}$, et désignons par $\bar{\omega}$ l'homomorphisme canonique de P sur $P/\mathfrak{p}$. Les applications $x \to \bar{\omega}(\gamma(x,1))$ et $y \to \bar{\omega}(\gamma(1,y))$ (où 1 représente l'élément unité de K) sont des homomorphismes λ_0 et μ_0 de L et de M dans P_0 . On a $\lambda_0(1) \neq 0$, $\mu_0(1) \neq 0$, ce qui montre que λ_0 et μ_0 sont des isomorphismes. Les restrictions de λ_0 et de μ_0 à K coïncident l'une

avec l'autre et donnent un isomorphisme ρ_o de K sur un sous-corps K_o de U_o. Il est clair que $U_o = K_o\langle \lambda_o(L) \cup \mu_o(M)\rangle$. On peut inclure K dans un ensemble U tel qu'il existe une application bi-univoque σ de U_o sur U qui coïncide avec ρ_o^{-1} sur K_o . Par transport de structure, on définit sur U une structure de corps telle que σ soit un isomorphisme de U_o sur U . Si on pose $\lambda = \sigma \circ \lambda_o$, $\mu = \sigma \circ \mu_o$, il est clair que $((K,U), \lambda, \mu)$ est une extension composée de (K,L) et de (K,M).

Soit $((K,U), \lambda, \mu)$ une extension composée de (K,L) et de (K,M). Les notations étant les mêmes que plus haut, un intérêt particulier s'attache au cas où l'idéal $\mathfrak{P}$ se réduit à $\{0\}$. Pour qu'il en soit ainsi, il faut et suffit que (P', γ') soit un produit kroneckerien des structures d'algèbres de L et de M par rapport à K . On peut encore mettre cette condition sous la forme suivante : $(x_i)_{i \in I}$ et $(y_j)_{j \in J}$ désignant des familles libres par rapport à K d'éléments de L et de M respectivement, la famille $(\lambda(x_i)\mu(x_j))_{(i,j) \in I \times J}$ est libre par rapport à K (on observera que les familles libres dont nous parlons ici sont libres au sens des structures d'espaces vectoriels des ensembles considérés ; on distinguera soigneusement cette notion de celle de famille algèbriquement libre introduite au § 9).

Définition 2.- On dit qu'une extension composée $((K,U), \lambda, \mu)$ d'extensions (K,L) et (K,M) d'un corps K est librement composée si la condition suivante est satisfaite : $(x_i)_{i \in I}$ et $(y_j)_{j \in J}$ étant des familles libres par rapport à K d'éléments de L et de M respectivement, la famille $(\lambda(x_i)\mu(y_j))_{(i,j) \in I \times J}$ d'éléments de U est toujours libre par rapport à K .

Pour que $((K,U),\lambda,\mu)$ soit librement composée, il est évidemment nécessaire et suffisant que, F et G désignant des parties finies quelconques de L et de M respectivement, U' le corps $K\langle\lambda(F)\cup\mu(G)\rangle$, λ' et μ' les restrictions de λ et de μ à $K\langle F\rangle$ et à $K\langle G\rangle$ respectivement, l'extension composée $((K,U'),\lambda',\mu')$ de $(K,K\langle F\rangle)$ et de $(K,K\langle G\rangle)$ soit toujours librement composée.

Si (K,L) et (K,M) sont des extensions quelconques d'un corps K, ces extensions n'admettent en général pas d'extension librement composée ; pour qu'elles en admettent une, il faut et suffit qu'un produit kroneckerien des structures d'algèbres de L et de M par rapport à K soit un anneau d'intégrité.

Définition 3.- Des extensions (K,L) et (K,M) d'un corps K sont dites étrangères l'une à l'autre si elles admettent au moins une extension librement composée.

Dans ce qui va suivre, nous aurons souvent l'occasion de considérer des extensions (K,L) et (K,M) d'un corps K telles que L et M soient des sous-corps d'un même corps V. Posons alors $U = K\langle L\cup M\rangle$, et désignons par λ et μ les applications identiques de L et de M respectivement dans U ; $((K,U),\lambda,\mu)$ est alors une extension composée de (K,L) et de (K,M). Nous conviendrons pour simplifier de désigner cette extension composée par (K,U).

Proposition 1.- Soit (K,V) une extension d'un corps K, et soient L et M des sous-corps de V contenant K ; posons $U = K\langle L\cup M\rangle$. Soient $\mathcal{O}$ un sous-anneau de L contenant K et dont le corps des quotients soit L, et B une base d'espace vectoriel de $\mathcal{O}$ par rapport à K. L'espace vectoriel $\sum_{b\in B} Mb$ est alors l'anneau $M[\mathcal{O}]$. Pour que (K,U) soit librement composée de (K,L) et de (K,M), il faut et suffit que B soit libre par rapport à M.

Si b et b' sont des éléments de B , on a $bb' \in \sigma$, d'où $bb' \in \sum_{b \in B} Kb \subset \sum_{b \in B} Mb$. On en conclut que $P = \sum_{b \in B} Mb$ est un anneau. Si on désigne par 1 l'élément unité de K , on a $1 \in \sum_{b \in B} Kb$, d'où $1 \in P$, et par suite $M \subset P$, $\sigma \subset P$ et $M[\sigma] \subset P$; comme P est évidemment contenu dans $M[\sigma]$, on a $P = M[\sigma]$. Désignons par C une base d'espace vectoriel de M par rapport à K . Supposons d'abord que (K,U) soit librement composée de (K,L) et de (K,M). Soit alors $\sum_{b \in B} \mu(b)b = 0$ une relation linéaire entre éléments de B à coefficients $\mu(b) \in M$. Chaque $\mu(b)$ peut se mettre sous la forme $\sum_{c \in C} a(b,c)c$, avec $a(b,c) \in K$. Il n'y a qu'un nombre fini de paires $(b,c) \in B \times C$ telles que $a(b,c) \neq 0$, et on a $\sum_{(b,c) \in B \times C} a(b,c)bc = 0$. Or la famille $(bc)_{(b,c) \in B \times C}$ est libre par rapport à K ; on a donc $a(b,c)=0$ pour tout $(b,c) \in B \times C$, d'où $\mu(b)=0$ pour tout $b \in B$, ce qui montre que B est libre par rapport à M .

Supposons maintenant réciproquement que B soit libre par rapport à M . Posons $\gamma(x,y) = xy$ (où $x \in \sigma$, $y \in M$) . La famille $(bc)_{(b,c) \in B \times C}$ est une base de la structure d'espace vectoriel de P par rapport à K (Alg. II, prop. ,), d'où il résulte que (P,γ) est un produit kroneckerien des structures d'espaces vectoriels de σ et de M par rapport à K . Soit B^* une base d'espace vectoriel de L par rapport à K . Si $b_1^*,\ldots,b_m^*$ sont m éléments distincts de B^* , on peut écrire $b_i^* = b_i t^{-1}$ $(1 \leqslant i \leqslant m)$, où $t,b_1,\ldots,b_m$ sont dans σ . Les éléments $b_1,\ldots,b_m$ sont alors linéairement indépendants par rapport à K ; il résulte de ce qui précède que la famille $(b_i c)_{1 \leqslant i \leqslant m, c \in C}$ est libre par rapport à K ; il en est donc de même de la famille $(b_i^* c)_{1 \leqslant i \leqslant m, c \in C}$. Ceci démontre que la famille $(b^* c)_{(b^*,c) \in B^* \times C}$ est libre par rapport à K

Si on pose $\gamma'(x,y)=xy(x\in L, y\in M)$, et si on désigne par P_1 l'ensemble des combinaisons linéaires à coefficients dans K l'éléments de $\gamma'(L\times M)$, on voit que (P_1,γ') est un produit kroneckerien des structures d'espaces vectoriels de L et de M par rapport à K , donc que (K,U) est librement composée de (K,L) et de (K,M).

Corollaire 1.- Les notations étant celles de la prop.1, supposons de plus que L soit algèbrique par rapport à K . On a alors $\sum_{b\in B} Mb = U$. Si (K,U) est librement composée de (K,L) et de (K,M), B est une base de U par rapport à M .

Il est clair que $U = M\langle L\rangle = M\langle\sigma\rangle$. Le corol.1 résulte donc immédiatement de la prop.4, §2 .

Remarque. Soit C une base de M par rapport à K . Il résulte alors du corol.1 que, si L est algèbrique par rapport à K , on a $U = \sum_{(b,c)\in B\times C} Kbc$, d'où on déduit facilement que $U = \sum_{c\in C} Lc$. Si de plus (K,U) est librement composée de (K,L) et de (K,M), C est une base de U par rapport à L .

Corollaire 2.- Les notations étant celles de la prop.1, supposons de plus que (K,L) soit finie. Pour que (K,U) soit librement composée de (K,L) et de (K,M), il est alors nécessaire et suffisant que $[U : M]=[L : K]$.

Cela résulte immédiatement de la prop.1 et du corol.1 .

Corollaire 3.- Les notations étant celles de la prop.1, soit de plus N un sous-corps de M contenant K . Si (K,U) est librement composée de $(N,N\langle L\rangle)$ et de (N,M) .

En effet, B est alors une base de $N[\sigma]$ par rapport à N , et le corps des quotients de $N[\sigma]$ est évidemment $N\langle L\rangle$.

Proposition 2.- Soient (K,U) une extension d'un corps K , L et M des sous-corps de V contenant K et U le corps $K\langle L \cup M \rangle$. Supposons les extensions (K,L) et (K,M) étrangères l'une à l'autre, et désignons par A et B des bases de transcendance de L et de M par rapport à K . Pour que (K,U) soit librement composée de (K,L) et de (K,M), il est alors nécessaire et suffisant que les conditions suivantes soient satisfaites : A et B n'ont pas d'élément commun et $A \cup B$ est algèbriquement libre par rapport à K .

Supposons d'abord que (K,U) soit librement composée de (K,L) et de (K,M). Il résulte alors immédiatement de la prop.1 que $L \cap M = K$, d'où $A \cap B = \emptyset$. Désignons par B^* l'ensemble des éléments de la forme $x_1^{e_1} \ldots x_n^{e_n}$, ou $x_i \in B$, $0 \leqslant e_i < +\infty$ $(1 \leqslant i \leqslant n)$. L'ensemble B^* est libre par rapport à K , donc aussi, en vertu de la prop.1, par rapport à L , ce qui montre que B est algèbriquement libre par rapport à L , et, a fortiori, par rapport à $K\langle A \rangle$. Il en résulte que $A \cup B$ est algèbriquement libre par rapport à K (prop.1, § 9) .

Supposons maintenant les conditions satisfaites. Formons un produit kroneckerien (P,γ) des structures d'algèbres de L et de M par rapport à K , et désignons par φ l'homomorphisme de P dans U qui est défini par la condition que $\varphi(\gamma(x,y)) = xy$ pour tout $(x,y) \in L \times M$. Nous voulons démontrer que l'idéal $\mathfrak{p} = \varphi^{-1}(0)$ se réduit à $\{0\}$. Les combinaisons linéaires à coefficients dans K d'éléments de $\gamma(K[A] \times K[B])$ forment, comme on le voit tout de suite, un sous-anneau $\mathcal{O}$ de P . Tout élément de $\mathcal{O}$ peut se mettre sous la forme $f(x'_1, \ldots, x'_r, y'_1, \ldots, y'_s)$, où f est un polynome en r+s lettres à coefficients dans K et où $x'_i = \gamma(x_i, 1)$, $x_i \in A$ $(1 \leqslant i \leqslant r)$, tandis que $y'_j = \gamma(1, y_j)$, $y_j \in B$ $(1 \leqslant j \leqslant s)$.

On peut de plus supposer $x_i \neq x_{i'}$ pour $i \neq i'$ et $y_j \neq y_{j'}$ pour $j \neq j'$. On a $\varphi(z) = f(x_1,..,x_r,y_1,...,y_s)$. Puisque $A \cup B$ est algèbriquement libre par rapport à K , la condition $\varphi(z) = 0$ entraîne $f = 0$, d'où $z = 0$; on voit donc que la restriction φ_0 de φ à $\mathcal{O}$ est un isomorphisme. Puisque (K,L) et (K,M) sont étrangères l'une à l'autre, P est un anneau d'intégrité ; soit P_1 un corps des quotients de P . Désignons par Z_1 le corps des quotients de $\mathcal{O}$ dans P_1 . Tout élément de la forme $\gamma(x,1)$, $x \in L$, est algèbrique par rapport à Z_1 puisque $Z_1 \supset \mathcal{O} \supset \gamma(K[A] \times \{1\})$ on voit de même que tout élément de la forme $\gamma(1,y)$, $y \in M$, est algèbrique par rapport à Z_1 . Puisque tout élément de P est combinaison linéaire à coefficients dans K de produits d'éléments des formes précédentes, on voit que tout élément de P est algèbrique par rapport à Z_1 . Soit alors z un élément de $\mathcal{P}$ et soit $g(X) = X^h + u_1X^{h-1} + ... + u_h$ le polynome minimal de z par rapport à Z_1 . Ecrivons $u_i = u_i'/v$ $(1 \leqslant i \leqslant h)$, où $u_1',...,u_h',v$ sont des éléments de $\mathcal{O}$. On a donc $vz^h + \sum_{i=1}^{h} u_i' z^{h-i} = 0$. De l'égalité $\varphi(z)=0$, on déduit que $\varphi_0(u_h')=0$. Puisque φ_0 est un isomorphisme, on a $u_h'=0$, d'où $u_h = 0$, ce qui montre que g(X) est divisible par X . Puisque g(X) est le polynome minimal de z , on doit avoir $g(X)=X$, d'où $z=0$, ce qui achève la démonstration.

Proposition 3.- Soient (K,L) et (K,M) des extensions d'un corps K . Supposons que (K,L) soit purement transcendante. Les extensions (K,L) et (K,M) sont alors étrangères l'une à l'autre.

Soit B une base de transcendance de L par rapport à K telle que $L = K\langle B \rangle$.

Il suffit évidemment de démontrer la prop.3 quand B est fini.

Soit alors n le nombre d'éléments de B ; introduisons n lettres $X_1,\ldots,X_n$ et formons le corps $M\langle X_1,\ldots,X_n\rangle$ des fractions rationnelles en $X_1,..,X_n$ à coefficients dans M . Il existe un isomorphisme de $K\langle B\rangle$ sur $K\langle X_1,..,X_n\rangle$ qui coïncide avec l'identité sur K . Il suffit donc de démontrer que les extensions $(K,K\langle X_1,..,X_n\rangle)$ et (K,M) sont étrangères l'une à l'autre, ce que nous ferons en montrant que $(K,M\langle X_1,..,X_n\rangle)$ est librement composée de ces extensions. Soit C l'ensemble des monomes $X_1^{e_1}\ldots X_n^{e_n}$ $(0\leqslant e_i<\infty,\ 1\leqslant i\leqslant n)$; C est donc une base de $K[X_1,\ldots,X_n]$ par rapport à K ; de plus, C est libre par rapport à M , et notre assertion résulte de la prop.1 .

Corollaire.- Soient (K,V) une extension d'un corps K , et L et M des sous-corps de V contenant K . Supposons que (K,L) soit purement transcendante et que (K,M) soit finie. On a alors $[L\langle M\rangle : L] = [M : K]$.

Cela résulte immédiatement des prop.2 et 3 et du corol.2 à la prop.1 .

---

§ 11. EXTENSIONS SEPARABLES.

Proposition 1.- *Soit* (K,L) *une extension algèbrique d'un corps* K *de caractéristique* $p>0$. *Pour que cette extension soit séparable, il est nécessaire et suffisant que* $(x_i)_{i\in I}$ *désignant une famille d'éléments de* L *qui est libre par rapport à* K , *la famille* $(x_i^p)_{i\in I}$ *soit toujours libre par rapport à* K .

On voit tout de suite qu'il suffit de démontrer la prop.1 dans le cas où (K,L) est finie et où $(x_i)_{i\in I}$ est une base de L par rapport à K . Si la famille $(x_i^p)_{i\in I}$ est libre par rapport à K , on a $\left[K\langle L^p\rangle : K\right] \geqslant \left[L : K\right]$, d'où $L = K\langle L^p\rangle$, ce qui montre que (K,L) est séparable (prop.3, § 6). Inversement, supposons (K,L) séparable. Si $x = \sum_{i\in I} a_i x_i \in L$ (avec $a_i \in K$, $i\in I$), on a $x^p = \sum_{i\in I} a_i^p x_i^p \in \sum_{i\in I} Kx_i^p$, d'où $L^p \subset \sum_{i\in I} Kx_i^p$. Or on a $x_i x_j = \sum_{k\in I} c_{ijk} x_k$ $(i,j\in I)$, avec $c_{ijk} \in K$ $(i,j,k\in I)$, d'où $x_i^p x_j^p = \sum_{k\in I} c_{ijk}^p x_k^p$, ce qui montre que $\sum_{i\in I} Kx_i^p$ est un sous-anneau de L . On peut mettre l'élément unité 1 de K sous la forme $\sum_{i\in I} e_i x_i$, $e_i \in K$; on a donc $1 = 1^p = \sum_{i\in I} e_i^p x_i^p \in \sum_{i\in I} Kx_i^p$, et par suite $K\left[L^p\right] = \sum_{i\in I} Kx_i^p$. Or on sait que $L = K\langle L^p\rangle = K\left[L^p\right]$ (prop.3, § 6 et prop.4, § 2) ; on a donc $L = \sum_{i\in I} Kx_i^p$. Or le nombre d'éléments de I est égal à $\left[L : K\right]$; il en résulte que la famille $(x_i^p)_{i\in I}$ est libre.

Définition 1.- *Soit* (K,L) *une extension quelconque d'un corps* K *de caractéristique* p 0 . *Nous dirons que cette extension est séparable si elle satisfait à la condition suivante :* $(x_i)_{i\in I}$ *étant une famille quelconque d'éléments de* L *qui est libre par rapport à* K , *la famille* $(x_i^p)_{i\in I}$ *est encore libre par rapport à* K . *Si* K *est de caractéristique* 0 , *toute extension de* K *est considérée comme séparable.*

Il résulte de la prop.1 que cette définition n'entre pas en conflit avec celle précédemment donnée de la notion d'extension algèbrique séparable.

Proposition 2.- Soit (K,L) une extension d'un corps K . Si cette extension est séparable, elle est étrangère à toute extension radicielle de K. Sinon, il existe une extension finie (K,K') de K qui n'est pas étrangère à (K,L) et qui possède la propriété que $K'^{p} \subset K$ (où p est la caractéristique de K , qui est alors nécessairement $\neq 0$).

Supposons d'abord (K,L) séparable, et soit (K,K') une extension radicielle de K . Si K est de caractéristique 0 , on a K'=K , et les extensions (K,L), (K,K') sont étrangères l'une à l'autre. Supposons K de caractéristique $p>0$. Formons une extension algèbriquement fermée (L,L^*) de L ; il existe un isomorphisme de K' sur un sous-corps K" de L^* qui coïncide avec l'identité sur K . Pour montrer que (K,L) et (K,K') sont étrangères, il suffira de montrer que $(K,K''\langle L\rangle)$ est librement composée de (K,K") et de (K,L). Soit $(x_i)_{i\in I}$ une famille quelconque d'éléments de L qui est libre par rapport à K ; il suffira de montrer que $(x_i)_{i\in I}$ est encore libre par rapport à K" (prop.1, §10). Observons d'abord qu'on démontre tout de suite par récurrence sur f que la famille $(x_i^{p^f})_{i\in I}$ est libre par rapport à K pour tout entier $f\geqslant 0$. Ceci dit, supposons que $\sum_{i\in I} u_i x_i = 0$, $u_i \in K''$. Il n'y a qu'un nombre fini d'éléments $u_i \neq 0$; il existe donc un entier $f\geqslant 0$ tel que $u_i^{p^f} \in K$ pour tout $i\in I$. Or on a $\sum_{i\in I} u_i^{p^f} x_i^{p^f} = 0$, d'où $u_i^{p^f} = 0$ et $u_i = 0$ pour tout $i\in I$, ce qui démontre notre assertion. Supposons maintenant que l'extension (K,L) ne soit pas séparable ; il existe donc une famille $(x_i)_{i\in I}$ d'éléments de L , libre par rapport à K , telle que la famille $(x_i^p)_{i\in I}$ ne soit pas libre par rapport à K . Il existe une

une famille $(a_i)_{i \in I}$ d'éléments de K telle que $\sum_{i \in I} a_i x_i^p = 0$, que $a_i \neq 0$ pour au moins un $i \in I$ et que $a_i = 0$ pour tous les i sauf un nombre fini. Pour chaque i, le polynome $X^p - a_i$ admet un zéro b_i dans L^* . Soit K' le corps $K\langle \{b_i\}_{i \in I} \rangle$. L'extension (K,K') est évidemment finie ; de plus, on a $K'^p = K^p \langle \{b_i^p\}_{i \in I} \rangle \subset K$. On a $\sum_{i \in I} b_i^p x_i^p = 0$, d'où $\sum_{i \in I} b_i x_i = 0$. L'extension $(K, K'\langle L \rangle)$ n'est donc pas librement composée de (K,K') et de (K,L) (prop.1, §10). L'extension (K,K') étant algèbrique, cela implique que (K,K') et (K,L) ne sont pas étrangères l'une à l'autre (prop.2, § 10). La prop.2 est donc démontrée.

Corollaire.- Toute extension (algèbrique ou non) d'un corps parfait est séparable.

Proposition 3.- Soient (K,L) une extension d'un corps K et M un sous-corps de L contenant K . Si (K,L) est séparable, il en est de même de (K,M). Si (K,L) est séparable (K,M) algèbrique, (M,L) est séparable. Si (K,M) et (M,L) sont séparables, (K,L) est séparable.

La proposition est évidente dans le cas où K est de caractéristique 0 . Supposons donc K de caractéristique $p > 0$. La première assertion de la proposition résulte immédiatement des définitions. Supposons que (K,M) soit algèbrique et (K,L) séparable. Introduisons une extension algèbriquement fermée (L,L) de L , et désignons par M' un sous-corps de L contenant M tel que (M,M') soit finie et que $M'^p \subset M$; en vertu de la prop.2, il suffira de montrer que (M,M') et (M,L) sont étrangères l'une à l'autre. Ecrivons $M' = M\langle y_1, .., y_h \rangle$, d'où $y_i^p \in M$ $(1 \leqslant i \leqslant m)$. Puisque (K,M) est algèbrique, l'extension $(K, K\langle y_1^p, .., y_h^p \rangle)$ est finie ; soit $(x_1, .., x_n)$ une base de $K\langle y_1^p, \ldots, y_h^p \rangle$ par rapport à K .

Puisque (K,M) est séparable, la famille $(x_j^p)_{1\leqslant j\leqslant n}$ est libre par rapport à K et constitue par suite une nouvelle base de $K\langle y_1^p,\ldots,y_h^p\rangle$ par rapport à K . On peut donc mettre y_i^p sous la forme $y_i^p = \sum_{j=1}^{n} a_{ij}x_j^p$, avec $a_{ij}\in K$ $(1\leqslant i\leqslant h,\ 1\leqslant j\leqslant n)$. Pour chaque (i,j) il existe un $b_{ij}\in L^*$ tel que $b_{ij}^p = a_{ij}$; soit K' le sous-corps de L^* qui résulte de l'adjonction à K des éléments b_{ij} $(1\leqslant i\leqslant h, 1\leqslant j\leqslant n)$. L'extension (K,K') est donc finie ; de plus, K'^p résulte de l'adjonction des a_{ij} à K^p , d'où $K'^p\subset K$. Enfin, les formules $y_i = \sum_{j=1}^{n} b_{ij}x_j$ montrent que M' est contenu dans $M\langle K'\rangle$. Ceci dit, les extensions (K,L) et (K,M) étant séparables, il résulte de la prop.2 que $\left[L\langle K'\rangle : L\right] = \left[K' : K\right] = \left[M\langle K'\rangle : M\right]$; cela signifie que l'extension $(M,L\langle K'\rangle)$ est librement composée de (M,L) et de $(M,M\langle K'\rangle)$. Puisque $M'\subset M\langle K'\rangle$, il en résulte immédiatement que $(M,L\langle M'\rangle)$ est librement composée de (M,L) et de (M,M'), donc que (M,L) et (M,M') sont étrangères l'une à l'autre. La deuxième assertion de la prop.3 est donc démontrée. Supposons maintenant que (K,M) et (M,L) soient séparables. Si K' est un sous-corps de L^* contenant K et tel que (K,K') soit radicielle et finie, on a $\left[M\langle K'\rangle : M\right] = \left[K' : K\right]$; de plus $(M\langle K'\rangle)^p = M^p\langle K'^p\rangle$ est contenu dans M , d'où, puisque (M,L) est séparable, $\left[L\langle K'\rangle : L\right]\left[M\langle K'\rangle : M\right] = \left[K' : K\right]$. Ceci démontre que (K,L) est séparable. La prop.3 est donc démontrée.

<u>Définition 2.- Soit</u> (K,L) <u>une extension d'un corps</u> K . <u>On dit qu'une partie</u> B <u>de</u> L <u>est une base séparante de</u> L <u>par rapport à</u> K <u>(ou une base séparante de</u> (K,L) <u>) si</u> B <u>est une base de transcendance de</u> L <u>par rapport à</u> K <u>telle que l'extension</u> $(K\langle B\rangle, L)$ <u>soit séparable.</u>

<u>Proposition 4.- Une extension</u> (K,L) <u>d'un corps</u> K <u>qui admet une base séparante est séparable.</u>

Soit B une base séparante de (K,L). L'extension $(K,K\langle B\rangle)$ est séparable en vertu de la prop.3, §10 et de la prop.2 ci-dessus. Il résulte de là et de la prop.3 que (K,L) est séparable.

La réciproque de la prop.4 n'est pas vraie en général : une extension séparable n'admet pas nécessairement de base séparante. On a cependant le résultat suivant :

Proposition 5.- Soit (K,L) une extension séparable d'un corps K . Supposons que $L = K\langle F\rangle$, où F est une partie finie de L . L'ensemble F contient alors une base séparante de (K,L).

Nous procéderons par récurrence sur le degré de transcendance d de (K,L). La proposition est évidente si d=0 . Supposons la vraie des extensions dont les degrés de transcendance sont moindres que d (où d est supposé >0). L'ensemble F contient certainement une base de transcendance B_0 de L par rapport à K (prop.2, §9). Si K est de caractéristique 0 , B_0 est une base séparante. Supposons donc K de caractéristique $p>0$. Si $K\langle L^p\rangle = L$, on a $(K\langle B_0\rangle)\langle L^p\rangle = L$, et l'extension $(K\langle B_0\rangle, L)$, qui est algèbrique, est séparable (prop.3, §6). Supposons donc que $K\langle L^p\rangle \neq L$ (on peut d'ailleurs montrer qu'il en est nécessairement ainsi dès que $d>0$). Il existe alors un élément $x\in F$ non contenu dans $K\langle L^p\rangle$; l'élément x est nécessairement transcendant par rapport à K , car sinon, l'extension (K,L) étant séparable, on aurait $x\in K\langle x^p\rangle \subset K\langle L^p\rangle$. Nous allons montrer que $(K\langle x\rangle, L)$ est séparable. Soient $u_1,..,u_n$ des éléments de L qui sont linéairement indépendants par rapport à $K\langle x\rangle$; supposons pour un moment que $u_1^p,\ldots,u_n^p$ soient linéairement dépendants par rapport à $K\langle x\rangle$. On voit alors tout de suite qu'il existe des polynomes $f_1,..,f_n$ en une lettre X à coefficients dans K , non tous nuls, tels que $\sum_{i=1}^{n} f_i(x)u_i^p = 0$. Chaque entier pouvant se mettre sous la forme $kp+l$, où $0\leq l<p$, on peut écrire

$f_i(X) = \sum_{j=0}^{p=1} g_{ij}(X^p)X^j$, où $g_{ij} \in K[X]$ $(1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant p-1)$. On a $\sum_{j=0}^{p-1}(\sum_{i=1}^{n} u_i^p g_{ij}(x^p))x^j = 0$. Or chacun des éléments $\sum_{i=1}^{n} u_i^p g_{ij}(x^p)$ appartient à $K\langle L^p\rangle$, et x est de degré p par rapport à $K\langle L^p\rangle$ (prop.2, §6). On a donc $\sum_{i=1}^{n} u_i^p g_{ij}(x^p) = 0$ $(1 \leqslant i \leqslant n)$. Ecrivons $g_{ij}(X) = \sum_{k=1}^{M} a_{ijk}X^k$, $a_{ijk} \in K$. Les éléments x^k $(0 \leqslant k < \infty)$ étant linéairement indépendants par rapport à K , il en est de même des $x^k u_i$ $(0 \leqslant k < \infty,\ 1 \leqslant i \leqslant n)$ (cf. prop. , Alg.II,), donc aussi des $x^{kp}u_i^p$, puisque (K,L) est séparable. On doit donc avoir $a_{ijk} = 0$ pour tous les (i,j,k), d'où $f_i = 0$ $(1 \leqslant i \leqslant n)$, ce qui amène une contradiction. On a $L = (K\langle x\rangle)\langle F\rangle$, et le degré de transcendance de l'extension $(K\langle x\rangle, L)$ est d-1 (~~EXM~~ th. 2, §9). Il en résulte que F contient une base séparante B_1 de l'extension $(K\langle x\rangle, L)$. Il est clair que $B_1 \cup \{x\}$ est une base séparante de (K,L) .

Corollaire 1.- Soit (K,L) une extension séparable de K telle que $L = K\langle F\rangle$, où F est une partie finie de L , et soit d le degré de transcendance de cette extension. Il existe alors une partie F_1 de L dont le nombre d'éléments est soit d soit d+1 telle que $L = K\langle F_1\rangle$.

Soit en effet B une base séparante de (K,L). Si $L = K\langle B\rangle$, on peut prendre $F_1 = B$. Sinon, l'extension $(K\langle B\rangle, L)$ est finie et séparable ; il existe donc alors un $x \in L$ tel que $L = (K\langle B\rangle)\langle x\rangle$, et on peut prendre $F_1 = B \cup \{x\}$.

Corollaire 2.- Soient (K,U) une extension d'un corps K et L et M des sous-corps de U contenant K qui possèdent les propriétés suivantes : l'extension (K,L) est séparable, et il existe une base de transcendance B de L par rapport à K qui est algèbriquement libre par rapport à M . L'extension $(M, M\langle L\rangle)$ est alors séparable.

Pour démontrer que $(M, M\langle L\rangle)$ est séparable, il suffit évidemment de montrer que, si F est une partie finie quelconque de L , l'extension $(M, M\langle F\rangle)$ est séparable. Tenant compte de la prop.4, § 9 , on voit alors tout de suite que l'on peut se ramener au cas où L est de la forme $K\langle F\rangle$, F désignant une partie finie de L . L'extension (K,L) admet dans ce cas une base séparante B_o, et B_o est algèbriquement libre par rapport à M (cf. l.c. plus haut). Tout élément de L étant séparable et algèbrique par rapport à $M\langle B_o\rangle$, l'extension $(M\langle B_o\rangle , M\langle L\rangle)$ est séparable, et B_o est une base séparante de $(M, M\langle L\rangle)$.

---

§ 12. CORPS RELATIVEMENT ALGÈBRIQUEMENT FERMÉS.

Définition 1.- Un sous-corps K d'un corps L est dit relativement algèbriquement fermé dans L quand tout élément de L qui est algèbrique par rapport à K est contenu dans K .

Proposition 1.- Soit (K,L) une extension d'un corps K purement transcendante. Le corps K est alors relativement algèbriquement fermé dans L .

Soit en effet x un élément de L qui est algèbrique par rapport à K . Il résulte du corol. à la prop.3, § 10 que $\left[K\langle x\rangle : K\right]=\left[L\langle x\rangle : L\right] = 1$, d'où $x \in K$.

Proposition 2.- Soient (K,U) une extension d'un corps K , L un sous-corps de U contenant K dans lequel K est relativement algèbriquement fermé, et B une partie de U qui est algèbriquement libre par rapport à L . Le corps $K\langle B\rangle$ est alors relativement algèbriquement fermé dans $L\langle B\rangle$.

Soit x un élément de $L\langle B\rangle$ qui est algèbrique par rapport à $K\langle B\rangle$. Il existe alors des parties finies B_1, B_2 de B telles que x appartienne à $L\langle B_1\rangle$ et soit algèbrique par rapport à $K\langle B_2\rangle$. Il suffira donc de démontrer la prop.2 dans le cas où B est fini. Dans ce cas, procédant par récurrence sur le nombre d'éléments de B , on se ramène tout de suite au cas où B se compose d'un seul élément. Pour démontrer la prop.2 dans ce cas, nous établirons d'abord deux lemmes.

Lemme 1.- Soit $K\langle X\rangle$ le corps des fractions rationnelles en une lettre X à coefficients dans un corps K . Supposons qu'un élément $R \in K\langle X\rangle$ satisfasse à une condition de la forme $R^n + f_1 R^{n-1} + \ldots + f_n = 0$, où $f_1, \ldots, f_n$ sont dans $K[X]$. On a alors $R \in K[X]$.

On peut représenter R comme quotient de deux éléments de $K[X]$; parmi toutes les représentations de cette espèce, choisissons-en une, soit $R = f/g$, dans laquelle le degré du dénominateur g est le plus petit possible.

Nous allons montrer que g est de degré 0, d'où il résultera que $R \in K[X]$. Supposons en effet que g soit de degré >0 ; il existe alors une extension (K,K') de K dans laquelle g admet un zéro x_0 . Or on a $f^n + \sum_{i=1}^{n} f_i g^i f^{n-i} = 0$, d'où $f(x_0)=0$. Il en résulte que f et g sont tous deux divisibles dans $K[X]$ par le polynome minimal φ de x par rapport à K , et que R admet la représentation $R = (f/\varphi)/(g/\varphi)$, ce qui est impossible puisque g/φ est de degré plus petit que g .

Lemme 2. Soit (K,K^*) une extension algèbriquement fermée d'un corps K , et soit a un élément de K^* qui est transcendant par rapport à K . L'ensemble des transformées de a par tous les automorphismes de l'extension (K,K^*) est alors infini.

On peut inclure a dans une base de transcendance B de K^* par rapport à K . Soit B_1 l'ensemble des éléments autres que a de B , et soit $K_1 = K\langle B_1 \rangle$. Désignons par n un entier >0 quelconque ; l'élément a étant transcendant par rapport à K_1 (prop.1, § 9), il existe un homomorphisme σ_0 de $K_1[a]$ sur $K_1[a^n]$ qui coïncide avec l'identité sur K_1 et qui applique a sur a^n . Si f est un polynome $\neq 0$ en une lettre à coefficients dans K_1, on a $\sigma_0(f(a)) = f(a^n) \neq 0$, car a^n est évidemment transcendant par rapport à K_1 . Il en résulte que σ_0 peut se prolonger par un isomorphisme σ_1 de $K_1\langle a \rangle$ sur $K_1\langle a^n \rangle$. L'extension $(K_1\langle a \rangle , K^*)$ étant algèbrique et algèbriquement fermée, et $K_1\langle a \rangle$ étant algèbrique par rapport à $K_1\langle a^n \rangle$, l'extension $(K_1\langle a^n \rangle , K)$ est algèbrique et algèbriquement fermée, et on peut prolonger σ_1 par un automorphisme σ de K^* (th.3, § 3) ; σ est un automorphisme de (K_1,K^*), et, a fortiori, de (K,K^*). L'ensemble des $a^n (1 \leqslant n < \infty)$ étant évidemment infini, le lemme 2 est démontré.

Ceci dit, revenons à la démonstration de la prop.2. Introduisons une exten
extension algèbriquement fermée (L,L^*) de L et formons le corps $L^*\langle X \rangle$

des fractions rationnelles en une lettre X à coefficients dans L^* ; il suffira de démontrer que $K\langle X\rangle$ est relativement algèbriquement fermé dans $L\langle X\rangle$. Soit r un élément de $L\langle X\rangle$ qui est algèbrique par rapport à $K\langle X\rangle$. On a donc une égalité de la forme

$$r^n + \sum_{i=1}^{n} u_i r^{n-i} = 0 \qquad u_i \in K\langle X\rangle \ , \ 1 \leqslant i \leqslant n \ .$$

On peut écrire $u_i = f_i/g$ $(1 \leqslant i \leqslant n)$, avec $f_1,\dots,f_n,g$ dans $K[X]$. On a $(gr)^n + \sum_{i=1}^{n} f_i g^{i-1}(gr)^{n-i} = 0$. Or, les éléments $f_i g^{i-1}$ sont dans $L[X]$: il résulte donc du lemme 1 que $gr \in L[X]$. Posons $h = gr = \sum_{j=0}^{k} a_j X^j$, avec $a_j \in L$ $(0 \leqslant j \leqslant k)$. Soit σ un automorphisme quelconque de l'extension (K,L^*) ; on peut prolonger σ par un automorphisme $\tilde{\sigma}$ de $(K,L^*\langle X\rangle)$ qui change X en lui-même. On a donc

$$(\tilde{\sigma}(h))^n + \sum_{i=1}^{n} f_i g^{i-1}(\tilde{\sigma}(h))^{n-i} = 0 \ .$$

Introduisons une nouvelle lettre Y , et observons que le polynome $Y^n + \sum_{i=1}^{n} f_i g^{i-1} Y^{n-i}$ dont les coefficients sont dans $L^*\langle X\rangle$, ne peut avoir qu'un nombre fini de zéros dans $L^*\langle X\rangle$. L'ensemble des $\tilde{\sigma}(h)$ (σ parcourant l'ensemble des automorphismes de l'extension (K,L^*)) est donc fini. Or, $\tilde{\sigma}(h) = \sum_{j=0}^{k} \sigma(a_j)X^j$; il résulte donc du lemme 2 que $a_0,\dots,a_k$ sont algèbriques par rapport à K . Le corps K étant relativement algèbriquement fermé dans L , on a $a_j \in K$ $(0 \leqslant j \leqslant k)$ d'où $r \in K\langle X\rangle$. La prop.2 est donc démontrée.

Proposition 3.- Soient (K,L) et (K,M) des extensions d'un corps K . Supposons que K soit relativement algèbriquement fermé dans L et que l'une au moins des extensions (K,L) ou (K,M) soit séparable. Les extensions (K,L) et (K,M) sont alors étrangères l'une à l'autre.

Soit B une base de transcendance de M par rapport à K . Les extensions (K,L) et $(K,K\langle B\rangle)$, étant étrangères l'une à l'autre (prop.3, §10), admettent une extension librement composée, soit $((K,U_1), \lambda , \mu_1)$.

Soit (U_1,U) une extension algèbriquement fermée de U_1 ; puisque M est algèbrique par rapport à $K\langle B\rangle$, on peut prolonger μ_1 par un isomorphisme μ de M sur un sous-corps de U . L'ensemble $\mu(B) = \mu_1(B)$ est algèbriquement libre par rapport à $\Lambda(L)$; on voit donc qu'on peut supposer sans restreindre la généralité que L et M sont des sous-corps d'un corps algèbriquement fermé U et que B est algèbriquement libre par rapport à L . Nous allons montrer que, dans ces conditions, $(K,L\langle M\rangle)$ est librement composée de (K,L) et de (K,M). Il suffit pour cela de montrer que, F étant une partie finie quelconque de M , $(K,L\langle F\rangle)$ est librement composée de (K,L) et de $(K,K\langle F\rangle)$. Soit B_o une base de transcendance de $K\langle F\rangle$ par rapport à K ; si (K,M) est séparable, nous supposerons de plus que B_o est une base séparante de $(K,K\langle F\rangle)$. En tout état de cause, nous désignerons par M_o le corps formé des éléments de $K\langle F\rangle$ qui sont séparables par rapport à $K\langle B_o\rangle$; il existe donc un élément $x\in M_o$ tel que $M_o = (K\langle B_o\rangle)\langle x\rangle$. (cf. prop.5, §11). Introduisant une lettre X , nous désignerons par $\varphi(X)$ et $\psi(X)$ les polynomes minimaux de x par rapport à $K\langle B_o\rangle$ et à $L\langle B_o\rangle$ respectivement. Le corps U étant algèbriquement fermé, on peut écrire

$$\varphi(X) = \prod_{i=1}^{n}(X-x_i) \; ; \qquad \psi(X) = \prod_{j=1}^{m}(X-y_j)$$

ou les x_i, y_j sont des éléments de U . Puisque $\varphi(x)=0$, $\varphi(X)$ est divisible par $\psi(X)$ dans $(L\langle B_o\rangle)[X]$, d'où $\varphi(y_j)=0$ $(1\leqslant j\leqslant m)$ et $\prod_{i=1}^{n}(y_j-x_i)=0$. Chacun des y_j est donc un élément de l'ensemble $\{x_1,\ldots,x_n\}$. Or $x_1,\ldots,x_n$ sont algèbriques par rapport à $K\langle B_o\rangle$. On en déduit que les coefficients de ψ (qui appartiennent à $K[y_1,\ldots,y_m]$) sont algèbriques par rapport à $K\langle B_o\rangle$. Mais ces coefficients appartiennent à $L\langle B_o\rangle$: on déduit alors de la prop.2 que les coefficients de ψ sont dans $K\langle B_o\rangle$. Puisque $\varphi(X)$ est le polynome minimal de x par rapport à $K\langle B_o\rangle$, on a $\psi = \varphi$, d'où

$\left[L\langle M_0\rangle : L\langle B_0\rangle\right] = \left[M_0 : K\langle B_0\rangle\right]$. Posons $M_1 = K\langle F\rangle$; si (K,M) est séparable, on a $M_0 = M_1$; sinon, on peut du moins affirmer que (M_0, M_1) est radicielle et finie. De plus, si (K,M) n'est pas séparable, (K,L) l'est, et il en est de même de $(M_0, M_0\langle L\rangle)$ (cf. corol.2 à la prop.5, § 11, se souvenant que $(K, L\langle B_0\rangle)$ est librement composée de (K,L) et de $(K, K\langle B_0\rangle)$). Puisque $L\langle M_0\rangle = M_0\langle L\rangle$, on déduit de la prop.2 § 11 et du corol.2 à la prop.1, § 10 que $(L\langle M_1\rangle : L\langle M_0\rangle) = \left[M_1 : M_0\right]$, d'où

$$\left[L\langle M_1\rangle : L\langle B_0\rangle\right] = \left[L\langle M_1\rangle : L\langle M_0\rangle\right]\left[L\langle M_0\rangle : L\langle B_0\rangle\right]$$
$$= \left[M_1 : M_0\right]\left[M_0 : K\langle B_0\rangle\right] = \left[M_1 : K\langle B_0\rangle\right]$$

La formule $\left[L\langle M_1\rangle : L\langle B_0\rangle\right] = \left[M_1 : K\langle B_0\rangle\right]$ est donc établie dans tous les cas. Il résulte de la prop.1, § 10 qu'une base $(\eta_1, .., \eta_p)$ de M_1 par rapport à $K\langle B_0\rangle$ est aussi une base de $L\langle M_1\rangle = L\langle F\rangle$ par rapport à $L\langle B_0\rangle$. Soit $(\xi_\alpha)_{\alpha \in A}$ une base de $K\langle B_0\rangle$ par rapport à K. L'extension $(K, L\langle B_0\rangle)$ étant librement composée de (K,L) et de $(K, K\langle B_0\rangle)$, la famille $(\xi_\alpha)_{\alpha \in A}$ est libre par rapport à L (prop.1, § 10). Il résulte de là que la famille $(\xi_\alpha \eta_i)_{\alpha \in A}$, $1 \leqslant i \leqslant p$ qui est une base de $K\langle F\rangle$ par rapport à K, est libre par rapport à L, ce qui montre que $(K, L\langle F\rangle)$ est librement composée de (K,L) et de $(K, K\langle F\rangle)$ (prop.1, § 10). La prop.3 est ainsi démontrée.

Proposition 4.- Soient (K,U) une extension d'un corps K, L et M des sous-corps de U contenant K et B une base de transcendance de M par rapport à K. Supposons que K soit relativement algèbriquement fermé dans L, que B soit algèbriquement libre par rapport à L et que l'une au moins des extensions (K,L) ou (K,M) soit séparable. Le corps M est alors relativement algèbriquement fermé dans $M\langle L\rangle$.

Si un élément $x \in M\langle L\rangle = L\langle M\rangle$ est algèbrique par rapport à M, il existe des parties finies F et F' de M telles que x appartienne à $L\langle F\rangle$ et soit algèbrique par rapport à $K\langle F'\rangle$. Tenant compte de la prop.4, § 9, on voit qu'il suffira de démontrer la prop.4 dans le cas où il existe une partie finie F de M telle que $M = K\langle F\rangle$, et qu'on peut supposer que, si (K,M) est séparable, B est une base séparante de cette extension. On sait que $K\langle B\rangle$ est relativement algèbriquement fermé dans $L\langle B\rangle$ (prop.2) ; de plus, si (K,L) est séparable, il en est de même de $(K\langle B\rangle, L\langle B\rangle)$ (corOl.2 à la prop.5, § 11). Supposons d'abord que (K,L) soit séparable. Il résulte alors de la prop.3 que $(K\langle B\rangle, L\langle B\rangle)$ et $(K\langle B\rangle, M\langle x\rangle)$ sont étrangères l'une à l'autre. En vertu du corol.2 à la prop.1, § 10, on a $\left[M\langle x\rangle : K\langle B\rangle\right] = \left[L\langle M \cup \{x\}\rangle : L\langle B\rangle\right] = \left[L\langle M\rangle : L\langle B\rangle\right] = \left[M : K\langle B\rangle\right]$, d'où $\left[M\langle x\rangle : M\right] = 1$ et $x \in M$. Supposons maintenant que (K,L) ne soit pas séparable ; le corps K est alors de caractéristique $p > 0$ et (K,M) est séparable. Il existe un entier $f > 0$ tel que $x' = x^{p^f}$ soit séparable par rapport à M (prop.2, § 6). Les extensions $(K\langle B\rangle, M)$ et $(M, M\langle x'\rangle)$ étant séparables, il en est de même de $(K\langle B\rangle, M\langle x'\rangle)$, (prop.3, § 11). Le même raisonnement que plus haut (appliqué à x' au lieu de x) montre alors que $x' \in M$. Soit $(u_1,..,u_m)$ une base de M par rapport à $K\langle B\rangle$; puisque $(K\langle B\rangle, M)$ est séparable, $(u_1^{p^f},...,u_m^{p^f})$ est aussi une base de M par rapport à $K\langle B\rangle$. Par ailleurs, il résulte du corol.1 à la prop.1, § 10 et de la prop.3 que $(u_1,..,u_m)$ et $(u_1^{p^f},..,u_m^{p^f})$ sont des bases de $L\langle M\rangle$ par rapport à $L\langle B\rangle$. Ecrivons $x = \sum_{i=1}^{m} v_i u_i$, $v_i \in L\langle B\rangle$ $(1 \leqslant i \leqslant m)$; on a $x' = \sum_{i=1}^{m} v_i^{p^f} u_i^{p^f}$. D'autre part, on peut mettre x' sous la forme $x' = \sum_{i=1}^{m} w_i u_i^{p^f}$ avec $w_i \in K\langle B\rangle$ $(1 \leqslant i \leqslant m)$. On en conclut que $v_i^{p^f} = w_i \in K\langle B\rangle$ $(1 \leqslant i \leqslant m)$. Puisque $K\langle B\rangle$ est relativement algèbriquement fermé dans $L\langle B\rangle$ (prop.2), il résulte de là que $v_i \in K\langle B\rangle$ $(1 \leqslant i \leqslant m)$, d'où $x \in M$. La prop. 4 est donc démontrée.
