RÉDACTION N° 099

COTE : NBR 010

TITRE : LIVRE II
CHAPITRE V. CORPS COMMUTATIFS (ÉTAT 3)

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 154

NOMBRE DE FEUILLES : 154

LIVRE II

CHAPITRE V

CORPS COMMUTATIFS (Etat 3)

Sommaire

Commentaires.

La rédaction actuelle a profité très largement, d'une part des améliorations et idées nouvelles de la rédaction Chevalley, d'autre part des parties du livre de Weil sur la Géomètrie algèbrique qui traitent de la théorie des corps. Les innovations les plus importantes se trouvent dans les §§ 4 et 5 ; au § 4 , une idée de Weil (où les "éléments primordiaux" sont utilisés) permet de donner une définition générale des extensions séparables (algèbriques ou non) en termes d'isomorphismes et d'en déduire aussitôt le critère de Mac Lane (§ 4, th.2) sur lequel reposent toutes les démonstrations qui suivent. Au § 5, la composition des corps est dominée par les idées de produit tensoriel et d'extensions linéairement disjointes ; le th. fondamental (th.1) est démontré suivant une méthode de Weil, qui utilise les dérivations.

Le rédacteur a adopté le point de vue de Chevalley, d'après lequel les corps ordonnés doivent se trouver dans le chapitre sur les relations d'ordre en général dans les anneaux et les corps (chap.VI) ; il a en outre adjoint un nouveau § sur les corps cycliques, sur l'utilité duquel il ne peut se prononcer, et laisse la parole aux spécialistes d'arithmétique (commutative ou non).

Au moment d'envoyer cette rédaction au tirage, le rédacteur a eu connaissance des nouvelles méthodes Cartan pour traiter plus rapidement le § 3 (fabrication d'extensions universelles à l'aide de la notion de produit tensoriel d'une infinité d'algèbres, qui devra être exposée au chap.III) ; il n'a pas eu le temps de modifier la rédaction actuelle en conséquence, mais est d'avis que la rédaction suivante devra s'inspirer de ces méthodes.

LIVRE II

CHAPITRE V

CORPS COMMUTATIFS (Etat 3)

§ 1. Corps premiers. Caractéristique.

1. Corps premiers.

On sait (chap.I, § 9, n°2) que l'intersection d'une famille quelconque de sous-corps d'un corps K (commutatif ou non) est un sous-corps de K ; en particulier, l'intersection P de tous les sous-corps de K est le plus petit sous-corps de K ; il ne contient aucun sous-corps distinct de P .

DEFINITION 1. On dit qu'un corps est premier s'il ne contient aucun sous-corps distinct de lui-même.

Tout corps (commutatif ou non) contient donc un corps premier et un seul ; nous allons déterminer la structure de tous les corps premiers.

Pour cela, remarquons que, si K est un corps quelconque, ε l'élément unité de K , l'application $n \to n.\varepsilon$ est une représentation de l'anneau $\mathbb{Z}$ des entiers rationnels dans K (chap.I, § 8, n°8). L'ensemble des entiers $n \in \mathbb{Z}$ tels que $n.\varepsilon = 0$ est un idéal (p) de $\mathbb{Z}$, où $p \geqslant 0$ est la caractéristique (chap.I, § 8, n°8) du corps K ; l'image A de $\mathbb{Z}$ par la représentation $n \to n.\varepsilon$ est un sous-anneau isomorphe à $\mathbb{Z}/(p)$, contenu dans tout sous-corps de K , donc dans le sous-corps premier P de K . Il peut se produire deux cas :

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

2^o $p>0$; comme A est contenu dans P , il ne peut contenir de diviseurs de 0 , donc $\mathbb{Z}/(p)$ ne doit pas contenir de diviseurs de 0 , ce qui implique que la relation $p=mn$ $(m>0,\ n>0)$ entraîne $m=p$ ou $n=p$, et par suite que p est un nombre premier (chap.I, §8,n°7) ; l'anneau $\mathbb{Z}/(p)$ est alors un corps, et par suite P est identique à A et isomorphe à $\mathbb{Z}/(p)$. En résumé :

Théorème 1.- La caractéristique d'un corps K (commutatif ou non) est égale à 0 ou à un nombre premier. Si K est de caractéristique 0, le sous-corps premier de K est isomorphe au corps $\mathbb{Q}$ des nombres rationnels; si K est de caractéristique $p>0$, le sous-corps premier de K est isomorphe au corps $\mathbb{Z}/(p)$.

2. Exposant caractéristique. Corps parfaits.

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

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

Il est évident que $(xy)^p=x^py^p$. Nous allons montrer que $(x+y)^p=x^p+y^p$. C'est évident si p=1. Si $p>1$, on sait que $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$ et que $\binom{p}{0}=\binom{p}{p}=1$; il nous suffira donc de montrer que, lorsque $1<k<p$, $\binom{p}{k}$ est un multiple de p , ou encore que $\binom{p}{k}\varepsilon=0$ dans K . Or, on a $k!\binom{p}{k}=p(p-1)..(p-k+1)$, donc $(k!\varepsilon)(\binom{p}{k}\varepsilon)=p(p-1)..(p-k+1)\varepsilon = 0$; comme $k!\varepsilon = \prod_{h=1}^{k} h\varepsilon$ et que $h\varepsilon\neq 0$ pour $1\leqslant h<p$, on a $k!\varepsilon\neq 0$, donc $\binom{p}{k}\varepsilon=0$. L'application $x \to x^p$ est donc une représentation de K dans lui-même ; comme elle n'est pas identiquement nulle, c'est un isomorphisme de K sur un sous-corps de K (chap.I, § 9, th.1).

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

En effet, $x \to x^{p^f}$ est obtenu en itérant f fois l'isomorphisme $x \to x^p$.

Quels que soient les entiers f et $n > 0$, on a donc dans K

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

Définition 2. On dit qu'un corps commutatif K, d'exposant caractéristique p, est parfait, si l'application $x \to x^p$ est un automorphisme de K (autrement dit, si pour tout $y \in K$, il existe $x \in K$ tel que $x^p = y$). On dit que K est imparfait s'il n'est pas parfait.

Tout corps de caractéristique 0 est parfait, car $x \to x^p$ est alors l'application identique. Tout corps fini est parfait, car une application biunivoque d'un ensemble fini dans lui-même est une permutation de cet ensemble.

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

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

Exercices.- 1) Soit A un anneau sans diviseur de 0, commutatif ou non, ayant ou non un élément unité. Montrer que la caractéristique p de A (chap.I, § 8, n° 8) est 0 ou un nombre premier. Si A admet un élément unité, A contient un sous-anneau isomorphe à $\mathbb{Z}/(p)$.

2) Soit A un anneau d'intégrité, $\mathfrak{p}$ un idéal premier (chap.I, § 8, exerc.13) de A. Si la caractéristique de A est un nombre premier $p>0$, la caractéristique de $A/\mathfrak{p}$ est p ; si la caractéristique

de A est 0, la caractéristique de $A/\mathfrak{p}$ est 0 s'il n'existe aucun nombre premier p tel que $pA \subset \mathfrak{p}$; dans le cas contraire, il n'y a qu'un seul nombre premier p ayant cette propriété, et il est égal à la caractéristique de $A/\mathfrak{p}$. Montrer que c'est toujours ce second cas qui se présente lorsque $A/\mathfrak{p}$ est fini.

§ 2. Extensions algèbriques et extensions transcendantes.

1. Adjonction.

Soit K un corps, E une extension (ou surcorps) de K . Etant donnée une famille quelconque $x = (x_\iota)_{\iota \in I}$ d'éléments de E , on sait (chap.IV , §) qu'on désigne par $K(x_\iota)_{\iota \in I}$ (ou $K(x)$, ou encore $K(x_1, x_2, \ldots, x_n)$ lorsque I est l'intervalle $[1,n]$ de $\mathbb{N}$) le plus petit sous-corps de E contenant K et les éléments de la famille (x_ι) ; nous dirons que $K(x_\iota)_{\iota \in I}$ est obtenu par adjonction à K des éléments de la famille (x_ι) , et que l'ensemble des x_ι est un système de générateurs de $K(x_\iota)_{\iota \in I}$ par rapport à K . On sait que $K(x_\iota)_{\iota \in I}$ ne dépend que de l'ensemble A des éléments de la famille (x_ι) et qu'on le désigne encore par la notation $K(A)$.

Proposition 1. Si M et N sont deux parties quelconques de E , on a $K(M \cup N) = K(M)(N) = K(N)(M)$.

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

Remarque.- Si P est le sous-corps premier (§ 1) de E , pour toute partie A de E le corps $P(A)$, est le plus petit sous-corps de E contenant A . Pour tout sous-corps K de E , on a $P(K) = K$; si K est un sous-corps de E , A une partie quelconque de E , on a $K(A) = P(K \cup A)$; en particulier, si K et K' sont deux sous-corps de E , on a $P(K \cup K') = K(K') = K'(K)$: ce corps est le plus petit

sous-corps de E contenant K et K', ou encore la borne supérieure de K et K' dans l'ensemble des sous-corps de E , ordonné par inclusion (cf. §5).

On sait (chap.IV, § , prop.) que le corps $K(x_\iota)_{\iota \in I}$ est identique à l'ensemble des éléments $f((x_\iota))$, où f parcourt l'ensemble $K(X_\iota)_{\iota \in I}$ des fractions rationnelles par rapport à la famille d'indéterminées $(X_\iota)_{\iota \in I}$, à coefficients dans K , telles que l'élément $f((x_\iota))$ soit défini. Comme dans une fraction rationnelle par rapport aux X_ι ne figurent qu'un nombre fini des X_ι, on voit que :

Proposition 2.- Le corps K(A), obtenu par adjonction à K d'une partie quelconque A de E , est la réunion des corps K(F), où F parcourt l'ensemble des parties finies de A .

On peut encore démontrer cette proposition de la façon suivante : lorsque F parcourt l'ensemble des parties finies de A , l'ensemble $\mathfrak{F}$ des corps K(F), ordonné par inclusion, est filtrant pour la relation $\subset$, car pour deux parties finies quelconques M,N de A , on a $K(M) \subset K(M \cup N)$ et $K(N) \subset K(M \cup N)$. Si nous prouvons que la réunion L des corps de $\mathfrak{F}$ est encore un corps, la prop.2 en résultera, puisque L contient $K \cup A$ et est contenu dans K(A) . Or, plus généralement :

Proposition 3.- Soit $\mathfrak{F}$ un ensemble de sous-corps d'un corps E , filtrant pour la relation $\subset$. La réunion L des corps de $\mathfrak{F}$ est un corps.

En effet, si x et y sont deux éléments de L , il existe deux corps R,S de l'ensemble $\mathfrak{F}$ tels que $x \in R$, $y \in S$; si T est un corps appartenant à $\mathfrak{F}$, tel que $R \subset T$ et $S \subset T$, x et y appartiennent à T , donc il en est de même de $x+y$, xy et x^{-1} si $x \neq 0$; ces éléments appartenant à L , L est un corps.

Définition 1.- On dit qu'une extension E d'un corps K est de type fini par rapport à K si E possède un système de générateurs fini par rapport à K .

La prop.2 montre donc que toute extension E d'un corps K est réunion des extensions de K de type fini, contenues dans E .

Une extension $K(x)$ de E , engendrée par un ensemble formé d'un seul élément x , est dite extension simple de K .

2. Eléments algèbriques.

On sait qu'une extension E d'un corps K est une algèbre, et par suite un espace vectoriel sur K . dont la dimension (linéaire) par rapport à K est appelée le degré de E par rapport à K , et notée $[E:K]$ lorsqu'elle est finie (le nombre $[E:K]$ n'est donc défini que dans ce dernier cas). L'étude de la restriction du corps des scalaires d'un espace vectoriel entraîne en particulier que (chap.II, §5, cor. de la prop.1) :

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

$$[F:K] = [E:K][F:E] \tag{1}$$

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

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

En effet, quand le degré d'une extension de K est 1, cette extension est identique à K .

Il est clair que toute extension E de K de degré fini est aussi de type fini, puisqu'une base de E (considéré comme espace vectoriel sur K)

est aussi dans ce cas un système de générateurs de E par rapport à K ; mais, comme nous le verrons un peu plus loin ($n^o 5$), la réciproque est inexacte.

Définition 2. Etant donnée une extension E d'un corps K , on dit qu'un élément $x \in E$ est algébrique par rapport à K (ou sur K) si l'extension $K(x)$ est de degré fini par rapport à K ; ce degré s'appelle alors le degré de x par rapport à K . Un élément de E qui n'est pas algébrique sur K est dit transcendant par rapport à K (ou sur K).

Théorème 2.- a) Pour qu'un élément $x \in E$ soit algébrique sur K , il faut et il suffit qu'il existe un polynome $g \neq 0$ dans $K[X]$ tel que $g(x)=0$.

b) Si x est de degré n par rapport à K , il existe un polynome $f \in K[X]$ et un seul de degré n , tel que le coefficient de X^n dans f soit égal à 1 , et que l'on ait $f(x)=0$; ce polynome est appelé pôlynome minimal de x par rapport à K .

c) Le polynome minimal f de x est irréductible ; l'ensemble des polynomes $g \in K[X]$ tels que $g(x)=0$ est l'idéal principal (f).

d) L'application $g \to g(x)$ est un homomorphisme de l'anneau $K[X]$ sur le corps $K(x)$; $K(x)$ est isomorphe à l'anneau quotient $K[X]/(f)$ et les éléments $1=x^0, x, x^2, \ldots, x^{n-1}$ forment une base de $K(x)$ considéré comme algèbre sur K .

Si $K(x)$ est de degré fini n sur K , les $n+1$ éléments $1, x, \ldots, x^n$ de $K(x)$ forment un système lié par rapport à K , donc il existe $n+1$ éléments a_k $(0 \leqslant k \leqslant n)$ de K non tous nuls et tels que $\sum_{k=0}^{n} a_k x^k = 0$, ce qui signifie que, pour le polynome $g = \sum_{k=0}^{n} a_k X^k \neq 0$ de $K[X]$, on a $g(x)=0$.

Réciproquement, supposons qu'il existe au moins un polynome $g \neq 0$ de $K[X]$ tel que $g(x)=0$; l'ensemble des polynomes $g \in K[X]$ tels que

$g(x)=0$ est donc un idéal $\neq(0)$ dans $K[X]$; par suite (chap.IV, §1, prop.) c'est un idéal <u>principal</u> (f), où f est de degré $m>0$; on peut toujours supposer en outre que le coefficient de X^m dans f soit égal à 1 . L'application $g \to g(x)$ de l'anneau $K[X]$ dans $K(x)$ est une représentation, et l'image de $K[X]$ par cette représentation est un sous-anneau de $K(x)$ contenant K et isomorphe à $K[X]/(f)$. Comme $K(x)$ est un corps, il s'en suit que $K[X]/(f)$ n'a pas de diviseur de 0 ; donc la relation $f=gh$ dans $K[X]$ entraîne que l'un des deux polynomes g,h est une constante, car on en déduit $gh \equiv 0\ (f)$ donc $g \equiv 0$ ou $h \equiv 0$ (mod.f) mais comme les degrés de g et de h sont au plus égaux au degré de f , l'un de ces deux polynomes doit être égal au produit de f par une constante. Autrement dit, f est un polynome <u>irréductible</u> dans $K[X]$; il en résulte (chap.IV, § ,prop.) que (f) est un idéal <u>maximal</u> dans $K[X]$, et par suite que $K[X]/(f)$ est un corps (chap.I, §9, th.2); comme l'image de $K[X]$ par la représentation $g \to g(x)$ est isomorphe à ce corps, contient K et est contenue dans $K(x)$, elle est <u>égale à</u> $K(x)$. Enfin, pour deux polynomes g,h de $K[X]$, la relation $g(x)=h(x)$ équivaut à $g \equiv h$ (mod.f) ; pour tout polynome $g \in K[X]$, il existe un polynome h et un seul tel que $g \equiv h$ (mod.f) et $\deg h < m$, savoir le <u>reste</u> de la division de g par f ; tout élément de $K(x)$ peut donc s'écrire d'<u>une manière et d'une seule</u> comme combinaison linéaire de $1,x,x^2,..,x^{m-1}$ à coefficients dans K ; ces m éléments forment par suite une <u>base</u> de $K(x)$, ce qui prouve que le degré de x par rapport à K est égal au degré du polynome f , et achève la démonstration.

COROLLAIRE.- <u>Soit E une extension de K , x un élément de E algébrique sur K ; pour tout sous-corps F de E tel que $K \subset F$, x est algébrique sur F, et son degré par rapport à F est au plus égal à son degré par rapport à K</u>

En effet, si f est le polynome minimal de x par rapport à K , on a $f \in F[X]$ et $f(x)=0$; x est donc algèbrique par rapport à F., et son polynome minimal par rapport à F divise f , donc son degré est au plus égal à celui de f .

Exemples.- * 1) Dans le corps des nombres complexes $\mathbb{C}$, le nombre i est algèbrique et de degré 2 sur le corps premier $\mathbb{Q}$; en effet dans $\mathbb{Q}[X]$ le polynome X^2+1 est irréductible, car dans le cas contraire, il aurait un facteur du premier degré $X-a$, où $a \in \mathbb{Q}$, et on ne peut avoir $a^2+1=0$, puisque $x^2+1 \geqslant 1 > 0$ pour tout $x \in \mathbb{Q}$. Le corps $\mathbb{Q}(i)$ engendré par i est donc une extension de degré 2 de $\mathbb{Q}$; il est formé des nombres complexes $a+bi$, où a et b parcourent $\mathbb{Q}$. *

2) Soit K un corps, F le corps K(X) des fractions rationnelles à une indéterminée sur K . Soit E le sous-corps $K(X^3)$ de F ; on a $F=E(X)$, et X est algèbrique sur E , puisqu'il est racine du polynome Y^3-X^3 de l'anneau $E[Y]$; ce polynome est d'ailleurs irréductible dans $E[Y]$, car dans le cas contraire il aurait un facteur du premier degré, et il y aurait donc deux polynomes non nuls u,v de $K[X]$ tels que $(u(X^3))^3=X^3(v(X^3))^3$, ce qui est absurde, car si m et n sont les degrés de u et de v , on en tire $9m=9n+3$ ou $3m=3n+1$. F est donc de degré 3 sur E , et tout élément de F peut s'écrire d'une seule manière $a(X^3)+Xb(X^3)+X^2c(X^3)$, où a,b,c sont trois fractions rationnelles quelconques de K(X).

3. Extensions algèbriques.

Définition 3.- On dit qu'une extension E d'un corps K est une extension algèbrique de K (ou est algèbrique sur K) si tout élément de E est algèbrique sur K. Une extension de K qui n'est pas algèbrique sur K est dite transcendante sur K .

Proposition 4.- Toute extension de degré fini d'un corps K est algébrique sur K .

En effet, si E est une extension de degré fini de K , pour tout $x \in E$, on a $[K(x):K] \leqslant [E:K]$, donc x est algébrique sur K .

On voit en outre, d'après le cor.1 du th.1, que le degré de tout $x \in E$ par rapport à K divise le degré de E par rapport à K .

La réciproque de la prop.4 est inexacte ; nous donnerons plus tard (§ 3, n°2) des exemples d'extensions algébriques de degré infini.

Proposition 5.- Soit E une extension d'un corps K . Si A est une partie de E formée d'éléments algébriques sur K , l'extension K(A) est algébrique sur K . Si A est fini, K(A) est de degré fini sur K .

Comme K(A) est la réunion des corps K(F), où F parcourt l'ensemble des parties finies de A (prop.2), on peut se borner au cas où A est fini. Raisonnons par récurrence sur le nombre n des éléments de A , la proposition étant évidente pour n=0 . Soient a_i $(1 \leqslant i \leqslant n)$ les éléments de A ; posons $L=K(a_1,a_2,\ldots,a_{n-1})$; on a $K(A)=L(a_n)$, et a_n , étant algébrique sur K , est algébrique sur L ; donc $L(a_n)$ est de degré fini par rapport à L ; comme par hypothèse L est de degré fini sur K , $K(A)=L(a_n)$ est de degré fini sur K d'après le th.1 .

COROLLAIRE.- Soit $E=K(a_1,a_2,\ldots,a_m)$ une extension algébrique de K de type fini ; soit n_1 le degré de a_1 sur K , n_i $(2 \leqslant i \leqslant m)$ le degré de a_i sur $K(a_1,a_2,\ldots,a_{i-1})$; les éléments $a_1^{j_1} a_2^{j_2} \ldots a_m^{j_m}$ $(0 \leqslant j_i \leqslant n_i - 1$ pour $1 \leqslant i \leqslant m)$ forment une base de E par rapport à K ; E est donc de degré $n_1 n_2 \ldots n_m$ sur K ; en outre, l'idéal $\mathfrak{a}$ des relations algébriques entre les a_i (formé des polynomes $f \in K[X_1,X_2,\ldots,X_m]$ tels que $f(a_1,a_2,\ldots,a_m)=0$; cf. chap.IV, § , prop.) est un idéal maximal dans $K[X_1,X_2,\ldots,X_m]$, et E est isomorphe à $K[X_1,X_2,\ldots,X_m]/\mathfrak{a}$.

La première partie du corollaire résulte du th.2 ci-dessus, et de la prop.1 du chap.II, § 5 ; on a donc $E \subset K[a_1, a_2, \ldots, a_m]$, et par suite $E = K[a_1, a_2, \ldots, a_m]$; comme $K[a_1, a_2, \ldots, a_m]$ est un anneau isomorphe à $K[X_1, X_2, \ldots, X_m]/\mathfrak{a}$ (chap.IV, § , prop.), le fait que E est un corps entraîne que l'idéal $\mathfrak{a}$ est maximal (chap.I, § 9, th.2).

Proposition 6.- Soit E une extension d'un corps K . Pour que E soit une extension algébrique de K , il faut et il suffit que tout anneau A tel que $K \subset A \subset E$ soit un corps.

La condition est nécessaire ; en effet, si E est algébrique, $x \neq 0$ un élément d'un anneau A tel que $K \subset A \subset E$, x est algébrique sur K ; soit $f = \sum_{k=0}^{n} a_k X^k$ son polynome minimal par rapport à K ; on a $a_0 \neq 0$ sans quoi f ne serait pas irréductible (car il ne peut être égal à X , en vertu de l'hypothèse $x \neq 0$) ; comme $f(x) = 0$, on a $x^{-1} = a_0^{-1} \sum_{k=1}^{n} a_k x^{k-1}$, et par suite $x^{-1} \in A$, A est un corps.

La condition est suffisante. Supposons en effet qu'elle soit remplie, et soit x un élément quelconque $\neq 0$ de E . Le sous-anneau $K[x]$ de E , engendré par $K \cup \{x\}$, est l'ensemble des f(x), où f parcourt l'anneau de polynomes $K[X]$ (chap.IV, § , prop.). Comme par hypothèse $K[x]$ est un corps, il existe un polynome $g = \sum_{k=0}^{n} \beta_k X^k$ tel que $x^{-1} = g(x)$, c'est-à-dire $\sum_{k=0}^{n} \beta_k x^{k+1} - 1 = 0$, ce qui montre (th.2) que x est algébrique sur K .

4. Transitivité des extensions algébriques. Extensions relativement algébriquement fermées.

Proposition 7.- Soient E et F deux extensions d'un corps K , telles que $K \subset E \subset F$. Pour que F soit algébrique par rapport à K , il faut et il suffit que E soit algébrique par rapport à K , et F algébrique par rapport à E .

La condition est nécessaire, car si F est algèbrique sur K , tout élément de $E \subset F$ est algèbrique sur K , et tout élément de F , étant algèbrique sur K , est algèbrique sur E (cor. du th.2).

La condition est suffisante. En effet, supposons-la remplie, et soit x un élément quelconque de F . Par hypothèse, x est algébrique sur E ; soit $g \in E[X]$ le polynome minimal de x par rapport à E , A l'ensemble (fini) de ses coefficients. Les éléments de A étant algèbriques sur K , K(A) est une extension de degré fini de K (prop.5) et comme x est algèbrique sur K(A) (th.2), $K(A \cup \{x\})$ est de degré fini sur K(A) ; par suite (th.1) $K(A \cup \{x\})$ est de degré fini sur K , ce qui montre (prop.4) que x est algèbrique sur K .

Définition 4.- On dit qu'un sous-corps K d'un corps E est relativement algèbriquement fermé dans E si tout élément de E algèbrique sur K appartient à K .

Autrement dit, K est la seule extension algèbrique de K contenue dans E .

Lorsqu'il ne risquera pas d'y avoir confusion entre cette notion et celle de "corps algèbriquement fermé" (qui sera définie au §3,n°1), nous nous permettrons de dire que K est "algèbriquement fermé dans E " au lieu de "relativement algèbriquement fermé dans E ".

Proposition 8.- Soit E une extension d'un corps K . L'ensemble L des éléments de E algèbriques sur K est un corps, qui est algèbriquement fermé dans E .

En effet, d'après la prop.5 le corps K(L) est une extension algèbrique de K , donc $K(L) \subset L$, et par suite K(L)=L , L est un corps. D'autre part, si $x \in E$ est algèbrique par rapport à L , il est aussi algèbrique par rapport à K (prop.7), donc appartient à L .

Nous dirons que l'extension L de K formée des éléments de E algébriques par rapport à K est la fermeture algébrique de K dans E ; c'est la plus grande extension algébrique de K contenue dans E .

5. Familles algébriquement libres. Extensions transcendantes pures.

Définition 5.- Dans une extension E d'un corps K , on dit qu'une famille $(x_\iota)_{\iota\in I}$ d'éléments de E est algébriquement libre par rapport à K (ou sur K) si la relation $f((x_\iota))=0$, où f est un polynome de l'anneau $K\left[X_\iota\right]_{\iota\in I}$, entraîne $f=0$.

Lorsqu'une famille (x_ι) n'est pas algébriquement libre sur K , on dit qu'elle est algébriquement liée sur K .

Deux éléments x_α, x_β d'une famille algébriquement libre (x_ι), dont les indices sont distincts sont eux-mêmes distincts, sans quoi on aurait $f(x_\alpha, x_\beta)=0$ en posant $f=X_\alpha-X_\beta$. On dira qu'une partie L de E est une partie algébriquement libre sur K (ou un système algébriquement libre sur K) si la famille définie par l'application biunivoque de L sur lui-même est algébriquement libre (auquel cas toute famille définie par une application biunivoque d'un ensemble d'indices sur L est aussi une famille algébriquement libre). Les éléments d'une partie algébriquement libre seront encore dits algébriquement indépendants sur K . Si une partie de E n'est pas algébriquement libre, on dit qu'elle est algébriquement liée (ou est un système algébriquement lié) par rapport à K , et que ses éléments sont algébriquement dépendants par rapport à K.

Proposition 4.- Pour qu'une famille $(x_\iota)_{\iota\in I}$ d'éléments de E soit algébriquement libre sur K , il faut et il suffit que toute sous-famille finie de $(x_\iota)_{\iota\in I}$ soit algébriquement libre sur K .

La condition est évidemment nécessaire. Elle est suffisante, car dans tout polynome $f\in K\left[X_\iota\right]_{\iota\in I}$ il ne figure qu'un nombre fini d'indéterminées X_ι .

La partie vide de E est algèbriquement libre. Dire qu'une partie $\{x\}$ de E réduite à un élément est algèbriquement libre sur K signifie (th2) que x est transcendant sur K ; tout élément d'une partie algèbriquement libre de E est transcendant sur K .

Remarque.- Il est clair qu'une partie algèbriquement libre de E est formée d'éléments linéairement indépendants par rapport à K , ou encore est une partie libre de E , considéré comme espace vectoriel sur K (chap.II, §1, déf.7); mais la réciproque est inexacte, puisqu'une base d'une extension algèbrique de K n'est pas algèbriquement libre. Lorsqu'il sera nécessaire d'éviter toute confusion, nous dirons qu'une partie de E qui est libre pour la structure d'espace vectoriel de E sur K , est linéairement libre sur K .

Soit $(x_\iota)_{\iota\in I}$ une famille algèbriquement libre dans une extension E d'un corps K ; l'application $f \to f((x_\iota))$ de l'anneau $K[X_\iota]_{\iota\in I}$ dans E est alors un isomorphisme de cet anneau sur l'anneau $K[X_\iota]_{\iota\in I}$ engendré par la réunion de K et de l'ensemble des x_ι (chap.IV, §2, prop.). Il en résulte que $K[x_\iota]_{\iota\in I}$ est un anneau d'intégrité, et que son corps des quotients est isomorphe au corps des fractions rationnelles $K(X_\iota)_{\iota\in I}$; mais le corps des quotients de $K[x_\iota]_{\iota\in I}$ n'est autre que le corps $K(x_\iota)_{\iota\in I}$ engendré par la famille (x_ι).

Posons alors la définition suivante :

Définition 6.- On dit qu'une extension E d'un corps K est une extension transcendante pure de K s'il existe une famille $(x_\iota)_{\iota\in I}$ d'éléments de E , algèbriquement libre sur K , et telle que $E = K(x_\iota)_{\iota\in I}$.

Nous venons de démontrer que :

Théorème 3.- Pour qu'une extension d'un corps K soit une extension transcendante pure de K , il faut et il suffit qu'elle soit isomorphe à un corps de fractions rationnelles sur K .

Nous verrons plus loin comme conséquence d'une propriété plus générale (§ 5, cor.de la prop.8) que, dans une extension transcendante pure E sur K , tout élément de E qui n'appartient pas à K est transcendant sur K (ou encore que K est algèbriquement fermé par rapport à E). Mais inversement, lorsque K est algèbriquement fermé par rapport à une de ses extensions E , E n'est pas nécessairement une extension transcendante pure de K (cf.exerc.2).

6. Bases de transcendance.

Proposition 10.- *Soit E une extension d'un corps K , M et N deux parties de E . Les propriétés suivantes sont équivalentes :*

a) $M \cup N$ *est algèbriquement libre sur* K *et* $M \cap N = \emptyset$;

b) M *est algèbriquement libre sur* K , *et* N *est algèbriquement libre sur* $K(M)$;

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

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

1° a) entraîne b). Il est évident que, si $M \cup N$ est algèbriquement libre sur K , il en est de même de M . Supposons que N ne soit pas algèbriquement libre sur $K(M)$; il existerait alors (prop.9) une famille finie $(x_i)_{1 \leqslant i \leqslant m}$ d'éléments distincts de N , et un polynome non nul $f \in K(M)[X_1, X_2, \ldots, X_m]$, tel que $f(x_1, x_2, \ldots, x_m) = 0$.

On peut toujours supposer (chap.III, § 1, prop.) que les coefficients de f appartiennent à l'anneau $K[M]$, et par suite sont des polynomes par rapport à un nombre fini d'éléments distincts $y_1, y_2, \ldots, y_n$ de M . Mais alors, la relation $f(x_1, \ldots, x_m) = 0$ peut s'écrire $g(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$, où g est un polynome de $K[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$, dont les coefficients ne sont pas tous nuls ; comme la famille formée des x_i et des y_j est algèbriquement libre par hypothèse, une telle relation est impossible.

2^{o} b) entraîne a). Il suffit de montrer que, si $x_1,..,x_m$ sont des éléments de M en nombre fini, $y_1,y_2,..,y_n$ des éléments de M en nombre fini, l'ensemble des x_i et des y_j est algébriquement libre sur K (prop.9) Supposons qu'il n'en soit pas ainsi, et qu'il existe un polynome $f \in K[X_1,..,X_m,Y_1,..,Y_n]$ non nul et tel que $f(x_1,..,x_m,y_1,..,y_n)=0$. Si $g=f(X_1,..,X_m,y_1,..,y_n)$, g est un polynome de l'anneau $K(M)[X_1,..,X_m]$ et la relation $f(x_1,..,x_m,y_1,..,y_n)=0$ s'écrit $g(x_1,..,x_m)=0$. Comme M est algébriquement libre sur K(M), les coefficients de g sont nuls ; mais chaque coefficient de g est de la forme $\varphi(y_1,..,y_n)$ où $\varphi \in K[Y_1,..,Y_n]$; comme M est algébriquement libre sur K, et que les polynomes φ ne sont pas tous nuls par hypothèse, nous arrivons encore à une contradiction.

COROLLAIRE.- Soit E une e extension de K, A une partie de E algébriquement libre sur K. Si $K' \subset E$ est une extension algébrique de K, A est algébriquement libre sur K'.

Supposons en effet qu'il existe une partie finie M de A qui soit algébriquement liée sur K', et soit N une partie algébriquement libre maximale de M ; posons $P = M \cap \complement N$. Par hypothèse P n'est pas vide, et tout élément $x \in P$ est algébrique sur K'(N) (prop.10) ; comme $K'(N)=K(N)(K')$, et que tout élément de K' est algébrique sur K, et a fortiori sur K(N) (cor. du th.1), on voit (prop.5) que K'(N) est une extension algébrique de K(N) ; il en résulte (prop.7) que tout $x \in P$ est algébrique sur K(N) ; en vertu de la prop.10, ce résultat est contraire à l'hypothèse que M est algébriquement libre sur K.

Définition 7.- Dans une extension E d'un corps K, on dit qu'une partie B de E est une base de transcendance de E par rapport à K, si B est un élément maximal dans l'ensemble (ordonné par inclusion) des parties de E algébriquement libres sur K.

Proposition 11.- Pour que B soit une base de transcendance d'une extension E de K , il faut et il suffit que B soit algèbriquement libre sur K , et que E soit une extension algèbrique de K(B).

En effet, si B est une base de transcendance de E , et $x \notin B$, $B \cup \{x\}$ ne peut être algèbriquement libre sur K par définition, donc (prop.10) x est algèbrique sur K(B). Réciproquement, si B est algèbriquement libre sur K , et E algèbrique sur K(B) , pour tout $x \notin B$, $B \cup \{x\}$ ne peut être algèbriquement libre sur K , d'après la prop.10, donc B est une base de transcendance de E .

Théorème 4. (Steinitz).- Toute extension d'un corps K admet une base de transcendance par rapport à K . En d'autres termes (prop.11 et th.3) toute extension d'un corps K est extension algèbrique d'une extension transcendante pure de K .

Ce théorème est une conséquence du théorème plus précis suivant :

Théorème 5.- Soit E une extension d'un corps K , S une partie de E telle que E soit une extension algèbrique de K(S) , L une partie algèbriquement libre de E (par rapport à K) contenue dans S . Il existe une base de transcendance B de E par rapport à K telle que $L \subset B \subset S$.

En effet, l'ensemble $\mathfrak{F}$ des parties algèbriquement libres de S ordonné par inclusion, est un ensemble de caractère fini (Ens.R , §7, n°11) d'après la prop.9 ; il est donc inductif (Ens.R , § 7,n°9) et par suite il en est de même de l'ensemble $\mathfrak{G}$ des parties libres de S contenant L . En vertu du th. de Zorn, $\mathfrak{G}$ admet un élément maximal B ; d'après la prop.10, tout élément $x \in S$ est algèbrique sur K(B), car on a, soit $x \in B$, soit $x \notin B$, et dans ce dernier cas $B \cup \{x\}$ ne peut être algèbriquement libre. Le corps K(S) est donc une extension algèbrique de K(B) (prop.5), et comme E est une extension algèbrique de K(S), E est une extension algèbrique de K(B) (prop.7),

donc B est une base de transcendance de E (prop.11).

COROLLAIRE ("théorème d'échange").- Soit E une extension de K , S une partie de E telle que E soit une extension algébrique de K(S), L une partie algébriquement libre de E (par rapport à K) ; il existe une partie S' de S telle que $L \cup S'$ soit une base de transcendance de E .

Il suffit en effet d'appliquer le th.5 en remplaçant l'ensemble S qui figure dans l'énoncé de ce théorème par $L \cup S$.

Remarque.- Si E est une extension transcendante pure de K , F une extension algébrique de E , distincte de E , F peut fort bien être une extension transcendante pure de K (cf. n° 2, exemple 2).

7. Degré de transcendance d'une extension.

Théorème 6.- Soient E une extension d'un corps K , B et C deux bases de transcendance de E par rapport à K ; les ensembles B et C sont équipotents.

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

a) B fini. Soit n le nombre d'éléments de B ; il suffit de montrer que C a au plus n éléments. Nous raisonnerons par récurrence sur n , la proposition étant évidente pour n=0 . Soit x un élément de C n'appartenant pas à B ; en vertu du th. d'échange (cor. du th.5) il existe une partie B' de B telle que $\{x\} \cup B'$ soit une base de transcendance de E ; comme B est une base de transcendance de E , on ne peut avoir B'=B , donc B' a au plus n-1 éléments. Soit K'=K(x), et $C' = C \cup \complement \{x\}$; B' et C' sont toutes deux algébriquement libres sur le corps K' (prop.10), et comme K'(B')=K(B) , K'(C')=K(C) , E est algébrique sur K'(B') et K'(C'), donc (prop.11) B' et C' sont deux bases de transcendance de E par rapport à K' ; comme B' a au plus

n-1 éléments, C' a au plus n-1 éléments, donc C a au plus n éléments.

b) B infini. Nous allons montrer ici que C a une puissance au moins égale à celle de B . En effet, pour tout $x \in C$, il existe une partie finie F_x de B telle que x soit algèbrique par rapport à $K(F_x)$: il suffit de prendre pour F_x une partie finie de B telle que les coefficients du polynome minimal de x par rapport à K(B) appartiennent tous à $K(F_x)$. Soit $F = \bigcup_{x \in C} F_x$; il existe une application sur F d'un ensemble somme (Ens.R, §4,n°5) de la famille (F_x), c'est-à-dire d'une partie d'un ensemble équipotent à l'ensemble produit $C \times \mathbb{N}$; or $C \times \mathbb{N}$ est équipotent à C (Ens.R, §7,n°7), donc (Ens.R , §7,n°4) F a une puissance au plus égale à celle de C . Si la puissance de C était strictement inférieure à celle de B , il en serait de même de celle de F , et par suite F serait une partie de B distincte de B . Mais tout élément de C est algèbrique sur K(F), donc prop.7) tout élément de E est algèbrique sur K(F), et par suite F est une base de transcendance de E (prop.11), ce qui contredit l'hypothèse que B est aussi une base de transcendance de E .

Définition 8.- Soit E une extension d'un corps K admettant une base de transcendance finie par rapport à K . Le nombre d'éléments d'une quelconque des bases de transcendance de E par rapport à K est alors appelé le degré de transcendance, ou la dimension algèbrique de E par rapport à K , et noté $\dim_K E$.

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

D'après le th.5, toute extension de K de type fini a un degré de transcendance fini par rapport à K .

On aura soin de ne pas confondre le degré de transcendance de E par rapport à K , avec le degré (ou dimension linéaire) de E par rapport à K , qui est toujours infini lorsque le degré de transcendance n'est pas nul (prop.4).

Théorème 7.- Soit E une extension de K , F une extension de E . Si deux des nombres $\dim_K E$, $\dim_E F$, $\dim_K F$ sont définis, il en est de même du troisième, et on a

$$\dim_K F = \dim_K E + \dim_E F \quad . \tag{2}$$

D'après la déf.8, ce théorème résultera de la proposition plus générale suivante :

Proposition 12.- Soit E une extension de K , F une extension de E . Si M est une base de transcendance de E par rapport à K , N une base de transcendance de F par rapport à E , on a $M \cap N = \emptyset$, et $M \cup N$ est une base de transcendance de F par rapport à K .

En effet, N est algébriquement libre sur E , donc a fortiori sur $K(M) \subset E$; par suite (prop.10) $M \cap N = \emptyset$ et $M \cup N$ est algébriquement libre sur K . S'il existait un élément $x \notin M \cup N$ tel que $M \cup N \cup \{x\}$ soit algébriquement libre sur K , $N \cup \{x\}$ serait algébriquement libre sur $K(M)$ (prop.10), donc aussi sur E , qui est une extension algébrique de $K(M)$ (cor. de la prop.10), ce qui est absurde puisque N est base de transcendance de F par rapport à E .

Exercices.- 1) Soit (E_ι) une famille d'extensions d'un corps K , contenues dans une extension G de K . Si F_ι est la fermeture algébrique de K dans E_ι , montrer que la fermeture algébrique de K dans $E = \bigcap_\iota E_\iota$, est le corps $F = \bigcap_\iota F_\iota$.

2) a) Soit E une extension transcendante pure d'un corps K . Montrer que tout élément x de E n'appartenant pas à K est transcendant sur K (en considérant, parmi les parties finies (nécessairement non vides) F , algèbriquement libres sur K et telles que $x \in K(F)$, une partie ayant le plus petit nombre d'éléments possible, se ramener au cas où $E=K(y)$, y étant transcendant sur K ; montrer alors que y est algèbrique sur $K(x)$).

b) Soit K le corps $\mathbb{C}(X)$ des fractions rationnelles à une indéterminée X sur le corps $\mathbb{C}$ des nombres complexes. Montrer que, dans l'anneau $K[Y]$, le polynome Y^3-X^3+1 est irréductible ; soit E l'extension de K engendrée par une racine z de ce polynome (cf. § 3). Montrer que tout élément de E n'appartenant pas à $\mathbb{C}$ est transcendant sur $\mathbb{C}$, mais que E n'est pas une extension transcendante pure de $\mathbb{C}$ (pour établir ce dernier point, montrer que, quels que soient les nombres complexes a,b,c non nuls et les polynomes u,v,w de $\mathbb{C}[X]$, premiers entre eux deux à deux, et dont un au moins n'est pas réduit à une constante, on a $au^3+bv^3+cw^3=0$. Pour cela, raisonner par l'absurde : parmi les systèmes de nombres a,b,c et de polynomes u,v,w satisfaisant aux conditions précédentes et tels que $au^3+bv^3+cw^3=0$, prendre un système formé de trois nombres a_0,b_0,c_0 et de trois polynomes u_0,v_0,w_0 , tel que le plus grand des degrés de u_0,v_0,w_0 soit le plus petit possible, et montrer qu'il est absurde de supposer que ce degré d est >0 , en formant un autre système (a,b,c,u,v,w) tel que $au^3+bv^3+cw^3=0$, et pour lequel le plus grand des degrés de u,v,w est >0 et $<d$) .

§ 3. Corps algèbriquement fermés. Extensions universelles.

1. Corps algèbriquement fermés.

Proposition 1.- Pour un corps K, les quatre propriétés suivantes sont équivalentes :

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

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

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

(AF"') Une extension algèbrique quelconque de K est nécessairement identique à K.

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

Reste à voir que les conditions (AF") et (AF"') sont équivalentes. Si K satisfait à la condition (AF"), un élément algèbrique sur K est nécessairement de degré 1 sur K (§ 2, th.2), donc appartient à K, ce qui établit (AF"').

Réciproquement, supposons que K satisfasse à la condition (AF"'), et montrons qu'un polynome irréductible f de $K[X]$ est nécessairement de degré 1. En effet, l'idéal principal (f) est alors maximal dans $K[X]$, donc l'anneau quotient $K[X]/(f)$ est un corps E ; soit φ l'homomorphisme canonique de $K[X]$ sur E ; $\varphi(K)=K'$ est un corps isomorphe à K,

et si n est le degré de f , E est une extension de degré n de K' , car tout polynome de $K[X]$ est congru module f à un polynome et un seul de degré $\leqslant n-1$, donc les images par φ de $1, x, x^2, .., x^{n-1}$ forment une base de E par rapport à K' . Si on identifie K et K' au moyen de l'isomorphisme φ , on peut donc dire que E est une extension de degré n de K ; comme K satisfait à (AF"'), on a $n=1$.

Définition 1.- On dit qu'un corps K est algèbriquement fermé lorsqu'il satisfait aux quatre conditions équivalentes (AF),(AF'),(AF"),(AF"').

On distinguera soigneusement cette notion de celle de corps relativement algèbriquement fermé dans une de ses extensions (§ 2,n° 4).

On déduit de la prop.1 les corollaires suivants :

Corollaire 1.- Soit E un corps algèbriquement fermé, K un sous-corps de E . La fermeture algèbrique de K dans E est un corps algèbriquement fermé.

En effet, si F est la fermeture algèbrique de K dans E , tout polynome de $F[X]$ a une racine dans E ; cette racine est un élément algèbrique sur F , donc (§ 2,prop.7) sur K , et par suite appartient à F .

Corollaire 2.- Un corps algèbriquement fermé est parfait.

En effet, si K est algèbriquement fermé, p son exposant caractéristique (§ 1,n°2), pour tout $x \in K$ l'équation $X^p - x = 0$ a une racine dans K , autrement dit, il existe $y \in K$ tel que $y^p = x$.

Exemples.- * 1) Le corps $\mathbb{C}$ des nombres complexes est algèbriquement fermé (cf.Top.Gén.,chap.VIII, § 1).*

2) Un corps fini K n'est jamais algèbriquement fermé ; en effet, soit $(x_i)_{1 \leqslant i \leqslant n}$ la suite finie formée de ses éléments. Le polynome $f = 1 + \prod_i (X - x_i)$ de $K[X]$ ne peut évidemment avoir aucune racine dans K , donc (prop.1), K n'est pas algèbriquement fermé.

2. Extensions algèbriquement fermées.

Nous allons maintenant démontrer qu'il existe des corps algèbriquement fermés ; de façon précise :

Théorème 1 (Steinitz).- *Etant donné un corps* K , *il existe une extension algèbrique* E *de* K *qui est un corps algèbriquement fermé.*

Supposons le problème résolu, et soit E une extension algèbrique de K qui soit algèbriquement fermée. Pour tout $x \in E$, soit f_x le polynome minimal de x par rapport à K (§2, th.2) ; f_x est un polynome irréductible de l'anneau $K[X]$. Réciproquement, si f est un polynome irréductible de $K[X]$, dans lequel le coefficient du terme de plus haut degré est 1 , il existe au moins un $x \in E$ tel que $f(x)=0$ d'après la condition (AF') ; le polynome minimal f_x de x par rapport à K divise donc f , et comme f est irréductible, $f_x = f$; en outre, l'ensemble M_f des $x \in E$ tels que $f_x = f$ est fini , ayant un nombre d'éléments au plus égal au degré de f (chap.IV, § , prop.). Il existe donc une correspondance biunivoque entre M_f et une partie (finie) du sous-ensemble $\{f\} \times N$ dans l'ensemble produit $K[X] \times N$. Comme les M_f forment une partition de E , il existe donc une application biunivoque de E sur une partie de l'ensemble $K[X] \times N$. Autrement dit, si le théorème est vrai, on peut définir, sur une partie E' de $K[X] \times N$, une structure de corps algèbriquement fermé, telle qu'il existe un sous-corps K' de E' isomorphe à K , et dont E' soit une extension algèbrique.

Guidés par ces considérations, nous allons démontrer le théorème en définissant une telle structure sur une partie de $K[X] \times N$. Pour cela, nous aurons, dans ce qui suit, à considérer des structures de corps définies sur des parties (variables) d'un ensemble donné A . Une telle structure étant donnée, soit B la partie de A sur laquelle elle est définie ; soit S la partie de $A \times A \times A \times A$ formée des éléments

de la forme $(x,y,x+y,xy)$ quand x et y parcourent B ; il est clair que la connaissance de S détermine complètement B , qui est la projection de S sur le premier facteur de $A\times A\times A\times A$, et les lois de composition $(x,y)\to x+y$ et $(x,y)\to xy$ de la structure de corps sur B ; on peut donc identifier l'ensemble des structures de corps sur des parties de A avec l'ensemble $\mathfrak{S}$ des parties S de $A\times A\times A\times A$ qui leur sont ainsi attachées ; c'est ce que nous ferons dans ce qui va suivre. On notera que la relation $S\subset S'$ pour deux parties appartenant à $\mathfrak{S}$, signifie que le corps dont S est la structure est un sous-corps de celui dont S' est la structure. Cela étant :

Lemme.- L'ensemble $\mathfrak{S}$ des structures de corps sur des parties de A , ordonné par inclusion, est inductif.

En effet, soit $\mathfrak{T}$ une partie totalement ordonnée de $\mathfrak{S}$; soit $\mathfrak{F}$ l'ensemble des parties B de A sur lesquelles sont définies les structures de corps $S\in\mathfrak{T}$; pour montrer que $\mathfrak{T}$ admet une borne supérieure dans $\mathfrak{S}$, il suffira de faire voir que la réunion S_0 des ensembles $S\in\mathfrak{T}$ est une structure de corps définie sur la réunion B_0 des ensembles $B\in\mathfrak{F}$. Remarquons d'abord que si $(x_i)_{1\leqslant i\leqslant n}$ est une famille finie quelconque d'éléments de B_0 , il existe un $B\in\mathfrak{F}$ tel que tous les x_i appartiennent à B : en effet, chaque x_i appartient à un $B_i\in\mathfrak{F}$, et comme $\mathfrak{T}$ est totalement ordonné, il existe un des B_i qui contient tous les autres. Cela prouve d'abord que, pour tout couple (x,y) d'éléments de B_0 , il existe un élément et un seul de S_0 dont les deux premières coordonnées sont x et y ; nous définirons $x+y$ et xy comme étant les deux dernières coordonnées de cet élément. Ayant ainsi défini l'addition et la multiplication dans B_0 , il reste à voir que ces lois définissent bien une structure de corps sur cet ensemble ;

or, chacun des axiomes des structures de corps ne fait intervenir qu'un nombre fini d'éléments ; ces éléments appartiennent tous à un même corps $B \in \mathfrak{F}$, et par suite tous les axiomes des corps sont bien vérifiés pour la structure S_0 .

Ce lemme étant démontré, prenons pour A l'ensemble $K[X] \times N$. Soit $\dot{K}$ l'ensemble des éléments de A de la forme $\dot{x} = (X-x, 0)$, où x parcourt K ; il est clair que $x \to \dot{x}$ est une application biunivoque de K sur $\dot{K}$, et on peut, par transport de structure, définir au moyen de cette application une structure de corps $\dot{S}$ sur $\dot{K}$ isomorphe à la structure de corps de K ; si $f = \sum_k a_k X^k$ est un polynome de $K[X]$, nous poserons $\dot{f} = \sum_k \dot{a}_k X^k$. Cela posé, considérons, dans l'ensemble $\mathfrak{S}$ des structures de corps sur des parties de A , le sous-ensemble $\mathfrak{S}_0$ formé des structures S telles que : a) $S \supset \dot{S}$; b) quel que soit l'élément $z=(f(X),m)$ dans la partie de A sur laquelle S est définie, on a $\dot{f}(z)=0$ (au sens de la structure S).

L'ensemble $\mathfrak{S}_0$ contient évidemment $\dot{S}$, donc n'est pas vide ; en outre, il est <u>inductif</u> : en effet, si $\mathfrak{T}$ est une partie totalement ordonnée de $\mathfrak{S}_0$, il résulte du lemme que la réunion S des éléments de $\mathfrak{T}$ appartient à $\mathfrak{S}$, et il est clair que S satisfait aux conditions a) et b) . D'après le th. de Zorn, $\mathfrak{S}_0$ admet un élément maximal S_0 ; soit L_0 la partie de A sur laquelle S_0 est définie, munie de la structure de corps S_0 ; il résulte de a) que $\dot{K}$ est un sous-corps de L_0 , et de b) que L_0 est une extension <u>algèbrique</u> de $\dot{K}$. Nous allons montrer que L_0 est un corps <u>algèbriquement fermé</u>, ce qui (en identifiant K et $\dot{K}$) démontrera le théorème. Soit en effet L une extension algèbrique de L_0 ; nous allons montrer qu'on a nécessairement $L=L_0$. En effet, soit H le complémentaire de L_0 par rapport à L , et B le complémentaire de L_0 par rapport à A . Tout élément $y \in H$ est algèbrique sur L_0 , donc

donc sur $\dot{K}$; soit f_y le polynome de $K[X]$ tel que $\dot{f}_y$ soit le polynome minimal de y par rapport à $\dot{K}$ (§ 2,th.2). Soit G la partie de $K[X]$ formée des polynomes g tels qu'il existe au moins un $y \in H$ tel que $f_y=g$; pour un $g \in G$, les $y \in H$ tels que $f_y=g$ sont tels que $\dot{g}(y)=0$ dans L , et par suite sont en nombre fini ; soit M_g l'ensemble de ces éléments. D'autre part, pour un $g \in G$ donné, les éléments $z=(g(X),m)$ de A qui appartiennent à L_o sont tels que $\dot{g}(z)=0$ dans L_o, d'après b, et par suite sont en nombre fini ; l'ensemble P_g des éléments $(g(X),m)$ qui n'appartiennent pas à L_o est donc infini. Il existe donc, pour tout $g \in G$, une application biunivoque φ_g de M_g dans P_g ; comme les M_g forment une partition de H , et que les P_g sont deux à deux sans élément commun, il existe une application biunivoque φ de H dans B qui, sur chaque ensemble M_g , se réduit à φ_g ; pour cette application, $\varphi(y)$ est donc de la forme (f_y,m), quel que soit $y \in H$. Posons alors $L_1=L_o \cup \varphi(H)$; soit φ_1 l'application biunivoque de L sur L_1 qui se réduit à l'application identique sur L_o, et coïncide avec φ dans H ; on peut, par cette application, transporter à L_1 la structure de corps donnée sur L ; soit S_1 la structure ainsi définie sur L_1 . On a $S_1 \supset S_o$, ce qui implique $S_1 \supset \dot{S}$; d'autre part, S_1 satisfait à la condition b), d'après la définition de φ . Comme S_o est maximal dans $\mathfrak{S}_o$, on a nécessairement $S_1=S_o$, d'où $L_1=L_o$ et par suite $L=L_o$.

C.Q.F.D.

Remarque.- En particulier, un corps fini K admet une extension algèbrique E algèbriquement fermée. E est un corps infini, sans quoi (n^o1) il ne serait pas algèbriquement fermé ; c'est donc une extension algèbrique de degré infini par rapport à K (car toute extension de degré fini sur K est un corps fini) .

Etant donnée une extension algèbriquement fermée E de K, tout polynome $f \in K[X]$ de degré >0 a au moins une racine dans E (prop.1) ; si x est une quelconque de ces racines on peut donc former l'extension $K(x)$, c'est-à-dire adjoindre à K une racine d'un polynome quelconque de degré >0 de $K[X]$. Si f est irréductible dans $K[X]$, nous avons vu qu'il est identique (à un facteur près) au polynome minimal (§ 2, th.2) d'une quelconque de ses racines dans E. A tout polynome irréductible de degré n dans $K[X]$ correspond donc au moins une extension algèbrique de degré n de K, contenue dans E.

3. Extensions universelles.

Toute extension algèbriquement fermée E d'un corps K a la propriété de contenir (à une isomorphie près) toute extension de K dont le degré de transcendance est au plus égal à celui de E. De façon précise :

Théorème 2 (Steinitz).- Soient K, K' deux corps isomorphes, et soit f un isomorphisme de K sur K'. Soit E' une extension algèbriquement fermée de K', L une extension de K dont le degré de transcendance par rapport à K est au plus égal à celui de E' par rapport à K'. Dans ces conditions, il existe un isomorphisme de L dans E' qui prolonge f.

Soit $(a_\mu)_{\mu \in M}$ une base de transcendance de L par rapport à K, $(b_\nu)_{\nu \in N}$ une base de transcendance de E' par rapport à K'. On sait (chap.IV, §) qu'on peut prolonger l'isomorphisme f en un isomorphisme $u \to \bar{u}$ de l'anneau $K[X_\mu]_{\mu \in M}$ sur l'anneau $K'[X_\mu]_{\mu \in M}$; comme par hypothèse M a une puissance au plus égale à celle de N, il existe une application biunivoque φ de M dans N ; il est clair alors que si, à tout élément $u((a_\mu))$ de $K[a_\mu]_{\mu \in M}$ on fait correspondre l'élément

$\bar{u}((b_{\varphi(\mu)}))$ de $K'[b_\nu]_{\nu\in N}$, on définit un isomorphisme de l'anneau $K[a_\mu]_{\mu\in M}$ dans l'anneau $K'[b_\nu]_{\nu\in N}$, qui prolonge f, et se prolonge d'une seule manière (chap.I, § 9, prop.4) en un isomorphisme du corps $K(a_\mu)_{\mu\in M}$ dans le corps $K'(b_\nu)_{\nu\in N}$. Comme L est une extension algébrique de $K(a_\mu)_{\mu\in M}$, on peut donc se limiter désormais à démontrer le théorème lorsqu'on suppose, dès le début, que L est une extension algébrique de K.

Nous utiliserons le lemme suivant :

Lemme.- Soient K,K' deux corps isomorphes, φ un isomorphisme de K sur K'. Soit E une extension de K, E' une extension de K', x un élément de E algébrique sur K, u(X) son polynome minimal par rapport à K (§ 2, th.2). Soit $\bar{u}(X)$ le polynome de $K'[X]$ qui correspond à u(X) par l'extension à $K[X]$ de l'isomorphisme φ (autrement dit, chaque coefficient de $\bar{u}$ est transformé par φ du coefficient du terme de même degré dans u ; cf.chap.IV, §) ; si $\bar{u}$ admet une racine x' dans E', l'isomorphisme φ peut se prolonger d'une manière et d'une seule en un isomorphisme de $K(x)$ sur $K'(x')$, qui applique x sur x'.

En effet, l'idéal des polynomes de $K'[X]$ dont x' est racine est transformé par l'extension de φ à $K[X]$ de l'idéal des polynomes de $K[X]$ dont x est racine, car $\bar{u}(X)$ est le polynome minimal de x' (puisqu'il est irréductible et que le coefficient de son terme de plus haut degré est 1) ; le lemme est donc une conséquence de la prop. du chap. IV, § , compte tenu du th.2 du § 2.

Ce lemme étant démontré, soit Φ l'ensemble des isomorphismes d'un sous-corps (variable) de L contenant K, sur un sous-corps de E' contenant K', qui prolongent f ; nous ordonnerons cet ensemble par la relation de prolongement (Ens. R, § 6, n°2), ce qui revient à ordonner par inclusion les ensembles représentatifs (Ens.R, § 3, n° 5)

de ces isomorphismes dans $L \times E'$. L'ensemble Φ, ainsi ordonné, est inductif ; en effet, si Ψ est une partie totalement ordonnée de Φ, l'ensemble $\mathfrak{F}$ des sous-corps de L sur lesquels sont définis les isomorphismes $g \in \Psi$, est totalement ordonné ; donc la réunion de ces sous-corps est un sous-corps B_0 de L (§ 2, prop.3) ; et il est immédiat que la réunion des ensembles représentatifs des $g \in \Psi$ est l'ensemble représentatif d'une application g_0 de B_0 dans E' qui prolonge tous les $g \in \Psi$; en outre, comme deux éléments quelconques x,y de B_0 appartiennent à un même corps $B \in \mathfrak{F}$, on a (en désignant par g l'isomorphisme de l'ensemble Ψ défini sur B) $g_0(x-y)=g(x-y)=g(x)-g(y)=g_0(x)-g_0(y)$, et de même $g_0(xy)=g_0(x)g_0(y)$, ce qui prouve que g_0 est un isomorphisme de B_0 dans E' .

Il existe donc, d'après le th. de Zorn, un élément maximal h_0 de Φ ; c'est un isomorphisme d'un sous-corps L_0 de L sur un sous-corps L'_0 de E' . Nous allons voir que $L_0=L$. Supposons en effet qu'il existe un élément $x \in L$ n'appartenant pas à L_0 ; x est algèbrique sur K , et par suite sur L_0 ; soit $u(X)$ son polynome minimal par rapport à L_0, $\bar{u}(X)$ le transformé de $u(X)$ par l'extension à $L_0[X]$ de l'isomorphisme h_0 . D'après la prop.1, $\bar{u}$ admet une racine x' dans E' ; en vertu du lemme , on peut prolonger h_0 en un isomorphisme de $L_0(x)$ sur $L'_0(x')$, ce qui est contraire à la définition de h_0 . C.Q.F.D.

COROLLAIRE.- Deux extensions algèbriquement fermées E,E' d'un corps K, ayant même degré de transcendance sur K, sont isomorphes.

En effet, si M,M' sont des bases de transcendance de E,E' respectivement, elles sont équipotentes, et par suite il existe un isomorphisme de K(M) sur K(M'). On peut donc se borner au cas où E et E' sont des extensions algèbriques de K . D'après le th.2, il existe un isomorphisme f de E sur un sous-corps F' de E' , laissant invariants

les éléments de K ; F' est une extension algèbriquement fermée de K , contenue dans E' ; comme E' est algèbrique sur K , il est aussi algèbrique sur F' , et par suite identique à F' .

D'après le th.2, si Ω est une extension algèbrique de K , algèbriquement fermée, toute extension algèbrique de K est isomorphe à une extension de K contenue dans Ω ; c'est pourquoi nous dirons qu'une telle extension Ω , qui existe toujours d'après le th.1, et est déterminée à une isomorphie près d'après le cor. du th.2, est une <u>extension algèbrique universelle</u> de K .

Plus généralement, soit $(E_\iota)_{\iota \in I}$ une famille quelconque d'extensions d'un corps K . Pour chaque $\iota \in I$, soit M_ι une base de transcendance de E_ι par rapport à K . Soit M un ensemble dont la puissance est au moins égale à celle de chacun des M_ι (par exemple l'ensemble produit $\prod_{\iota \in I} M_\iota$) ; et soit Ω une extension algèbrique universelle de l'extension transcendante pure $K(X_\mu)_{\mu \in M}$. D'après le th.2, chacune des extensions E_ι est isomorphe à une extension de K contenue dans Ω ; nous dirons que Ω est une <u>extension universelle</u> de K , pour la famille d'extensions (E_ι).

En particulier, une extension algèbrique universelle de l'extension transcendante pure $K(X_n)_{n \in \mathbb{N}}$ est une extension universelle pour toute famille d'extensions de K dont les bases de transcendance sont <u>dénombrables</u>.

<u>Exercices.</u>- 1) a) Si K est un corps infini, toute extension algèbrique de K est équipotente à K (utiliser le fait que l'ensemble des parties finies d'un ensemble infini A est équipotent à A) En déduire que, si E est une extension quelconque de K , M une base de transcendance de E par rapport à K , E est équipotent à $K \times M$.

b) Si K est un corps fini, toute extension de K ayant un degré de transcendance fini est dénombrable. Si une extension E de K a une base de transcendance infinie M , E est équipotent à M .

2) Soit K un corps, f un polynome de l'anneau $K[X, Y]$. Montrer que, si f, considéré comme polynome en Y , est réductible sur le corps K(X) , il est égal au produit de deux polynomes non constants dans $K[X,Y]$ (montrer que si on a une relation de la forme $\varphi(X)f(X,Y)=g(X,Y)h(X,Y)$, où g et h sont deux polynomes de $K[X,Y]$ et φ un polynome de $K[X]$, il existe aussi deux polynomes g_1, h_1 de $K[X,Y]$ tels que $f=g_1h_1$; pour cela, considérer φ, f, g et h comme des polynomes en X sur K(Y) et décomposer ces polynomes en facteurs dans une extension algèbriquement fermée Ω de K(Y) ; remarquer enfin que le p.g.c.d. dans $\Omega[X]$ de deux polynomes de $K[X]$ appartient à $K[X]$).

3) Soit E une extension d'un corps K , x un élément de E transcendant sur K ; dans l'extension transcendante pure K(x), tout élément y s'écrit sous la forme $f(x)/g(x)$, où f et g sont deux polynomes de $K[X]$ premiers entre eux (et bien déterminés à un facteur de K près) ; on appelle <u>degré</u> de y par rapport à x le plus grand des degrés de f et g .

a) Montrer que si y est de degré n par rapport à x , K(x) est une extension algèbrique de degré n de K(y) (montrer que le polynome gy-f est irréductible sur K(y), en utilisant l'exerc.2).

b) En déduire que tout $y \in K(x)$ tel que K(y)=K(x) est de la forme $(ax+b)/(cx+d)$, où a,b,c,d sont des éléments de K tel que $ad-bc\neq 0$; réciproque. Trouver tous les automorphismes de K(x) laissant invariants les éléments de K .

c) Si y est de degré n par rapport à x , et z de degré m par rapport à y , z est de degré mn par rapport à x .

§ 4. Isomorphismes. Dérivations. Extensions séparables.

Sauf mention expresse du contraire, les corps que nous considèrerons dans le reste du chapitre seront des sous-corps d'un corps Ω algèbriquement fermé (mais par ailleurs quelconque). Pour tout sous-corps K de Ω, nous désignerons par $\overline{K}$ la fermeture algébrique de K dans Ω (§ 2, n°4), qui est un corps algèbriquement fermé (§ 3, cor. de la prop. 1).

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

Définition 1.- Soit K un corps, E, F deux surcorps de K (non nécessairement supposés contenus dans une même extension de K). On dit qu'un isomorphisme de E dans F est un isomorphisme relatif à K s'il laisse invariant tout élément de K.

Conformément à la convention faite ci-dessus, les extensions de K que nous allons considérer seront supposées contenues dans Ω (sauf mention expresse du contraire) ; aussi, par abus de langage, nous entendrons par isomorphisme relatif à K d'une extension $E \subset \Omega$ de K, un isomorphisme de E (relatif à K) dans Ω.

Il est immédiat que si f est un isomorphisme quelconque d'un sous-corps E de Ω sur un sous-corps de Ω, l'ensemble des éléments de E qui sont invariants par f est un sous-corps de E ; tout isomorphisme de E dans Ω peut donc être considéré comme un isomorphisme relatif à un sous-corps de E. En particulier, si P est le sous-corps premier de Ω (§ 1), f un isomorphisme de P dans Ω, le sous-corps de P formé des éléments invariants par f est nécessairement identique à P ; autrement dit, le seul isomorphisme de P dans Ω est l'automorphisme identique de P.

Proposition 1.- Tout isomorphisme de $E \subset \Omega$ relatif à un de ses sous-corps K peut être prolongé en un endomorphisme de Ω (relatif à K).

C'est une conséquence immédiate du th.2 du § 3.

Inversement, il est clair que la restriction à E de tout endomorphisme de Ω (relatif à K) est un isomorphisme de E (relatif à K) ; l'étude des isomorphismes d'un sous-corps de Ω revient donc à l'étude des restrictions à ce sous-corps des endomorphismes de Ω .

Soit K un sous-corps de Ω . Si x est un élément de Ω qui est algèbrique (resp. transcendant) sur K , tout endomorphisme de Ω relatif à K transforme x en un élément algèbrique (resp. transcendant) sur K .

Inversement, si x et y sont deux éléments de Ω transcendants sur K , il existe un isomorphisme de K(x) sur K(y), relatif à K , et appliquant x sur y : il suffit pour le définir de faire correspondre à tout élément f(x) de K(x) ($f \in K(X)$), l'élément f(y). Cet isomorphisme se prolongeant en un endomorphisme de Ω , il existe donc toujours un endomorphisme de Ω relatif à K , transformant x en y .

En particulier, on peut prendre $y=x^n$, et on voit donc qu'il existe une infinité d'éléments distincts de Ω qui peuvent être transformés de x par un endomorphisme de Ω .

Au contraire, nous allons voir que si x est algèbrique sur K , il n'y a qu'un nombre fini d'éléments de Ω qui sont transformés de x par un endomorphisme de Ω .

Définition 2.- Etant donné un sous-corps K de Ω , on dit que deux éléments x,y de Ω , algèbriques sur K , sont conjugués (par rapport à K) s'ils ont même polynome minimal (§ 2, th.2) par rapport à K .

Si $x \in \Omega$ est algèbrique sur K , et si f est son polynome minimal (par rapport à K), tout élément $y \in \Omega$ conjugué de x est racine de f (§ 2, th.2) ; réciproquement, tout polynome irréductible de $K[X]$

est à un facteur constant près, le polynome minimal de chacune de ses racines dans Ω ; donc les conjugués de x dans Ω sont identiques aux racines du polynome minimal de x dans Ω ; elles sont par suite en nombre fini, au plus égal au degré de x sur K .

Proposition 2.- Soient K un sous-corps de Ω , x,y deux éléments de Ω algèbriques sur K . Pour qu'il existe un endomorphisme de Ω relatif à K , transformant x en y , il faut et il suffit que x et y soient conjugués par rapport à K .

En effet, soit $f = \sum_{k=0}^{n} a_k X^k$ le polynome minimal de x ; on a $f(x)=0$ d'où, pour tout endomorphisme σ de Ω relatif à K , $\sigma(f(x))=0$; mais $\sigma(f(x)) = \sum_{k=0}^{n} a_k(\sigma(x))^k$, puisque $\sigma(a_k)=a_k$ par hypothèse ; donc $\sigma(f(x))=f(\sigma(x))=0$, ce qui montre que $\sigma(x)$ est conjugué de x par rapport à K . Inversement, si x et y ont même polynome minimal par rapport à K , l'automorphisme identique de K sur lui-même peut se prolonger en un isomorphisme de K(x) sur K(y) appliquant x sur y (§ 3,prop.2), et ce dernier se prolonge en un endomorphisme de Ω (prop.1), d'où la proposition.

2. Eléments purement inséparables.

Définition 3.- Soit K un sous-corps de Ω . On dit qu'un élément $x \in \Omega$ est purement inséparable par rapport à K (ou sur K) s'il est invariant par tous les endomorphismes de Ω relatifs à K .

Il est clair que si x est purement inséparable sur K , il est aussi purement inséparable sur tout sous-corps E de Ω contenant K .

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

En premier lieu, si $x \in \Omega$ est purement inséparable sur K , x est algèbrique sur K ; en effet, si x était transcendant sur K , $1/x$ serait aussi transcendant sur K , donc (n° 1) il existerait un endomorphisme de Ω transformant x en $1/x \neq x$. Soit alors f le polynome minimal de x par rapport à K , n son degré ; si x est purement inséparable sur K , il n'a pas d'autre conjugué sur K que lui-même (prop.2), donc toutes les racines de f dans Ω sont identiques à x , et comme Ω est algèbriquement fermé, on a (§ 3,prop.1) $f=(X-x)^n$. Si $n>1$, x est aussi racine de $f'=n(X-x)^{n-1}$; comme $f' \in K[X]$ et que f est le polynome minimal de x , cela n'est possible que si $f'=0$ dans $K[X]$, 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, soit p^e la plus haute puissance de p qui divise n ; on a donc $n=p^e n'$, et $n' \not\equiv 0 \pmod{p}$. On peut alors écrire $f=(X^{p^e}-x^{p^e})^{n'}$; dans f le coefficient de $X^{p^e(n'-1)}$ est $-n'x^{p^e}$; comme $f \in K[X]$, et que n' n'est pas multiple de la caractéristique, on a $x^{p^e} \in K$; autrement dit x est racine du polynome $X^{p^e}-x^{p^e}$, qui appartient à $K[X]$, ce qui entraîne $n'=1$, $n=p^e$, et $f=X^{p^e}-x^{p^e}$. Ce dernier raisonnement montre en outre que, pour tout entier $h<e$ $x^{p^h} \notin K$.

Inversement, supposons qu'il existe un entier $m \geqslant 0$ tel que $x^{p^m} \in K$; pour tout endomorphisme σ de Ω relatif à K , on a donc $\sigma(x^{p^m})=x^{p^m}$, c'est-à-dire $(\sigma(x))^{p^m}=x^{p^m}$, ce qui s'écrit $(\sigma(x)-x)^{p^m}=0$ (§ 1), et entraîne par suite $\sigma(x)=x$.

Il est immédiat que l'ensemble des éléments de Ω purement inséparables sur K est un sous-corps de Ω contenant K : ce n'est autre en effet que le sous-corps de Ω attaché (chap.II, §5,n°6) à l'ensemble $\mathfrak{E}$ des endomorphismes du corps Ω relatifs à K ; d'après la prop.3,

Ce sous-corps est formé des racines de tous les polynomes $X^{p^e}-x$, où x parcourt K et e l'ensemble des entiers $\geqslant 0$. Un tel polynome (irréductible ou non) n'admet qu'une seule racine dans Ω, car si y et z en sont deux racines, on a $y^{p^e} = z^{p^e}$, c'est-à-dire $(y-z)^{p^e}=0$, d'où $y=z$. Nous désignerons cette racine par la notation $x^{p^{-e}}$ (ou x^{1/p^e}).

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

En effet, soit $x=a^{p^{-e}}$, $y=b^{p^{-e}}$, où a et b sont deux éléments quelconques de K. On a $x^{p^e}=a$, $y^{p^e}=b$, d'où $a+b=(x+y)^{p^e}$ (§ 1, cor. de la prop.1), et il en résulte par définition, que $x+y=(a+b)^{p^{-e}}$; on vérifie de la même manière que $xy=(ab)^{p^{-e}}$, d'où la proposition.

Nous désignerons par $K^{p^{-e}}$ l'image de K par l'isomorphisme $x \to x^{p^{-e}}$; c'est une extension algébrique de K, en général de degré infini ; pour $e < f$, on a $K^{p^{-e}} \subset K^{p^{-f}}$. Le sous-corps de Ω formé des éléments purement inséparables sur K est la réunion des corps $K^{p^{-e}}$, lorsque e parcourt l'ensemble des entiers $\geqslant 0$; nous le désignerons par la notation $K^{p^{-\infty}}$; c'est une extension algébrique de K.

Proposition 5.- Le corps $K^{p^{-\infty}}$ est le plus petit sous-corps parfait de Ω contenant K.

En effet, l'isomorphisme $x \to x^p$ applique $K^{p^{-e}}$ sur $K^{p^{-e+1}}$, puisque la relation $x^{p^e}=a$ entraîne $(x^p)^{p^{e-1}} = a$; c'est donc un automorphisme de $K^{p^{-\infty}}$. Inversement, si E est un sous-corps parfait de Ω contenant K, l'application $x \to x^{p^e}$ est un automorphisme de E pour tout $e \geqslant 0$; pour tout $a \in K$, il existe donc $x \in E$ tel que $x^{p^e}=a$, c'est-à-dire que $K^{p^{-e}} \subset E$, ce qui montre que $K^{p^{-\infty}} \subset E$.

COROLLAIRE.- Pour que les seuls éléments de Ω purement inséparables sur K soient les éléments de K , il faut et il suffit que K soit parfait.

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

Exemple.- Soit K_0 un corps de caractéristique $p > 0$, et $K=K_0(X)$ le corps des fractions rationnelles à une indéterminée X sur K . Le corps K est imparfait, car dans K , X ne peut être égal à la puissance p-ème d'une fraction rationnelle $f(X)/g(X)$; on en déduirait en effet que $(f(X))^p=X(g(X))^p$; si m et n sont les degrés respectifs de f et g , les polynomes qui figurent aux deux membres de cette égalité auraient des degrés égaux respectivement à mp et np+1, ce qui est absurde.

Définition 4.- On dit qu'une extension E de K , contenue dans Ω est une extension purement inséparable de K (ou est purement inséparable sur K) si tous ses éléments sont purement inséparables sur K .

Il revient au même de dire que les extensions purement inséparables de K sont les extensions de K contenues dans $K^{p^{-\infty}}$; ce sont des extensions algèbriques de K . Si A est un ensemble quelconque d'éléments purement inséparables sur K , K(A) est une extension purement inséparable de K .

Proposition 6.- Le degré d'une extension purement inséparable de K , de degré fini, est une puissance de p .

En effet, soit $E=K(a_1,a_2,\ldots,a_m)$ une extension purement inséparable de K , de degré fini ; chacun des a_i est purement inséparable sur K , donc aussi sur $K(a_1,\ldots,a_{i-1})$. La proposition résulte donc de la prop.3 du § 4 et du cor. de la prop.5 du § 2.

3. Indépendance linéaire des isomorphismes.

Les endomorphismes de Ω par rapport à K (au sens défini dans ce § , c'est-à-dire des endomorphismes de la structure de corps de Ω) sont aussi des endomorphismes particuliers de la structure d'espace vectoriel de Ω par rapport à K ; si nous désignons cet espace vectoriel par Ω_K , afin d'éviter toute confusion, les endomorphismes du corps Ω , relatifs à K , appartiennent donc à l'anneau $\mathscr{L}(\Omega_K)$. Or (chap.II, § 5,n°6) $\mathscr{L}(\Omega_K)$ est muni d'une structure d'espace vectoriel à gauche sur le corps Ω , le produit au d'un élément $a \in \Omega$ et d'un endomorphisme u de Ω_K étant l'endomorphisme $x \to au(x)$. Quand nous parlerons d'une combinaison linéaire à coefficients dans Ω d'une famille (u_ι) d'endomorphismes du corps Ω (relatifs à K), il s'agira de cette structure d'espace vectoriel ; autrement dit, ce sera un endomorphisme de Ω_K (mais non plus du corps Ω) de la forme $x \to \sum_\iota a_\iota u_\iota(x)$, où $a_\iota \in \Omega$. Dire que les u_ι sont linéairement indépendants signifie donc que, pour toute famille (a_ι) d'éléments de Ω non tous nuls (mais nuls sauf un nombre fini d'entre eux) il existe $x \in \Omega$ tel que $\sum a_\iota u_\iota(x) \neq 0$.

Plus généralement, étant donné un sous-espace vectoriel V de l'espace Ω_K , nous dirons que les u_ι sont linéairement indépendants dans V si, pour toute famille (a_ι) d'éléments de Ω non tous nuls, il existe x appartenant à V tel que $\sum_\iota a_\iota u_\iota(x) \neq 0$. Cela signifie que les restrictions des u_ι à V , qui sont des éléments de l'ensemble $\mathscr{L}(V, \Omega_K)$ des applications linéaires de V dans Ω_K , sont linéairement indépendants pour la structure d'espace vectoriel à gauche de $\mathscr{L}(V, \Omega_K)$ sur le corps Ω (induite sur $\mathscr{L}(V, \Omega_K)$ par la structure de l'espace vectoriel produit Ω^V).

Cela étant, le fait qu'il s'agit d'endomorphismes de la structure de corps de Ω entraîne l'importante conséquence suivante :

Théorème 1.- Soit $(u_\iota)_{\iota\in I}$ une famille d'endomorphismes de Ω relatifs à K, et soit E un sous-corps de Ω contenant K. Si les restrictions des u_ι à E sont des isomorphismes de E (relatifs à K) distincts deux à deux, les u_ι sont linéairement indépendants dans E.

En effet, les u_ι étant considérés comme des éléments de l'espace vectoriel $\mathcal{L}(E,\Omega_K)$ sur Ω, supposons qu'ils soient linéairement dépendants. Il existe alors au moins une relation primordiale $\sum_\iota \mu_\iota u_\iota = 0$ entre les u_ι (c'est-à-dire (chap.II, § 5, n°4) que (μ_ι) est un élément primordial du sous-espace de $\Omega^{(I)}$ formé des (λ_ι) tels que $\sum_\iota \lambda_\iota u_\iota = 0$). Comme E est un sous-corps de Ω, les relations $x\in E$, $y\in E$ entraînent $xy\in E$, donc

$$\sum_\iota \mu_\iota u_\iota(xy) = 0 \tag{1}$$

et comme les u_ι sont des endomorphismes de Ω

$$\sum_\iota \mu_\iota u_\iota(y)u_\iota(x) = 0 \tag{2}$$

quels que soient x et y dans E. Mais cela signifie que, quel que soit $y\in E$, les $\mu_\iota u_\iota(y)$ sont les coefficients d'une relation linéaire entre les u_ι ; comme par hypothèse $\sum_\iota \mu_\iota u_\iota = 0$ est une relation primordiale, il existe pour tout $y\in E$, un élément $\rho(y)\in\Omega$ tel que pour tout $\iota\in I$

$$\mu_\iota u_\iota(y) = \rho(y)\mu_\iota \tag{3}$$

(chap.II, § 5, prop.2). On déduit aussitôt de cette relation que, si α,β sont deux indices distincts de I tels que $\mu_\alpha\neq 0$ et $\mu_\beta\neq 0$, on a $u_\alpha(y)=u_\beta(y)$ pour tout $y\in E$, contrairement à l'hypothèse. Il ne peut donc y avoir qu'un seul $\varkappa\in I$ tel que $\mu_\varkappa\neq 0$, mais alors la relation $\sum_\iota \mu_\iota u_\iota = 0$ se réduit à $u_\varkappa = 0$, ce qui est absurde.

Remarque.- Le même raisonnement s'applique, plus généralement, au cas où les u_i sont des représentations d'un monoïde multiplicatif E dans le corps Ω (considéré comme muni de la loi multiplicative seule) ; dans l'espace vectoriel Ω^E des applications de E dans Ω, les u_i sont linéairement indépendantes si aucune d'entre elles n'est identiquement nulle, et si elles sont distinctes deux à deux.

Proposition 7.- Si V est un sous-espace vectoriel, de dimension finie n, de l'espace Ω_K, tout ensemble d'endomorphismes de Ω, relatifs à K linéairement indépendants dans V, a au plus n éléments.

En effet, soient u_i $(1 \leqslant i \leqslant n+1)$ $n+1$ endomorphismes de Ω relatifs à K. Soit $(a_j)_{1 \leqslant j \leqslant n}$ une base de V par rapport à K. Le système d'équations

$$\sum_{i=1}^{n+1} \xi_i u_i(a_j) = 0 \qquad (1 \leqslant j \leqslant n) \tag{4}$$

par rapport aux $\xi_i \in \Omega$ est un système linéaire homogène de n équations à n+1 inconnues à coefficients dans Ω, donc il admet une solution (a_i) non triviale formée d'éléments de Ω. Mais on déduit de (4) que, quels que soient les $\lambda_j \in K$, on a $\sum_{i=1}^{n+1} a_i \left(\sum_{j=1}^{n} \lambda_j u_i(a_j) \right) = 0$; d'après l'hypothèse sur les u_i, cela s'écrit aussi $\sum_{i=1}^{n+1} a_i u_i \left(\sum_{j=1}^{n} \lambda_j a_j \right) = 0$, et comme (a_j) est une base de V, on a donc $\sum_{i=1}^{n+1} a_i u_i(x) = 0$ pour tout $x \in V$, ce qui prouve que les u_i sont linéairement dépendants dans V.

4. Extensions séparables.

La prop.7 limite supérieurement le nombre maximum des endomorphismes de Ω relatifs à K, linéairement indépendants dans un sous-espace de dimension finie de Ω_K. Mais cette borne supérieure peut ne pas être atteinte : par exemple lorsque K est un corps imparfait, et V un sous-espace vectoriel de Ω_K contenu dans $K^{p^{-\infty}}$,

la restriction à V de tout endomorphisme de Ω est l'application identique, autrement dit le nombre maximum des endomorphismes linéairement indépendants dans V est 1 .

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

Cette définition peut encore s'exprimer de la façon suivante : soient $(a_i)_{1 \leqslant i \leqslant n}$ n éléments de E , linéairement indépendants par rapport à K ; dire que n endomorphismes u_i $(1 \leqslant i \leqslant n)$ de Ω sont linéairement dépendants dans le sous-espace V ayant pour base (a_i) signifie (prop.7) qu'il existe n éléments ξ_i $(1 \leqslant i \leqslant n)$ de Ω , non tous nuls, et satisfaisant aux n équations

$$(5) \qquad \sum_{i=1}^{n} \xi_i u_i(a_j) = 0 \qquad (1 \leqslant j \leqslant n)$$

Cela équivaut à dire que la matrice $(u_i(a_j))$ de ce système n'est pas inversible, ou que son déterminant est nul. Par suite, pour que E soit séparable sur K , il faut et il suffit que, pour toute suite $(a_i)_{1 \leqslant i \leqslant n}$ de n éléments de E linéairement indépendants sur K , il existe n endomorphismes u_i de Ω tels que le déterminant $\det(u_i(a_j))$ ne soit pas nul.

D'après la déf.5, si E est séparable sur K , toute extension de K contenue dans E est séparable sur K ; inversement, si S est un système de générateurs de E sur K tel que, pour toute partie finie M de S , K(M) soit séparable sur K , alors E est séparable sur K : tout sous-espace vectoriel de E (sur K) de dimension finie, est en effet contenu dans une extension K(M) de cette forme.

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

La condition est nécessaire. Supposons en effet que E soit séparable sur K, et soit $(a_i)_{1\leqslant i\leqslant n}$ une famille de n éléments de E linéairement indépendants sur K. Par hypothèse, il existe n endomorphismes u_i $(1\leqslant i\leqslant n)$ de Ω relatifs à K tels que $\det(u_i(a_j))\neq 0$. Une relation de la forme $\sum_{j=1}^{n}\lambda_j a_j^p=0$, où les $\lambda_j\in K$, entraîne pour $1\leqslant i\leqslant n$ $\sum_{j=1}^{n}\lambda_j u_i(a_j^p)=0$, ou encore $\sum_{j=1}^{n}\lambda_j(u_i(a_j))^p=0$; or, le déterminant $\det((u_i(a_j))^p)$ est égal à $(\det(u_i(a_j)))^p$, donc $\neq 0$; on en conclut qu'on a nécessairement $\lambda_j=0$ pour tout indice j, autrement dit que les a_j^p sont linéairement indépendants sur K.

La condition est suffisante. Remarquons d'abord qu'elle entraîne aussitôt que si $(a_i)_{1\leqslant i\leqslant n}$ est linéairement libre sur K, il en est de même de chacune des familles $(a_i^{p^e})_{1\leqslant i\leqslant n}$ (par récurrence sur l'entier $e>0$). Cela étant, soit $(a_i)_{1\leqslant i\leqslant n}$ une famille d'éléments de E linéairement libre sur K, et supposons que le nombre maximum d'endomorphismes de Ω relatifs à K, linéairement indépendants dans le sous-espace vectoriel de Ω_K engendré par les a_i, soit $<n$. Pour chaque endomorphisme u de Ω relatif à K, considérons l'élément $(u(a_i))_{1\leqslant i\leqslant n}$ de l'espace vectoriel Ω^n sur le corps Ω ; soit W le sous-espace de Ω^n engendré par ces éléments lorsque u parcourt l'ensemble $\mathfrak{E}$ des endomorphismes de Ω relatifs à K ; l'hypothèse signifie que W a une dimension au plus égale à $n-1$. Pour tout endomorphisme $v\in\mathfrak{E}$, soit $\overline{v}$ l'endomorphisme de l'espace vectoriel Ω^n défini par $\overline{v}((x_i))=(v(x_i))$; pour tout endomorphisme $u\in\mathfrak{E}$, on a $\overline{v}((u(a_i)))=(v(u(a_i)))$, et comme $v\circ u$ appartient à $\mathfrak{E}$, on voit que

$\overline{v}(W) \subset W$. Par suite (chap.II, § 5, prop.10), le sous-corps de Ω attaché à W (pour la base canonique de Ω^n) est contenu dans le sous-corps attaché à l'ensemble d'endomorphismes ξ , c'est-à-dire ($n^o 2$) dans le sous-corps $K^{p^{-\infty}}$ de Ω . Il en résulte (chap.II, § 5,th.2) qu'il existe un système d'équations de W à coefficients dans $K^{p^{-\infty}}$, et comme W est de dimension $< n$, il existe une famille $(\mu_i)_{1 \leqslant i \leqslant n}$ d'éléments de $K^{p^{-\infty}}$, non tous nuls, et tels que $\sum_{i=1}^{n} \mu_i u(a_i) = 0$ pour tout endomorphisme u de Ω relatif à K . En particulier, en prenant pour u l'automorphisme identique de Ω , il vient $\sum_{i=1}^{n} \mu_i a_i = 0$. Or, il existe un entier $e \geqslant 0$ tel que tous les éléments $\mu_i^{p^e}$ appartiennent à K ; comme de la relation $\sum_{i=1}^{n} \mu_i a_i = 0$, on tire, en élevant à la puissance p^e-ème, $\sum_{i=1}^{n} \mu_i^{p^e} a_i^{p^e} = 0$, on voit que les $a_i^{p^e}$ seraient linéairement dépendants sur K , contrairement à l'hypothèse. C.Q.F.D.

Remarque.- La définition d'une extension séparable E de K paraît dépendre du corps algébriquement fermé Ω dans lequel on considère E comme plongée ; le th.2 montre qu'elle est en réalité indépendante de ce corps.

Le critère du th.2 peut encore s'énoncer de la façon suivante :

Proposition 8.- Pour qu'une extension $E \subset \Omega$ de K soit séparable sur K , il faut et il suffit qu'elle soit linéairement disjointe du corps $K^{p^{-\infty}}$, par rapport au corps K (chap.III, § 2,$n^o 3$).

En effet, soit $(a_i)_{1 \leqslant i \leqslant n}$ une famille finie d'éléments de E linéairement libre sur K ; la relation $\sum_{i=1}^{n} \lambda_i a_i^{p^e} = 0$, où $\lambda_i \in K$, est équivalente à $\sum_{i=1}^{n} \lambda_i^{p^{-e}} a_i = 0$ (prop.4) ; si E est séparable, (a_i) est donc linéairement libre sur chacun des corps $K^{p^{-e}}$, et par suite sur $K^{p^{-\infty}}$, donc E est linéairement disjoint de $K^{p^{-\infty}}$ (chap.III, § 2,cor. de la prop.5). Réciproquement, si E est linéairement disjoint

de $K^{p^{-1}}$ (et a fortiori si E est linéairement disjoint de $K^{p^{-\infty}}$), toute famille $(a_i)_{1 \leqslant i \leqslant n}$ d'éléments de E linéairement libre sur K l'est aussi sur $K^{p^{-1}}$, donc (a_i^p) est linéairement libre sur K, et E est séparable sur K.

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

En effet, on a alors $K^{p^{-\infty}} = K$, et toute extension de K est linéairement disjointe de K par rapport à K.

Corollaire 2.- L'intersection d'une extension séparable et d'une extension purement inséparable de K (contenues dans Ω) est identique à K.

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

On notera que l'intersection d'une extension E de K et de $K^{p^{-\infty}}$ peut se réduire à K sans que E soit séparable sur K (exerc. 18).

Corollaire 3.- Pour qu'une extension E de K soit séparable, il suffit qu'il existe une base (a_ι) de E par rapport à K, telle que la famille (a_ι^p) soit linéairement libre sur K.

En effet, cette condition signifie que la famille (a_ι) est linéairement libre sur $K^{p^{-1}}$, donc (chap.III, § 2, cor. de la prop.5) entraîne que E est linéairement disjoint de $K^{p^{-1}}$, et par suite (prop.8) que E est séparable sur K.

Il est clair que, si E est une extension séparable de K, toute extension de K contenue dans E est séparable sur K. En outre :

Proposition 9.- Soit E une extension séparable de K, F une extension séparable de E ; alors F est une extension séparable de K.

En effet, soit (a_λ) une base de E par rapport à K, (b_μ) une base de F par rapport à E ; alors (chap.II, § 5, prop.1), $(a_\lambda b_\mu)$ est une base de F par rapport à K. Une relation de la forme $\sum_{\lambda,\mu} c_{\lambda\mu} a_\lambda^p b_\mu^p = 0$,

où les $a_{\lambda\mu} \in K$ s'écrit $\sum_{\mu} (\sum_{\lambda} a_{\lambda\mu} a_{\lambda}^{p}) b_{\mu}^{p} = 0$; comme les b_{μ}^{p} sont linéairement indépendants sur E, on a, pour tout indice μ, $\sum_{\lambda} a_{\lambda\mu} a_{\lambda}^{p} = 0$; comme les a_{λ}^{p} sont linéairement indépendants sur K, cela entraîne $a_{\lambda\mu} = 0$ pour tout couple (λ, μ). La proposition résulte donc du cor.3 de la prop.8.

2 On notera par contre que lorsque F est une extension séparable de K, E une extension de K contenue dans F, F n'est pas nécessairement séparable sur E (cf. n°7).

5. Extensions algébriques séparables.

Pour les extensions algébriques de K, contenues dans Ω, la prop.1 se précise de la manière suivante :

Proposition 10.- Si E est une extension algébrique de K contenue dans Ω, tout isomorphisme de E relatif à K peut être prolongé en un automorphisme de Ω (relatif à K).

En effet, comme $E \subset \Omega$, tout isomorphisme f de E relatif à K se prolonge en un isomorphisme g de Ω relatif à K ; mais $g(\Omega)$ est une extension algébrique de K, donc contenue dans Ω ; comme en outre $g(\Omega)$ est algébriquement fermée, on a $g(\Omega) = \Omega$. La prop.7 et le th.1 entraînent, pour les extensions algébriques de degré fini, que :

Proposition 11.- Si $E \subset \Omega$ est une extension algébrique de K de degré fini, le nombre des isomorphismes de E relatifs à K est fini et au plus égal au degré $[E:K]$.

Définition 6.- Lorsqu'une extension algébrique $E \subset \Omega$ de K est telle que le nombre des isomorphismes de E relatifs à K soit fini, ce nombre est appelé facteur séparable du degré de E par rapport à K, et noté $[E : K]_s$.

La raison de cette dénomination apparaîtra un peu plus loin (n°6)

Pour toute extension purement inséparable E de K , on a donc $[E:K]_s = 1$.

Proposition 12.- *Soit $E \subset \Omega$ une extension algébrique de K , $F \subset \Omega$ une extension algébrique de E . Soit $(f_\lambda)_{\lambda \in L}$ la famille des isomorphismes distincts de E relatifs à K , chacun d'eux étant prolongé (d'une seule manière) en un automorphisme de $\bar{K}$; soit de même $(g_\mu)_{\mu \in M}$ la famille des isomorphismes distincts de F relatifs à E , chacun d'eux étant prolongé (d'une seule manière, d'ailleurs quelconque) en un automorphisme de $\bar{K}$. Tout isomorphisme de F relatif à K se prolonge alors d'une manière et d'une seule en un automorphisme de $\bar{K}$ de la forme $f_\lambda \circ g_\mu$.*

En effet, soit h un isomorphisme de F relatif à K ; sur E , il coïncide avec un f_λ et un seul, donc $f_\lambda^{-1} \circ h$ est un isomorphisme de F relatif à E , donc égal sur F à un g_μ ; autrement dit, on a $h(x) = f_\lambda(g_\mu(x))$ pour tout $x \in F$. Réciproquement, il est clair que tout automorphisme $f_\lambda \circ g_\mu$, restreint à F , donne un isomorphisme de F relatif à K ; en outre, on ne peut avoir $f_\lambda(g_\mu(x)) = f_{\lambda_1}(g_{\mu_1}(x))$ pour tout $x \in F$ que si $\lambda = \lambda_1$, $\mu = \mu_1$; en effet, pour $x \in E$, on en tire $f_\lambda(x) = f_{\lambda_1}(x)$, donc $\lambda = \lambda_1$, d'où résulte $g_\mu(x) = g_{\mu_1}(x)$ pour tout $x \in F$, c'est-à-dire $\mu = \mu_1$.

L'ensemble des isomorphismes de F relatifs à K est donc en correspondance biunivoque avec l'ensemble $L \times M$; en particulier :

COROLLAIRE.- *Si deux des trois nombres $[E:K]_s$, $[F:K]_s$, $[F:E]_s$ sont définis, il en est de même du troisième, et on a*

$$[F:K]_s = [F:E]_s \, [E:K]_s . \tag{6}$$

Proposition 13.- *Pour qu'une extension algébrique $E \subset \Omega$ de K de degré fini soit séparable sur K , il faut et il suffit que $[E:K]_s = [E:K]$.*

La condition est évidemment nécessaire, comme il résulte de la déf. 5 appliquée au sous-espace vectoriel V=E . Pour voir qu'elle est

suffisante, supposons que E soit de degré n sur K , et soit V un sous-espace de E , de dimension $p \leqslant n$; il existe alors une base $(a_i)_{1 \leqslant i \leqslant n}$ de E par rapport à K , telle que les p premiers vecteurs a_i forment une base de V . Par hypothèse, il existe n isomorphismes distincts u_i de E relatifs à K $(1 \leqslant i \leqslant n)$; ils sont linéairement indépendants dans E (th.1), donc la matrice carrée $(u_i(a_j))$ est de rang n ; en particulier les p premières colonnes de cette matrice sont linéairement indépendantes, d'où résulte qu'il existe p indices distincts $i_1, i_2, .., i_p$ tels que le déterminant d'ordre p $\det(u_{i_k}(a_j))$ $(1 \leqslant k \leqslant p,\ 1 \leqslant j \leqslant p)$ ne soit pas nul ; l'extension E est donc séparable sur K .

Proposition 14.- Si E est une extension algèbrique séparable de K , on a $K(E^p)=E$. Réciproquement, si E est une extension algèbrique de degré fini de K , telle que $K(E^p)=E$, E est séparable .

En effet, soit E une extension de degré n de K , $(a_i)_{1 \leqslant i \leqslant n}$ une base de E par rapport à K . Si E est séparable sur K , les a_i^p $(1 \leqslant i \leqslant n)$ sont linéairement indépendants sur K (th.2), donc forment une base de E par rapport à K ; a fortiori $K(E^p)=E$, puisque les combinaisons linéaires des a_i^p à coefficients dans K appartiennent à $K(E^p)$. Réciproquement, supposons que $K(E^p)=E$; remarquons que tout produit $a_i a_j$ est une combinaison linéaire des a_k à coefficients dans K ; il en résulte que $a_i^p a_j^p$ est une combinaison linéaire des a_k^p à coefficients dans K ; autrement dit, l'ensemble des combinaisons linéaires des a_i^p à coefficients dans K est un anneau contenant K et contenu dans E ; c'est donc un corps (§ 2, prop.6), et comme il contient E^p , c'est le corps $K(E^p)$. Comme on a supposé $K(E^p)=E$, on voit que les a_i^p sont linéairement indépendants ; donc (cor.3 de la prop.8), E est séparable sur K .

Si maintenant E est une extension algèbrique séparable de K , de degré infini, E est réunion des extensions F de degré fini de K , contenues dans E ; pour chacune de ces extensions, $K(F^p)=F$, d'où résulte que E est réunion des $K(F^p)$, et a fortiori que $K(E^p)=E$.

Lorsque E est une extension algèbrique de K , de degré infini sur K , la condition $K(E^p)=E$ n'est plus suffisante pour que E soit séparable ; en effet, le corps $K^{p^{-\infty}}$ vérifie cette condition.

Corollaire.- Soit E une extension algèbrique séparable de K ; si (a_ι) est une base de E par rapport à K , (a_ι^p) est aussi une base de E par rapport à K .

En effet, la famille (a_ι^p) est linéairement libre sur K (th.2) ; d'autre part, le raisonnement de la prop.14 montre que $K(E^p)$ est formé des combinaisons linéaires des a_ι^p à coefficients dans K ; comme $K(E^p)=E$, (a_ι^p) est une base de E .

Proposition 15.- Soit E une extension séparable de K , F une extension algèbrique de K contenue dans E . Dans ces conditions, E est une extension séparable de F .

Soit (a_λ) une base de F par rapport à K , (b_μ) une base de E par rapport à F . Montrons que (b_μ^p) est une famille linéairement libre par rapport à F , ce qui démontrera la proposition (cor.3 de la prop.8). Supposons en effet qu'on ait une relation de la forme $\sum_\mu \beta_\mu b_\mu^p = 0$, où les β_μ appartiennent à F . Comme (a_λ^p) est une base de F par rapport à K (cor. de la prop.14), on peut écrire $\beta_\mu = \sum_\lambda \alpha_{\lambda\mu} a_\lambda^p$, où les $\alpha_{\lambda\mu}$ appartiennent à K . On a donc $\sum_{\lambda,\mu} \alpha_{\lambda\mu}(a_\lambda b_\mu)^p = 0$; mais $(a_\lambda b_\mu)$ est une base de E par rapport à K , donc (th.2) la famille $(a_\lambda b_\mu)^p$ est linéairement libre sur K , ce qui entraîne $\alpha_{\lambda\mu} = 0$ pour tout couple (λ, μ), d'où $\beta_\mu = 0$ pour tout μ .

COROLLAIRE.- Toute extension algèbrique E d'un corps parfait K est un corps parfait.

En effet, si F est une extension quelconque de E , F est une extension séparable de K , donc est séparable sur E d'après la prop. 15 .

6. Eléments algèbriques séparables.

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

Proposition 16.- Pour qu'un élément $x \in \Omega$, algèbrique et de degré n par rapport à K , soit séparable sur K , il faut et il suffit qu'il ait n conjugués distincts par rapport à K (ou, ce qui revient au même, que toutes les racines dans Ω du polynome minimal de x par rapport à K soient simples).

La proposition est une conséquence immédiate de la déf.7 et de la prop.13, puisqu'un isomorphisme de K(x) rélatif à K est entièrement déterminé par sa valeur pour l'élément x , et que $\left[K(x):K\right]= n$.

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

En effet, toute racine de f dans Ω est racine d'un facteur irréductible de f , et un tel facteur ne peut avoir que des racines simples dans Ω .

En particulier :

COROLLAIRE 2.- Si $x \in \Omega$ est algèbrique et séparable sur K , il est séparable sur toute extension F de K contenue dans Ω .

Proposition 17.- Pour qu'un élément $x \in \Omega$, algèbrique sur K , soit séparable sur K , il faut et il suffit que $K(x^p)=K(x)$.

En effet, si $E=K(x)$, on a $E^p=K^p(x^p)$, donc $K(E^p)=E^p(K) = K^p(K)(x^p)=K(x^p)$; la proposition résulte donc de la prop. 14 .

On en déduit une seconde démonstration du cor.2 de la prop.15, car si x est séparable sur K , et F est une extension quelconque de K , on a $F(x^p)=K(F)(x^p)=K(x^p)(F)=K(x)(F)=K(F)(x)=F(x)$, donc x est séparable sur F .

Proposition 18.- Si A est une partie de Ω formée d'éléments algébriques et séparables sur K , K(A) est une extension (algébrique) séprable de K .

Il suffit de montrer que, pour toute partie finie F de K(A), K(F) est séparable ; comme chaque élément de F est contenu dans une extension de K obtenue par adjonction à K d'un nombre fini d'éléments de A , K(F) est contenu dans un corps K(B), où B est une partie finie de A ; il suffit donc de prouver qu'un tel corps K(B) est séparable sur K . Soit $(a_i)_{1 \leqslant i \leqslant n}$ une suite finie formée par les éléments de B ; raisonnons par récurrence sur n , la proposition étant évidente pour n=1 . Si on pose $E=K(a_1, a_2, \ldots, a_{n-1})$, on a $K(B)=E(a_n)$; a_n étant algébrique et séparable sur K , est algébrique et séparable sur E (cor.2 de la prop.16) donc K(B) est séparable sur E ; comme par hypothèse E est séparable sur K , K(B) est séparable sur K (prop.9).

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

La condition est évidemment nécessaire d'après la déf.7 ; elle est suffisante d'après la prop.18, puisque $E=K(E)$.

Proposition 19.- Pour tout élément $x \in \Omega$, algébrique sur K , il existe un entier $m \geqslant 0$ tel que x^{p^m} soit séparable sur K .

En effet, pour tout entier $m \geqslant 0$, on a $K \subset K(x^{p^{m+1}}) \subset K(x^{p^m}) \subset K(x)$ donc le degré de $K(x^{p^m})$ sur K est fini et décroissant en fonction de m ; il existe donc un entier m tel que $K(x^{p^{m+1}})=K(x^{p^m})$, ce qui signifie que x^{p^m} est séparable sur K (prop. 17).

Proposition 20.- Dans une extension algébrique E de K , l'ensemble E_0 des éléments de E séparables sur K est une extension (séparable) de K ; E est une extension purement inséparable de E_0 ; si l'un des deux nombres $[E:K]_s$, $[E_0:K]$ est défini, il en est de même de l'autre et on a $[E:K]_s=[E_0:K]$.

En effet, d'après la prop.18, on a $K(E_0) \subset E_0$, donc $K(E_0)=E_0$; E_0 est par suite la plus grande extension séparable de K contenue dans E. D'après la prop.19, pour tout $x \in E$, il existe un entier m tel que $x^{p^m} \in E_0$, donc (prop.3 et déf.4) E est une extension purement inséparable de E_0. Enfin, comme les deux nombres $[E_0:K]$ et $[E_0:K]_s$ sont définis simultanément et égaux lorsqu'ils sont définis (déf.5 et prop.13), et que $[E:E_0]_s = 1$; la dernière partie de la proposition résulte du cor. de la prop.12.

COROLLAIRE.- Si E est une extension de K de degré fini, $[E:K]_s$ est un diviseur de $[E:K]$.

En effet, on déduit de la prop.20 que (§ 2, th.1)

$$[E:K] = [E:K]_s \, [E:E_0] \tag{7}$$

Cela justifie donc le nom de "facteur séparable du degré" donné à $[E:K]_s$: on voit en outre qu'on est amené à poser de même la définition suivante :

Définition 8.- Lorsqu'une extension algébrique E de K est de degré fini par rapport à la plus grande extension séparable E_0 de K contenue dans E, ce degré est appelé facteur inséparable du degré de E par rapport à K, et noté $[E:K]_i$.

Lorsque deux des trois nombres $[E:K]$, $[E:K]_s$, $[E:K]_i$ sont définis, il en est donc de même du troisième et la formule (7) s'écrit encore

$$[E:K] = [E:K]_s \, [E:K]_i \tag{8}$$

En outre, d'après les prop.6 et 20, le facteur inséparable du degré de E par rapport à K, lorsqu'il est défini, est une puissance de l'exposant caractéristique p.

Remarques.- 1) Il ne faudrait pas croire que le facteur inséparable du degré $[E:K]$ soit égal à la plus haute puissance de p qui divise ce degré. On peut en effet donner des exemples de corps d'exposant caractéristique $p > 1$ admettant des extensions séparables de degré p (cf. § 7, prop.4).

2) Soit $x \in \Omega$ un élément algébrique sur K , et soit e le plus petit des entiers $m \geqslant 0$ tels que x^{p^m} soit séparable sur K (prop.19) ; e est appelé l'exposant de x par rapport à K . Le corps $K(x^{p^e})$ est une extension séparable de K contenue dans K(x), et x est purement inséparable sur $K(x^{p^e})$, donc K(x) est une extension purement inséparable de $K(x^{p^e})$; il en résulte (prop.15) que $K(x^{p^e})$ est la plus grande extension séparable de K contenue dans K(x) . De cette remarque et de la prop.19, on déduit que e est aussi le plus petit des entiers $m \geqslant 0$ tels que x^{p^m} appartienne à $K(x^{p^e})$; donc (prop.3), x est de degré p^e par rapport à $K(x^{p^e})$. Si n est le degré de x , n_0 le degré de x^{p^e} par rapport à K , on a donc $n = n_0 p^e$; il en résulte que, si $g(X)$ est le polynome minimal de x^{p^e} par rapport à K , le polynome minimal de x par rapport à K est $g(X^{p^e})$, car ce polynome a évidemment pour racine x , est de degré n , et le coefficient de x^n est égal à 1 . Si y_i $(1 \leqslant i \leqslant n_0)$ sont les racines de g dans Ω (qui sont toutes simples), les racines de $g(X^{p^e})$ dans Ω sont les n_0 éléments distincts $y_i^{p^e}$, qui sont donc les conjugués de x dans Ω , et dont chacun est racine multiple d'ordre p^e du polynome minimal de x .

Notons encore que e est le plus grand des entiers m tels que le polynome minimal de x par rapport à K puisse s'écrire $h(X^{p^m})$, où $h \in K[X]$; en effet, s'il existait un entier $m > e$ ayant cette propriété, le degré n_1 de h serait $< n_0$; si z_j $(1 \leqslant j \leqslant r)$ sont

sont les racines distinctes de h dans Ω , on aurait donc $r \leqslant n_1 < n_o$; or, les conjugués de x sont les éléments $z_j^{p^{-m}}$, et il y aurait au plus $n_1 < n_o$ conjugués distincts de x dans Ω , ce qui est absurde.

3) Soit E une extension algèbrique de K , E_o la plus grande extension séparable de K contenue dans E . Pour tout élément x de E , le degré de x par rapport à E_o est p^e , où e est l'exposant de x par rapport à K (prop.3). Il en résulte que p^e est un diviseur du facteur inséparable $[E:K]_i$ du degré de E par rapport à K (lorsque ce nombre est défini) ; autrement dit, si $[E:K]_i = p^f$, on a $e \leqslant f$ pour tout élément $x \in E$. Mais il faut noter que f peut être strictement supérieur au plus grand des exposants des éléments de E . Par exemple, soit P un corps de caractéristique p , K=P(X,Y) un corps de fractions rationnelles à deux indéterminées sur P . Soit $E=K(X^{1/p},Y^{1/p})$; l'exemple du n°2 montre que $X^{1/p} \notin K = P(Y)(X)$; de même, on a $Y^{1/p} \notin K(X^{1/p})$, car dans le cas contraire, on aurait $Y \in K(X,Y^p) = K(X)(Y^p)$, contrairement à l'exemple du n° 2 . On a donc $[E:K] = [K(X^{1/p})(Y^{1/p}):K(X^{1/p})]\ [K(X^{1/p}):K] = p^2$, alors que $E \subset K^{1/p}$.

Définition 9.- On dit qu'un sous-corps K d'un corps E est relativement algèbriquement quasi-fermé dans E si tout élément de E algèbrique et séparable sur K appartient à K .

Si E est une extension quelconque de K , l'ensemble des éléments de E qui sont algèbriques et séparables sur K est un sous-corps de E , contenu dans la fermeture algèbrique $\overline{K} \cap E$ de K dans E (prop.20) ; ce corps est algèbriquement quasi-fermé dans E (prop.15) ; on dit que c'est la quasi-fermeture algèbrique de K dans E . En particulier, nous noterons K_s la quasi-fermeture algèbrique de K dans $\overline{K}$ (ou dans Ω) ;

pour toute extension E de K , la quasi-fermeture algébrique de K dans E est donc $K_s \cap E$.

7. Extensions transcendantes séparables. Bases de transcendance séparantes.

Proposition 21.- Toute extension transcendante pure d'un corps K est séparable sur K .

En effet, soit E une extension transcendante pure de K , contenue dans Ω ; soit $(a_\iota)_{\iota \in I}$ une base de transcendance de E sur K , engendrant E . Soit $(x_i)_{1 \leqslant i \leqslant n}$ une famille d'éléments de E , linéairement libre sur K ; montrons que (x_i) est linéairement libre par rapport à $K^{p^{-\infty}}$. On peut écrire $x_i = f_i((a_\iota))/g_i((a_\iota))$ où f_i et g_i sont des polynomes non nuls de $K[X_\iota]_{\iota \in I}$; s'il existe une relation de la forme $\sum_{i=1}^{n} \lambda_i x_i = 0$ avec $\lambda_i \in K^{p^{-\infty}}$, elle peut s'écrire, en la multipliant par le produit des $g_i((a_\iota))$, sous la forme $\sum_{i=1}^{n} \lambda_i h_i((a_\iota)) = 0$, où les h_i sont des polynomes non nuls de $K[X_\iota]_{\iota \in I}$. Soient z_k $(1 \leqslant k \leqslant m)$ les monomes distincts $\prod_{\iota \in I} a_\iota^{r_\iota}$ qui figurent avec un coefficient non nul dans un au moins des h_i ; on peut donc écrire $h_i((a_\iota)) = \sum_{k=1}^{m} a_{ik} z_k$, avec $a_{ik} \in K^{p^{-\infty}}$. Or, la famille $(a_\iota)_{\iota \in I}$ est algébriquement libre sur $K^{p^{-\infty}}$, puisque ce dernier corps est une extension algébrique de K (§ 2, cor. de la prop. 10). Il en résulte que la relation $\sum_{i=1}^{n} \lambda_i h_i((a_\iota)) = 0$ équivaut au système d'équations linéaires par rapport aux λ_i

$$\sum_{i=1}^{n} \lambda_i a_{ik} = 0 \qquad (1 \leqslant k \leqslant m)$$

Mais les coefficients de ce système appartiennent à K ; si le système admet une solution non triviale (λ_i) formée d'éléments de $K^{p^{-\infty}}$, il admet aussi une solution non triviale (μ_i) formée d'éléments de K (chap. II, §5, th. 1) ; on aurait donc $\sum_{i=1}^{n} \mu_i h_i((a_\iota)) = 0$ et par suite $\sum_{i=1}^{n} \mu_i x_i = 0$ contrairement à l'hypothèse.

Remarques.- 1) Nous retrouverons la prop.21 comme cas particulier d'une proposition plus générale au § 5 (§ 5, prop.8).

2) La prop.21 permet de montrer que, dans une extension séparable quelconque E de K, il peut y avoir des extensions F de K telles que E ne soit pas une extension séparable de F. Il suffit de prendre pour E l'extension transcendante simple $E=K(X)$, pour F l'extension $F=K(X^p)$ (p exposant caractéristique) ; comme X est transcendant sur K, E est une extension séparable de K, mais E n'est pas une extension séparable de F, car X est purement inséparable sur F d'après la prop.3, et n'appartient pas à F (cf. n°2, exemple).

Définition 10.- On dit qu'une base de transcendance B (par rapport à K) d'une extension E de K est séparante, si E est une extension (algébrique) séparable de $K(B)$.

D'après la prop.21 et la prop.9, si E possède une base de transcendance séparante par rapport à K, E est séparable sur K. Mais inversement, si E est une extension séparable de K, une base de transcendance quelconque de E par rapport à K ne sera pas nécessairement une base de transcendance séparante, comme le montre le dernier des exemples donnés ci-dessus ; et d'autre part, il y a des extensions séparables de K qui n'admettent aucune base de transcendance séparante.

Par exemple, soit x un élément de Ω transcendant sur K ; soit E l'extension de K engendrée par l'ensemble des éléments $x^{p^{-n}}$, où n parcourt l'ensemble des entiers $\geqslant 0$. E est séparable, car si on pose $E_n=K(x^{p^{-n}})$, toute extension de type fini de K contenue dans E est contenue dans un E_n, et E_n est une extension transcendante pure de K, donc séparable sur K (prop.21).

Mais E n'admet pas de base de transcendance séparante sur K ; en effet, on a $\dim_K E = 1$; une base de transcendance de E sur K se compose donc d'un seul élément y ; soit m le plus petit des entiers n tels que $y \in K_n$; comme K_m est extension algèbrique de K(y), $x^{p^{m-1}}$ est algèbrique et non séparable sur K(y), puisqu'il est purement inséparable sur K_m et n'appartient pas à K_{m-1}.

Toutefois, on a la proposition suivante :

Proposition 22.- Soit E une extension séparable de type fini de K. Pour toute partie finie F de E telle que E=K(F), il existe une base de transcendance séparante de E par rapport à K, contenue dans F.

Le corps E ayant un degré de transcendance fini d sur K, nous procéderons par récurrence sur d, la proposition étant évidente si d=0. Supposons donc la proposition démontrée pour les extensions de K de type fini et de degré de transcendance $< d$. L'ensemble F contient une base de transcendance B_0 de E ; si on a $K(E^p)=E$, on a a fortiori $K(B_0)(E^p)=E$; comme E est algèbrique et de degré fini sur $K(B_0)$, E est une extension séparable de $K(B_0)$ (prop.14), donc B_0 est une base de transcendance séparante de E par rapport à K. Supposons donc $K(E^p) \neq E$ (on peut d'ailleurs montrer qu'il en est nécessairement ainsi dès que $d > 0$; cf. exerc.). Il existe un élément $x \in F$ non contenu dans $K(E^p)$; x est transcendant sur K, sans quoi il serait algèbrique et séparable sur K, et on aurait (prop.17), $x \in K(x^p) \subset K(E^p)$ contrairement à l'hypothèse. Nous allons montrer que E est une extension séparable de K(x).

Soit donc $(u_i)_{1 \leqslant i \leqslant n}$ une famille d'éléments de E linéairement libre par rapport à K(x) ; supposons que les u_i^p soient linéairement dépendants par rapport à K(x). Il existerait donc (chap.III, § 1, prop.) n polynomes $f_i \in K[X]$ $(1 \leqslant i \leqslant n)$ non tous nuls, et tels que $\sum_{i=1}^{n} f_i(x) u_i^p = 0$. Comme chaque entier $\geqslant 0$ peut s'écrire sous la forme

$kp+j$, où k est un entier $\geqslant 0$ et $0 \leqslant j \leqslant p-1$, on peut écrire $f_i(X) = \sum_{j=0}^{p-1} g_{ij}(X^p)X^j$, où $g_{ij} \in K[X]$ $(1 \leqslant i \leqslant n)$. On a donc la relation $\sum_{j=0}^{p-1} (\sum_{i=1}^{n} u_i^p g_{ij}(x^p))x^j = 0$. Or, chacun des éléments $\sum_{i=1}^{n} u_i^p g_{ij}(x^p)$ appartient à $K(E^p)$; comme $x \notin K(E^p)$ et $x^p \in K(E^p)$, x est de degré p sur $K(E^p)$ (prop.3) ; on en déduit $\sum_{i=1}^{n} u_i^p g_{ij}(x^p) = 0$ pour $0 \leqslant j \leqslant p-1$. Soit $g_{ij}(X) = \sum_k a_{ijk}X^k$, où $a_{ijk} \in K$. Les éléments x^k $(k \in \mathbb{N})$ étant linéairement indépendants par rapport à K , et les u_i $(1 \leqslant i \leqslant n)$ linéairement indépendants par rapport à $K(x)$, les $x^k u_i$ sont linéairement indépendants par rapport à K (chap.II, § 5, prop.1 et § 3,th.2); comme E est séparable sur K , les $x^{rp}u_i^p$ sont linéairement indépendants sur K ; les relations $\sum_{i=1}^{n} u_i^p g_{ij}(x^p) = 0$ entraînent donc $a_{ijk} = 0$ pour tous les (i,j,k), et par suite $f_i = 0$ pour $1 \leqslant i \leqslant n$, contrairement à l'hypothèse.

Cela étant, comme E est séparable de type fini sur $K(x)$, et a un degré de transcendance $d-1$ sur $K(x)$ (§ 2,th.7),il existe une base de transcendance séparante B_1 de E par rapport à $K(x)$, contenue dans $F \cap \complement\{x\}$; l'ensemble $B = B_1 \cup \{x\}$ est alors une base de transcendance de E par rapport à K (§ 2,prop.12), et comme $K(B) = K(x)(B_1)$, B est une base de transcendance séparante de E par rapport à K .

8. Dérivations dans les corps.

Nous avons défini au chap.IV (§) la notion de dérivation d'une algèbre A sur un corps K . Etant donné une extension $E \subset \Omega$ de K , nous entendrons dans ce qui suit par *dérivation de E relative à K* toute dérivation de E , prenant ses valeurs dans Ω , E et Ω étant considérés comme des algèbres sur K (ce qui implique que, si D est une telle dérivation, on a $Da = 0$ pour tout $a \in K$).

Si D est une dérivation de E relative à K , on sait (chap.IV, §) que cette dérivation peut se prolonger à tout anneau $E[X_\iota]_{\iota\in I}$ de polynomes sur E , de la manière suivante : si, pour tout polynome $f\in E[X_\iota]_{\iota\in I}$, on désigne par f^D le polynome (de $\Omega[X_\iota]_{\iota\in I}$) obtenu en appliquant la dérivation D a chaque coefficient de f , l'application $f\to f^D$ est une dérivation.

Proposition 23.- Soit E une extension de K contenue dans Ω , D une dérivation de E relative à K . Soit $F=E(x_\iota)_{\iota\in I}$ une extension de E contenue dans Ω , $\mathfrak{a}$ l'idéal de $E[X_\iota]_{\iota\in I}$ formé des polynomes f tels que $f((x_\iota))=0$. Etant donnée une famille $(u_\iota)_{\iota\in I}$ d'éléments de Ω , pour qu'il existe une dérivation $\bar{D}$ sur F , prolongeant D et telle que $\bar{D}x_\iota = u_\iota$ pour tout ι , il faut et il suffit que pour tout polynome $f\in\mathfrak{a}$, on ait

$$f^D((x))+\sum_\iota \frac{\partial f}{\partial X_\iota}u_\iota = 0 \qquad (10)$$

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

Il suffit de prolonger la dérivation D à l'anneau $E[x_\iota]_{\iota\in I}$ puisqu'on sait (chap.IV, §) qu'une dérivation sur un anneau d'intégrité se prolonge d'une manière et d'une seule au corps des quotients de cet anneau. Tout élément de $E[x_\iota]_{\iota\in I}$ est de la forme $g((x_\iota))$, où $g\in E[X]_{\iota\in I}$; d'après les règles de calcul des dérivations, on doit donc avoir, pour toute dérivation $\bar{D}$ prolongeant D ,

$$\bar{D}(g((x_\iota))) = g^D((x_\iota))+\sum_\iota \frac{\partial g}{\partial x_\iota}\,\bar{D}x_\iota$$

d'où la nécessité de la condition (10) pour tout polynome $f\in\mathfrak{a}$. Inversement, si cette condition est vérifiée, on définit $\bar{D}$ dans $K[x_\iota]_{\iota\in I}$ en prenant pour tout élément $g((x_\iota))$, où $g\in K[X_\iota]_{\iota\in I}$,

$$\bar{D}(g((x_\iota))) = g^D((x_\iota)) + \sum_\iota \frac{\partial g}{\partial X_\iota}u_\iota$$

En effet, si g et h sont deux polynomes tels que $g((x_\iota))=h((x_\iota))$ g-h appartient à l'idéal $\mathfrak{a}$, et la condition (10) prouve que $\overline{D}(g((x_\iota)))=\overline{D}(h((x_\iota)))$; donc $\overline{D}$ est bien définie pour tout élément de $K[x_\iota]_{\iota\in I}$; on vérifie aussitôt que c'est bien une dérivation.

COROLLAIRE.- Soit (f_λ) un système de générateurs de l'idéal $\mathfrak{a}$; pour que la condition (10) soit vérifiée pour tout polynome $f\in\mathfrak{a}$ il suffit qu'elle soit vérifiée pour les f_λ.

En effet, tout polynome $f\in\mathfrak{a}$ s'écrit par hypothèse $f=\sum_\lambda \varphi_\lambda f_\lambda$ où les φ_λ sont des polynomes quelconques ; on a donc $f^D=\sum_\lambda \varphi_\lambda^D f_\lambda+\sum_\lambda \varphi_\lambda f_\lambda^D$, et de même $\frac{\partial f}{\partial x_\iota}=\sum_\lambda \frac{\partial \varphi_\lambda}{\partial x_\iota} f_\lambda+\sum_\lambda \varphi_\lambda \frac{\partial f_\lambda}{\partial x_\iota}$; comme $f_\lambda((x_\iota))=0$ par hypothèse pour tout λ, on voit que l'on a

$$f^D((x_\iota))+\sum_\iota \frac{\partial f}{\partial x_\iota} u_\iota=\sum_\lambda \varphi_\lambda((x_\iota))(f_\lambda^D((x_\iota))+\sum_\iota \frac{\partial f_\lambda}{\partial x_\iota} u_\iota)$$

d'où le corollaire.

Appliquons le critère de la prop.23 aux divers types d'extensions d'un corps :

Proposition 24.- Soit F une extension transcendante pure de E, (x_ι) une famille algèbriquement libre d'éléments de F telle que $F=E((x_\iota))$; pour toute dérivation D de E relative à K et toute famille (u_ι) d'éléments de Ω, il existe une dérivation $\overline{D}$ et une seule sur F, prolongeant D et telle que $\overline{D}x_\iota=u_\iota$ pour tout ι.

En effet, l'idéal $\mathfrak{a}$ de la prop.23 est ici réduit à 0, donc les conditions (10) sont vérifiées.

Proposition 25.- Soit F une extension algèbrique séparable de E ; toute dérivation D de E relative à K se prolonge d'une manière et d'une seule en une dérivation $\overline{D}$ de F.

Montrons d'abord que si le prolongement est possible, il est unique. En effet, pour tout élément $x\in F$, soit $f\in E[X]$ le polynome minimal de x par rapport à E ; d'après (10), on doit avoir $f^D(x)+f'(x)\overline{D}x=0$;

comme x est séparable sur E , x est racine simple de f , donc $f'(x)\neq 0$, ce qui montre que $\overline{D}x$ est déterminé.

Montrons maintenant que la dérivation D peut être prolongée à toute extension de degré fini L de E contenue dans F ; si $L=E(x_1,x_2,\dots,x_n)$, il suffit de raisonner par récurrence sur n , la proposition étant évidente pour $n=0$. Or, si on pose $M=E(x_1,x_2,\dots,x_{n-1})$, on a $L=M(x_n)$, et x_n est séparable sur M ; par hypothèse, D se prolonge en une dérivation $\overline{D}$ de M relative à K ; soit g le polynome minimal de x_n par rapport à M ; pour qu'il existe une dérivation $\overline{D}_1$ sur L prolongeant $\overline{D}$, il faut et il suffit, d'après le cor. de la prop.23, que l'on puisse déterminer $\overline{D}_1x$ dans Ω de sorte qu'il satisfasse à la relation

$$g^D(x)+g'(x)\overline{D}_1x=0$$

ce qui est toujours possible, puisque $g'(x)\neq 0$.

Cela étant, l'application $x \to \overline{D}x$ de F dans Ω déterminée comme il a été vu plus haut est bien une dérivation de F ; en effet, si x et y sont deux éléments quelconques de F , ils appartiennent à E(x,y), et nous venons de voir qu'il existe dans ce corps une dérivation qui coïncide nécessairement avec $\overline{D}$; on a donc bien $\overline{D}(x+y)=\overline{D}x+\overline{D}y$ et $\overline{D}(xy)=x\overline{D}y+y\overline{D}x$.

Proposition 26.- Soit F une extension purement inséparable de E , de degré fini et >1 par rapport à E ; il existe une dérivation $\neq \overline{D}$ de F , non identiquement nulle, et qui se réduit à 0 dans E .

En effet, il existe un système de générateurs $(x_i)_{1\leqslant i\leqslant n}$ de F par rapport à E , tel que $x_n\notin E(x_1,x_2,\dots,x_{n-1})=L$; x_n est purement inséparable sur L ; soit $f=X^{p^e}-a$ son polynome minimal par rapport à L. Si D est la dérivation identiquement nulle dans L , on a $f^D=0$; comme $f'(x)=0$, on voit que pour toute valeur de $u\in\Omega$, la relation $f^D(x)+f'(x)u=0$ est vérifiée, et par suite (cor.de la prop.23) il existe une dérivation $\overline{D}$ de $F=L(x_n)$ prolongeant D et telle que $\overline{D}x=u$.

Théorème 3.- Pour qu'une extension de type fini E d'un corps K soit algébrique et séparable sur K, il faut et il suffit que la dérivation identiquement nulle soit la seule dérivation de E relative à K.

En effet, si E est une extension algébrique séparable de K, une dérivation de E relative à K est un prolongement à E de la dérivation identiquement nulle de K ; comme ce prolongement est unique (prop.25), c'est la dérivation identiquement nulle.

Réciproquement, soit $E=K(x_1,x_2,..,x_n)$ une extension de type fini de K, et posons $E_0=K$ et $E_i=K(x_1,x_2,..,x_i)$ pour $1\leqslant i\leqslant n$. Soit h le plus petit des entiers i tels que $E=E_n$ soit algébrique et séparable sur E_i ; si $h>0$, $E_h = E_{h-1}(x_h)$ n'est pas algébrique séparable sur E_{h-1} (prop.9); si x_h est transcendant sur E_{h-1}, il existe sur E_h une dérivation D relative à K et non identiquement nulle (prop.24) ; si x_h est algébrique sur E_{h-1}, x_h n'est pas séparable sur E_{h-1} ; soit p^e la plus petite puissance de p telle que $x_h^{p^e}$ soit séparable sur E_{h-1}; il existe alors sur $E_h=E_{h-1}(x^{p^e})(x)$ une dérivation D relative à K et non identiquement nulle, d'après la prop.26. Dans les deux cas, on peut prolonger à $E=E_n$ la dérivation D (prop.25), ce qui achève la démonstration.

Si E n'est pas une extension de type fini de K, il peut se faire que la seule dérivation de E relative à K soit la dérivation identiquement nulle, sans que E soit séparable sur K ; par exemple si $p>1$ et, si on prend $E=K^{p^{-\infty}}$, toute dérivation D de E est identiquement nulle, car pour tout $x\in E$ il existe $y\in E$ tel que $x=y^p$, d'où $Dx=p.Dy=0$.

COROLLAIRE.- **Soient f_i $(1\leqslant i\leqslant n)$ n polynomes de $K[X_1,X_2,\ldots,X_n]$, x_i $(1\leqslant i\leqslant n)$ n éléments de Ω tels que $f_i(x_1,x_2,..,x_n)=0$ pour $1\leqslant i\leqslant n$.**

Si le déterminant $\det(\frac{\partial f_i}{\partial x_j})$ n'est pas nul, l'extension $K(x_1,x_2,\ldots,x_n)$ est algèbrique et séparable sur K .

En effet, si D est une dérivation quelconque de $K(x_1,x_2,\ldots,x_n)$ relative à K , on déduit des n relations $f_i(x_1,x_2,\ldots,x_n)=0$ que

$$\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j} Dx_j = 0 \qquad (1 \leqslant i \leqslant n)$$

d'où, en vertu de l'hypothèse, $Dx_j=0$ pour $1 \leqslant j \leqslant n$, et par suite $Dx=0$ pour tout $x \in K(x_1,x_2,\ldots,x_n)$.

Les dérivations d'une extension E de K , relatives à K , sont des applications linéaires particulières de l'espace vectoriel E dans l'espace vectoriel Ω (sur le corps K) ; il est immédiat qu'elles forment un sous-espace vectoriel (par rapport à Ω) de l'espace vectoriel Ω^E . On déduit du th.3 que :

Proposition 27.- Soit E une extension séparable et de type fini d'un corps K ; si r est la dimension (algèbrique) de E par rapport à K , l'espace des dérivations de E relatives à K est de dimension (linéaire) r par rapport à Ω .

En effet, soit $(x_i)_{1 \leqslant i \leqslant r}$ une base de transcendance séparante de E par rapport à K ; chacune des dérivations $\frac{\partial}{\partial x_i}$ dans le corps $K(x_1,x_2,\ldots,x_r)$ se prolonge en une dérivation unique D_i du corps E (prop.25). Les D_i sont linéairement indépendantes par rapport à Ω , car pour tout indice j , on a $D_i x_j=0$ pour $i \neq j$, $D_j x_j=1$; d'une relation $\sum_{i=1}^{r} \lambda_i D_i=0$, on tire donc $\lambda_j=0$ pour tout indice j . Soit alors D une dérivation quelconque de E , et posons $Dx_i=u_i$ pour $1 \leqslant i \leqslant r$, $D'=D-\sum_{i=1}^{r} u_i D_i$; D' est une dérivation sur E et on a $D'x_i=0$ pour $1 \leqslant i \leqslant r$, d'où $D'x=0$ dans $K(x_1,x_2,\ldots,x_r)$, et a fortiori (prop.25), $D'x=0$ dans E ; on a donc $D=\sum_{i=1}^{r} u_i D_i$, ce qui achève la démonstration.

Exercices.- 1) Soit E une extension algèbriquement fermée d'un corps K , ayant un degré de transcendance fini sur K . Montrer que tout endomorphisme de E , relatif à K , est un automorphisme de E (si f est un endomorphisme de E relatif à K , remarquer que f(E) a même degré de transcendance que E par rapport à K).

Montrer que pour toute extension algèbriquement fermée F de K , ayant un degré de transcendance infini sur K , il existe des endomorphismes de F relatifs à K , qui ne sont pas des automorphismes de F .

2) Les seuls éléments de Ω qui sont invariants par tout automorphisme de Ω relatif à K sont les éléments purement inséparables sur K .

3) Soit Ω un corps non commutatif, K un sous-corps de Ω , E une extension de K contenue dans Ω . Soit (u_ι) une famille d'isomorphismes de E dans Ω , relatifs à K ; pour que les u_ι soient linéairement dépendants dans E (c'est-à-dire qu'il existe une famille (λ_ι) d'éléments non tous nuls de Ω telle que $\sum_\iota \lambda_\iota u_\iota(x)=0$ pour tout $x \in E$) il est nécessaire qu'il existe deux indices α,β distincts et un élément $\mu \in \Omega$ non nul, tel que l'on ait identiquement $u_\alpha(x)=\mu u_\beta(x)\mu^{-1}$ pour tout $x \in E$.

4) Soit E une extension séparable d'un corps K , (a_{ij}) une matrice dont les éléments appartiennent à E . Montrer que si les colonnes de cette matrice sont linéairement indépendantes par rapport à K , il en est de même des colonnes de la matrice (a_{ij}^p) (considérer les colonnes de (a_{ij}) comme des vecteurs d'un espace vectoriel de dimension finie sur E , et raisonner par récurrence sur la dimension de cet espace).

9) Soit E une extension d'un corps K . On dit qu'une partie M de E est p-<u>indépendante</u> par rapport à K si, pour toute partie M' de M distincte de M , le corps $K(E^p)(M')$ est distinct de $K(E^p)(M)$. On dit que M est une p-<u>base</u> (ou une <u>base d'imperfection</u>) de E par rapport à K si M est p-indépendante par rapport à K et si $E=K(E^p)(M)$.

a) Pour que M soit p-indépendante par rapport à K , il faut et il suffit que toute partie finie de M le soit.

b) Soit M une partie de E p-indépendante par rapport à K . Si $x \in E$ n'appartient pas à $K(E^p)(M)$, montrer que $M \cup \{x\}$ est une partie p-indépendante de E (utiliser le fait que si x et y sont deux éléments purement inséparables sur un corps L , appartenant à $L^{p^{-1}} \cap L$, les relations $y \in L(x)$ et $x \in L(y)$ sont équivalentes).

c) Soit S une partie de E telle que $E=K(E^p)(S)$, M une partie de E p-indépendante sur K ; montrer qu'il existe une p-base B de E par rapport à K telle que $M \subset B \subset S$.

d) Pour qu'une famille finie $(x_i)_{1 \leqslant i \leqslant r}$ d'éléments distinct soit p-indépendante sur K , il faut et il suffit que les p^r éléments $z_{\nu_1 \nu_2 \ldots \nu_r} = x_1^{\nu_1} x_2^{\nu_2} \ldots x_r^{\nu_r}$ soient linéairement indépendants par rapport à $K(E^p)$ ($0 \leqslant \nu_i < p$ pour $1 \leqslant i \leqslant r$). En particulier, pour que E ait une p-base de r éléments par rapport à K , il faut et il suffit que $\left[E:K(E^p)\right] = p^r$; le nombre r est encore appelé le <u>degré d'imperfection</u> de E par rapport à K . Si r=0, c'est-à-dire $K(E^p)=E$, on dit que E est <u>relativement parfait</u> par rapport à K ; toute extension algèbrique séparable de K est relativement parfaite sur K .

e) Si une partie M de K est p-indépendante par rapport à <u>un</u> sous-corps parfait de K , elle est p-indépendante par rapport à <u>tout</u> sous-corps parfait de K ; on dit alors qu'elle est <u>absolument</u>

p-indépendante. Une p-base de K par rapport à tout sous-corps parfait de K est dite p-base absolue de K ; si le nombre r de ses éléments est fini, r est appelé le degré d'imperfection absolu de K ; on a $p^r = [K:K^p] = [K^{1/p}:K]$.

Si $E \supset K$ est parfait, E est relativement parfait sur K .

6) Soit E une extension de K , F une extension de E .

a) Si B est une p-base de E par rapport à K , C une p-base de F par rapport à E , il existe une p-base de F par rapport à K contenue dans $B \cup C$.

b) Si F est une extension séparable de E , deux des trois propositions suivantes entraînent la troisième : α) B est une p-base de E par rapport à K ; β) C est une p-base de F par rapport à E ; γ) $B \cup C$ est une p-base de F par rapport à K et $B \cap C = \phi$ (on utilisera le fait que, si (c_γ) est une base de F par rapport à E , (c_γ^p) est une base de $K(F^p)$ par rapport à $K(E^p)$, et de $E(F^p)$ par rapport à E).

c) Si F est une extension séparable de E , C une p-base de F par rapport à E , montrer que, pour tout entier $k \geqslant 0$, $K(F^{p^k})$ est séparable sur $K(E^{p^k})$, et que C^{p^k} est une p-base de $K(F^{p^k})$ par rapport à $K(E^{p^k})$ (remarquer que $K^{p^{-k}}$ est contenu dans $E^{p^{-\infty}}$, et par suite linéairement disjoint de F par rapport à E). En déduire que, si B_k est une p-base de $K(E^{p^k})$ par rapport à K , $B_k \cup C^{p^k}$ est une p-base de $K(F^{p^k})$ par rapport à K . Cas où $E = K$.

7) a) Soit E une extension purement inséparable d'un corps K , contenue dans un corps $K^{p^{-n}}$. Soit B une p-base de E par rapport à K ; montrer qu'on a $E = K(B)$ (remarquer que pour tout entier $k \geqslant 0$, il existe une p-base de $K(E^{p^k})$ par rapport à K contenue dans B^{p^k}). Pour que le degré $[E:K]$ soit fini, il faut et il suffit que le degré d'imperfection m_0 de E sur K (nombre d'éléments de B) soit fini ;

m_0 est alors le nombre minimum de générateurs de E sur K . Si m_k est le degré d'imperfection de $K(E^{p^k})$ sur K , on a $m_{k+1} \leqslant m_k$ pour tout k , et si $f = \sum_k m_k$, on a $[E:K] = p^f$.

b) On suppose que $E \subset K^{p^{-1}}$; soit K_0 un sous-corps de K tel que E soit <u>séparable</u> sur K_0 . Montrer que l'ensemble B^p est p-indépendant par rapport à K_0 dans K (remarquer sur, si (a_μ) est une base de K sur K_0 , (a_μ^p) est une base de $K_0(K^p)$ sur K_0). Soit C une partie de K , sans élément commun avec B^p , et telle que $B^p \cup C$ soit une p-base de K par rapport à K_0 ; montrer que $B \cup C$ est une p-base de E par rapport à K_0 .

c) On suppose de nouveau $E \subset K^{p^{-n}}$, et que E soit séparable sur un sous-corps K_0 de K . Montrer que, si K a un degré d'imperfection fini sur K_0 , E a même degré d'imperfection que K sur K_0 (utiliser b)

7 bis) Soit E une extension de K , F une extension de type fini de E . Montrer que si le degré d'imperfection de E par rapport à K est fini, le degré d'imperfection de F par rapport à K est au moins égal au degré d'imperfection de E par rapport à K (se ramener aux deux cas suivants : 1° F est séparable sur E ; 2° $F=E(x)$, où $x^p \in E$).

8) Soit F une extension séparable de K . Si $E \subset F$ est une extension relativement parfaite de K , montrer que F est séparable sur E .

9) Soit E une extension séparable de K , B une p-base de E par rapport à K .

a) Montrer que B est algèbriquement libre sur K (considérer une relation algèbrique du plus petit degré possible entre les éléments de B , et mettre les degrés des variables qui y figurent sous la forme $kp+h$ avec $0 \leqslant h \leqslant p-1$). En déduire que si E a un degré de transcendance fini sur K , le degré d'imperfection de E sur K est au plus égal à son degré de transcendance.

b) Montrer que E est séparable et relativement parfait sur K(B).

10) Pour qu'une extension E de K , ayant un degré de transcendance fini sur K , admette une base de transcendance séparante sur K , il faut et il suffit que son degré d'imperfection sur K soit égal à son degré de transcendance sur K (utiliser l'exerc.6b) et l'exerc.9b)). Toute p-base de E sur K est alors une base de transcendance séparante de E sur K .

11) Montrer qu'une extension transcendante E relativement parfaite d'un corps K ne peut être engendrée par un nombre fini d'éléments (si T est une base de transcendance de E , montrer qu'on aurait $\left[E:K(T^p)\right] \leqslant \left[E:K(T)\right]$ et prouver que cette conclusion est absurde lorsque T n'est pas vide). En déduire une nouvelle démonstration de la prop.22 (utiliser l'exerc. 9b)).

12) Si une extension E de K admet une base de transcendance séparante T sur K , l'intersection L des corps $K(E^{p^n})$, où n parcourt l'ensemble des entiers $\geqslant 0$, est algébrique sur K (le démontrer d'abord lorsque E a un degré de transcendance fini sur K , en remarquant que L est relativement parfait sur K , et utilisant les exerc. 8, 6b) , 9a) et 10 ; puis ramener à ce cas le cas général, en considérant, pour un élément x de L , une partie finie T_0 de T telle que les coefficients du polynome minimal de x sur K(T) appartiennent à $K(T_0)$; montrer que x est séparable sur $K(T_0^{p^n})$ pour tout n , et en déduire que si $F=K(T_0)(x)$, x appartient à l'intersection des corps $K(F^{p^n})$).

13) Soit E une extension algébrique séparable d'un corps K . Montrer que le plus petit corps parfait E^{p^∞} contenu dans E (intersection des corps E^{p^n} pour n entier $\geqslant 0$) est algébrique sur le plus petit corps parfait K^{p^∞} contenu dans K (si $x \in E^{p^\infty}$,

montrer que $x^{p^{-n}} \in K(x)$, en remarquant que $x \in K(x^{p^n})$. En déduire que les coefficients du polynome minimal de x par rapport à K appartiennent à tous les K^{p^n}).

14) Soit E une extension séparable de K, ayant un degré de transcendance fini sur K.

a) Si E admet une base de transcendance séparante sur K, pour toute base de transcendance T de E sur K, il existe un entier $m \geqslant 0$ tel que $K(E^{p^m})$ soit séparable sur K(T).

b) Inversement, s'il existe une base de transcendance T_0 de E sur K et un entier $m \geqslant 0$ tels que $K(E^{p^m})$ soit séparable sur $K(T_0)$, pour toute base de transcendance T de E sur K, il existe un entier n tel que $K(E^{p^n})$ soit séparable sur K(T).

c) En déduire que, si la condition de b) est vérifiée, E admet une base de transcendance séparante sur K (étant donnée une p-base B de E sur K, une base de transcendance S de E sur K contenant B (exerc. 9a)), montrer que S est une base de transcendance séparante, en utilisant l'exerc. 9 b)).

15) Soient E une extension de K, F une extension de E.

a) Si E admet une base de transcendance séparante sur K, et F une base de transcendance séparante sur E, F admet une base de transcendance séparante sur K.

b) Si F admet une base de transcendance séparante sur K, et si E a un degré de transcendance fini sur K, E admet une base de transcendance séparante sur K (se ramener au cas où F a un degré de transcendance fini sur K, et appliquer l'exerc. 14c)).

c) Si F admet une base de transcendance séparante finie sur K, et est séparable sur E, F admet une base de transcendance séparante sur E (utiliser les exerc. 10 et 6 b)).

16) Soit K un corps ayant un degré d'imperfection absolu égal à 1. Pour qu'une extension E de K soit séparable sur K , il faut et il suffit que E ne contienne aucun élément purement inséparable sur K et n'appartenant pas à K (soit a un élément de K formant une p-base absolue de K ; montrer que $K^{p^{-1}} = K(a^{p^{-1}})$ et E sont linéairement disjoints sur K).

17) Soit f un polynome irréductible dans $K[X]$; montrer que, dans $K[X]$, le polynome $f(X^p)$ est irréductible ou est puissance p-ème d'un polynome irréductible, suivant qu'il existe ou non un coefficient de f qui n'est pas puissance p-ème d'un élément de K .

18) Soit K_0 un corps de caractéristique $p>0$, K l'extension transcendante pure $K_0(X,Y)$; on considère dans $\overline{K}$ une racine θ du polynome $f=Z^{2p}+XZ^p+Y \in K[Z]$. Montrer que l'extension $E=K(\theta)$ n'est pas séparable sur K , mais qu'il n'existe pas d'élément de E purement inséparable sur K et n'appartenant pas à K (remarquer d'abord que f est irréductible dans $K[Z]$; s'il existait $\beta \in E$ tel que $\beta^p \in K$, $\beta \notin K$, f serait réductible dans $K(\beta)[Z]$; en déduire, d'après l'exerc.17, que $X^{1/p}$ et $Y^{1/p}$ appartiendraient à E , et que par suite on aurait $[E:K] \geqslant p^2$).

19) Soit E une extension d'un corps K de caractéristique $p > 0$. Montrer que toute dérivation de E relative à K est identiquement nulle dans $K(E^p)$; si B est une p-base de E relative à K , pour tout $x \in B$, il existe une dérivation D de E relative à K , telle que $Dx=1$ et $Dy=0$ pour tout $y \in B$ distinct de x ; en particulier, si le degré d'imperfection de E sur K est fini, la dimension de l'espace des dérivations de E relatives à K est égale à ce degré.

Déduire de ces résultats que si F est une extension séparable de E , toute dérivation de E relative à K peut se prolonger en une dérivation de F relative à K (utiliser l'exerc. 6b)).

20) Soit E une extension séparable de K ayant un degré de transcendance fini sur K . Soit B une base de transcendance de E sur K , et pour tout $n \geqslant 0$, soit S_n le sous-corps des éléments $x \in E$ tels que $x^{p^n} \in K(B)$. Montrer que S_n admet une base de transcendance séparante sur K (utiliser les exerc. 7c) et 10)).

§ 5. Composition des corps.

1. Corps composés.

Etant données deux extensions E,F d'un même corps K , contenues dans Ω , le corps $E(F)=F(E)=K(E \cup F)$ n'est autre que la borne supérieure de E et de F dans l'ensemble des sous-corps de Ω , ordonné par inclusion ; on dit encore (par abus de langage) que ce corps est l'extension de K composée des extensions E et F .

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

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

Proposition 1.- Soient E et F deux extensions de K , A (resp. B) un anneau contenu dans E (resp. F), contenant K , et tel que E (resp.F) soit corps des quotients de A (resp. B) .

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

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

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

La propriété a) est évidente, puisque $K(E \cup F)$ contient A et B. Si on remarque que le produit de deux éléments de la base (b_μ) est une combinaison linéaire des b_μ à coefficients dans K, on voit que l'ensemble des combinaisons linéaires $\sum_\mu a_\mu b_\mu$ à coefficients $a_\mu \in A$ est un anneau ; comme il contient B, donc K, il contient aussi A, et par suite C ; mais il est aussi contenu dans tout anneau contenant $A \cup B$, donc est identique à C. Comme l'application $(x,y) \longrightarrow xy$ de $A \times B$ dans C est bilinéaire, il existe une application linéaire φ de $A \otimes B$ dans C telle que $\varphi(x \otimes y) = xy$ (chap.III, §1, n°2) ; on vérifie aussitôt que φ est une représentation pour les structures d'algèbre (sur K) de A B et de C, ce qui démontre b).

Enfin, si E et F sont linéairement disjoints sur K, il en est évidemment de même de A et B. Réciproquement, si A et B sont linéairement disjoints sur K, A et F sont linéairement disjoints, car si une famille d'éléments de Ω est libre par rapport à l'anneau B, elle est libre par rapport au corps des quotients F de B (chap.III, §1, prop.); le même raisonnement prouve ensuite que E et F sont linéairement disjoints sur K, ce qui achève la démonstration.

Proposition 2.- Soit E une extension quelconque de K, F une extension algébrique de K, F_0 la plus grande extension séparable de K contenue dans F (quasi-fermeture algébrique de K dans F). Le corps composé E(F) est algébrique sur E, et $E(F_0)$ est la quasi-fermeture algébrique de E dans E(F) ; si le nombre $[F:K]$ (resp. $[F:K]_s$, $[F:K]_i$ est défini, il en est de même de $[E(F):E]$ (resp. $[E(F):E]_s$, $[E(F):E]_i$, et on a $[E(F):E] \leq [F:K]$ (resp. $[E(F):E]_s \leq [F:K]_s$, $[E(F):E]_i \leq [F:K]_i$) ; pour que l'on ait $[E(F):E] = [F:K]$, il faut et il suffit alors que E et F soient linéairement disjoints sur K.

Comme tous les éléments de F (resp. F_0) sont algèbriques (resp. algèbriques et séparables) sur K, ils le sont aussi sur $E \supset K$ (§ 2 cor. du th.2 et § 4, cor.2 de la prop.16), donc E(F) (resp. $E(F_0)$) est une extension algèbrique (resp. algèbrique et séparable) de E (§ 2, rpop.5 et § 4, prop.18) ; en outre les éléments de F, étant purement inséparables sur F_0, le sont a fortiori sur $E(F_0)$, donc E(F) est purement inséparable sur $E(F_0)$, et $E(F_0)$ est bien la quasi-fermeture algèbrique de E dans E(F).

Le plus petit anneau C contenant $E \cup F$ est contenu dans E(F) ; comme E(F) est une extension algèbrique de E, C est un corps (2, prop.6), donc identique à E(F). Par suite, si (b_μ) est une base de F sur K, E(F) est identique à l'ensemble des combinaisons linéaires $\sum_\mu a_\mu b_\mu$ à coefficients dans E ; il en résulte aussitôt que si $[F:K]$ est fini, on a $[E(F):E] \leqslant [F:K]$ (chap.II, § 3, cor.2 du th.3) ; le même raisonnement, appliqué à F_0 au lieu de F, montre que $[E(F):E]_s \leqslant [F:K]_s$ lorsque le second membre est défini ; appliqué à E(F) considéré comme composé de $E(F_0)$ et de F sur F_0, il montre que $[E(F):E]_i \leqslant [F:K]_i$ lorsque le second membre est défini. Enfin, pour que E et F soient linéairement disjoints sur K, il faut et il suffit que (b_μ) soit une famille linéairement libre par rapport à E ; donc, lorsque $[F:K]$ est défini, la condition $[E(F):E] = [F:K]$ est nécessaire et suffisante pour que E et F soient linéairement disjoints sur K.

COROLLAIRE.- *Soient E et F deux extensions algèbriques de K ; le composé K(E ∪ F) est algèbrique sur K ; la quasi-fermeture algèbrique de K dans K(E ∪ F) est composée des quasi-fermetures algèbriques de K dans E et F respectivement ; on a*

(1) $$\begin{cases} [K(E\cup F):K] \leqslant [E:K]\,[F:K] \\ [K(E\cup F):K]_s \leqslant [E:K]_s\,[F:K]_s \\ [K(E\cup F):K]_i \leqslant [E:K]_i\,[F:K]_i \end{cases}$$

lorsque les seconds membres de ces inégalités sont définis. Enfin lorsque les nombres $[E:K]$ et $[F:K]$ sont définis, la relation $[K(E\cup F):K]=[E:K]\,[F:K]$ est nécessaire et suffisante pour que E et F soient linéairement disjoints sur K .

Comme $K(E\cup F)=E(F)$ est algèbrique sur E , et E algèbrique sur K $K(E\cup F)$ est algèbrique sur K (§2,rpop.7) ; si E_0 (resp. F_0) est la quasi-fermeture algèbrique de K dans E (resp. F), $K(E_0\cup F_0)=E_0(F_0)$ est algèbrique et séparable sur K (§ 4,prop.9) ; d'autre part, d'après la prop.2, tout élément de $K(E\cup F)$ est purement inséparable sur $E(F_0)=F_0(E)$, et tout élément de $F_0(E)$ est purement inséparable sur $F_0(E_0)=K(E_0\cup F_0)$, donc tout élément de $K(E\cup F)$ est purement inséparable sur $K(E_0\cup F_0)$. De là se déduit aussitôt le reste du corollaire, tenant compte de la formule (1) du § 2 et de la prop.2 .

La relation $[E(F):E]_s \leqslant [F:K]_s$ peut encore se déduire directement de la définition du symbole $[E:K]_s$ (§4,déf.6) et de la remarque immédiate suivante : tout isomorphisme de E(F) relatif à E donne, par restriction à F , un isomorphisme de F relatif à K .

2. Corps algèbriquement disjoints.

Proposition 3.- Soient E et F deux extensions de K . S'il existe une base de transcendance B de E sur K qui est algèbriquement libre sur F , toute partie de E (resp? F) algèbriquement libre sur K est algèbriquement libre sur F (resp. E), et $E\cap F$ est une extension algèbrique de K .

En effet, soit M une partie de F algèbriquement libre sur K ; comme B est algèbriquement libre sur E , et a fortiori sur K(M) ,

on a $B \cap M = \emptyset$, et M est algèbriquement libre sur $K(B)$ (§ 2, prop. 10). Comme E est extension algèbrique de $K(B)$, M est aussi algèbriquement libre sur E (§ 2, cor. de la prop. 10). Si on prend en particulier pour M une base de transcendance de F sur K , on voit en permutant les rôles de E et F que toute partie de E , algèbriquement libre sur K , est aussi algèbriquement libre sur F . Enfin, si un élément de $E \cap F$ était transcendant sur K , il formerait une partie de E algèbriquement libre sur K , mais non sur F .

Lorsque les extensions E et F de K satisfont aux conditions de la prop. 3, on dit qu'elles sont algèbriquement disjointes sur K .

COROLLAIRE 1.- Si E et F sont algèbriquement disjoints sur K , les fermetures algèbriques $\bar{E}$ et $\bar{F}$ de E et F sont algèbriquement disjointes sur K .

En effet, une base de transcendance B de E sur K est aussi base de transcendance de $\bar{E}$ sur K ; si elle est algèbriquement libre sur F , elle l'est aussi sur $\bar{F}$ (§ 2, cor. de la prop. 10).

COROLLAIRE 2.- Si la dimension algèbrique de F sur K est finie on a $\dim_E E(F) \leqslant \dim_K F$; pour que E et F soient algèbriquement disjoints sur K , il faut et il suffit que $\dim_E E(F) = \dim_K F$.

En effet, une base de transcendance C de F sur K est telle que $E(F) = E(C)(F)$ soit algèbrique sur $E(C)$, puisque tout élément de F est algèbrique sur $K(C)$, et a fortiori sur $E(C)$; donc C contient une base de transcendance de $E(F)$ sur E , et pour que E et F soient algèbriquement disjoints, il faut et il suffit que C soit une base de transcendance de $E(F)$ sur E .

COROLLAIRE 3.- Si les dimensions algèbriques de E et F sur K sont finies, on a

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

Pour que E et F soient algèbriquement disjoints sur K , il faut et il suffit que $\dim_K K(E \cup F) = \dim_K E + \dim_K F$.

C'est une conséquence immédiate du cor.1 ci-dessus, et de la formule (2) du § 2 .

Proposition 4.- Si E et F sont algèbriquement disjointes sur K , et si F est séparable sur K , E(F) est séparable sur E .

Il suffit de montrer que, pour toute partie finie M de F , E(M) est séparable sur E ; comme $E(M)=E(L)$, où $L=K(M)$, on voit qu'on peut se borner à démontrer la proposition lorsque F est de type fini sur K . En nous bornant à ce cas, soit B une base de transcendance séparante de F sur K (§ 4, prop.22) ; comme B est algèbriquement libre sur E par hypothèse, E(B) est une extension transcendante pure de E , donc séparable sur E (§ 4, prop.21) ; comme tout élément de F est algèbrique et séparable sur K(B) , il est a fortiori algèbrique et séparable sur E(B) , donc E(F) est séparable sur E(B), et par suite (§ 4,prop.9)sur E.

2 Si on ne suppose pas E et F algèbriquement disjoints, E(F) peut ne pas être séparable sur E même lorsque F est séparable sur K . Par exemple, soit x un élément transcendant sur K , a un élément purement inséparable sur K , n'appartenant pas à K ; alors x+a est transcendant sur K , donc E=K(x) et F=K(x+a) sont des extensions transcendantes pures de K , et par suite séparables sur K . Mais E(F) contient a=(x+a)-x , qui est purement inséparable sur E , et n'appartient pas à E , puisque K(a) n'est pas séparable sur K .

COROLLAIRE.- Si E et F sont séparables sur K et algèbriquement disjoints sur K , K(E∪F) est séparable sur K .

En effet, K(E∪F) est séparable sur E , et E séparable sur K . (§ 4, prop.9).

Proposition 5.- Soient E et F deux extensions de K algèbriquement disjointes sur K ; si E est une extension transcendante pure de K , et si L est la fermeture algèbrique de K dans F , E(L) est la fermeture algèbrique de E dans E(F).

Toute base de transcendance de E sur K est aussi une base de transcendance de E(L) sur L , puisque L est algèbrique sur K ; donc E(L) et F sont algèbriquement disjoints sur L , et on peut se borner à considérer le cas où L=K , c'est-à-dire où K est algèbriquement fermé dans F . On a alors E=K(B) , où B est algèbriquement libre sur K , d'où E(F)=F(B) ; si un élément x de F(B) est algèbrique par rapport à K(B) , il existe des parties finies B_1, B_2 de B telles que x appartienne à $F(B_1)$ et soit algèbrique par rapport à $K(B_2)$; il suffit donc de démontrer la proposition lorsque B est fini. Dans ce cas, procédant par récurrence sur le nombre d'éléments de B , on se ramène aussitôt au cas où B se réduit à un seul élément ; autrement dit, on doit démontrer que, si K est algèbriquement fermé dans F , le corps K(X) des fractions rationnelles en X , à coefficients dans K , est algèbriquement fermé dans F(X).

Nous utiliserons pour cela le lemme suivant :

Lemme.- Si $h \in K(X)$ satisfait à une équation de la forme

$$h^n + f_1 h^{n-1} + \ldots + f_n = 0$$

où les f_i sont des polynomes de $K[X]$, on a $h \in K[X]$.

En effet, parmi toutes les expressions de h comme quotient de deux polynomes, soit u/v une expression où le dénominateur a le plus petit degré possible ; montrons que $v \in K$. En effet, dans le cas contraire, v aurait une racine x_0 dans $\overline{K}$; comme on a $u^n + \sum_{k=1}^{n} f_k u^{n-k} v^k = 0$, on a aussi $(u(x_0))^n = 0$, donc $u(x_0) = 0$; mais alors u et v sont divisibles par le polynome minimal φ de x par rapport à K , et on a $h = (u/\varphi)/(v/\varphi)$, contrairement à l'hypothèse faite sur v .

Ce lemme étant démontré, soit w un élément de $F(X)$ algèbrique sur $K(X)$; on a donc une relation de la forme

$$w^n + \sum_{k=1}^{n} u_k w^{n-k} = 0$$

où les $u_k \in K(X)$; posons $u_k = f_k/g$, où les f_k et g appartiennent à $K[X]$; en posant $h = gw$, on a $h^n + \sum_{k=1}^{n} f_k g^{k-1} h^{n-k} = 0$. Comme les $f_k g^{k-1}$ appartiennent à $K[X]$, donc à $F[X]$, le lemme prouve que $h \in F[X]$. Soit donc $h = \sum_{j=0}^{m} a_j X^j$, avec $a_j \in F$ $(0 \leqslant j \leqslant m)$. Tout endomorphisme σ de $\overline{F}$ relatif à K se prolonge d'une seule manière en un endomorphisme de $\overline{F}(X)$ relatif à $K(X)$, laissant invariant X (chap.IV, § , prop.), que nous noterons encore σ. Pour un tel endomorphisme, $\sigma(h)$ est conjugué de h par rapport à $K(X)$; donc, comme $\sigma(h) = \sum_{j=0}^{m} \sigma(a_j) X^j$, les $\sigma(a_j)$ ne peuvent prendre qu'un nombre fini de valeurs pour tous les endomorphismes σ de $\overline{F}$ relatifs à K ; cela entraîne (§ 4, n° 1) que chacun des a_j est algèbrique sur K, donc appartient à K par hypothèse. La proposition est ainsi démontrée.

Lorsqu'on ne suppose pas que E est une extension transcendante pure de K, la prop.5 n'est plus exacte en général (exerc.3). Mais on a la proposition suivante :

Proposition 6.- *Soient* E *et* F *deux extensions de* K *algèbriquement disjointes sur* K ; *si* L *est la quasi-fermeture algèbrique de* K *dans* F $E(L)$ *est la quasi-fermeture algèbrique de* E *dans* $E(F)$.

Comme $E(L)$ et F sont algèbriquement disjoints sur L, on peut se borner au cas où $L = K$, c'est-à-dire où K est algèbriquement quasi-fermé dans F. Soit B une base de transcendance de E sur K, et H la fermeture algèbrique de K dans F ; H est donc purement inséparable sur K. D'après la prop.5, $H(B)$ est la fermeture algèbrique de $K(B)$ dans $F(B)$; or, si un polynome f a ses coefficients purement inséparables sur K, il existe un entier $m \geqslant 0$ tel que la puissance p^m-ème de chacun de ces

de ces coefficients appartienne à K , et par suite f^{p^m} a ses coefficients dans K ; donc H(B) est purement inséparable sur K(B) . Cela étant, soit x un élément de E(F) algébrique sur E donc sur K(B) ; il existe un nombre fini d'éléments u_i $(1 \leqslant i \leqslant n)$ de E tels que x appartienne à l'extension algébrique $F(B)(u_1,u_2,..,u_n)$ de F(B). Soit r un entier tel que les $u_i^{p^r}$ soient tous séparables sur F(B) ; $y=x^{p^r}$ appartient donc à l'extension algébrique séparable $M=F(B)(u_1^{p^r},\ldots,u_n^{p^r})$ de F(B). Soit $(v_j)_{1 \leqslant j \leqslant q}$ une base de M par rapport à F(B) , formée de monômes par rapport aux $u_i^{p^r}$, donc d'éléments de E . On peut écrire $y = \sum_{j=1}^{q} b_j v_j$, où les $b_j \in F(B)$; comme M est séparable sur F(B) , il existe q endomorphismes σ_i $(1 \leqslant i \leqslant q)$ de Ω relatifs à F(B), tels que $\det(\sigma_i(v_j)) \neq 0$ (§ 4, n°4) ; comme on a $\sigma_i(y)= \sum_{j=1}^{q} b_j \sigma_i(v_j)$ pour $1 \leqslant i \leqslant q$, on voit que les b_j s'expriment rationnellement en fonction des $\sigma_i(y)$ et des $\sigma_i(v_j)$; mais comme y et les v_j sont algébriques sur K(B) , et que les σ_i sont des endomorphismes de Ω relatifs à K(B) , les $\sigma_i(y)$ et $\sigma_i(v_j)$ sont algébriques sur K(B) , et il en est de même des b_j . Comme les b_j appartiennent à F(B) , ils sont, d'après ce qu'on a vu plus haut, purement inséparables sur K(B) ; donc il existe un entier $s \geqslant 0$ tel que les $b_j^{p^s}$ appartiennent à K(B) ; on en déduit que $y^{p^s} = \sum_{j=1}^{q} b_j^{p^s} v_j^{p^s}$ appartient à E , puisque les $v_j \in E$; donc x est purement inséparable sur E , ce qui achève la démonstration.

COROLLAIRE.- *Soient E et F deux extensions de K algébriquement disjointes sur K . Si L (resp. M) est la quasi-fermeture algébrique de K dans E (resp. F), K(L∪M) est la quasi-fermeture algébrique de K dans K(E∪F).*

En effet, si $x \in E(F)$ est algébrique et séparable sur K , il est algébrique et séparable sur E , donc appartient à E(M). Comme E et M sont algébriquement disjointes sur K , et que x est algébrique et séparable sur M , il appartient à M(L)=K(L∪M).

2

Remarque.- Les prop. 5 et 6 ne sont plus exactes lorsqu'on ne suppose plus que E et F soient algèbriquement disjoints ; par exemple, si x est transcendant sur K , a algèbrique et séparable sur K et $a \notin K$, et si on prend E=K(x) , F=K(x+a), K est algèbriquement fermé dans E et F (cf.cor.de la prop.8) mais n'est pas algèbriquement quasi-fermé dans K(E F) puisque $a \in K(E \cup F)$.

3. Critères de disjonction linéaire.

La notion d'extensions algèbriquement disjointes peut se rattacher à celle d'extension linéairement disjointes : en effet, si B et C sont des bases de transcendance sur K de deux extensions E , F de K respectivement, dire que $B \cup C$ est algèbriquement libre sur K signifie, comme on le voit aussitôt, que les algèbres $K[B]$ et $K[C]$ sur K sont linéairement disjointes sur K ; la prop.1 montre qu'il revient au même de dire que les extensions transcendantes pures K(B) et K(C) sont linéairement disjointes sur K .

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

D'autre part, si E et F sont linéairement disjointes, la prop.1 montre que le produit tensoriel $E \otimes F$ (relatif à K) est un anneau d'intégrité (dont le corps des quotients est isomorphe à $K(E \cup F)$) ; mais ici encore, cette condition nécessaire n'est pas suffisante pour que E et F soient linéairement disjointes sur K : en effet, supposons par exemple que E et F soient identiques à une même extension transcendante pure K(x) de K ; E et F ne sont pas linéairement disjointes, mais $E \otimes F$ est un anneau d'intégrité, car si y est un élément de Ω

transcendant sur $K(x)$, $K(x)$ et $K(y)$ sont linéairement disjointes, et le produit tensoriel de ces deux corps est isomorphe à $E \otimes F$.

En général, on a le critère suivant :

Proposition 7.- Pour que deux extensions E,F de K soient linéairement disjointes sur K, il faut et il suffit que le produit tensoriel $E \otimes F$ (relatif à K) soit un anneau d'intégrité, et que E et F soient algèbriquement disjointes sur K. Le corps composé $K(E \cup F)$ est alors isomorphe au corps des quotients de l'anneau d'intégrité $E \otimes F$.

Nous venons de voir que les conditions sont nécessaires. Prouvons qu'elles sont suffisantes. On sait (prop.1) que, si C est le plus petit sous-anneau de Ω contenant $E \cup F$, il existe une représentation φ de l'anneau $M=E \otimes F$ sur C, telle que $\varphi(x \otimes y)=xy$; il nous suffira de montrer que φ est un isomorphisme.

Soit A (resp. B) une base de transcendance de E (resp. F) sur K ; comme E et F sont algèbriquement disjoints, $K(A)$ et $K(B)$ sont linéairement disjoints sur K, et par suite, l'application φ, restreinte au sous-anneau $N=K(A) \otimes K(B)$ de M, est un isomorphisme de N dans C. Soit P le corps des quotients de M, $Q \subset P$ le corps des quotients de N ; P est une extension algèbrique de Q ; en effet, tout élément de $E'=E \otimes \{1\}$ est algèbrique sur $K(A) \otimes \{1\}$, donc a fortiori sur Q ; de même tout élément de $F'=\{1\} \otimes F$ est algèbrique sur Q ; comme tout élément de M est somme de produits d'un élément de E' et d'un élément de F', il est algèbrique sur Q, et il en est donc de même de tout élément de P. Soit alors z un élément de M tel que $\varphi(z)=0$, et soit $f(X)=X^n+\sum_{i=1}^{n} u_i X^{n-i}$ son polynome minimal sur Q ; on peut écrire $u_i=v_i/w$, où les v_i et w appartiennent à M ; on a donc $wz^n+\sum_{i=1}^{n} v_i z^{n-i}=0$; de la relation $\varphi(z)=0$ on déduit donc $\varphi(v_n)=0$.

Mais φ , restreinte à M est un isomorphisme, donc $v_n=0$, et $f(X)$ est divisible par X ; comme il est minimal, il est identique à X , ce qui prouve que $z=0$, et achève la démonstration.

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

En effet, $\sigma(E) \otimes \tau(F)$ est isomorphe à $E \otimes F$, donc est un anneau d'intégrité ; la prop.7 prouve alors que $\sigma(E)$ et $\tau(F)$ sont linéairement disjointes sur K . L'existence de l'endomorphisme φ résulte de la prop. du chap.III; § .

Proposition 8.- Soient E et F deux extensions de K , algèbriquement disjointes sur K . Si E est une extension transcendante pure de K , E et F sont linéairement disjointes sur K .

Soit B une partie de E algèbriquement libre sur K et telle que $E=K(B)$; E est le corps des quotients de $K[B]$, et d'après la prop.1, il suffit de montrer que F et $K[B]$ sont linéairement disjointes sur K . Or B est algèbriquement libre sur F ; cela signifie que les monômes par rapport aux éléments de B sont linéairement indépendants sur F ; comme ces monômes forment une base de $K[B]$ sur K , $K[B]$ et F sont linéairement disjointes sur K .

COROLLAIRE.- Si E est une extension transcendante pure de K , tout élément de E n'appartenant pas à K est transcendent sur K .

En effet, E est linéairement disjoint de toute extension algèbrique de K d'après la prop.8 , donc son intersection avec une telle extension se réduit à K .

Proposition 9.- Soient E et F deux extensions de K , algébriquement disjointes sur K . Si E est séparable sur K , et si K est algébriquement quasi-fermé dans F , E et F sont linéairement disjointes sur K .

Soit A une partie de E linéairement libre sur K , et supposons qu'elle ne soit pas linéairement libre sur F . Il existe donc au moins une relation linéaire primordiale (chap.II, § 5, n°5) $\sum_{i=1}^{n} w_i x_i = 0$ entre des éléments distincts x_i de A , les coefficients w_i appartenant à F, aucun de ces coefficients n'étant nul ; on peut supposer en outre que $w_m = 1$. Comme les w_i n'appartiennent pas tous à K , le corps $L = K(w_1, .., w_m)$ est contenu dans F et non identique à K ; d'après l'hypothèse, L n'est donc pas une extension algébrique séparable de K . Il en résulte (§ 4, th.3) qu'il existe une dérivation D de L relative à K , non identiquement nulle et prenant ses valeurs dans F ; les éléments Dw_i ne peuvent évidemment être tous nuls. Considérons alors le sous-corps $M = K(x_1, x_2, .., x_m)$ de E ; il est séparable sur K ; soit B une base de transcendance séparante de M sur K , formée d'un certain nombre des x_i (§ 4, prop.22) ; B est algébriquement libre par rapport à F d'après l'hypothèse ; a fortiori, elle est algébriquement libre sur L , donc (§ 4, prop.24) la dérivation D de L peut se prolonger en une dérivation de L(B), que nous noterons encore D telle que $Dy = 0$ pour tout $y \in B$. M est une extension algébrique séparable de K(B) , donc a fortiori de L(B) ; D peut donc encore se prolonger en une dérivation de L(M) , que nous notons toujours D . Comme D est nulle dans K(B) , et que M est algébrique et séparable sur K(B) , D est nulle dans M (§ 4, th.3) ; en particulier, $Dx_i = 0$ pour $1 \leqslant i \leqslant m$. Cela étant, la relation $D(\sum_{i=1}^{m} w_i x_i) = 0$ s'écrit $\sum_{i=1}^{m} Dw_i . x_i = 0$;

les Dw_i ne sont pas tous nuls, mais $Dw_m=0$, ce qui contredit l'hypothèse que la relation $\sum_{i=1}^{m} w_i x_i=0$ est primordiale (chap.II, 5,prop.2). La proposition est donc démontrée.

Théorème 1.- Soient E et F deux extensions de K , dont l'une au moins est séparable sur K . Pour que E et F soient linéairement disjointes sur K , il faut et il suffit qu'elles soient algèbriquement disjointes sur K , et que les quasi-fermetures algèbriques $K_s \cap E$ et $K_s \cap F$ de K dans E et F soient linéairement disjointes sur K .

Les conditions de l'énoncé sont évidemment nécessaires ; prouvons qu'elles sont suffisantes. Supposons que E soit séparable sur K , et posons $L=K_s \cap E$, $M=K_s \cap F$. Pour voir que E et F sont linéairement disjoints sur K , il suffit de prouver (fig.1) d'une part que F et E(M) sont linéairement disjoints sur M , de l'autre que E et M sont linéairement disjoints sur K (chap.III, § 2,prop.6). Or, comme E(M) est une extension algèbrique de E , E(M) et F sont algèbriquement disjoints sur M ; M est algèbriquement quasi-fermé dans F par définition ; enfin, E(M) est une extension séparable de E , puisque tout élément de M est algèbrique et séparable sur K , et a fortiori sur E ; ~~puisque tout élément~~ donc (§ 4,prop.9) E(M) est une extension séparable de K ; comme M est algèbrique sur K , E(M) est aussi une extension séparable de M (§ 4,prop.15). La prop.9 montre donc que F et E(M) sont linéairement disjoints sur M .

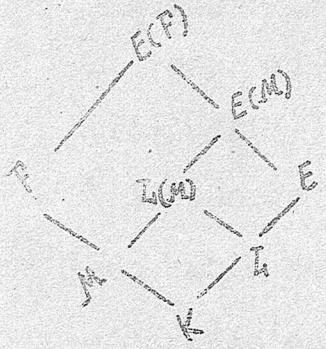

fig. 1

Montrons maintenant que M et E sont linéairement disjoints sur K ; comme par hypothèse L et M sont linéairement disjoints sur K , il suffit de prouver que E et L(M) sont linéairement disjoints sur L .

Or, L(M) est algèbrique sur L , donc algèbriquement disjointe de E sur L ; L(M) est séparable sur L puisque M est algèbrique et séparable sur K ; enfin, L est algèbriquement quasi-fermé dans E par définition. La prop.9 s'applique de nouveau, et montre que E et L(M) sont linéairement disjointes sur L . C.Q.F.D.

2 Les conditions de l'énoncé ne sont plus suffisantes lorsqu'on ne suppose plus que l'une au moins des extensions E,F est séparable sur K (exerc. 4).

Proposition 10.- Soient E et F deux extensions de K , algèbriquement disjointes sur K , et dont l'une au moins est séparable sur K . Si L (resp. M) est la fermeture algèbrique de K dans E (resp. F), F(L) (resp. E(M)) est la fermeture algèbrique de F (resp. E) dans E(F)=F(E).

Supposons par exemple que E soit séparable sur K . Alors F(E) est séparable sur F (prop.4) ; comme F(L) est algèbrique sur F , F(E) est séparable sur F(L) (§ 4,prop.15). Or, comme E est séparable sur L (§ 4,prop.15), L est la quasi-fermeture algèbrique de K dans E , donc (prop.6) F(L) est la quasi-fermeture algèbrique de F dans F(E) ; puisque F(E) est séparable sur F(L) , F(L) est aussi la fermeture algèbrique de F dans F(E) .

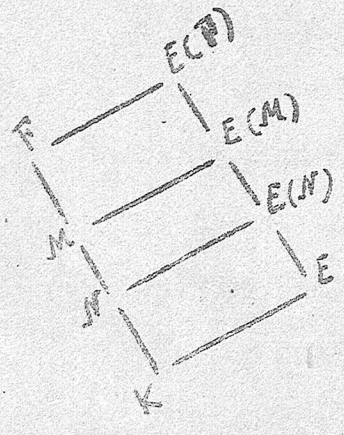

fig. 2

Soit maintenant $N \subset M$ la quasi-fermeture algèbrique de K dans F (fig.2) ; N étant algèbrique et séparable sur K , E(N) est algèbrique et séparable sur E , donc sur K (§ 4,prop.9), et par suite sur N (§ 4,prop.15) ; comme E(N) et F sont algèbriquement disjoints sur N , et que N est algèbriquement quasi-fermé dans F , F et E(N) sont linéairement disjoints sur N (prop.9) . En outre, E(N) est la quasi-fermeture algèbrique de E dans E(F) (prop.6).

Soit alors x un élément de E(F) algébrique sur E ; il est purement inséparable sur E(M) , donc il existe un entier $r \geqslant 0$ tel que $x^{p^r} \in E(M)$. Soit (b_μ) une base de E(M) sur M ; x peut s'écrire d'une manière sous la forme $x = \sum_\mu a_\mu b_\mu$, où les $a_\mu \in F$; on a donc $\sum_\mu a_\mu^{p^r} b_\mu^{p^r} \in E(M)$. Or, les $b_\mu^{p^r}$ sont linéairement indépendants par rapport à M , puisque E(M) est séparable sur M ; comme E(M) et F sont linéairement disjoints sur M , une combinaison linéaire des $b_\mu^{p^r}$ à coefficients dans F ne peut appartenir à E(M) que si ces coefficients appartiennent à M ; on a donc $a_\mu^{p^r} \in M$, donc $a_\mu \in M$ pour tout indice μ , ce qui prouve que $x \in E(M)$.

COROLLAIRE.- Le corps K(L∪M) , composé de L et M , est la fermeture algébrique de K dans K(E∪F).

En effet, si $x \in E(F)$ est algébrique sur K , il est algébrique sur E , donc appartient à E(M) ; comme E et M sont algébriquement disjoints sur K et que E est séparable sur K , x , qui est algébrique sur K , et a fortiori sur M , appartient à M(L)=K(L∪M) d'après la prop.10.

4. Extensions régulières.

Définition 1.- On dit qu'une extension E de K est régulière sur K (ou est une extension régulière de K) si E et la fermeture algébrique K̄ de K dans Ω sont linéairement disjointes sur K .

Il est clair que si E est une extension régulière de K , toute extension F de K contenue dans E est régulière sur K . Inversement, si S est un système de générateurs de E sur K , et si pour toute partie finie M de S , K(M) est une extension régulière de K , E est une extension régulière de K .

Il est clair que toute extension de K̄ est régulière sur K̄ . Toute extension transcendante pure de K est régulière sur K d'après la prop. 8 .

Proposition 11.- Pour qu'une extension E de K soit régulière sur K , il faut et il suffit que E soit séparable sur K et que K soit algébriquement fermé dans E .

En effet, si E et $\bar{K}$ sont linéairement disjoints sur K , il en est de même a fortiori de E et $K^{p^{-\infty}}$, donc (§ 4,prop.8), E est séparable sur K ; en outre $E \cap \bar{K} = K$, donc K est algébriquement fermé dans E . Réciproquement, si ces deux conditions sont vérifiées, E et $\bar{K}$ sont algébriquement disjointes sur K ; comme la quasi-fermeture algébrique de K dans E est K (puisque E est séparable), elle est linéairement disjointe sur K de la quasi-fermeture algébrique de K dans $\bar{K}$; donc E et $\bar{K}$ sont linéairement disjoints en vertu du th.1 .

Proposition 12.- Si E est une extension régulière de K , et F une extension régulière de E , F est une extension régulière de K .

En effet, F est séparable sur K (§ 4,prop.9), et comme $\bar{K} \subset \bar{E}$, K est algébriquement fermé dans F .

Proposition 13.- Soient E et F deux extensions de K , algébriquement disjointes sur K .

a) Si F est régulière sur K , E et F sont linéairement disjoints sur K et E(F) est régulière sur E .

b) Inversement, si E(F) est régulière sur E , et si E et F sont linéairement disjointes sur K , F est régulière sur K .

c) Si E et F sont régulières sur K , K(E∪F) est régulière sur K .

a) Si F est régulière sur K , les quasi-fermetures algébriques de K dans E et F sont linéairement disjointes sur K , donc, d'après le th.1, il en est de même de E et F ; E(F) est séparable sur E (prop. 4), et la fermeture algébrique de E dans E(F) est égale à E (prop.10) ; donc E(F) est régulière sur E .

b) Si $E(F)$ est régulière sur E, $E(F)$ et $\bar{E}$ sont linéairement disjoints sur E ; si en outre E et F sont linéairement disjoints sur K, $\bar{E}$ et F sont linéairement disjoints sur K (chap.III, § 2, prop.6), et a fortiori F et $\bar{K}$ sont linéairement disjoints sur K.

c) Si E et F sont régulières sur K, $E(F)$ est régulière sur E, donc, d'après la prop. 12, $E(F)$ est régulière sur K.

Exercices.- 1) Soient E et F deux extensions de K.

a) Si B est une p-base de E sur K, C une p-base de F sur K montrer que $B \cup C$ contient une p-base de $K(E \cup F)$ sur K. En particulier, si E et F ont des degrés d'imperfection finis sur K, le degré d'imperfection de $K(E \cup F)$ sur K est au plus égal à la somme des degrés d'imperfection de E et F.

b) Si E et F sont linéairement disjoints sur K, montrer que $B \cup C$ est une p-base de $K(E \cup F)$ sur K.

2) Soient $E = \mathbb{R}(X)$, $F = \mathbb{R}(X+1)$ deux extensions transcendantes pures du corps des nombres réels $\mathbb{R}$. Montrer que E et F ne sont pas algébriquement disjoints sur $\mathbb{R}$, mais que $E \cap F = \mathbb{R}$ montrer qu'une relation telle que $p(X+1)s(X) = q(X+1)r(X)$, où p/q et r/s sont deux fractions rationnelles irréductibles à coefficients réels, est impossible, en décomposant les deux membres dans $\mathbb{C}[X]$.

3) Soit P un corps de caractéristique $p > 0$, $K = P(X,Y)$ un corps de fractions rationnelles à deux indéterminées sur P. Soit $E = K(U, (X+YU^p)^{1/p})$, $F = K(V, (X+YV^p)^{1/p})$ où U et V sont deux indéterminées sur K. Montrer que E et F sont linéairement disjoints sur K, que K est algébriquement fermé dans E et dans F, mais non dans $K(E \cup F)$ (pour voir que E et F sont linéairement disjoints sur K, montrer que $(X+YV^p)^{1/p}$ n'appartient pas à $E(V)$; pour voir que K est algébriquement fermé dans E, montrer que si $x \in E$ et $x^p \in K$, on a $x \in K$).

4) Soit P un corps de caractéristique $p>0$, $K=P(X,Y,Z,T)$ un corps de fractions rationnelles à quatre indéterminées sur P . Soient U_1,V_1,U_2,V_2 quatre indéterminées sur K ; on considère les corps $E=K(U_1,V_1,(XU_1^p+YV_1^p)^{1/p},(ZU_1^p+TV_1^p)^{1/p})$ et $F=K(U_2,V_2,(XU_2^p+ZV_2^p)^{1/p}$, $(YU_2^p+TV_2^p)^{1/p})$. Montrer que E et F sont algèbriquement disjoints sur K , que K est algèbriquement fermé dans E et dans F , mais que E et F ne sont pas linéairement disjoints sur K .

5) Soient E et F deux extensions de K , L un sous-corps de E contenant K . Pour que E et F soient algèbriquement disjointes sur K , il faut et il suffit que L et F soient algèbriquement disjointes sur K , et que E et L(F) soient algèbriquement disjointes sur L .

6) Soient E et F deux extensions de K algèbriquement disjointes sur K ; soit L (resp. M) la quasi-fermeture algèbrique de K dans E (resp. F). Soit σ(resp. τ) un isomorphisme de E (resp. F) relatif à K sur un sous-corps E' (resp. F') de Ω , tels que E' et F' soient algèbriquement disjoints sur K . S'il existe un isomorphisme φ de $K(L \cup M)$ sur $K(\sigma(L) \cup \tau(M))$, qui coïncide avec σ sur L et avec τ sur M , montrer qu'il existe un isomorphisme de $K(E \cup F)$ sur $K(E' \cup F')$ prolongeant φ , coïncidant avec σ sur E et avec τ sur F . (Se ramener au cas particulier où K=L , en utilisant la prop. 9 . Ordonner alors par prolongement l'ensemble $\mathfrak{F}$ des isomorphismes ψ définis sur un E(Z) , où $Z \supset K$ est un sous-corps variable de F , qui coïncident avec σ sur E et avec τ sur Z . En utilisant le th. de Zorn, se ramener aux trois cas suivants: a) F est une extension transcendante simple de K ; b) $F=K(\theta)$, où θ est algèbrique et séparable sur K ; c) $F=K(\theta)$, où $\theta^p \in K$. Dans les deux premiers cas, on utilisera le th.1 .)

7) Soit E une extension non séparable de K . Montrer qu'il existe une extension F de K , de degré fini, contenue dans $K^{1/p}$, telle que l'intersection de $K^{1/p}$ et de $K(E \cup F)$ soit distincte de F (considérer dans $K^{1/p}$ une famille de m éléments p-indépendante sur K , p-dépendante sur E , et telle que m-1 des éléments de cette famille soient p-indépendants sur E).

8) Soient x,y deux racines distinctes d'un polynome irréductible $f \in K[X]$. Montrer que les extensions K(x) et K(y) ne sont pas linéairement disjointes sur K . Donner un exemple où $K(x) \cap K(y) = K$.

§ 6. Extensions normales. Théorie de Galois.

1. Extensions normales. Extensions galoisiennes.

Proposition 1.- Si E est une extension algébrique de K , tout endomorphisme de E relatif à K est un automorphisme de E .

En effet, soit u un endomorphisme de E relatif à K ; montrons que $u(E)=E$. Pour tout $x \in E$, soit F_x l'ensemble des conjugués de x (par rapport à K) qui appartiennent à E ; F_x est un ensemble fini pour tout $x \in E$, et E est la réunion des F_x lorsque x parcourt E . Or, pour tout $y \in F_x$, u(y) est conjugué de y , donc de x , et appartient à E par hypothèse ; on a donc $u(F_x) \subset F_x$, et comme u est biunivoque, $u(F_x)=F_x$, puisque F_x est fini ; d'où la proposition.

COROLLAIRE 1.- Pour que tout isomorphisme de $E \subset \Omega$ relatif à K soit un automorphisme de E , il faut et il suffit que, pour tout $x \in E$, tous les conjugués de x par rapport à K appartiennent à E .

La condition est nécessaire, car tout conjugué de x est transformé de x par un isomorphisme de E relatif à K (§ 4, prop.2). Réciproquement, la condition est suffisante, car pour tout isomorphisme u de E relatif à K et tout $x \in E$, u(x) étant conjugué de x appartient à E , d'où $u(E) \subset E$.

COROLLAIRE 2.- Pour que tout isomorphisme de $E \subset \Omega$ relatif à K soit un automorphisme de E, il faut et il suffit que tout polynome irréductible $f \in K[X]$ qui admet une racine dans E se décompose en un produit de facteurs du premier degré dans $E[X]$.

En effet, cette condition est équivalente à celle du cor.1 .

Définition 1.- On dit qu'une extension N d'un corps K est normale sur K si elle est algèbrique sur K et si tout polynome irréductible $f \in K[X]$ qui admet une racine dans N se décompose en un produit de facteurs du premier degré dans $N[X]$.

Cette définition est indépendante du corps algèbriquement fermé Ω dans lequel N est plongé. Mais le cor.2 de la prop.1 montre que, pour qu'une extension algèbrique $N \subset \Omega$ de K soit normale sur K , il faut et il suffit que tout isomorphisme de N relatif à K soit un automorphisme de N .

Définition 2.- On dit qu'une extension N d'un corps K est galoisienne sur K si elle est normale et séparable sur K .

Il est clair que K est une extension galoisienne de lui-même ; la fermeture algèbrique $\bar{K}$ de K dans Ω est une extension normale de K (§ 4, prop.10).

Si N est une extension normale de K , et E une extension de K contenue dans N , tout isomorphisme de N relatif à E est a fortiori un isomorphisme de N relatif à K , donc N est une extension normale de E .

On notera par contre que si E est une extension normale de K et F une extension normale de E , F n'est pas nécessairement une extension normale de K (cf. exerc. 2).

Proposition 2.- Soient K,K' deux corps isomorphes, φ_0 un isomorphisme de K sur K' . Soient Ω une extension algèbriquement fermée de K , Ω' une extension algèbriquement fermée de K' . Si N est une extension normale de K contenue dans Ω , φ et ψ deux isomorphismes de N

dans Ω' prolongeant φ_0, on a $\varphi(M)=\psi(M)$; le corps $M'=\varphi(M)=\psi(M)$ est une extension normale de K' ; il existe un automorphisme σ de M relatif à K et un automorphisme σ' de M' relatif à K' , tels que $\psi=\varphi\circ\sigma=\sigma'\circ\varphi$.

La déf.1 montre que $\varphi(M)$ et $\psi(M)$ sont des extensions normales de K' ; comme $\psi\circ\varphi^{-1}$ est un isomorphisme de $\varphi(M)$ sur $\psi(M)$, relatif à K' , on a $\varphi(M)=\psi(M)$; enfin, il est clair que $\varphi^{-1}\circ\psi$ est un automorphisme de M .

Proposition 3.- Soit (M_ι) une famille d'extensions normales d'un corps K , contenues dans Ω ; l'intersection $\bigcap_\iota M_\iota$ et le corps $K(\bigcup_\iota M_\iota)$ engendré par la réunion des M_ι sont des extensions normales de K .

En effet, soit f un endomorphisme quelconque de Ω ; par hypothèse, on a $f(M_\iota)\subset M_\iota$ pour tout ι , donc si $M=\bigcap_\iota M_\iota$, on a $f(M)\subset M_\iota$ pour tout ι , d'où $f(M)\subset M$, M est normale sur K ; d'autre part, si $M=K(\bigcup_\iota M_\iota)$, f(M) est engendré par la réunion des $f(M_\iota)=M_\iota$, donc est identique à M .

De la prop.3 on déduit en particulier que si E est une extension algébrique quelconque de K , il existe une plus petite extension M de E , normale sur K , savoir l'intersection des extensions normales de K contenant M (il en existe, par exemple $\bar{K}$) ; nous dirons que M est l'extension normale de K engendrée par l'extension E .

Proposition 4.- Soit A un ensemble d'éléments de Ω , algébriques sur A , et soit B l'ensemble de tous les éléments de Ω conjugués des éléments de A par rapport à K . Le corps K(B) est l'extension normale de K engendrée par K(A) .

En effet, pour tout endomorphisme u de Ω relatif à K , on a $u(B)\subset B$, donc $u(K(B))\subset K(B)$, ce qui montre que K(B) est normale

sur K ; d'après le cor. de la prop.2, toute extension de K(A) normale sur K contient B , donc K(B) est l'extension normale de K engendrée par K(A) .

COROLLAIRE 1.- Si E est une extension algèbrique de degré fini de K , l'extension normale N de K engendrée par E est de degré fini sur K ; si en outre E est séparable sur K , il en est de même de N .

En effet, on a E=K(A) , où A est un ensemble fini ; l'ensemble B des conjugués des éléments de A étant fini, K(B)=N est de degré fini sur K . En outre, si les éléments de A sont séparables sur K , il en est de même de leurs conjugués par rapport à K , donc (§ 4,prop.18) N est séparable sur K .

COROLLAIRE 2.- Si (f_ι) est une famille de polynomes de $K[X]$, A l'ensemble des racines de tous les f_ι dans Ω , K(A) est une extension normale de K .

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

En particulier, si f est un polynome quelconque (irréductible ou non) de $K[X]$, $x_1,x_2,..,x_n$ ses racines distinctes dans Ω , le corps $N=K(x_1,x_2,..,x_n)$ est une extension normale de K , qu'on appelle le corps des racines du polynome f ; dans l'anneau $N[X]$, f est égal à un produit de facteurs du premier degré (distincts ou non).

On notera qu'en général, même si f est irréductible dans $K[X]$, le corps $K(x_1)$ obtenu par adjonction à K d'une racine x_1 de f dans Ω , n'est pas identique au corps des racines de f (exerc.2). Lorsque f est irréductible dans $K[X]$, et que $K(x_1)$ est identique au corps des racines de f pour une racine x_1 , on a $K(x_j)=K(x_1)$ pour toute autre racine x_j de f , puisque $K(x_j)$ est transformé de $K(x_1)$ par un endomorphisme de Ω relatif à K . On dit dans ce cas que l'équation $f(x)=0$ est une équation normale (sur K) ;

si en outre le corps des racines de f est séparable sur K, on dit que $f(x)=0$ est une équation galoisienne sur K.

Proposition 5.- *Soit N une extension normale de K, E une extension de K contenue dans N. Tout isomorphisme de E relatif à K peut se prolonger en un automorphisme de N.*

En effet, un isomorphisme f de E relatif à K peut être prolongé en un endomorphisme $\bar{f}$ de Ω ; la restriction de $\bar{f}$ à N est un automorphisme de N, qui prolonge f.

2. Groupe de Galois d'une extension normale.

Définition 3.- *Etant donnée une extension normale N d'un corps K, on appelle groupe de Galois* (ou simplement *groupe*) *de N relatif à K le groupe des automorphismes de N relatifs à K.*

Soit f un polynome (irréductible ou non) de $K[X]$, x_i $(1\leqslant i\leqslant n)$ ses racines distinctes dans Ω, $N=K(x_1,x_2,\dots,x_n)$ le corps des racines de f. Tout automorphisme σ de N relatif à K, restreint à l'ensemble $\{x_1,x_2,\dots,x_n\}$, est une permutation de cet ensemble; et réciproquement, lorsque l'on connaît $\sigma(x_i)$ pour $1\leqslant i\leqslant n$, $\sigma(x)$ est déterminé pour tout élément x de N (§ 2, cor. de la prop.5). Par suite, le groupe Γ de N est isomorphe au groupe des permutations des x_i, formé des restrictions des automorphismes $\sigma\in\Gamma$ à l'ensemble des x_i ; il est donc isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}_n$ (mais en général il n'est pas isomorphe à $\mathfrak{S}_n$ lui-même ; autrement dit, une permutation arbitraire des x_i n'est pas en général la restriction d'un automorphisme de N)

Proposition 6.- *Soit N une extension normale de K, Γ son groupe par rapport à K. L'ensemble des éléments de N invariants par tous les automorphismes de Γ est la plus grande extension purement inséparable $\tilde{N}=N\cap K^{p^{-\infty}}$ de K contenue dans N ; et tout automorphisme de N relatif à K est un automorphisme de N relatif à $\tilde{N}$.*

En effet, la restriction à N d'un endomorphisme de Ω relatif à K est un automorphisme de N relatif à K , et réciproquement un tel automorphisme est restriction d'un endomorphisme de Ω (§ 4, prop. 1) ; la première partie de la proposition résulte donc de la définition des éléments purement inséparables sur K ; la seconde partie est évidente.

COROLLAIRE.- Si N est une extension galoisienne de K , tout élément de N invariant par tous les automorphismes du groupe de Galois de N (relatif à K) appartient à K .

Lorsque N est une extension normale quelconque de K , on peut identifier le groupe de Galois de N relatif à K au groupe de Galois de N relatif à $\tilde{N}$.

Proposition 7. Soit N une extension normale de K . La plus grande extension séparable N_0 de K contenue dans N (quasi-fermeture algébrique de K dans N) est une extension galoisienne de K ; tout automorphisme de N_0 relatif à K se prolonge d'une manière et d'une seule en un automorphisme de N ; les corps N_0 et $\tilde{N} = N \cap K^{p^{-\infty}}$ sont linéairement disjoints sur K , et N est leur composé.

En effet, pour tout endomorphisme σ de Ω relatif à K , et tout élément $x \in N_0$, $\sigma(x)$ est séparable sur K et appartient à N , donc $\sigma(x) \in N_0$, ce qui montre que N_0 est normale (et par suite galoisienne) sur K ; comme N est purement inséparable sur N_0 , tout automorphisme de N_0 se prolonge d'une seule manière en un isomorphisme de N , qui est nécessairement un automorphisme de N (§ 4, n°2) ; en particulier, on voit que l'application du groupe de Galois Γ de N sur le groupe de Galois Γ_0 de N_0 qui, à tout $\sigma \in \Gamma$, fait correspondre sa restriction à N_0 , est un isomorphisme de Γ sur Γ_0 . Comme N_0 est linéairement

disjoint de $K^{p^{-\infty}}$ sur K (§ 4, prop.8), il est a fortiori linéairement disjoint de $\widetilde{M}=K^{p^{-\infty}}\cap M$. Reste à montrer que $M=K(M_0\cup\widetilde{M})$. Pour cela, on peut se limiter au cas où M est de degré fini sur K . En effet, si M est une extension normale quelconque de K , x un élément de M , il existe une extension normale M de K , contenant x , contenue dans M et de degré fini sur K , par exemple l'extension normale engendrée par K(x) ; si nous prouvons que $x\in K(\widetilde{M}\cup M_0)$, on aura a fortiori $x\in K(\widetilde{M}\cup M_0)$, puisque $\widetilde{M}\subset\widetilde{M}$ et $M_0\subset M_0$.

Or, tout élément x de M est séparable par rapport à $\widetilde{M}$, car, si x_i $(1\leqslant i\leqslant m)$ sont les conjugués distincts de x , relatifs à K, le polynome $f=\prod_{i=1}^{m}(X-x_i)$ est invariant par tout automorphisme de M relatif à K et par suite (prop.6) a ses coefficients dans $\widetilde{M}$; comme $f(x)=0$, et que f a toutes ses racines simples, le polynome minimal de x par rapport à $\widetilde{M}$ n'a que des racines simples, ce qui montre que x est séparable sur $\widetilde{M}$. Cela étant, si M est de degré fini sur K , et a fortiori sur $\widetilde{M}$, on a $[M:\widetilde{M}]=[M:\widetilde{M}]_s$ d'après ce qui précède ; or, $[M:\widetilde{M}]_s$ est égal à l'ordre du groupe de Galois de M sur K (prop.6) , donc égal à l'ordre du groupe de Galois de M_0 sur K , isomorphe au précédent ; on a donc $[M:\widetilde{M}]=[M_0:K]$. Comme $[K(\widetilde{M}\cup M_0):\widetilde{M}]=[M_0:K]$ (§ 5, prop.2), on a $K(\widetilde{M}\cup M_0)=M$.

<u>Théorème 1.- Soit M une extension galoisienne de K , E une extension quelconque de K</u> (contenue dans Ω). <u>Les corps E et M sont linéairement disjoints sur</u> $E\cap M$; <u>E(M) est une extension galoisienne de M , et tout automorphisme de M relatif à</u> $E\cap M$ <u>se prolonge d'une seule manière en un automorphisme de E(M) relatif à M</u> .

On peut évidemment se borner au cas où $E\cap M=K$, ce que nous supposerons dans la suite de la démonstration.

Lemme.- Lorsque $E \cap N = K$, on a , pour tout $x \in N$, $\left[E(x) : E\right] = \left[K(x) : K\right]$ et $E(x) \cap N = K(x)$.

En effet, soient x_i $(1 \leqslant i \leqslant m)$ les conjugués de x par rapport à E (tous distincts, puisque x est séparable sur K , et a fortiori sur E); les x_i sont transformés de x par des endomorphismes de Ω relatifs à E (donc à K) et par suite sont conjugués de x par rapport à K ; ils appartiennent donc à N . Le polynome minimal $f(X) = \prod_{i=1}^{m} (X - x_i)$ de x par rapport à E a donc ses coefficients dans $E \cap N = K$ et comme il divise le polynome minimal de x par rapport à K , il est identique à ce dernier, ce qui prouve que x a même degré m sur K et sur E .

D'autre part, il est évident que $E(x) \cap N \supset K(x)$. Inversement, montrons que si $y \in E(x) \cap N$, on a $y \in K(x)$. On peut écrire par hypothèse $y = \sum_{k=0}^{m-1} a_k x^k$, où les a_k appartiennent à E ; les éléments $y_i = \sum_{k=0}^{m-1} a_k x_i^k$ $(1 \leqslant i \leqslant m)$ sont donc transformés de y par les m isomorphismes distincts de $E(x)$ relatifs à E , autrement dit, sont conjugués de y par rapport à E , et a fortiori par rapport à K ; comme $y \in N$, on a aussi $y_i \in N$ pour $1 \leqslant i \leqslant m$. Mais alors, dans les m équations linéaires $y_i = \sum_{k=0}^{m-1} a_k x_i^k$ $(1 \leqslant i \leqslant m)$ par rapport aux a_k , les coefficients et les seconds membres appartiennent à N ; comme le déterminant du système est le déterminant de Vandermonde $V(x_1, x_2, \ldots, x_m) = \prod_{i<j} (x_j - x_i) \neq 0$, le système a une seule solution, qui est nécessairement formée d'éléments de N ; les a_k appartiennent donc à $E \cap N = K$, d'où $y \in K(x)$.

Ce lemme étant démontré, le théorème 1 sera établi si nous le démontrons lorsque N est de degré fini sur K . En effet, pour prouver qu'une famille finie $(x_i)_{1 \leqslant i \leqslant n}$ d'éléments de N , linéairement libre sur K , est aussi linéairement libre sur E , il suffit de voir que l'extension normale M de K , engendrée par $x_1, x_2, \ldots, x_n$, est linéairement disjointe de E par rapport à K .

Supposons donc que $N=K(a_1,a_2,..,a_m)$, et démontrons par récurrence sur h que $K(a_1,a_2,..,a_h)$ est linéairement disjoint de E par rapport à K et que $E(a_1,a_2,..,a_h)\cap N = K(a_1,a_2,..,a_h)$. La proposition est évidente pour $h=0$; supposons la vraie pour le corps $L=K(a_1,a_2,..,a_{h-1})$; d'après le lemme, on a $\left[L(a_h):L\right]=\left[E(L)(a_h):E(L)\right]$, et $E(L)(a_h)\cap N = L(a_h)$. Or la première de ces relations prouve que $L(a_h)=K(a_1,a_2,...a_h)$ et $E(L)=E(a_1,a_2,..,a_{h-1})$ sont linéairement disjoints sur L (§ 5, prop.2) ; par suite $L(a_h)$ et E sont linéairement disjoints sur K , puisque, par l'hypothèse de récurrence E et L sont linéairement disjoints sur K (chap. III, § 2, prop.6). D'autre part, on a $E(a_1,a_2,..,a_h)=E(L)(a_h)$, ce qui achève la démonstration par récurrence.

Comme N et E sont linéairement disjoints sur K et N séparable sur K , E(N) est séparable sur E (§ 5, prop.2), et tout automorphisme σ de N relatif à K se prolonge d'une seule manière en un isomorphisme de E(N) relatif à E (§ 5, cor.de la prop.7), qui applique E(N) dans $E(\sigma(N))=E(N)$; ce qui achève la démonstration.

COROLLAIRE 1.- Soit N une extension normale de K , E une extension quelconque de K (contenue dans Ω) ; E(N) est une extension normale de E , et tout automorphisme de N relatif à $E\cap N$ se prolonge d'une seule manière en un automorphisme de E(N) relatif à E .

On peut encore se borner au cas où $E\cap N=K$. Soit N_0 la quasi-fermeture algébrique de K dans N ; N_0 est une extension galoisienne de K (prop.7) et $E\cap N_0=K$, donc $E(N_0)$ est une extension galoisienne de E et tout automorphisme de N_0 relatif à K se prolonge d'une seule manière en un automorphisme de $E(N_0)$ relatif à E (th.1). Cela étant, tout automorphisme σ de N relatif à K , restreint à N_0 , est un automorphisme de N_0 ; soit $\bar{\sigma}$ l'automorphisme de $E(N_0)$ (relatif à E) qui prolonge la restriction de σ à N_0 ; comme $E(N_0)$ est la quasi-fermeture

algèbrique de E dans E(N) , $\bar{\sigma}$ se prolonge d'une seule manière en un isomorphisme σ' de E(N) relatif à E , isomorphisme qui coïncide donc nécessairement avec σ sur N ; on a par suite $\sigma'(E(N))=E(\sigma(N))=E(N)$, ce qui montre que E(N) est normale sur E et achève de prouver le corollaire.

COROLLAIRE 2.- Soient M et N deux extensions normales de K , telles que $M \cap N=K$. Alors $K(M \cup N)$ est une extension normale de K , et le groupe de Galois de $K(M \cup N)$ par rapport à K est isomorphe au produit des groupes de Galois de M et N par rapport à K .

Pour tout automorphisme σ de M (resp. tout automorphisme τ de N) relatif à K , soit $\bar{\sigma}$ (resp. $\bar{\tau}$) le prolongement unique de σ (resp. τ) en un automorphisme de $K(M \cup N)$ relatif à N (resp. M) ; prolongeons d'une manière quelconque chacun des τ (resp. $\bar{\tau}$) à $\bar{K}$, et désignons encore ce prolongement par $\bar{\sigma}$ (resp. $\bar{\tau}$). Alors (§ 4,prop.12), tout isomorphisme φ de $K(M \cup N)$ relatif à K peut se mettre d'une seule manière sous la forme $\bar{\sigma} \circ \bar{\tau}$ puisque les $\bar{\tau}$ décrivent l'ensemble des isomorphismes de $K(M \cup N)$ relatifs à M lorsque τ parcourt le groupe de Galois de N relatif à K (cor.1) ; en outre, φ coïncide avec σ sur M et avec τ sur N . On en déduit d'abord que φ applique $K(M \cup N)$ sur lui-même ; en outre, l'application $(\sigma, \tau) \longrightarrow \bar{\sigma} \circ \bar{\tau}$ du produit $\Gamma_1 \times \Gamma_2$ des groupes de Galois de M et N relatifs à K , dans le groupe de Galois Γ de $K(M \cup N)$ relatif à K , est une application biunivoque de $\Gamma_1 \times \Gamma_2$ sur Γ . Reste à voir que c'est une représentation, ce qui est immédiat, car $(\bar{\sigma} \circ \bar{\tau}) \circ (\bar{\sigma}' \circ \bar{\tau}')$ coïncide avec $\sigma\sigma'$ sur M et avec $\tau\tau'$ sur N , donc est égal à $(\overline{\sigma\sigma'}) \circ (\overline{\tau\tau'})$.

3. La théorie de Galois.

Soit N une extension normale d'un corps K , Γ le groupe de Galois de N relatif à K . Lorsque nous parlerons, dans ce n^{o} , d'un sous-corps

E de N , il sera toujours sous-entendu que E contient K ; pour un tel sous-corps, N est une extension normale de E , et le groupe de Galois de N par rapport à E est le sous-groupe $g(E)$ de Γ formé des automorphismes $\sigma \in \Gamma$ laissant invariant chaque élément de E . Inversement, si Δ est un sous-groupe quelconque de Γ , l'ensemble des éléments de N qui sont invariants par tous les automorphismes $\sigma \in \Delta$ est un sous-corps de N (contenant K) (chap.II, § 5, prop.9), que nous désignerons par $k(\Delta)$. Si $\mathcal{K}$ désigne l'ensemble des sous-corps de N , $\mathcal{G}$ l'ensemble des sous-groupes de Γ , nous définissons ainsi une application g de $\mathcal{K}$ dans $\mathcal{G}$, et une application k de $\mathcal{G}$ dans $\mathcal{K}$; la théorie de Galois est l'étude de ces deux applications.

Proposition 8.- Soit (E_ι) une famille de sous-corps de N , E le corps $K(\bigcup_\iota E_\iota)$; on a $g(E) = \bigcap_\iota g(E_\iota)$.

En effet, si F_σ est le sous-corps de N formé des éléments invariants par un automorphisme σ de N , $g(E)$ est l'ensemble des σ tels que $E \subset F_\sigma$; si F_σ contient tous les E_ι , il contient E , et réciproquement.

COROLLAIRE.- L'application g de $\mathcal{K}$ dans $\mathcal{G}$ est décroissante.

Autrement dit, si E , E' sont deux sous-corps de N tels que $E \subset E'$, on a $g(E) \supset g(E')$.

Proposition 9.- Soit (Δ_ι) une famille de sous-groupes de Γ , Δ le plus petit sous-groupe de Γ contenant $\bigcup_\iota \Delta_\iota$; on a $k(\Delta) = \bigcap_\iota k(\Delta_\iota)$.

En effet, l'ensemble des automorphismes de N qui laissent invariants un élément $x \in N$ est un sous-groupe Γ_x de Γ , et $k(\Delta)$ est l'ensemble des x tels que $\Delta \subset \Gamma_x$; si Γ_x contient tous les Δ_ι , il contient Δ , et réciproquement.

COROLLAIRE.- L'application k de $\mathcal{G}$ dans $\mathcal{K}$ est décroissante.

Autrement dit, si Δ , Δ' sont deux sous-groupes de Γ tels que $\Delta \subset \Delta'$, on a $k(\Delta) \supset k(\Delta')$.

Nous nous proposons de chercher des conditions pour que g et k établissent une <u>correspondance biunivoque</u> entre $\mathcal{G}$ et $\mathcal{K}$, autrement dit, pour que g soit une application biunivoque de $\mathcal{K}$ sur $\mathcal{G}$, et k son application réciproque ; il faut et il suffit pour cela (<u>Ens</u>. R , § 2, n°12) que l'on ait $k(g(E))=E$ pour tout sous-corps E de N , et $k(g(\Delta))=\Delta$ pour tout sous-groupe Δ de Γ .

Il résulte aussitôt des définitions que l'on a toujours

$$k(g(E)) \supset E \tag{1}$$

$$g(k(\Delta)) \supset \Delta \tag{2}$$

pour tout sous-corps E de N et tout sous-corps Δ de Γ .

<u>Proposition 10</u>.- <u>Pour tout sous-corps E de N , le corps</u> $k(g(E))$ <u>est la plus grande extension purement inséparable de E contenue dans N</u> .

En effet, $k(g(E))$ n'est autre que l'ensemble des éléments de N , (considéré comme extension normale de E) invariants par tous les automorphismes de N relatifs à E ; la proposition résulte donc de la prop.6.

COROLLAIRE.- <u>Pour que</u> $k(g(E))=E$ <u>pour tout sous-corps E de N , il faut et il suffit que N soit galoisienne sur K</u> .

En effet, si N est séparable sur K , elle est séparable sur E ; pour tout sous-corps E de N (contenant K) , donc $k(g(E))=E$; réciproquement, si N n'est pas séparable sur K , on a $N_0 \neq N$, et $k(g(N_0))=N$, puisque $g(N_0)$ est réduit à la permutation identique.

Afin d'obtenir une condition pour que $g(k(\Delta))=\Delta$ pour tout sous-groupe Δ de Γ , nous démontrerons d'abord la proposition suivante :

<u>Proposition 11</u>.- <u>Soit L un corps commutatif,</u> Δ <u>un groupe fini d'automorphismes de L , d'ordre n , K le sous-corps de L formé des éléments invariants par tous les automorphismes de</u> Δ . <u>Le corps L</u>

est une extension galoisienne de K , de degré n , et Δ est identique au groupe de Galois de L par rapport à K .

Soient σ_i $(1 \leqslant i \leqslant n)$ les éléments du groupe Δ ; dans l'espace vectoriel $\mathcal{E}(L)$ sur L , formé des endomorphismes du groupe additif de L (chap.II, § 5, n°6), considérons le sous-espace $\mathcal{M}$ engendré par les σ_i , c'est-à-dire formé des endomorphismes $\sum_{i=1}^{n} \lambda_i \sigma_i$, où $\lambda_i \in L$; les σ_i étant deux à deux distincts, sont linéairement indépendants dans $\mathcal{E}(L)$ (§ 4, th.1), donc $\mathcal{M}$ est de dimension n sur L ; d'autre part, le produit de deux σ_i appartenant à Δ , $\mathcal{M}$ est un sous-anneau de l'anneau d'endomorphismes $\mathcal{E}(L)$. Cela étant, K est le sous-corps de L attaché (chap.II, § 5) à l'anneau d'endomorphismes $\mathcal{M}$, c'est-à-dire formé des $x \in L$ tels que $\varphi(yx)=\varphi(y)x$ pour tout $y \in L$ et tout $\varphi \in \mathcal{M}$; car cette relation s'écrit $\sum_{i=1}^{n} \lambda_i \sigma_i(yx) = \sum_{i=1}^{n} \lambda_i \sigma_i(y)x$ c'est-à-dire $\sum_{i=1}^{n} \lambda_i(\sigma_i(x)-x)\sigma_i(y)=0$ quels que soient $y \in L$ et $\lambda_i \in L$, ce qui entraîne $\sigma_i(x)=x$ pour tout indice i . Le th.3 du chap.II, § 5 montre alors que L est de degré n sur K ; comme les σ_i sont n automorphismes distincts de L relatifs à K , L est séparable sur K , et les σ_i sont les seuls isomorphismes de L relatifs à K ; d'où résulte que L est galoisienne sur K et que Δ est le groupe de Galois de L par rapport à K .

COROLLAIRE.- Soit N une extension normale de K . Si le groupe Γ de N relatif à K est fini (ou, ce qui revient au même, si la quasi-fermeture algébrique N_0 de K dans N est de degré fini sur K) , on a $g(k(\Delta))=\Delta$ pour tout sous-groupe Δ de Γ .

En effet, tout sous-groupe Δ de Γ est alors fini; soit n l'ordre d'un tel sous-groupe. D'après la prop.11, le corps $E=k(\Delta)$ est tel que N soit une extension galoisienne de degré n sur E , et le groupe $g(k(\Delta))$ de N par rapport à E est identique à Δ .

On peut montrer que cette condition suffisante pour que $g(k(\Delta))=\Delta$ pour tout sous-groupe Δ de Γ, est aussi nécessaire (exerc. 13). Nous verrons dans l'Appendice comment, en général, on peut caractériser les sous-groupes Δ de Γ tels que $g(k(\Delta))=\Delta$, par l'emploi d'un langage emprunté à la Topologie.

Nous pouvons résumer les résultats obtenus dans le théorème suivant :

Théorème 2 (théorème fondamental des extensions galoisiennes).- Soit N une extension normale d'un corps K, Γ son groupe de Galois par rapport à K. Soit $\mathcal{K}$ l'ensemble des sous-corps de N contenant K, $\mathcal{G}$ l'ensemble des sous-groupes de Γ. Pour tout sous-corps $E \in \mathcal{K}$ soit $g(E)$ le sous-groupe de Γ formé des automorphismes $\sigma \in \Gamma$ laissant invariant chaque élément de E. Pour tout sous-groupe Δ de Γ, soit $k(\Delta)$ le sous-corps de N formé des éléments invariants par tous les automorphismes $\sigma \in \Delta$. Si N est une extension galoisienne de K, de degré fini sur K, g et k sont deux applications biunivoques réciproques de $\mathcal{K}$ sur $\mathcal{G}$ et de $\mathcal{G}$ sur $\mathcal{K}$ respectivement. Pour tout sous-corps E de N contenant K, l'ordre de $g(E)$ est alors égal au degré $[N:E]$, l'indice $(\Gamma : g(E))$ est égal au degré $[E:K]$.

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

COROLLAIRE 1.- Dans la correspondance biunivoque entre $\mathcal{K}$ et $\mathcal{G}$ définie par g, à l'intersection d'une famille (E_i) de sous-corps de N correspond le sous-groupe de Γ engendré par la réunion des sous-groupes $\Delta_i = g(E_i)$, au sous-corps de N engendré par la réunion des E_i correspond l'intersection des sous-groupes Δ_i.

C'est une conséquence évidente du fait que g est strictement décroissante.

Lorsque N n'est pas séparable sur K, $g(\bigcap_i E_i)$ peut être distinct du groupe engendré par la réunion des $g(E_i)$ et $k(\bigcap_i \Delta_i)$ distinct du sous-groupe engendré par la réunion des $k(\Delta_i)$ (cf. exerc. 10).

COROLLAIRE 2.- Pour que deux sous-groupes Δ_1, Δ_2 de Γ soient tels que les sous-corps $k(\Delta_1), k(\Delta_2)$ soient linéairement disjoints sur K, il faut et il suffit que l'on ait $(\Gamma : \Delta_1 \cap \Delta_2) = (\Gamma : \Delta_1)(\Gamma : \Delta_2)$

En effet, si on pose $E_1 = k(\Delta_1)$, $E_2 = k(\Delta_2)$, $E = k(\Delta_1 \cap \Delta_2)$, on a $E = K(E_1 \cup E_2)$ et la relation de l'énoncé équivaut à $[E:K] = [E_1:K][E_2:K]$, condition pour que E_1 et E_2 soient linéairement disjoints (§ 5, cor. de la prop. 2).

COROLLAIRE 3.- Si E est une extension algébrique séparable de K, de degré fini sur K, il n'existe qu'un nombre fini de corps F tels que $K \subset F \subset E$.

En effet, soit N l'extension normale de K engendrée par E ; N est une extension galoisienne de K, de degré fini sur K (cor.1 de la prop.4), donc il résulte du th.2 qu'il n'existe qu'un nombre fini de corps F tels que $K \subset F \subset N$.

4. Sous-corps conjugués. Sous-corps normaux.

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

Proposition 12.- Soit σ un automorphisme de N relatif à K. Pour tout sous-corps E de N et tout sous-groupe Δ de Γ, on a

$$g(\sigma(E)) = \sigma g(E) \sigma^{-1} \tag{3}$$

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

En effet, si $\tau \in \Gamma$ est tel que $\tau\sigma(x)=\sigma(x)$ pour tout $x \in E$, on en déduit que $\sigma^{-1}\tau\sigma(x)=x$ pour tout $x \in E$, donc $\sigma^{-1}\tau\sigma \in g(E)$, et réciproquement. De même, si $\sigma\tau\sigma^{-1}(y)=y$ pour tout $\tau \in \Delta$, on a $\tau\sigma^{-1}(y)=\sigma^{-1}(y)$ pour tout $\tau \in \Delta$, donc $\sigma^{-1}(y) \in k(\Delta)$ et réciproquement.

Proposition 13.- Si E est un sous-corps de N normal sur K, $g(E)$ est un sous-groupe distingué de Γ et le groupe de Galois de E relatif à K est isomorphe à $\Gamma/g(E)$. Si Δ est un sous-groupe distingué de Γ, $K(\Delta)$ est une extension normale de K.

Le fait que $g(E)$ est distingué dans Γ si E est normal sur K (resp. que $k(\Delta)$ est normale sur K si Δ est distingué dans Γ) résulte aussitôt de la formule (3) (resp. (4)) et de la prop.5. En outre si, pour tout automorphisme $\sigma \in \Gamma$, on désigne par σ_E la restriction de σ à E, σ_E est un automorphisme de E relatif à K, et l'application $\sigma \to \sigma_E$ est une représentation de Γ sur le groupe de Galois de E par rapport à K (prop.5) ; pour que σ_E soit l'automorphisme identique, il faut et il suffit que $\sigma \in g(E)$ par définition, d'où la proposition.

COROLLAIRE 1.- Si N est une extension galoisienne finie d'un corps K, dont le groupe de Galois relatif à K est abélien, tout sous-corps E de N contenant K est une extension galoisienne de K, dont le groupe par rapport à K est abélien.

Une extension galoisienne d'un corps K dont le groupe de Galois relatif à K est abélien est dite extension abélienne de K.

On dit de même qu'une équation $f(x)=0$, où f est un polynome irréductible de $K[X]$, est abélienne, si le corps des racines de f est une extension abélienne de K. On notera que dans ce cas, si x_i est une racine quelconque de f, $K(x_i)$ est identique au corps des racines de f, car c'est une extension abélienne de K

d'après le cor. de la prop.14, donc elle contient tous les conjugués de x_i, c'est-à-dire toutes les racines de f.

COROLLAIRE 2.- *Soit* N *une extension galoisienne de* K, *de degré fini sur* K. *Si le groupe de Galois* Γ *de* N *relatif à* K *est produit direct de deux de ses sous-groupes* Δ_1, Δ_2, *les sous-corps* $k(\Delta_1)$ *et* $k(\Delta_2)$ *sont des extensions galoisiennes de* K, *linéairement disjointes sur* K, *et* N *est le composé de ces deux sous-corps* (isomorphe à leur produit tensoriel).

En effet, Δ_1 et Δ_2 sont distingués dans Γ, donc $E_1 = k(\Delta_1)$ et $E_2 = k(\Delta_2)$ sont normales (et par suite galoisiennes) sur K ; si n_1, n_2 sont les ordres de Δ_1 et Δ_2, on a $(\Gamma : \Delta_1) = n_2$ et $(\Gamma : \Delta_2) = n_1$, donc $[E_1 : K] = n_2$ et $[E_2 : K] = n_1$. Par ailleurs, comme $\Delta_1 \cap \Delta_2$ est réduit à l'élément neutre, on a $N = K(E_1 \cup E_2)$; le degré $[N : K]$ étant égal à $n_1 n_2$, on en conclut que E_1 et E_2 sont linéairement disjoints sur K (§ 5, cor. de la prop.2).

5. Base normale. Elément primitif.

Définition 4.- Etant donnée une extension galoisienne N *d'un corps* K, *de degré fini sur* K, *on dit qu'une base de* N *par rapport à* K *est normale si deux quelconques de ses éléments sont conjugués.*

Autrement dit, une base normale de N sur K est formée de tous les conjugués d'un élément $\theta \in N$. Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base quelconque de N sur K, et soient σ_i $(1 \leqslant i \leqslant n)$ les automorphismes de N relatifs à K. On peut écrire $\sigma_i(a_j) = \sum_{k=1}^{n} \gamma_{ijk} a_k$, où $\gamma_{ijk} \in K$; si $\theta = \sum_{j=1}^{n} \lambda_j a_j$ $(\lambda_j \in K)$, on a $\sigma_i(\theta) = \sum_{j=1}^{n} \lambda_j \sigma_i(a_j) = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \gamma_{ijk} \lambda_j \right) a_k$; pour que les conjugués de θ forment une base de N sur K, il faut et il suffit donc que la matrice formée des $\mu_{ik} = \sum_{j=1}^{n} \gamma_{ijk} \lambda_j$ soit régulière, ou encore que son déterminant ne soit pas nul.

Théorème 3. - Si K est un corps infini, toute extension galoisienne de K, de degré fini sur K, admet une base normale par rapport à K.

Soit N une extension galoisienne de K, de degré n sur K, et soit $(a_i)_{1\leqslant i\leqslant n}$ une base quelconque de N sur K. Soient X_i $(1\leqslant i\leqslant n)$ n indéterminées sur N, et considérons le corps $F=N(X_1,X_2,..,X_n)$; il est composé (sur K) des extensions $E=K(X_1,X_2,..,X_n)$ et N. Comme $E\cap N=K$ (§5, cor. de la prop.8), E et N sont linéairement disjointes sur K, F est une extension galoisienne de E, de degré n sur E, et tout automorphisme σ de N relatif à K se prolonge d'une seule manière en un automorphisme de F relatif à E, que nous désignerons encore par σ (th.1). Nous allons montrer tout d'abord que les conjugués de l'élément $\theta=\sum_{i=1}^{n} a_iX_i$ de F, par rapport à E, forment une base normale de F par rapport à E.

Pour tout automorphisme σ de F relatif à E, nous poserons $\sigma(\theta)=\theta_\sigma$; on a $\theta_\sigma=\sum_{i=1}^{n}\sigma(a_i)X_i$; il faut prouver que les n éléments θ_σ (σ parcourant le groupe Γ des automorphismes de F relatif à E) sont linéairement indépendants sur E ; il suffit pour cela de voir que la relation $\sum_\sigma u_\sigma\theta_\sigma=0$, où les u_σ appartiennent à l'anneau de polynomes $K[X_1,X_2,\ldots,X_n]$, entraîne $u_\sigma=0$ pour tout σ (chap.III, § ,).

En premier lieu, notons que le déterminant $\det(\sigma(a_i))_{1\leqslant i\leqslant n,\,\sigma\in\Gamma}$ n'est pas nul (§4, n°4) ; des n équations linéaires $\theta_\sigma=\sum_{i=1}^{n}\sigma(a_i)X_i$ par rapport aux X_i, on tire donc $X_i=\sum_\sigma a_{i,\sigma}\theta_\sigma$, où les $a_{i,\sigma}$ appartiennent à N ; les n éléments θ_σ forment donc un système de générateurs de F par rapport à N, et comme le degré de transcendance de F sur N est égal à n, les n éléments θ_σ sont algébriquement indépendants sur N (§2, th.6). En remplaçant chaque X_i par son expression en fonction des θ_τ dans $u_\sigma(X_1,X_2,\ldots,X_n)$, on voit donc qu'il existe un polynome et un seul v_σ à coefficients dans N, par rapport à n indéterminées Y_τ ($\tau\in\Gamma$), tel que $u_\sigma(X_1,X_2,\ldots,X_n)=v_\sigma((\theta_\tau))$.

Cela étant, de la relation $\sum_\sigma u_\sigma\theta_\sigma=0$, on déduit, pour tout automorphisme ρ de F relatif à E , $\sum_\sigma u_\sigma\rho(\theta_\sigma)=0$, c'est-à-dire $\sum_\sigma u_\sigma\theta_{\rho\sigma}=0$, ou $\sum_\sigma \theta_{\rho\sigma}v_\sigma((\theta_\tau))=0$. Supposons que les v_σ ne soient pas tous nuls, et soit r le plus grand des degrés des v_σ par rapport à Y_ε (ε élément neutre de Γ) ; soit π un élément de Γ tel que v_π soit non nul et de degré r par rapport à Y_ε ; on peut donc écrire $v_\pi = Y_\varepsilon^r w_\pi + y_\pi$, où y_π est de degré $\leqslant r-1$ par rapport à Y_ε et où w_π est un polynome non nul ne contenant plus Y_ε . Cela étant, prenons $\rho=\pi^{-1}$; le polynome $\sum_\sigma \theta_{\rho\sigma}v_\sigma((\theta_\tau))$ est de degré $r+1$ par rapport à $\theta_\varepsilon=\theta$ et le coefficient de θ^{r+1} dans ce polynome est $w_\pi((\theta_\tau))$, qui n'est pas nul par hypothèse ; on ne peut donc avoir $\sum_\sigma \theta_{\rho\sigma}v_\sigma((\theta_\tau))=0$, contrairement à l'hypothèse.

Posons maintenant $\sigma(a_i)=\sum_{k=1}^n \gamma_{\sigma ik}a_k$, où $\gamma_{\sigma ik}\in K$; si on pose $z_{\sigma k}=\sum_{i=1}^n \gamma_{\sigma ik}X_i$, le fait que la base (θ_σ) est une base normale de F sur E signifie que le déterminant $\det(z_{\sigma k})_{1\leqslant k\leqslant n,\sigma\in\Gamma}$ n'est pas nul dans E . Or, c'est un polynome $\Phi(X_1,X_2,..,X_n)$ à coefficients dans K . Comme par hypothèse K est <u>infini</u>, il existe n éléments μ_i ($1\leqslant i\leqslant n$) de K tels que $\Phi(\mu_1,\mu_2,\ldots,\mu_n)\neq 0$ (chap.IV, § , th.) ; mais comme $\Phi(\mu_1,\mu_2,\ldots,\mu_n)$ n'est autre que le déterminant de la matrice des $\xi_{\sigma k}=\sum_{i=1}^n \gamma_{\sigma ik}\mu_i$, on voit que les conjugués de l'élément $\omega=\sum_{i=1}^n \mu_i a_i$ de E forment une base normale de E sur K .

C.Q.F.D.

Le théorème 3 est encore vrai lorsque le corps K est <u>fini</u> (cf. § 8, exerc. 9) .

Etant donnée une extension algébrique E d'un corps K , de degré fini sur K , on dit qu'un élément $\theta\in E$ est un <u>élément primitif</u> de E si $E=K(\theta)$ (autrement dit, si le degré de θ par rapport à K est égal à $[E:K]$).

Proposition 14 (théorème de l'élément primitif).- *Si K est un corps infini, toute extension algébrique séparable E de K, de degré fini sur K, admet un élément primitif* (autrement dit, est une extension algébrique *simple* de K).

En effet, soit N l'extension normale de K engendrée par E ; N est une extension galoisienne de K, de degré fini sur K ; soit Γ le groupe de Galois de N par rapport à K, Δ le groupe de Galois de N par rapport à E et m l'ordre de Δ ; l'indice $(\Gamma : \Delta)$ est égal au degré n de E sur K (th.2) ; dans chaque classe à gauche de Γ modulo Δ, nous prendrons un élément σ_i $(1 \leqslant i \leqslant n)$. Soit alors ω un élément de N tel que les conjugués $\sigma(\omega)$ $(\sigma \in \Gamma)$ de ω forment une base normale de N sur K. Soit $\theta = \sum_{\sigma \in \Delta} \sigma(\omega)$; θ appartient à E car pour tout automorphisme $\tau \in \Delta$, on a $\tau(\theta) = \sum_{\sigma \in \Delta} \tau\sigma(\omega) = \theta$ (prop.6) ; pour deux indices i, j distincts, on a $\sigma_i(\theta) \neq \sigma_j(\theta)$, car les 2m éléments $\sigma_i\sigma(\omega)$, $\sigma_j\sigma(\omega)$ $(\sigma \in \Delta)$ sont linéairement indépendants sur K ; par suite, θ a au moins n conjugués distincts, ce qui signifie qu'il est d'ordre n, d'où $E = K(\theta)$.

6. Fonctions symétriques des racines d'un polynome.

Soit K un corps quelconque, $N = K(X_1, X_2, \ldots, X_n)$ le corps des fractions rationnelles sur K, par rapport à n indéterminées X_i. Considérons dans l'anneau $N[Z]$, le polynome $f(Z) = \prod_{i=1}^{n} (Z - X_i)$ ayant pour racines les X_i ; on a $f(Z) = Z^n + \sum_{k=1}^{n} (-1)^k s_k Z^{n-k}$, où $s_k(X_1, X_2, \ldots, X_n) = \sum_{i_1 < i_2 < \cdots < i_k} X_{i_1} X_{i_2} \cdots X_{i_k}$; on dit (par abus de langage) que le polynome s_k est la *fonction symétrique élémentaire de degré* k des n indéterminées X_i (on a en particulier $s_1 = X_1 + X_2 + \ldots + X_n$, et $s_n = X_1 X_2 \ldots X_n$). Posons $E = K(s_1, s_2, \ldots, s_n)$; c'est un sous-corps de N, et le polynome f appartient à $E[Z]$; il est clair que N est le *corps des racines* $N(X_1, X_2, \ldots, X_n)$ de f. Comme toutes les racines de f sont simples,

N est donc une extension galoisienne finie de E . Montrons que le groupe de N par rapport à E est isomorphe au groupe symétrique $\mathfrak{S}_n$. En effet, pour toute permutation $\sigma \in \mathfrak{S}_n$, et toute fraction rationnelle g $N=K(X_1,X_2,\ldots,X_n)$, σg désigne la fraction rationnelle $g(X_{\sigma(1)},X_{\sigma(2)},\ldots,X_{\sigma(n)})$, et l'application $g \to \sigma g$ est un automorphisme du corps N , qui laisse invariant les s_k , donc tout élément de E ; et inversement, tout automorphisme de N relatif à E permute les X_i , donc coïncide avec un automorphisme de la forme $g \to \sigma g$, où $\sigma \in \mathfrak{S}_n$. Comme $\mathfrak{S}_n$ opère transitivement dans $\left[1,n\right]$, on voit en outre que deux quelconques des X_i sont conjugués par rapport à E , donc le polynome f est irréductible sur E .

Remarquons d'autre part que les s_k $(1 \leqslant k \leqslant n)$ forment un système algébriquement libre sur K , car N est une extension algébrique de E , donc (§ 2, th.7) a même degré de transcendance que E sur K ; E est donc une extension transcendante pure de K . En résumé :

Proposition 15.- Soient K un corps quelconque, S_k $(1 \leqslant k \leqslant n)$ n indéterminées. Sur le corps $F=K(S_1,S_2,\ldots,S_n)$, le polynome $f(Z)=Z^n+\sum_{k=1}^{n}(-1)^k S_k Z^{n-k}$ est irréductible et séparable ; le corps des racines N de ce polynome est une extension galoisienne de F , de degré n! sur F , dont le groupe de Galois relatif à F est isomorphe au groupe symétrique $\mathfrak{S}_n$.

Cela étant, on dit (par abus de langage) qu'une fraction rationnelle $g \in N=K(X_1,\ldots,X_n)$ est une fonction symétrique des n indéterminées X_i si pour toute permutation $\sigma \in \mathfrak{S}_n$, on a $\sigma g=g$. D'après la prop.6, toute fraction de cette nature appartient à E , donc il existe une fraction rationnelle $\varphi \in K(S_1,S_2,\ldots,S_n)$ telle que $g(X_1,X_2,\ldots,X_n)=\varphi(s_1,s_2,\ldots,s_n)$; en outre, comme les s_i sont algébriquement indépendants sur K , φ est déterminée de façon unique. En d'autres termes :

Proposition 16.- Toute fonction symétrique des n indéterminées X_1, à coefficients dans K, peut s'exprimer d'une manière et d'une seule comme fonction rationnelle (à coefficients dans K) des fonctions symétriques élémentaires des X_1.

Soit maintenant $f_1 = Z^n + \sum_{k=1}^{n} (-1)^k a_k Z^{n-k}$ un polynome quelconque de $K[Z]$; dans la fermeture algèbrique $\bar{K}$ de K, f_1 se décompose en un produit de n polynomes du premier degré, distincts ou non, $f_1(Z) = \prod_{i=1}^{n} (Z-a_i)$; on a $s_k(a_1,a_2,\ldots,a_n)=a_k$ pour $1 \leqslant k \leqslant n$. Pour toute fonction symétrique g des X_1, soit φ la fraction rationnelle telle que $g(X_1,X_2,\ldots,X_n)=\varphi(s_1,s_2,\ldots,s_n)$; on aura aussi $g(a_1,a_2,\ldots,a_n)=\varphi(a_1,a_2,\ldots,a_n)$ si les deux membres de cette relation sont définis.

7. Norme et trace dans les extensions algèbriques séparables.

Définition 5.- Soit E une extension algèbrique séparable d'un corps K, de degré fini n sur K ; soient σ_i $(1 \leqslant i \leqslant n)$ les n isomorphismes distincts de E relatifs à K. Pour tout élément x de E, on appelle norme et trace de x relatives à E et K, et on note respectivement $N_{E|K}(x)$ et $Tr_{E|K}(x)$ (ou simplement $N_E(x)$, $Tr_E(x)$, et même $N(x)$, $Tr(x)$ si aucune confusion n'en peut résulter) les éléments

$$N_{E|K}(x) = \sigma_1(x)\sigma_2(x)\ldots\sigma_n(x) \tag{5}$$

$$Tr_{E|K}(x) = \sigma_1(x)+\sigma_2(x)+\ldots+\sigma_n(x) \tag{6}$$

Il résulte immédiatement de cette définition que l'on a

$$N_{E|K}(xy)=N_{E|K}(x)N_{E|K}(y) \tag{7}$$

$$Tr_{E|K}(x+y) = Tr_{E|K}(x)+Tr_{E|K}(y) \tag{8}$$

Les éléments $N_{E|K}(x)$ et $Tr_{E|K}(x)$ appartiennent à K ; en effet, soit G l'extension normale de K engendrée par E ; G est galoisienne sur K et de degré fini par rapport à K ; pour tout automorphisme τ de G relatif à K, les $\tau\sigma_i$ sont n isomorphismes distincts de E relatifs à K, donc sont identiques aux σ_i à l'ordre près ; on a donc $\tau(N_{E|K}(x))=N_{E|K}(x)$ et $\tau(Tr_{E|K}(x))=Tr_{E|K}(x)$, ce qui prouve que $N_{E|K}(x)$ et $Tr_{E|K}(x)$ appartiennent à K (prop.6). On peut donc dire que $x \to Tr_{E|K}(x)$ est une représentation du groupe additif du corps E dans le groupe additif du corps K, et que l'application $x \to N_{E|K}(x)$, restreinte au groupe multiplicatif E^* du corps E, est une représentation de ce groupe dans le groupe multiplicatif K^* de K. En particulier on a $Tr_{E|K}(-x)=-Tr_{E|K}(x)$ et si $x\neq 0$, $N_{E|K}(x)\neq 0$ et $N_{E|K}(\frac{1}{x}) = \frac{1}{N_{E|K}(x)}$.

Pour tout $x \in K$, on a $Tr_{E|K}(x)=nx$ et $N_{E|K}(x)=x^n$.

Remarque.- Lorsque E est galoisienne sur K, les σ_i sont les éléments du groupe de Galois Γ de E sur K ; on peut considérer que l'application $x \to Tr(x)$ est produite par l'opérateur $\sigma_1+\sigma_2+\ldots+\sigma_n$ de l'algèbre A du groupe Γ par rapport à l'anneau $\mathbb{Z}$ des entiers rationnels : de façon générale, pour tout élément $\lambda = \sum_{i=1}^{n} h_i\sigma_i$ de cette algèbre, et tout $x \in E$, on pose $\lambda.x = \sum_{i=1}^{n} h_i\sigma_i(x)$; il est immédiat que cette loi de composition externe définit (avec l'addition dans E) une structure de A-module à gauche sur E.

Dans ce même cas, lorsqu'on considère les normes des éléments de E, on écrit de préférence x^σ au lieu de $\sigma(x)$, pour tout $\sigma \in \Gamma$; l'application $x \to N(x)$, restreinte au groupe multiplicatif E^*, peut alors être encore considérée comme produite par l'opérateur $\sigma_1+\sigma_2+\ldots+\sigma_n$ de l'algèbre A ; plus généralement, pour tout élément $\lambda = \sum_{i=1}^{n} h_i\sigma_i$ de cette algèbre, et tout $x \in E^*$, on pose

$$x^{\lambda} = \prod_{i=1}^{n} (x^{\sigma_i})^{h_i} = \prod_{i=1}^{r} (x^{h_i})^{\sigma_i}$$

Avec cette convention, on vérifie aussitôt que $(xy)^{\lambda} = x^{\lambda} y^{\lambda}$ $x^{\lambda+\mu} = x^{\lambda} y^{\mu}$ et $(x^{\lambda})^{\mu} = x^{\mu\lambda}$; en d'autres termes, la loi de groupe multiplicatif (abélien) de E^*, et la loi externe $(\lambda, x) \to x^{\lambda}$ définissent sur E^* une structure de A-module à gauche

Proposition 17.- Soit E une extension séparable de K, de degré fini sur K ; soit F une extension séparable de E, de degré fini sur E. Pour tout $x \in F$, on a

$$N_{F|K}(x) = N_{E|K}(N_{F|E}(x)) \tag{9}$$

$$Tr_{F|K}(x) = Tr_{E|K}(Tr_{F|E}(x)) . \tag{10}$$

En effet, soient σ_i $(1 \leqslant i \leqslant n)$ les isomorphismes de E relatifs à K (prolongés en des automorphismes de Ω) et τ_j $(1 \leqslant j \leqslant m)$ les isomorphismes de F relatifs à E ; on sait (§ 4, prop. 12) que les $\sigma_i \tau_j$ sont les mn isomorphismes de F relatifs à K. On a donc, pour tout $x \in F$,

$Tr_{F|K}(x) = \sum_{i=1}^{n} (\sum_{j=1}^{m} \sigma_i(\tau_j(x))) = \sum_{i=1}^{n} \sigma_i(\sum_{j=1}^{m} \tau_j(x)) = \sum_{i=1}^{n} \sigma_i(Tr_{F|E}(x)) =$
$= Tr_{E|K}(Tr_{F|E}(x))$, puisque $Tr_{F|E}(x)$ appartient à E. Démonstration analogue pour la formule (9).

COROLLAIRE 1.- Pour tout élément $x \in E$, on a

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

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

COROLLAIRE 2.- Soit E une extension séparable de K, de degré n sur K. Soit x un élément de E, de degré m sur K, et soit $f(Z) = Z^m + \sum_{k=1}^{m} a_k Z^{m-k}$ le polynome minimal de x par rapport à K. On a

$$N_{E|K}(x) = ((-1)^m a_m)^{\frac{n}{m}} \tag{11}$$

$$Tr_{E|K}(x) = -\frac{n}{m} a_1 . \tag{12}$$

En effet, appliquons le corollaire 1, en remplaçant E par $K(x)$ et F par E ; si x_i $(1 \leqslant i \leqslant m)$ sont les conjugués de x , on a $Tr_{K(x)|K}(x) = \sum_{i=1}^{m} x_i = -a_1$, et $N_{K(x)|K}(x) = \prod_{i=1}^{m} x_i = (-1)^m a_m$, d'où les formules (11) et (12).

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

Exercices.- 1) Toute extension algébrique d'un corps K , engendrée par un ensemble d'éléments dont chacun est de degré 2 sur K , est une extension normale de K .

* 2) Le polynome X^2-2 est irréductible dans $Q[x]$; soit a une de ses racines. Montrer que le polynome X^2-a est irréductible sur $Q(a)=E$; soit β une racine de ce polynome et $F=E(\beta) = Q(\beta)$. Montrer que F n'est pas une extension galoisienne de Q (prouver que le polynome X^2+1 est irréductible sur F). Quelle est l'extension galoisienne de Q engendrée par F ? Déterminer la structure de son groupe par rapport à Q , ainsi que celle des sous-groupes g(E) et g(F) . *

3) Soient N_1, N_2 deux extensions normales d'un corps K , N_0 leur intersection, N le corps composé de N_1 et N_2 . On désigne par Γ_1 , Γ_2 , Γ les groupes de N_1, N_2 et N respectivement, relatifs à K ; par Δ_1 , Δ_2 les sous-groupes de Γ_1 , Γ_2 correspondant au sous-corps N_0 de N_1 et N_2 respectivement. A toute classe $\bar{\sigma}_1$ modulo Δ_1 , dans Γ_1 , correspond la classe $\bar{\sigma}_2$ modulo Δ_2 , dans Γ_2 , formée des automorphismes appartenant à Γ_2 , dont la restriction à N_0 est identique à la restriction de tout automorphisme appartenant à la classe $\bar{\sigma}_1$; on définit ainsi un isomorphisme

φ de Γ_1 / Δ_1 sur Γ_2 / Δ_2 . Montrer que le groupe Γ est isomorphe au sous-groupe $\mathfrak{H}$ du groupe produit $\Gamma_1 \times \Gamma_2$, formé des couples (σ_1, σ_2) tels que, si $\bar{\sigma}_1$ et $\bar{\sigma}_2$ sont les classes de σ_1 et σ_2 respectivement dans Γ_1 / Δ_1 et Γ_2 / Δ_2 , on ait $\bar{\sigma}_2 = \varphi(\bar{\sigma}_1)$ (utiliser le th.1).

4) Pour que le groupe de Galois du corps des racines d'une équation sans racines multiples $f(x)=0$ $(f \in K[X])$ soit transitif (quand on le considère comme groupe de permutations des racines de f), il faut et il suffit que f soit irréductible.

5) Soit f un polynome irréductible et séparable de $K[X]$, F l'ensemble des racines de f dans K , Γ le groupe de Galois du corps des racines de l'équation $f(x)=0$, considéré comme groupe transitif de permutations de F . Pour qu'un corps $K(x_i)$ obtenu par adjonction d'une racine de f à K , contienne un sous-corps $E \supset K$ distinct de K et de $K(x_i)$, il faut et il suffit que le groupe Γ soit imprimitif (chap.I, § 7, n°7) .

5 bis) Soit f un polynome (irréductible ou non) de degré n dans $K[X]$, séparable sur K ; soient a_i $(1 \leqslant i \leqslant n)$ ses racines, $M=K(a_1, a_2, .., a_n)$ le corps des racines de f . Soit F le corps de fractions rationnelles $M(X_1, X_2, .., X_n)$, E le sous-corps $K(X_1, X_2, .., X_n)$; F est une extension galoisienne de E , et son groupe de Galois par rapport à E est isomorphe au groupe de Galois Γ de M par rapport à K . Si $\theta = a_1 X_1 + a_2 X_2 + \ldots + a_n X_n$, on a $F = E(\theta)$, et le polynome minimal de θ par rapport à E est un facteur irréductible g_1 du polynome

$$f = \prod_{\pi} (X - a_1 X_{\pi(1)} - a_2 X_{\pi(2)} - \ldots - a_n X_{\pi(n)})$$

où π parcourt le groupe symétrique $\mathfrak{S}_n$. On sait que chaque

permutation π définit un automorphisme $X_i \to X_{\pi(i)}$ $(1 \leqslant i \leqslant n)$ de E, que nous désignerons encore par π ; montrer que Γ est isomorphe au sous-groupe de $\mathfrak{S}_n$ formé des permutations telles que $\pi(g_1)=g_1$. En outre, si $f=g_1 g_2 \cdots g_r$ est une décomposition de f en facteurs irréductibles dans $E[X]$, pour tout k, il existe une permutation π_k telle que $g_k=\pi_k(g_1)$.

6) Soient f et g deux polynomes irréductibles et séparables de $K[X]$, m le degré de f, n le degré de g, α une racine de f, β une racine de g. Soit $f=f_1 f_2 \cdots f_r$ une décomposition de f en facteurs irréductibles dans $K(\beta)[X]$, $g=g_1 g_2 \cdots g_s$ une décomposition de g en facteurs irréductibles dans $K(\alpha)[X]$. Montrer que $r=s$, et qu'on peut permuter les g_j de sorte que, si m_i est le degré de f_i, n_i celui de g_i, on ait $m/n=m_i/n_i$ pour $1 \leqslant i \leqslant r$. (Soit N le corps des racines du polynome fg, Γ son groupe de Galois relatif à K ; soit σ_i un automorphisme appartenant à Γ, transformant α en une racine de f_i $(1 \leqslant i \leqslant r)$; montrer que si $i \neq j$, il ne peut exister d'automorphisme $\tau \in \Gamma$ laissant α invariant et transformant $\sigma_j^{-1}(\beta)$ en $\sigma_i^{-1}(\beta)$, en prouvant que dans ce cas il existerait un automorphisme appartenant à Γ, transformant une racine de f_i, en une racine de f_j, et laissant β invariant).

7) Soit f un polynome irréductible de $K[X]$, séparable sur K, et soient a_i $(1 \leqslant i \leqslant n)$ ses racines. Soit g un polynome quelconque de $K[X]$, et h un facteur irréductible du polynome $f(g(X))$; montrer que le degré de h est un multiple rn de n, et que h a exactement r racines communes avec chacun des polynomes $g(X)-a_i$ (considérer les conjugués d'une racine quelconque de h).

8) Soit N une extension normale de K, E une extension séparable de K (algèbrique ou non). Montrer que E et N sont linéairement disjoints sur le corps $E \cap N$ (utiliser le th.1).

9) Donner un exemple de deux extensions algébriques séparables E,N d'un corps K, telles que N soit galoisienne sur K et $E \cap N = K$, mais que l'extension normale de K engendrée par E soit contenue dans N.

10) Soit K un corps de caractéristique $p > 0$, X,Y deux indéterminées sur K, $N=K(X,Y)$, $E=K(X+Y,XY)$; N est une extension galoisienne de E (prop.16). Soit $F=N(X^{1/p},Y^{1/p},(X+Y)^{1/p^2})$. Montrer que F est une extension normale de E : soient $F_1=N(X^{1/p})$, $F_2=N(Y^{1/p})$; montrer que, dans le groupe de Galois Γ de F relatif à E, l'intersection des sous-groupes $g(F_1)$ et $g(F_2)$ se réduit à l'élément neutre de Γ, mais que le plus petit corps contenant F_1 et F_2 est distinct de F.

11) Soit E une extension algébrique de K, E_0 la quasi-fermeture algébrique de K dans E, $\tilde{E}=E \cap K^{p^{-\infty}}$ le sous-corps de E formé des éléments purement inséparables sur K. Si N est l'extension normale de K engendrée par E, la quasi-fermeture algébrique de K dans N est l'extension normale N_0 de K engendrée par E_0. Pour que $\tilde{N}=N \cap K^{p^{-\infty}}$ soit égal à $\tilde{E}$, il faut et il suffit que E soit une extension séparable de $\tilde{E}$.

12) Soit E une extension algébrique <u>quelconque</u> de K, Γ le groupe des <u>automorphismes</u> de E laissant invariants tous les éléments de K.

a) Le sous-corps S de E formé des éléments invariants par tout automorphisme $\sigma \in \Gamma$, est le plus petit sous-corps de E contenant K, tel que E soit une extension galoisienne de S et Γ est le groupe de E relatif à S. Pour que E soit une extension normale de K, il faut et il suffit que S soit une extension purement inséparable de K.

b) Soit S_0 la quasi-fermeture algèbrique de K dans S . Montrer que S_0 est le plus petit des sous-corps F de E contenant K et tels que E soit une extension normale de F .

c) Soit E_0 la quasi-fermeture algèbrique de K dans E . Montrer que l'on a $E=S(E_0)$ (utiliser l'exerc.11 ci-dessus, et la prop.6 du §5).

13) a) Soit N une extension normale de K , Γ son groupe de Galois par rapport à K . Si Γ est <u>infini</u> (c'est-à-dire si la quasi-fermeture algèbrique N_0 de K dans N est de degré infini sur K), montrer que Γ <u>n'est pas dénombrable</u> (en utilisant la prop.12 du §4, former un ensemble d'automorphismes de N_0 relatifs à K , ayant la puissance du continu).

b) En déduire que, dans ce cas, il existe des sous-groupes Δ de Γ tels que $g(k(\Delta))\neq\Delta$ (prendre pour Δ un groupe infini dénombrable).

14) Soient E,F deux extensions galoisiennes finies d'un corps K , telles que $E\cap F=K$; si, dans E (resp. F) les conjugués d'un élément α (resp. β) forment une base normale de E (resp. F) sur K , montrer que, dans $K(E\cup F)$ les conjugués de l'élément $\alpha\beta$ forment une base normale de $K(E\cup F)$ sur K .

15) Soit K un corps imparfait (donc infini), E une extension algèbrique de K de degré fini sur K . Pour que E soit une extension simple de K , il faut et il suffit que son degré d'imperfection par rapport à K soit égal à 0 ou à 1 (pour montrer que la condition ainsi est suffisante, remarquer que, si E_0 est la quasi-fermeture algèbrique de K dans E , on a $E=E_0(\alpha)$, et $E_0=K(\beta)$, et prouver que l'on peut trouver $\lambda\in K$ tel que $E=K(\alpha+\beta\lambda)$).

16) Soit E une extension algèbrique de K , de degré fini sur K . Si r est le degré d'imperfection de E par rapport à K et $r>0$,

montrer que r est le plus petit nombre d'éléments d'un système de générateurs de E par rapport à K (pour voir que E peut être engendré par un ensemble de r éléments, remarquer que, si E_0 est la quasi-fermeture algébrique de K dans E , il existe r éléments a_i $(1 \leqslant i \leqslant r)$ tels que $E=E_0(a_1,a_2,\ldots,a_r)$, et utiliser l'ex.15).

En déduire que, pour que toute extension algébrique de degré fini d'un corps imparfait K soit simple, il faut et il suffit que le degré d'imperfection absolu de K soit égal à 1 .

17) Soit E une extension algébrique d'un corps imparfait K , de degré fini sur K .

a) Montrer que si le degré d'imperfection de E par rapport à K est >1 , il existe une infinité de corps distincts F tels que $K \subset F \subset E$ (se ramener au cas où $K(E^p)=K$; si a et b sont deux éléments de E qui sont p-indépendants par rapport à K , les corps $K(a+\lambda b)$ sont tous distincts lorsque λ parcourt K) .

b) Réciproquement, montrer que si le degré d'imperfection de E par rapport à K est égal à 1 , il n'existe qu'un nombre fini de corps F tels que $K \subset F \subset E$ (utiliser l'exerc.7 bis du § 4, et le cor.3 du th.2 du § 6).

§ 7. Racines de l'unité. Corps finis.

1. Racines de l'unité.

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

On peut dire encore que les racines de l'unité dans un corps K sont les *éléments d'ordre fini* dans le groupe multiplicatif K^* des éléments $\neq 0$ de K ; elles forment évidemment un sous-groupe de K^* . Si x est une racine de l'unité d'ordre n dans le groupe K^* , l'ensemble des entiers

$m>0$ tels que x soit racine m-ème de l'unité (c'est-à-dire tels que $x^m=1$) est l'ensemble des multiples >0 de n ; en effet l'application $h \to x^h$ est une représentation du groupe additif $\mathbb{Z}$ sur un groupe cyclique d'ordre n , donc l'image réciproque de 1 par cette représentation est le sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$.

Soit p la caractéristique du corps K ; si $x \in K$ est une racine de l'unité, son ordre n n'est pas divisible par p ; en effet, si on avait $n=pm$ (m entier $\geqslant 1$), on aurait $(x^m)^p=1$, d'où $x^m=1$, ce qui absurde, puisque $m < n$.

Soit Ω un corps algèbriquement fermé; nous nous proposons d'étudier le groupe des racines de l'unité dans Ω . En premier lieu, remarquons que les racines n-èmes de l'unité dans Ω sont racines du polynome X^n-1 , dont les coefficients appartiennent au corps premier P contenu dans Ω ; les racines de l'unité sont donc algèbriques sur P , et on peut se borner au cas où $\Omega=\overline{P}$. Soit p la caractéristique de P ; pour tout $n \not\equiv 0$ (p), le polynôme X^n-1 n'a que des racines simples dans $\overline{P}$, car sa dérivée nX^{n-1} ne s'annule que pour $x=0$, qui n'est pas racine de X^n-1 ; il y a donc exactement n racines n-èmes distinctes de l'unité dans $\overline{P}$, et ce sont des éléments séparables sur P ; comme toute racine de l'unité dans $\overline{P}$ a un ordre non multiple de p , c'est un élément séparable sur P .

Proposition 1.- Le groupe G_p des racines de l'unité dans $\overline{P}$ (fermeture algèbrique d'un corps premier P de caractéristique p) est isomorphe au groupe $S_p/\mathbb{Z}$, où S_p est le sous-groupe du groupe additif Q formé des nombres rationnels pouvant s'écrire sous la forme r/s avec $s \not\equiv 0$ (mod. p).

En premier lieu, montrons que S_p est bien un sous-groupe de Q ; c'est évident si $p=0$, car alors $S_p=Q$; si $p>0$, pour voir que la

la différence de deux nombres rationnels $\frac{r}{s}$, $\frac{r'}{s'}$ appartenant à S_p est aussi un élément de S_p , il suffit de remarquer que si $s \not\equiv 0 \pmod{p}$ et $s' \not\equiv 0 \pmod{p}$, on a aussi $ss' \not\equiv 0 \pmod{p}$ puisque l'anneau $\mathbb{Z}/(p)$ est un corps.

Cela étant, le groupe $S_p/\mathbb{Z}$ peut être identifié à l'ensemble des $x \in S_p \cap [0,1[$, étant entendu que la loi de composition entre deux éléments x,y de cet ensemble est $(x,y) \to x+y-[x+y]$. Désignons par Φ l'ensemble des isomorphismes d'un sous-xxx groupe de $S_p/\mathbb{Z}$ sur un sous-groupe de G_p , ordonné par prolongement ; il est immédiat que Φ n'est pas vide (car l'unique application de l'ensemble $\{0\}$ sur l'ensemble $\{1\}$ appartient à Φ), et est inductif ; il possède donc un élément maximal φ ; nous allons montrer que φ est un isomorphisme de $S_p/\mathbb{Z}$ sur G_p .

Supposons donc que φ soit définie sur un sous-groupe H de $S_p/\mathbb{Z}$, distinct de $S_p/\mathbb{Z}$; comme le groupe $S_p/\mathbb{Z}$ est engendré par les nombres rationnels de la forme $1/s$, avec $s \not\equiv 0 \ (p)$, il existe un de ces entiers s au moins tel que $1/s \notin H$; soit m le plus petit de ces entiers. Soit q le plus petit entier tel que $q/m \in H$; q est l'ordre de la classe de $1/m$ dans le groupe quotient de $S_p/\mathbb{Z}$ par H , donc divise m ; en outre c'est un nombre premier, car si on avait $q=rs$, avec $r > 1$, $s > 1$, et $m=qt=rst$, on aurait $1/st=r/m \in H$, et $st < m$, contrairement à la définition de m . De plus, t est une puissance de q , car si on avait $t=su$, où s est un nombre premier distinct de q , $s/m=1/qu$ et $q/m=1/t$ appartiendraient à H d'après le choix de m ; comme il existe deux entiers λ , μ tels que $\lambda q + \mu s = 1$, $\lambda \frac{q}{m} + \mu \frac{s}{m} = \frac{1}{m}$ appartiendrait aussi à H , ce qui est absurde. On en déduit aisément qu'il n'existe dans H aucun élément ξ

tel que $q\xi = \frac{1}{t}$; en effet, si $t=q^h$ et $h>0$, on aurait $\xi = \frac{1}{q^{h+1}} + \frac{\lambda}{q}$ avec λ entier, donc $\xi - \lambda q^{h-1}.\frac{1}{q^h} = \frac{1}{q^{h+1}} = \frac{1}{m}$ appartiendrait à H contrairement à l'hypothèse ; si $t=1$, on aurait $\xi = \frac{k}{q}$, avec $1<k<q$; mais alors il existe un entier μ tel que $\mu\xi = \frac{1}{q} = \frac{1}{m}$, ce qui entraîne encore $\frac{1}{m} \in H$ contrairement à l'hypothèse.

Cela étant, posons $\psi(\frac{1}{t})=y$, et soit x une racine dans $\overline{P}$ du polynome X^q-y ; comme $y^t=1$, on a $x^m=1$, x est racine de l'unité, et n'appartient pas au groupe $\psi(H)$, puisque nous avons vu qu'il n'existe dans H aucun élément ξ tel que $q\xi = \frac{1}{t}$; en outre, comme q est premier, la relation $x^n \in \psi(H)$ entraîne $n \equiv 0 \pmod{q}$. Considérons alors le sous-groupe H_1 de $S_p/\mathbb{Z}$ engendré par H et $\frac{1}{m}$; nous allons définir une représentation ψ_1 de H_1 dans G_p en posant, pour $\xi = k.\frac{1}{m} + \eta$, où $\eta \in H$, $\psi_1(\xi) = x^k \psi(\eta)$. Il faut montrer que si on a $k.\frac{1}{m} + \eta = k'\frac{1}{m} + \eta'$, on a $x^k \psi(\eta) = x^{k'} \psi(\eta')$; or on a $(k'-k)\frac{1}{m} \in H$, donc $k'-k = \lambda q$ (λ entier), d'où $\eta - \eta' = \frac{\lambda}{t}$, et $\psi(\eta-\eta') = \psi(\eta)/\psi(\eta') = (\psi(\frac{1}{t}))^\lambda = y^\lambda = x^{\lambda q} = x^{k'-k}$. En outre, ψ_1 est un isomorphisme, car la relation $x^k \psi(\eta)=1$ entraîne $x^k \in \psi(H)$, donc $k=\mu q$ (μ entier), et par suite $x^k \psi(\eta) = \psi(\mu.\frac{1}{t}+\eta)=1$ entraîne $\eta + \mu\frac{1}{t} = 0$, c'est-à-dire $k.\frac{1}{m}+\eta = 0$ dans H_1. En raison de la définition de ψ, on voit que notre hypothèse $H \neq S_p/\mathbb{Z}$ est absurde, et que ψ est un isomorphisme de $S_p/\mathbb{Z}$ <u>dans</u> G_p. Il est immédiat en outre que ψ applique $S_p/\mathbb{Z}$ <u>sur</u> G_p, car pour tout $n \not\equiv 0 \pmod{p}$, il existe n éléments distincts $\xi_k = \frac{k}{n}$ de $S_p/\mathbb{Z}$ $(0 \leqslant k < n)$ tels que $n.\xi_k = 0$, donc il y a n racines n-èmes distinctes de l'unité dans l'image par ψ de $S_p/\mathbb{Z}$, ce qui prouve que cette image est identique à G_p.

COROLLAIRE.- <u>Pour tout</u> $n \not\equiv 0 \pmod{p}$ <u>le groupe des racines n-èmes de l'unité dans</u> $\overline{P}$ <u>est un groupe cyclique d'ordre</u> n.

On dit qu'une racine n-ème de l'unité est une racine n-ème primitive de l'unité si elle est d'ordre n ; on peut encore dire que les racines primitives n-èmes sont les éléments qui engendrent le groupe cyclique des racines n-èmes de l'unité. Leur nombre est donc égal au nombre des éléments d'ordre n dans le groupe cyclique $\mathbb{Z}/(n)$. Or, pour que la classe modulo n d'un entier x soit d'ordre n, il faut et il suffit que la relation $xy \equiv 0\ (n)$ (où y est entier), entraîne $y \equiv 0\ (\text{mod.}n)$; cela signifie encore que, dans l'anneau $\mathbb{Z}/(n)$, la classe de x est un élément régulier ; d'ailleurs, si un élément u de $\mathbb{Z}/(n)$ est régulier, il est aussi inversible dans cet anneau, car l'application $v \to uv$ de $\mathbb{Z}/(n)$ dans lui-même étant biunivoque, est une application sur $\mathbb{Z}/(n)$, puisque cet anneau est fini. En résumé :

Proposition 2.- Pour tout entier $n \not\equiv 0\ (\text{mod.}p)$, le nombre des racines primitives n-èmes de l'unité dans $\overline{F}$ est égal au nombre des éléments inversibles dans l'anneau $\mathbb{Z}/(n)$.

Ce nombre est désigné par la notation $\varphi(n)$ et s'appelle l'indicateur d'Euler de n ; lorsqu'un entier x est tel que sa classe dans l'anneau $\mathbb{Z}/(n)$ soit inversible, il existe deux entiers λ, μ tels que $\lambda x = 1 + \mu n$, donc le p.g.c.d. de x et n est égal à 1, et réciproquement ; on dit alors que x et n sont premiers entre eux, ou que chacun est premier avec l'autre (cf. chap. VI, §) ; $\varphi(n)$ peut donc encore être défini comme le nombre des entiers x premiers avec n et tels que $0 < x < n$. En particulier, si q est premier, on a $\varphi(q) = q-1$, puisque tout élément de $\mathbb{Z}/(q)$ autre que 0 est inversible.

On notera que, l'ordre d'une racine n-ème quelconque de l'unité est un diviseur de n ; inversement, pour tout diviseur d de n, une racine primitive d-ème de l'unité est racine n-ème de l'unité ; d'où résulte aussitôt que l'on a

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

2. Corps des racines n-èmes de l'unité.

Soit $K \subset \Omega$ un corps de caractéristique p , P le corps premier contenu dans K . Pour tout entier $n > 0$, on appelle *corps des racines n-èmes de l'unité* sur K , et on désigne par $R_n(K)$ l'extension de K obtenu en adjoignant à K toutes les racines n-èmes de l'unité dans Ω , c'est-à-dire les racines du polynome $X^n - 1$. si $n = mp^h$, où $m \not\equiv 0 \ (p)$, on a $X^n - 1 = (X^m - 1)^{p^h}$, donc $R_n(K) = R_m(K)$ on peut donc se borner au cas où $n \not\equiv 0 \ (p)$. Alors $R_n(K)$ est une extension galoisienne de K (§ 6, cor. 1 et 2 de la prop. 4) ; en outre, si ζ est une racine primitive n-ème de l'unité, toute racine n-ème de l'unité est une puissance de ζ , donc $R_n(K) = K(\zeta)$. Etudions le groupe de Galois Γ de $R_n(K)$ par rapport à K ; il est clair que deux automorphismes de $R_n(K)$ par rapport à K sont identiques si les images de ζ par ces automorphismes sont identiques ; or, pour tout $\sigma \in \Gamma$, $\sigma(\zeta)$ est une racine primitive n-ème de l'unité, puisque σ est un automorphisme du groupe des racines n-èmes de l'unité ; donc on a $\sigma(\zeta) = \zeta^s$, où s est un entier dont la classe modulo n est bien déterminée, et est un élément inversible de l'anneau $\mathbb{Z}/(n)$; désignons cette classe par $\chi(\sigma)$. Si τ est un second automorphisme appartenant à Γ , et $\tau(\zeta) = \zeta^t$, on a $\sigma(\tau(\zeta)) = \sigma(\zeta^t) = (\sigma(\zeta))^t = \zeta^{st}$, d'où $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$; autrement dit, l'application $\sigma \to \chi(\sigma)$ est un *isomorphisme* de Γ *dans* le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/(n)$. En résumé :

Proposition 3.- Etant donné un corps K de caractéristique p , pour tout $n \not\equiv 0 \ (p)$, le groupe de Galois par rapport à K du corps $R_n(K)$ des racines n-èmes de l'unité sur K , est un groupe abélien isomorphe à un sous-groupe du groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/(n)$.

COROLLAIRE.- Le degré de $R_n(K)$ par rapport à K est un diviseur de $\varphi(n)$.

On notera que $R_n(K)$ est composé des corps K et $R_n(P)$; par suite (§6, th.1) le groupe de Galois de $R_n(K)$ par rapport à K est isomorphe au groupe de Galois de $R_n(P)$ par rapport à $K \cap R_n(P)$, c'est-à-dire à un sous-groupe du groupe de Galois Γ_0 de $R_n(P)$ par rapport à P .

On notera que le groupe Γ_0 n'est pas toujours isomorphe au groupe de tous les éléments inversibles de $\mathbb{Z}/(n)$; autrement dit, le degré de $R_n(P)$ sur P peut être strictement inférieur à $\varphi(n)$ (cf. exerc. 3).

Posons $h=\varphi(n)$, et soient ζ_i $(1 \leqslant i \leqslant h)$ les racines primitives n-èmes de l'unité dans $\bar{P}$; le polynome $\Phi_n(X)=\prod_{i=1}^{h}(X-\zeta_i)$ appartient à $P[X]$, car il est invariant par tout automorphisme du groupe Γ_0 ; on dit que l'équation $\Phi_n(x)=0$ est l'équation de la division du cercle en n parties égales, ou équation cyclotomique d'indice n ; Φ_n est appelé le polynome cyclotomique d'indice n ; il n'est irréductible que lorsque l'ordre de Γ_0 est égal à $\varphi(n)$. Lorsque n est donné explicitement, on peut déterminer explicitement Φ_n par le procédé de récurrence suivant : comme nous avons vu que l'ensemble des racines n-èmes de l'unité est la réunion des ensembles de racines primitives d-èmes de l'unité lorsque d parcourt l'ensemble des diviseurs de n , on a

$$X^n-1 = \prod_{n \equiv 0\,(d)} \Phi_d(X) \tag{2}$$

ce qui détermine $\Phi_n(X)$ lorsqu'on connaît les $\Phi_d(X)$ pour tous les diviseurs $d < n$ de n ; comme on a $\Phi_1(X)=X-1$, on obtient bien ainsi une détermination de Φ_n par récurrence sur n . Par exemple, pour $n=q$ premier, on a

$$X^q-1=(X-1)\,\Phi_q(X)$$

d'où $\Phi_q(X) = X^{q-1}+X^{q-2}+\ldots+X+1$.

3. Corps finis.

Nous verrons au chap.VII qu'un corps fini K est nécessairement commutatif ; comme il ne peut contenir un corps isomorphe au corps infini $\mathbb{Q}$, il est de caractéristique $p > 0$; c'est donc une extension de son corps premier qu'on peut identifier à $\mathbb{F}_p = \mathbb{Z}/(p)$; cette extension est évidemment algèbrique et de degré fini sur $\mathbb{F}_p$. Soit n le degré de K sur $\mathbb{F}_p$; considéré comme espace vectoriel sur $\mathbb{F}_p$, K est isomorphe à $(\mathbb{F}_p)^n$, donc a $p^n = q$ éléments.

Le groupe multiplicatif K^* des éléments $\neq 0$ de K est un groupe fini d'ordre q-1 ; on a donc, pour tout $x \in K^*$, $x^{q-1} = 1$, et a fortiori $x^q = x$. Comme cette dernière relation est aussi vérifiée pour x=0, on voit que les q éléments ξ_i $(1 \leqslant i \leqslant q)$ de K sont racines du polynome $X^q - X$, d'où identiquement

$$X^q - X = \prod_{i=1}^{q} (X - \xi_i) \tag{3}$$

On peut donc dire que K est identique au corps des racines de $X^q - X$ dans une extension algèbriquement fermée de K.

Inversement, pour toute puissance $q = p^n$ de p, considérons, dans une extension algèbriquement fermée Ω de $\mathbb{F}_p$, les racines du polynome $X^q - X$, ou, ce qui revient au même, les éléments de Ω invariants par l'endomorphisme $x \to x^q$ de Ω (§ 1, prop.1) ; ils forment un corps $\mathbb{F}_q$, extension de degré fini de $\mathbb{F}_p$; la dérivée de $X^q - X$ étant égale à -1, toutes les racines de $X^q - X$ sont simples, donc $\mathbb{F}_q$ est un corps de q éléments. Si on tient compte de la prop.2 du §6, on voit donc que :

Proposition 4.- Un corps commutatif fini a nécessairement un nombre d'éléments q égal à une puissance p^n d'un nombre premier p. Si Ω est une extension algèbriquement fermée du corps premier $\mathbb{F}_p = \mathbb{Z}/(p)$, $\mathbb{F}_q$ le corps à q éléments formé des racines du polynome $X^q - X$ dans Ω,

tout corps fini ayant q éléments est isomorphe à $\mathbb{F}_q$ et est de degré n sur $\mathbb{F}_p$; $\mathbb{F}_q$ est la seule extension de degré n sur $\mathbb{F}_p$ contenue dans Ω .

Le groupe multiplicatif $\mathbb{F}_q^*$ des éléments $\neq 0$ de $\mathbb{F}_q$ est identique au groupe des racines (q-1)-èmes de l'unité dans Ω ; $\mathbb{F}_q$ est donc le corps des racines (q-1)-èmes de l'unité sur $\mathbb{F}_p$; comme q-1 n'est pas multiple de p , on voit que (cor. de la prop.1) :

Proposition 5.- Le groupe multiplicatif $\mathbb{F}_q^*$ des éléments $\neq 0$ du corps fini $\mathbb{F}_q$ est un groupe cyclique d'ordre q-1 ; si ζ est un générateur de ce groupe, on a $\mathbb{F}_q = \mathbb{F}_p(\zeta)$.

COROLLAIRE.- Etant donné un corps K de caractéristique p , pour tout nombre premier $r \neq p$, le groupe de Galois par rapport à K du corps $R_r(K)$ des racines r-èmes de l'unité sur K , est un groupe cyclique dont l'ordre divise r-1 .

C'est une conséquence de la prop.3 appliquée au cas n=r , compte tenu de la structure du groupe multiplicatif $\mathbb{F}_r^*$, donnée par la prop.5 .

Le corps $\mathbb{F}_q$ est une extension abélienne de $\mathbb{F}_p$ (prop.3) ; son groupe de Galois Γ par rapport à $\mathbb{F}_p$ est aussi le groupe de tous les automorphismes de $\mathbb{F}_q$, puisqu'un tel automorphisme laisse nécessairement invariant tous les éléments du corps premier $\mathbb{F}_p$. Soit σ l'automorphisme $x \to x^p$ de $\mathbb{F}_q$; les éléments de $\mathbb{F}_q$ invariants par σ sont les racines du polynome $X^p - X$ dans $\mathbb{F}_q$; il ne peut y en avoir plus de p , ce qui montre que le corps des éléments de $\mathbb{F}_q$ invariants par σ est identique à $\mathbb{F}_p$; si Γ' est le sous-groupe cyclique de Γ engendré par σ , $\mathbb{F}'_p$ est a fortiori le corps formé des éléments de $\mathbb{F}_q$ invariants par tous les automorphismes appartenant à Γ' ; donc (§6,th.2), on a $\Gamma' = \Gamma$; autrement dit :

Proposition 6.- Le groupe de Galois de $\mathbb{F}_q$ par rapport à $\mathbb{F}_p$ est le groupe cyclique d'ordre n formé des automorphismes $x \to x^{p^k}$ $(0 \leqslant k < n)$.

Exercices.- 1) Pour que l'on ait $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, il faut et il suffit que m soit un diviseur de n. Si m et n sont deux entiers >0 quelconques, δ leur p.g.c.d., μ leur p.p.c.m., l'intersection des corps $\mathbb{F}_{p^m}$ et $\mathbb{F}_{p^n}$ est le corps $\mathbb{F}_{p^\delta}$, leur composé le corps $\mathbb{F}_{p^\mu}$. Si $n=rm$, le groupe de Galois de $\mathbb{F}_{p^n}$ par rapport à $\mathbb{F}_{p^m}$ est un groupe cyclique d'ordre r, formé des automorphismes $x \to x^{p^{km}}$ $(0 \leqslant k < r)$.

2) Montrer que, dans $\mathbb{F}_{p^m}[X]$, le polynome $X^{p^{mn}} - X$ est le produit de tous les polynomes irréductibles dont le degré divise n, et dont le terme de plus haut degré a pour coefficient 1 (utiliser l'exerc.1). Soient h_i $(1 \leqslant i \leqslant r)$ les diviseurs premiers distincts de n ; montrer que le nombre des éléments $\zeta \in \mathbb{F}_{p^{mn}}$ tels que $\mathbb{F}_{p^{mn}} = \mathbb{F}_{p^m}(\zeta)$, est égal à

$$\nu = p^{mn} - \sum_i p^{mn/h_i} + \sum_{i<j} p^{mn/h_i h_j} - \sum_{i<j<k} p^{mn/h_i h_j h_k} + \cdots + (-1)^r p^{mn/h_1 h_2 \cdots h_r}$$

(remarquer qu'un tel élément est caractérisé par la propriété de n'appartenir à aucun des corps $\mathbb{F}_{p^{mn/h_i}}$). Montrer que l'on a

$$p^{mn} - \sum_i p^{mn/h_i} \leqslant \nu \leqslant p^{mn} - p^{mn/h_1 h_2 \cdots h_r}$$

Cas où n est une puissance d'un nombre premier.

Déduire de ce calcul la valeur du nombre des polynomes irréductibles, de degré n et dont le terme de plus haut degré a pour coefficient 1, dans l'anneau $\mathbb{F}_{p^m}[X]$.

3) a) Montrer que le corps $R_n(\mathbb{F}_p)$ des racines n-èmes de l'unité sur $\mathbb{F}_p$ est identique au corps $\mathbb{F}_{p^m}$, où m est le plus petit entier tel que p^m-1 soit multiple de n .

b) Montrer que pour tout nombre premier p non diviseur de 12, on a $\Phi_{12}(X)=X^4-X^2+1$ dans $\mathbb{F}_p[X]$, et déduire de a) que ce polynome est réductible dans chacun des anneaux $\mathbb{F}_p[X]$. Dans ce cas, $\mathbb{F}_p$ contient toujours des racines 12-èmes de l'unité différentes de 1 .

c) Montrer que le corps $\mathbb{F}_3$ ne contient aucune racine 13-ème de l'unité distincte de 1 , mais que le degré du corps $R_{13}(\mathbb{F}_3)$ sur $\mathbb{F}_3$ est égal à $3 < \varphi(13)=12$.

4) Soit ζ une racine primitive $(q-1)$-ème de l'unité dans $\mathbb{F}_q$ $(q=p^n)$, de sorte que tout élément de $\mathbb{F}_q^*$ se met sous la forme ζ^k $(0 \leqslant k \leqslant q-1)$. Montrer que les éléments de $\mathbb{F}_q^*$ qui sont puissances m-èmes d'un autre élément de $\mathbb{F}_q^*$ sont les $(q-1)/d$ éléments ζ^{hd} $(0 \leqslant h < (q-1)/d)$, où d est le p.g.c.d. de $q-1$ et de m ; chacun de ces éléments est alors puissance m-ème de d éléments distincts de $\mathbb{F}_q$.

5) Soit K un corps de caractéristique p , n un entier non divisible par p , ω_i $(1 \leqslant i \leqslant n)$ les n racines n-èmes de l'unité sur K . Démontrer que l'on a $\sum_{i=1}^{n} \omega_i^m = 0$ si m n'est pas multiple de n , et $\sum_{i=1}^{n} \omega_i^m = n$ si m est multiple de n .

6) Dans le corps $\mathbb{F}_q$ $(q=p^n \quad p \neq 2)$, le nombre ν des solutions (x_1, x_2) de l'équation $a_1x_1^2+a_2x_2^2=b$ $(a_1a_2 \neq 0)$ est donné par les formules suivantes :

1° si $b=0$ et si $-a_1a_2$ n'est pas un carré dans $\mathbb{F}_q$, $\nu = 1$;

2° si $b \neq 0$ et si $-a_1a_2$ n'est pas un carré dans $\mathbb{F}_q$, $\nu = q+1$;

3° si $b=0$ et si $-a_1a_2$ est un carré dans $\mathbb{F}_q$, $\nu = 2q-1$;

4° si $b \neq 0$ et si $-a_1a_2$ est un carré dans $\mathbb{F}_q$, $\nu = q-1$.

(Lorsque $-a_1a_2$ est un carré, ramener l'équation à la forme $yz=c$; lorsque $-a_1a_2$ n'est pas un carré, adjoindre à $\mathbb{F}_q$ une racine du polynome $X^2+a_1a_2$, et ramener l'équation à la forme $t^{q+1}=d$ dans $\mathbb{F}_{q^2}$, où $d \in \mathbb{F}_q$; utiliser l'exerc. 4).

7) a) Dans le corps $\mathbb{F}_q$ ($q=p^n$ $p\neq 2$), le nombre ν des solutions $(x_1,x_2,\ldots,x_{2m})$ de l'équation $a_1x_1^2+\ldots+a_{2m}x_{2m}^2 = b$ $(a_1\neq 0)$ est donné par les formules suivantes :

1° si $b=0$ et si $(-1)^m a_1a_2\ldots a_{2m}$ n'est pas un carré
$$\nu = q^{2m-1}-q^m+q^{m-1} ;$$

2° si $b\neq 0$ et si $(-1)^m a_1a_2\ldots a_{2m}$ n'est pas un carré
$$\nu = q^{2m-1}+q^{m-1} ;$$

3° si $b=0$ et si $(-1)^m a_1a_2\ldots a_{2m}$ est un carré ,
$$\nu = q^{2m-1}+q^m-q^{m-1} ;$$

4° si $b\neq 0$ et si $(-1)^m a_1a_2\ldots a_{2m}$ est un carré
$$\nu = q^{2m-1}-q^{m-1} .$$

(Raisonner par récurrence sur m , en utilisant l'exerc. 6).

b) Le nombre ν des solutions de l'équation
$a_1x_1^2+\ldots+a_{2m+1}x_{2m+1}^2=b$ $(a_1\neq 0)$ est donné par les formules suivantes :

1° si $b=0$, $\nu = q^{2m}$;

2° si $b\neq 0$ et si $(-1)^m ba_1a_2\ldots a_{2m+1}$ n'est pas un carré
$$\nu = q^{2m}-q^m ;$$

3° si $b\neq 0$ et si $(-1)^m ba_1a_2\ldots a_{2m+1}$ est un carré
$$\nu = q^{2m}+q^m$$

(se ramener au cas a)).

8) Soient s_i $(1\leqslant i\leqslant p)$ les fonctions symétriques élémentaires des entiers $1,2,\ldots,p-1$, où p est premier ; démontrer les congruences $s_i \equiv 0$ $(1\leqslant i\leqslant p-1)$, $(p-1)! \equiv -1 \pmod{p}$ (appliquer l'identité (3) dans $\mathbb{F}_p = \mathbb{Z}/(p)$).

9) a) Soit P un corps premier de caractéristique p , n un entier non multiple de p ; soient ω_i $(1 \leqslant i \leqslant n)$ les n racines n-èmes de l'unité sur P . Démontrer l'identité

$$f(X_1,X_2,..X_n)=\begin{vmatrix} X_1 & X_2 & \dots X_{n-1} & X_n \\ X_2 & X_3 & \dots X_n & X_1 \\ X_3 & X_4 & \dots X_1 & X_2 \\ \dots & \dots & \dots & \dots \\ X_n & X_1 & \dots X_{n-2} & X_{n-1} \end{vmatrix} = \prod_{i=1}^{n} (X_1+\omega_i X_2+\omega_i^2 X_3+..+\omega_i^{n-1} X_n)$$

dans l'anneau $P[X_1,X_2,..,X_n]$.

(Multiplier le déterminant du premier membre par le déterminant

$$\begin{vmatrix} 1 & \omega_1 & \omega_1^2 & \dots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \dots & \omega_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \end{vmatrix}$$

b) On suppose que $P=Q$ $(p=0)$ et $a=q^e$, où q est un nombre premier ; montrer que, dans le polynome f , tous les coefficients sont multiples de q , sauf ceux des termes X_i^n $(1 \leqslant i \leqslant n)$ qui sont égaux à 1 (pour chaque i , considérer la dérivée logarithmique $\frac{1}{f}\frac{\partial f}{\partial X_i}$; l'exprimer à l'aide de l'identité démontrée ci-dessus, et développer l'expression trouvée en série formelle par rapport aux puissances de $1/X_i$ puis utiliser l'exerc.5).

c) Soit P un corps premier de caractéristique $p > 0$, et $n=p^e$; montrer que $f(X_1,X_2,\dots,X_n)=(X_1+X_2+\dots+X_n)^n$ (utiliser b)).

10) Soit K un corps de caractéristique p , q un nombre premier $\neq p$, ζ une racine primitive q-ème de l'unité sur K , ν le degré par rapport à K du corps $R_q(K)=K(\zeta)$; le groupe de Galois de $E=R_n(K)$ par rapport à K est cyclique ; soit σ un automorphisme de $R_n(K)$ engendrant ce groupe, et soit s l'entier (tel que $0<s<q$) tel que

$\zeta^{\sigma} = \zeta^{s}$; λ est le plus petit des entiers k tels que $s^k \equiv 1$ (q).

a) Montrer qu'il existe un polynome $\psi(X)$, à coefficients entiers rationnels, tel que $\psi(s)=1$, que pour tout $x \in E$, $y=x^{\psi(\sigma)}$ soit tel que $y^{\sigma-s}$ soit une puissance q-ème dans E , et que réciproquement, tout élément y ayant cette propriété soit ~~propriété~~ produit d'une puissance q-ème et d'un élément de la forme $x^{\psi(\sigma)}$ (considérer, dans l'anneau $\mathbb{F}_q[X]$ le polynome $(X^{\lambda}-1)/(X-s)$).

b) Montrer que si $x \in E$ est tel que $x^{(\sigma-s)^2}$ soit puissance q-ème , $x^{\sigma-s}$ est déjà puissance q-ème (dans l'anneau $\mathbb{F}_q[X]$, développer $X^{\lambda}-1$ suivant les puissances de X-s) .

§ 8. Extensions cycliques.

1. Le théorème de Hilbert.

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

Soit E une extension cyclique d'un corps K , de degré n sur K ; son groupe sur K est donc isomorphe à $\mathbb{Z}/(n)$; or, les sous-groupes de $\mathbb{Z}/(n)$ sont les groupes cycliques $\mathbb{Z}/(d)$, où d parcourt l'ensemble des diviseurs de n , le groupe quotient de $\mathbb{Z}/(n)$ par $\mathbb{Z}/(d)$ étant isomorphe à $\mathbb{Z}/(\frac{n}{d})$. Par suite (§ 6, th.2), il y a correspondance biunivoque entre les diviseurs de n et les sous-corps de E contenant K : à tout diviseur d de n correspond un sous-corps F de E , cyclique et de degré d sur K , et tel que E soit cyclique et de degré $\frac{n}{d}$ sur F .

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

Théorème 1 (Hilbert).- Soit E une extension cyclique d'un corps K , σ un générateur du groupe (cyclique) de E par rapport à K .

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

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

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

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

("résolvante de Lagrange-Hilbert") ; comme les n automorphismes distincts σ^k $(0 \leqslant k \leqslant n-1)$ de E relatifs à K sont linéairement indépendants (§ 4, th. 1), il existe un $t_0 \in E$ tel que $y=u(t_0) \neq 0$; or, comme $x^{1+\sigma+\ldots+\sigma^{n-2}+\sigma^{n-1}} = N_{E|K}(x)=1$ par hypothèse, on a

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

d'où $xy^{\sigma}=y$, $x=y^{1-\sigma}$. Il est évident, inversement, que si $x=y^{1-\sigma}$ on a $N_{E|K}(x)=1$; enfin, la relation $y^{1-\sigma}=y_1^{1-\sigma}$ entraîne $y_1y^{-1}=(y_1y^{-1})^{\sigma}$; par suite y_1y^{-1} est invariant par tous les automorphismes de E relatifs à K , donc appartient à K .

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

$$z = \frac{1}{Tr_{E|K}(v)} \left(x\sigma(v)+(x+\sigma(x))\sigma^2(v)+\ldots+(x+\sigma(x)+\ldots+\sigma^{n-2}(x))\sigma^{n-1}(v)\right)$$

On a, en vertu de l'hypothèse $Tr_{E|K}(x) = \sum_{k=0}^{n-1} \sigma^k(x)=0$,

$$\sigma(z) = \frac{1}{Tr_{E|K}(v)} \left(\sigma(x)\sigma^2(v)+\ldots+(\sigma(x)+\sigma^2(x)+\ldots+\sigma^{n-2}(x))\sigma^{n-1}(v)-xv\right)$$

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

2. Extensions cycliques et équations binômes.

La première partie du th. de Hilbert va nous permettre de donner une génération simple d'une extension cyclique E de degré n sur un corps K , lorsqu'on fait les deux hypothèses suivantes : 1^0 n n'est pas multiple de la caractéristique p de K ; 2^0 K contient toutes les racines n-èmes de l'unité dans Ω .

En effet, soit alors $\zeta\in K$ une racine primitive n-ème de l'unité On a $N_{E|K}(\zeta)=\zeta^n=1$, donc il existe $\theta\in E$ tel que $\zeta=\theta^{1-\sigma}$, ou encore $\theta^\sigma=\zeta^{-1}\theta$; on tire aussitôt de là que $\theta^{\sigma^k}=\zeta^{-k}\theta$, donc les n conjugués de θ sont distincts, autrement dit θ est de degré n sur K , et par suite $E=K(\theta)$; d'autre part, on a $1=\zeta^n=(\theta^n)^{1-\sigma}$, donc $\sigma(\theta^n)=\theta^n$, ce qui prouve que θ^n appartient au corps K . En résumé :

Proposition 1.- Soit E une extension cyclique de degré n d'un corps K de caractéristique p , telle que $n\not\equiv 0\ (p)$, et que K contienne toutes les racines n-èmes de l'unité. Il existe alors un polynome irréductible de $K[X]$, de la forme X^n-a , tel que E soit engendré par une racine quelconque de ce polynome.

COROLLAIRE.- Pour qu'un élément $\xi\in E$ soit racine d'un polynome de $K[X]$ de la forme X^n-b , il faut et il suffit que $\xi=\lambda\theta^k$, où $\lambda\in K$; pour qu'en outre on ait $E=K(\xi)$, il faut et il suffit que k soit premier à n .

En effet, si $\xi^n = b \in K$, on a $(\xi^n)^\sigma = \xi^n$, ou $(\xi^{1-\sigma})^n = 1$; par suite $\xi^\sigma = \omega\xi$, où ω est une racine n-ème de l'unité ; on peut écrire $\omega = \xi^{-k} = (\theta^{\sigma-1})^k$, d'où $(\xi\theta^{-k})^\sigma = \xi\theta^{-k}$, ce qui entraîne $\xi\theta^{-k} \in K$; la réciproque est évidente. Si maintenant $E = K(\xi)$, les n conjugués $\xi^{\sigma^h} = \omega^h\xi$ de ξ $(0 \leqslant h \leqslant n-1)$ doivent être distincts, et réciproquement ; mais cela signifie que ω est racine primitive n-ème de l'unité, donc (§ 7) que k est premier à n.

La prop.1 admet la réciproque suivante :

Proposition 2.- Soit K un corps de caractéristique p, n un entier > 0 non divisible par p et tel que K contienne toutes les racines n-èmes de l'unité. Pour tout $a \in K$, le corps des racines E du polynome $X^n - a$ est une extension cyclique de K, engendrée par une quelconque des racines de $X^n - a$; le degré $[E:K] = d$ est un diviseur de n, égal au plus petit des nombres entiers $r > 0$ tels que a^r soit puissance n-ème d'un élément de K.

En effet, soit θ une racine de $X^n - a$; pour toute autre racine θ' de ce polynome, on a $\theta'^n = \theta^n$, ou $(\frac{\theta'}{\theta})^n = 1$, d'où $\theta' = \omega\theta$, où ω est une racine n-ème de l'unité, qui appartient par hypothèse à K ; donc $\theta' \in K(\theta)$, ce qui prouve que $E = K(\theta)$. Comme la dérivée de $X^n - a$ ne s'annule que pour $x = 0$, aucune racine de $X^n - a$ n'est multiple (sauf si $a = 0$, cas trivial que nous laissons de côté) ; donc E est une extension galoisienne de K. Soit Γ le groupe de E relatif à K, σ un élément quelconque de Γ ; comme $E = K(\theta)$, la donnée de $\sigma(\theta)$ détermine complètement $\sigma(x)$ pour tout $x \in E$; comme $\sigma(\theta)$ est racine de $X^n - a$, on a $\sigma(\theta) = \xi_\sigma\theta$, où ξ_σ est une racine n-ème de l'unité bien déterminée par σ. L'application $\sigma \longrightarrow \xi_\sigma$ est une application biunivoque de Γ dans le groupe multiplicatif H des racines n-èmes de l'unité ; en outre, c'est une représentation de Γ dans H, car si τ est un second élément

de Γ , on a $\sigma\tau(\theta)=\sigma(\tau(\theta))=\sigma(\zeta_\tau\theta)=\zeta_\tau\sigma(\theta)=\zeta_\sigma\zeta_\tau\theta$, d'où $\zeta_{\sigma\tau}=\zeta_\sigma\zeta_\tau$. On voit donc que Γ est isomorphe à un sous-groupe de H ; comme H est cyclique d'ordre n (§ 7,cor.de la prop.1), Γ est un groupe cyclique dont l'ordre d est un diviseur de n . Posons n=dh ; des relations $\sigma(\theta)=\zeta_\sigma\theta$ on déduit que $N_{E|K}(\theta)=\mu\theta^d$, où $\mu\in K$, d'où $\theta^d=b\in K$. Par suite on a $a=\theta^n=b^h$, d'où $a^d=b^{nh}=b^n$. S'il existait un nombre $r<d$ tel que $a^r=c^n$, où $c\in K$, on déduirait de la relation $\theta^n=a$ que $\theta^{rn}=c^n$, d'où $\theta^r=\omega c$, ω étant une racine n-ème de l'unité ; θ serait donc racine d'un polynome X^r-a de $K[X]$, ce qui est contraire au fait que θ est de degré d sur K .

Si P_n est le groupe multiplicatif des éléments de K^* qui sont puissances n-èmes d'éléments de K^*, le nombre d peut encore être défini comme l'ordre de la classe de a dans le groupe quotient K^*/P_n ; cela montre à nouveau que cet ordre est un diviseur de n , et que les entiers r tels que $a^r\in P_n$ sont les multiples de d .

3. Extensions cycliques de degré q^e (q premier et $\neq p$).

Poursuivons l'étude des extensions cycliques en considérant maintenant les cas où les deux hypothèses de la prop.1 ne sont plus nécessairement vérifiées. Nous commencerons par nous ramener au cas où le degré d'une telle extension sur le corps K est une puissance d'un nombre premier. Pour cela, remarquons que si E est une extension cyclique de K , de degré $n=mq^e$, où q est un nombre premier et $m\not\equiv 0\ (q)$, il existe deux sous-corps cycliques M,N de E , de degrés respectifs m et q^e sur K ; on a $M\cap N=K$, car le degré de $M\cap N$ sur K devant diviser à la fois q^e et m , ne peut être que 1 ; d'où résulte (§ 6,th.1) que M et N sont linéairement disjoints sur K et que E est leur composé.

En répétant ce raisonnement pour M , on voit que l'on peut se borner à étudier les extensions cycliques E de K dont le degré a la fome q^e , où q est premier.

Nous allons d'abord considérer le cas où $q \neq p$, et nous nous limiterons en outre au cas où K contient les racines q-èmes de l'unité (mais non les racines q^e-èmes).

Proposition 3.- Soit E une extension cyclique de degré q^e (q premier) d'un corps K de caractéristique $p \neq q$, contenant les racines q-èmes de l'unité. Soient ζ une racine primitive q-ème de l'unité, σ un automorphisme de E engendrant le groupe de Galois de E par rapport à K . Si F est le sous-corps de E de degré q^{e-1} sur K , il existe deux éléments α, β de F tels que $N_{F|K}(\beta) = \zeta$, que $\alpha^{\sigma-1} = \beta^q$, que le polynome $X^q - \alpha$ soit irréductible dans $F[X]$, et que, pour toute racine θ de ce polynome, on ait $E = K(\theta)$ et $\theta^\sigma = \beta\theta$.

Prenons pour simplifier l'écriture $m = q^{e-1}$; le groupe de E par rapport à F est un groupe cyclique d'ordre q , engendré par σ^m . Il existe un élément $\theta \in E$ racine d'un polynome irréductible $X^q - \alpha$ de $F[X]$, tel que $E = F(\theta)$, et que $\theta^{\sigma^m} = \zeta\theta$ (prop.1). On a aussi $E = K(\theta)$, car les seuls sous-corps de E distincts de E sont F et les sous-corps de F de degré q^h $(0 \leqslant h \leqslant e-1)$ sur K ; comme $K(\theta)$ n'est pas contenu dans F , il est identique à E . Comme on a aussi $E = K(\theta^\sigma)$, θ^σ n'appartient pas à F , donc $E = F(\theta^\sigma)$; or on a $(\theta^\sigma)^q = \alpha^\sigma \in F$, donc (cor. de la prop.1), on a $\theta^\sigma = \beta\theta^k$ avec $0 < k < q$ et $\lambda \in F$; de cette relation, on déduit par récurrence $\theta^{\sigma^h} = \lambda_h \theta^{k^h}$ pour tout entier h , avec $\lambda_h \in F$; en particulier, pour $h = q^e$, il vient $\theta = \lambda_h \theta^{k^h}$, autrement dit $\theta^{k^h - 1} \in F$, ce qui n'est possible que si $k^h - 1 \equiv 0 \pmod{q}$; mais on a $k^{q^e} \equiv k \pmod{q}$, donc on doit avoir $k \equiv 1 \ (q)$, c'est-à-dire $k = 1$. De la relation $\beta = \theta^{\sigma-1}$, on déduit alors

$N_{F|K}(\beta)=\beta^{1+\sigma+\sigma^2+..+\sigma^{m-1}} = \theta^{(\sigma-1)(1+\sigma+\sigma^2+...+\sigma^{m-1})} = \theta^{\sigma^m-1} = \zeta$

et $\alpha^{\sigma-1}=(\theta^q)^{\sigma-1} = \beta^q$.

La prop.3 admet la réciproque suivante :

Proposition 4. Soit F une extension cyclique de degré q^{e-1} (q premier) d'un corps K de caractéristique $p\neq q$, contenant les racines q-èmes de l'unité. Soit ζ une racine primitive q-ème de l'unité , σ un automorphisme de F engendrant le groupe de Galois de F par rapport à K . S'il existe un élément $\beta\in F$ tel que $N_{F|K}(\beta) = \zeta$, et si $\alpha\in F$ est tel que $\alpha^{\sigma-1}=\beta^q$, le corps des racines E du polynome $X^q-\lambda\alpha$ ($\lambda\in K^*$) de $F[X]$, est une extension cyclique de K , de degré q^e sur K , engendrée par une quelconque des racines θ de $X^q-\lambda\alpha$; σ se prolonge en un automorphisme de E (noté encore σ) engendrant le groupe de E par rapport à K , et tel que $\theta^\sigma=\beta\theta$. En outre, toute extension cyclique de K , de degré q^e et contenant F , est une extension de la forme précédente (pour un $\lambda\in K^*$ convenable).

Tout d'abord de $N_{F|K}(\beta)=\zeta$, on tire $N_{F|K}(\beta^q)=\zeta^q=1$, donc il existe bien $\alpha\in F$ tel que $\beta^q=\alpha^{\sigma-1}$, d'après le th.1 . Le polynome $X^q-\lambda\alpha$ est irréductible dans $F[X]$, sans quoi (prop.2), $[E:F]$ serait un diviseur de q distinct de q , donc on aurait $E=F$, et $\lambda\alpha=\mu^q$, avec $\mu\in F$. Or, on tire de cette dernière relation, $\lambda\alpha^\sigma=\mu^{q\sigma}$, d'où $\beta^q=\alpha^{\sigma-1}=(\mu^{\sigma-1})^q$, ce qui entraîne $\beta=\zeta^h\mu^{\sigma-1}$, où h est un entier ; on déduit de là que $N_{F|K}(\beta)=N_{F|K}(\zeta^h)=\zeta^{hq^{e-1}}=1$, contrairement à la définition de β . On a donc $[E:F]=q$, d'où $[E:K]=q^e$, et si θ est une racine quelconque de $X^q-\lambda\alpha$, $E=F(\theta)$. Cela étant, on a $(\beta\theta)^q=\beta^q\lambda\alpha=\lambda\alpha^{\sigma-1}\alpha=\lambda\alpha^\sigma$, autrement dit, $\beta\theta$ est racine du polynome $X^q-\lambda\alpha^\sigma$, transformé de $X^q-\lambda\alpha$ par σ ; par suite, il existe un isomorphisme de E dans Ω , relatif à K , qui prolonge σ et applique θ sur $\beta\theta$; nous désignerons encore cet isomorphisme par σ ;

comme σ transforme F en lui-même et que $\beta\theta$ est dans E , σ est un automorphisme de E . En outre, on a $\theta^{\sigma^m} = \beta^{1+\sigma+\sigma^2+\ldots+\sigma^{m-1}}\theta =$ $= N_{F|K}(\beta)\theta = \zeta\theta \neq \theta$ $(m=q^{e-1})$, et de même $\theta^{\sigma^n}=\theta$ $(n=q^e)$, donc σ est d'ordre q^e , ce qui montre que E est une extension cyclique de K de degré q^e ; on voit comme dans la démonstration de la prop.3 que $E=K(\theta)$. Si maintenant E_1 est une extension cyclique de K , de degré q^e sur K et contenant F , la prop.3 montre qu'il existe deux éléments α_1,β_1 de F tels que $N_{F|K}(\beta_1)=\zeta$, que $\alpha_1^{\sigma-1}=\beta_1^q$, et que E soit le corps des racines du polynome $X^q-\alpha_1$ de $F[X]$. On a donc $N_{F|K}(\frac{\beta_1}{\beta})=1$, et par suite il existe $\gamma\in F$ tel que $\beta_1=\gamma^{\sigma-1}\beta$, d'où $\alpha_1^{\sigma-1}=(\gamma^q)^{\sigma-1}\beta^q=(\gamma^q\alpha)^{\sigma-1}$, ce qui entraîne $\alpha_1=\lambda\gamma^q\alpha$ avec $\lambda\in K$ (th.1). Si θ_1 est une racine de $X^q-\alpha_1$, on a aussi $E=F(\frac{\theta_1}{\gamma})$ puisque $\gamma\in F$, donc E est corps des racines de $X^q-\lambda\alpha$.

Remarque.- Dans une extension cyclique F de degré q^{e-1} sur K , il n'existe pas toujours d'élément β tel que $N_{F|K}(\beta)=\zeta$, autrement dit, il n'existe pas toujours d'extension E de K , cyclique et de degré q^e sur K , et contenant F . Par exemple, si i est une racine du polynome X^2+1 de $Q[X]$, irréductible dans $Q[X]$, on a pour tout élément $x=a+bi$ de $Q(i)$ (a et b rationnels), $N(x)=a^2+b^2\neq -1$, donc $Q(i)$ n'est contenu dans aucune extension cyclique de degré 4 sur le corps Q .

4. Extensions cycliques de degré p^e .

Proposition 5.- Soit E une extension cyclique de degré p d'un corps K de caractéristique p . Il existe alors un polynome irréductible de $K[X]$, de la forme X^p-X-a , tel que E soit engendré par une racine quelconque de ce polynome.

En effet, on a, dans E , $\mathrm{Tr}_{E|K}(1)=0$, puisque K est de caractéristique p ; d'après le th.1, il existe un élément $\theta \in E$ tel que $\sigma(\theta)-\theta=1$, ou $\sigma(\theta)=\theta+1$ (en désignant par σ un automorphisme de E engendrant le groupe de E relatif à K) ; on déduit de là que $\sigma^h(\theta)=\theta+h$ pour $0 \leqslant h \leqslant p-1$, donc tous les conjugués de θ sont distincts, θ est de degré p sur K et on a $E=K(\theta)$; en outre le polynome minimal de θ est $\prod_{h=0}^{p-1}(X-\theta-h)$, donc se déduit du polynome $\prod_{h=0}^{p-1}(Y-h)$ en y remplaçant Y par $X-\theta$; mais $\prod_{h=0}^{p-1}(Y-h)=Y^p-Y$ (§ 7, formule (3)), donc le polynome minimal de θ est $(X-\theta)^p-(X-\theta)=X^p-X-a$, avec $a=\theta^p-\theta \in K$.

COROLLAIRE.- <u>Pour qu'un élément</u> $\xi \in E$ <u>engendre</u> E <u>sur</u> K <u>et soit racine d'un polynome de la forme</u> X^p-X-b <u>de</u> $K[X]$, <u>il faut et il suffit que</u> $\xi = k\theta+\lambda$, <u>où</u> $\lambda \in K$ <u>et</u> k <u>est un entier</u> $\neq 0$ (dans $\mathbb{Z}/(p)$).

En effet, la relation $x^p-x=y^p-y$ s'écrit $(x-y)^p=x-y$, donc est équivalente à $x-y \in \mathbb{Z}/(p)$; par hypothèse on a $\sigma(\xi) \neq \xi$, et $\sigma(\xi)$ est racine de X^p-X-b , donc $\sigma(\xi)=\xi+k$, où k est un entier $\neq 0$; on a donc $\sigma(\xi-k\theta)=\xi-k\theta$, d'où $\xi-k\theta \in K$; la réciproque est évidente.

La proposition 5 admet la réciproque suivante :

<u>Proposition 6</u>.- <u>Soit</u> K <u>un corps de caractéristique</u> p . <u>Pour tout</u> $a \in K$, <u>le polynome</u> X^p-X-a <u>est irréductible dans</u> $K[X]$, <u>ou a toutes ses racines dans</u> K ; <u>dans le premier cas, le corps des racines</u> E <u>du polynome</u> X^p-X-a <u>est une extension cyclique de</u> K , <u>de degré</u> p <u>sur</u> K , <u>engendrée par une quelconque des racines de</u> X^p-X-a .

En effet, si θ est une racine de X^p-X-a , les p éléments $\theta+h$ ($0 \leqslant h \leqslant p-1$) sont aussi racines de ce polynome ; comme ils sont distincts, ce sont toutes les racines de X^p-X-a , et ce sont des éléments séparables sur K , donc E est galoisienne sur K . Si σ est un élément du groupe de Galois Γ de E par rapport à K , on a $\sigma(\theta)=\theta+h_\sigma$, où $h_\sigma \in \mathbb{Z}/(p)$; en outre, pour deux automorphismes σ, τ , on a

$\sigma\tau(\theta) = \sigma(\tau(\theta)) = \sigma(\theta+h_\tau) = \theta+h_\sigma+h_\tau$, autrement dit $h_{\sigma\tau} = h_\sigma + h_\tau$, l'application $\sigma \to h_\sigma$ est une représentation de dans le groupe additif $\mathbb{Z}/(p)$, représentation qui est biunivoque puisqu'on a $E=K(\theta)$, et que la donnée de $\sigma(\theta)$ détermine complètement $\sigma(x)$ pour tout $x \in E$. Comme $\mathbb{Z}/(p)$ est cyclique d'ordre premier p , Γ est isomorphe à $\mathbb{Z}/(p)$ ou réduit à l'élément neutre ; dans le premier cas, les racines de X^p-X-a sont toutes conjuguées autrement dit X^p-X-a est irréductible.

Etudions maintenant les extensions cycliques de degré p^e , pour $e > 1$.

Proposition 7.- Soit E une extension cyclique de degré p^e d'un corps K de caractéristique p ; soit σ un automorphisme de E engendrant le groupe de Galois de E par rapport à K . Si F est le sous-corps de E de degré p^{e-1} sur K , il existe deux éléments α,β de F tels que $Tr_{F/K}(\beta)=1$, que $\sigma(\alpha)-\alpha = \beta^p-\beta$, que le polynome $X^p-X-\alpha$ soit irréductible dans $F[X]$, et que, pour toute racine θ de ce polynome, on ait $E=K(\theta)$ et $\sigma(\theta)=\theta+\beta$.

Posons encore $m=q^{e-1}$; le groupe de E par rapport à F est un groupe cyclique d'ordre p , engendré par σ^m . D'après la prop.5, il existe un élément $\theta \in E$, racine d'un polynome irréductible $X^p-X-\alpha$ de $F[X]$, tel que $E=F(\theta)$ et $\sigma^m(\theta)=\theta+1$. On voit comme dans la prop.3 que l'on a aussi $E=K(\theta)$; on a donc aussi $E=K(\sigma(\theta))$ et par suite $\sigma(\theta)$ n'appartient pas à F , d'où $E=F(\sigma(\theta))$; comme $\sigma(\theta^p)=\sigma(\theta)+\sigma(\alpha)$, le cor. de la prop.5 montre que $\sigma(\theta)=k\theta+\beta$ où k est entier et $\beta \in F$. De cette relation, on déduit par récurrence que $\sigma^h(\theta)=k^h\theta+\beta_h$ pour tout entier h , avec $\beta_h \in F$; en particulier, pour $h=p^e$, il vient $\theta=k^h\theta+\beta_h$, autrement dit, $(k^h-1)\theta \in F$, ce qui n'est possible que si $k^h-1 \equiv 0 \pmod{p}$; mais on a $k^{p^e} \equiv k \pmod{p}$, donc on doit avoir $k=1$. De la relation $\beta=(\sigma-1)(\theta)$, on déduit

$Tr_{F|K}(\beta)=(1+\sigma+\sigma^2+..+\sigma^{m-1})(\beta)=(\sigma-1)(1+\sigma+..+\sigma^{m-1})(\theta)=(\sigma^m-1)(\theta)=1$

et comme $\sigma(\theta^p)=(\sigma(\theta))^p=\theta^p+\beta^p$, on a $\sigma(\alpha)-\alpha=\theta^p+\beta^p-(\theta+\beta)-(\theta^p-\theta)=\beta^p-\beta$.

Réciproquement :

Proposition 8.- Soit F une extension cyclique de degré p^{e-1} d'un corps K de caractéristique p $(e>1)$; soit σ un automorphisme de F engendrant le groupe de Galois de F par rapport à K . Il existe deux éléments α,β de F tels que $Tr_{F|K}(\beta)=1$ et $\sigma(\alpha)-\alpha=\beta^p-\beta$; le corps des racines E du polynome $X^p-X-\alpha-\lambda$ $(\lambda\in K)$ de $F[X]$, est une extension cyclique de K , de degré p^e sur K , engendrée par une quelconque des racines θ de $X^p-X-\alpha-\lambda$; σ se prolonge en un automorphisme de E (noté encore σ) engendrant le groupe de E par rapport à K , et tel que $\sigma(\theta)=\theta+\beta$. En outre, toute extension cyclique de K , de degré p^e et contenant F , est une extension de la forme précédente.

En premier lieu, il existe des éléments $x\in F$ tels que $Tr_{F|K}(x)=x+\sigma(x)+\sigma^2(x)+...+\sigma^m(x)\neq 0$ $(m=p^{e-1})$ en vertu du th.1 du §4 ; si x_0 est un tel élément, on aura, en posant $\beta=x_0/Tr_{F|K}(x_0)$, $Tr_{F|K}(\beta)=1$; comme on a $Tr_{F|K}(x^p)=(Tr_{F|K}(x))^p$ par définition de la trace, pour tout $x\in F$, on a aussi $Tr_{F|K}(\beta^p)=1$, d'où $Tr_{F|K}(\beta^p-\beta)=0$; par suite (th.1), il existe $\alpha\in F$ tel que $\sigma(\alpha)-\alpha=\beta^p-\beta$. Le polynome $X^p-X-\alpha-\lambda$ est irréductible dans $F[X]$, sans quoi (prop.6) on aurait $E=F$, et $\alpha+\lambda=\mu^p-\mu$, avec $\mu\in F$. Or, on tire de cette relation que $\sigma(\alpha)+\lambda=\sigma(\mu^p)-\sigma(\mu)$, d'où $\beta^p-\beta=\sigma(\alpha)-\alpha=(\sigma(\mu)-\mu)^p-(\sigma(\mu)-\mu)$, ce qui s'écrit encore $(\beta-\sigma(\mu)+\mu)^p=\beta-\sigma(\mu)+\mu$; on aurait donc $\beta=\sigma(\mu)-\mu+\gamma$, avec $\gamma\in K$; mais on tire de là $Tr_{F|K}(\beta)=Tr_{F|K}(\gamma)=p^{e-1}\gamma=0$ contrairement à l'hypothèse. On a donc (prop.6) $[E:F]=p$, d'où $[E:K]=p^e$, et si θ est une racine quelconque de $X^p-X-\alpha-\lambda$, on a $E=F(\theta)$

Cela étant, on a $(\theta+\beta)^p = \theta^p+\beta^p = \theta+\beta+\sigma(\alpha)+\lambda$, autrement dit, $\theta+\beta$ est racine du polynome $X^p-X-\sigma(\alpha)-\lambda$, transformé de $X^p-X-\alpha-\lambda$ par σ ; par suite, il existe un isomorphisme de E dans Ω , relatif à K , qui prolonge σ et applique θ sur $\theta+\beta$; nous désignerons encore cet isomorphisme par σ ; comme σ transforme F en lui-même, et que $\theta+\beta \in E$, σ est un <u>automorphisme</u> de E . En outre, on a $\sigma^m(\theta)=\theta+(1+\sigma+\sigma^2+\ldots+\sigma^{m-1})(\beta) = \theta+Tr_{F|K}(\beta)=\theta+1$, et de même $\sigma^n(\theta)=\theta$ pour $n=p^e$, donc σ est d'ordre p^e , ce qui montre que E est une extension cyclique de K de degré p^e ; on voit comme dans la démonstration de la prop. 3 que $E=K(\theta)$.

Si maintenant E_1 est une extension cyclique de K , de degré p^e sur K et contenant F , la prop.7 montre qu'il existe deux éléments α_1,β_1 de F tels que $Tr_{F|K}(\beta_1)=1$, $\sigma(\alpha_1)-\alpha_1=\beta_1^p-\beta_1$, et que E_1 soit le corps des racines du polynome $X^p-X-\alpha_1$ de $F[X]$. On a donc $Tr_{F|K}(\beta_1-\beta)=0$, et par suite il existe $\gamma \in F$ tel que $\beta_1=\beta+\sigma(\gamma)-\gamma$ (th.1) , d'où $\sigma(\alpha_1)-\alpha_1=\sigma(\alpha+\gamma^p-\gamma)-(\alpha+\gamma^p-\gamma)$, ce qui entraîne (th.1) $\alpha_1=\alpha+\gamma^p-\gamma+\lambda$ avec $\lambda \in K$. Si θ_1 est racine de $X^p-X-\alpha_1$, on a aussi $E=F(\theta_1-\gamma)$ puisque $\gamma \in F$, donc E est corps des racines de $X^p-X-\alpha-\lambda$.

Par récurrence sur e , on voit donc que s'il existe des extensions cycliques de K , de degré p , il existe aussi des extensions cycliques de K de degré p^e , pour <u>tout</u> $e>1$; de façon plus précise, toute extension cyclique de K de degré p est contenue dans une extension cyclique de degré p^e pour tout entier e ; on notera la différence entre ce résultat et le résultat correspondant pour les extensions cyoliques de degré q^e , où $q \neq p$ (cf. n° 3).

Exercices.- 1) Soit K un corps, n un entier non divisible par la caractéristique de K ; on suppose que K contient les racines n-èmes de l'unité. Soit P_n le sous-groupe du groupe multiplicatif K^* des éléments $\neq 0$ de K , formé des puissances n-èmes d'éléments de K^*. Soit G un sous-groupe de K^* contenant P_n ; montrer que si l'indice $(G:P_n)$ est fini, le corps W obtenu par adjonction à K des racines de toutes les équations $x^n-a=0$, où a parcourt G , a un degré sur K égal à $(G:P_n)$ (décomposer le groupe abélien $G\,P_n$ en produit direct de groupes cycliques (*), et raisonner par récurrence sur le nombre des groupes facteurs, en utilisant le prop.2 et le cor. de la prop.1).

2) Les hypothèses sur K et n étant les mêmes que dans l'exerc.1 , soit K_o un sous-corps de K tel que K soit une extension normale de K_o. Soit $a \in K$ tel que le corps des racines W de X^n-a soit de degré n par rapport à K . Pour que W soit une extension galoisienne de K_o , il faut et il suffit que, pour tout automorphisme σ du groupe de K par rapport à K_o, il existe un entier et un élément $b \in K$ tels que $\sigma(a)=b^n a^r$ (utiliser le cor. de la prop1).

3) SoitK un corps de caractéristique p , n un entier non multiple de p ; pour qu'un polynome de $K[X]$ de la forme X^n-a soit irréductible, il faut et il suffit que, pour tout facteur premier q de n , a ne soit pas égal à la puissance q-ème d'un élément de K , et en outre, lorsque $n \equiv 0 \pmod 4$, que a ne soit pas de la forme $-4\,c^4$, avec $c \in K$. (Pour démontrer que la condition est suffisante, on se ramènera au cas où $n=q^e$ (q premier) en utilisant l'exerc.7 du § 6 ; on raisonnera alors par récurrence sur e , en déterminant, grâce à l'exerc.7 du § 6, la forme du terme constant de chaque facteur irréductible de $X^{q^e}-a$).

4) Soit E un corps quelconque, x un élément de E non contenu dans le sous-corps premier de E .

a) Montrer que parmi les sous-corps de E ne contenant pas x , il existe un sous-corps maximal K .

b) Montrer que E est une extension algèbrique de K (établir d'abord que x ne peut être transcendant sur K , puis utiliser le cor. de la prop.8 du § 5).

c) Soit q le degré de x par rapport à K . Montrer que, dans $K[X]$, tout polynome irréductible a un degré à 1 ou à un multiple de q , et que tout polynome de $K[X]$ dont le degré n'est pas multiple de q a une racine dans K ; K(x) est la seule extension de K dont le degré soit égal à q .

d) Si E est de caractéristique $p > 0$, et si x n'est pas séparable sur K , montrer que $x^p \in K$ et que E est purement inséparable sur K .

e) On suppose désormais que E est une extension <u>normale</u> de K et que x est séparable sur K . Montrer que E est une extension séparable (donc galoisienne) de K , et que K(x) est une extension cyclique de K , dont le degré q est premier.

f) Montrer que toute extension de K contenue dans E et de degré fini sur K est une extension cyclique de K , dont le degré est de la forme q^e (remarquer que si, dans un groupe fini Γ , tout sous-groupe distinct de Γ est contenu dans un sous-groupe $\Delta \neq \Gamma$, Γ est engendré par chacun des éléments n'appartenant pas à Δ). En outre, pour chaque exposant e , il existe au plus une extension de K contenue dans E et de degré q^e .

5) Soit K un corps tel que $E=K$ soit une extension de degré premier q de K .

a) Montrer que K est parfait.

b) Montrer que q est distinct de la caractéristique de K (appliquer la prop.8).

c) Montrer que K contient les racines q-èmes de l'unité, et que E est le corps des racines d'un polynome irréductible X^q-a de $K[X]$; en déduire que $q=2$ (dans le cas contraire, déduire de l'exerc.3 que $X^{q^2}-a$ serait irréductible). Montrer en outre que $-a$ est un carré dans K (exerc.3), que -1 n'est pas un carré dans K , et que si i est une racine de X^2+1 , on a $E=K(i)$.

6) Soit K un corps tel que $E=\overline{K}$ soit distinct de K et soit de degré fini sur K . Montrer que X^2+1 est irréductible dans $K[X]$, et que si i est une racine de ce polynome, on a $E \neq K(i)$ (si on avait $E=K(i)$, montrer qu'il existerait un corps F tel que $K(i) \subset F \subset E$, et que E soit une extension de degré premier de F ; appliquer alors l'exerc. 5).

7) Soit K un corps de caractéristique p , q un nombre premier $\neq p$, ζ une racine primitive q-ème de l'unité sur K , ν le degré par rapport à K du corps $E=R_q(K)=K(\zeta)$, τ un automorphisme de E engendrant le groupe (cyclique) de E par rapport à K , t l'entier $(0<t<q)$ tel que $\zeta^\tau = \zeta^t$. Soit F une extension cyclique de K , de degré q sur K ; montrer que E et F sont linéairement disjoints sur K , et que leur composé $L=K(E \cup F)$ est une extension cyclique de degré νq de K , dont F est l'unique sous-corps de degré q sur K ; en outre, on a $L=E(\theta)$, où θ est racine d'un polynome irréductible X^q-a de $E[X]$, tel que $a^{\tau-t}$ soit puissance q-ème dans E (utiliser la prop.1 et son corollaire ; si σ est un automorphisme de F engendrant le groupe de F par rapport à K , exprimer que $\theta^{\sigma\tau} = \theta^{\tau\sigma}$).

8) Les hypothèses sur K étant les mêmes que dans l'exerc.7, soit L une extension cyclique de K , de degré q^e sur K , et soit F l'unique sous-corps de L de degré q^{e-1} sur K ; E et L sont linéairement disjoints sur K , $L_0=K(E\cup L)$ est une extension cyclique de degré $\ge q^e$ sur K , $F_0=K(E\cup F)$ une extension cyclique de degré $\ge q^{e-1}$ sur K ; soit σ un automorphisme de L engendrant le groupe de L par rapport à K (ou celui de L_0 par rapport à E).

a) Montrer qu'il existe dans F_0 trois éléments α,β,γ tels que $X^q-\alpha$ soit irréductible dans $F_0[X]$, qu'on ait, pour toute racine θ de ce polynome, $L_0=F_0(\theta)$, ainsi que les relations : $\theta^\sigma=\beta\theta$, $\theta^\tau=\gamma\theta^t$, $N_{F_0|E}(\beta)=\zeta$, $\alpha^{\sigma-1}=\beta^q$, $\beta^{\tau-t}=\gamma^{\sigma-1}$, $\alpha^{\tau-t}=\gamma^q$ (utiliser le prop.3 et le cor. de la prop.1, et exprimer que σ et τ sont permutables dans L_0).

b) Inversement, soit F une extension cyclique de K , de degré q^{e-1} , telle qu'il existe dans F_0 trois éléments α,β,γ, satisfaisant aux relations $N_{F_0|E}(\beta)=\zeta$, $\alpha^{\sigma-1}=\beta^q$, $\beta^{\tau-t}=\gamma^{\sigma-1}$, $\alpha^{\tau-t}=\gamma^q$; montrer que le corps des racines L_0 du polynome $X^q-\lambda\alpha$, où $\lambda\in E^*$ est tel que $\lambda^{\tau-t}$ soit puissance q-ème d'un élément de E^* , est une extension cyclique de K , de degré $\ge q^e$ sur K , engendrée par une quelconque des racines de $X^q-\lambda\alpha$. En outre, toute extension cyclique L de K , de degré q^e sur K et contenant F , est telle que le corps $L_0=K(L\cup E)$ soit de la forme précédente pour un $\lambda\in E^*$ convenable (utiliser la prop.4, et montrer qu'on peut étendre les automorphismes σ et τ de F_0 au corps L_0 de sorte qu'ils restent permutables).

9) Soit K un corps de caractéristique p , E une extension cyclique de K , de degré n sur K . Montrer que E admet une <u>base normale</u> sur K (sans hypothèses sur le nombre d'éléments de K) . On remarquera pour cela que pour que les conjugués d'un élément $x\in E$ forment une base de E , il faut et il suffit que le déterminant

$$\begin{vmatrix} x & \sigma(x) & \sigma^2(x) & \dots & \sigma^{n-1}(x) \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & \dots & x \\ \dots & \dots & \dots & \dots & \dots \\ \sigma^{n-1}(x) & x & \sigma(x) & \dots & \sigma^{n-2}(x) \end{vmatrix}$$

(σ automorphisme engendrant le groupe de E par rapport à K) ne soit pas nul. En se ramenant au cas où n est une puissance d'un nombre premier (grâce à l'exerc.14 du § 6), on utilisera l'exerc.9 du § 7, et le th.1 du § 4 ; montrer qu'on est ainsi ramené à prouver la proposition suivante : soit H un espace vectoriel de dimension n sur un corps quelconque K , et V_i $(1 \leqslant i \leqslant n)$ n sous-espaces vectoriels de H tels que l'intersection de k quelconques des V_i $(1 \leqslant k \leqslant n)$ soit au plus de dimension n-k ; alors la réunion des V_i n'est pas identique à H . On démontrera d'abord cette proposition lorsque tous les V_i sont des hyperplans ; puis on se ramènera à ce cas particulier en prouvant le lemme suivant : soit H' un espace vectoriel de dimension n sur K ; soient V'_i $(1 \leqslant i \leqslant n)$ n sous-espaces vectoriels de H' , tels que la somme de k quelconques des V'_i $(1 \leqslant k \leqslant n)$ soit au moins de dimension k ; alors il existe une base (a'_i) de H' sur K telle que $a'_i \in V'_i$ pour $1 \leqslant i \leqslant n$.

APPENDICE

Extensions normales de degré infini.

Soit N une extension normale d'un corps K , Γ son gr.groupe par rapport à K ; nous nous proposons de compléter, dans cet Appendice, la théorie de Galois exposée au § 6, en étudiant le cas où Γ est un groupe quelconque (fini ou non). Nous conserverons les notations introduites au § 6, n°3 ; en outre, nous désignerons par $\mathfrak{F}$ l'ensemble des extensions de degré fini de K , contenues dans N . Si F est une telle extension, et σ un élément de Γ , on désignera par σ_F la restriction de σ à F ; pour tout sous-groupe Δ de Γ , on désignera par Δ_F l'ensemble des σ_F lorsque σ parcourt Δ ; lorsque F est une extension normale de K , on a $(\sigma\tau)_F=\sigma_F\tau_F$ et $(\sigma^{-1})_F = (\sigma_F)^{-1}$ pour deux éléments quelconques σ, τ de Γ .

Nous allons définir sur Γ une topologie de groupe (Top.gén., chap.III, § 1) qui nous permettra de compléter les résultats du § 6, en donnant la caractérisation du groupe $g(k(\Delta))$ pour tout sous-groupe de Γ .

Proposition 1.- Si, pour toute extension $F \in \mathfrak{F}$, on désigne par V_F le sous-groupe $g(F)$ de Γ , les V_F forment un système fondamental $\mathfrak{V}$ de voisinages de l'élément neutre ε de Γ , dans une topologie séparée compatible avec la structure de groupe de Γ .

En effet, les V_F formant une famille de sous-groupes de Γ , il suffit (Top.gén., chap.III, §1,n°2) de vérifier que $\mathfrak{V}$ est une base de filtre, que, pour tout $\sigma \in \Gamma$, $\sigma V_F \sigma^{-1}$ appartient à $\mathfrak{V}$ et que, pour $\sigma \neq \varepsilon$, il existe $F \in \mathfrak{F}$ tel que $\sigma \notin V_F$. Or (§ 6,prop.8) si F_1 et F_2 sont deux extensions de K de degré fini, F le composé de F_1 et F_2, on a $V_F=V_{F_1} \cap V_{F_2}$, et F est une extension de degré fini de K ;

d'autre part (§ 6, prop. 12), on a $\sigma V_F \sigma^{-1} = V_{\sigma(F)}$ pour tout sous-corps $F \in \mathfrak{F}$ et tout $\sigma \in \Gamma$, et $\sigma(F)$ est une extension de degré fini de K. Enfin, si $\sigma \neq \varepsilon$, il existe $a \in N$ tel que $\sigma(a) \neq a$; si on prend $F = K(a)$ on aura $\sigma \notin V_F$.

Quand nous considèrerons, dans ce qui suit, le groupe Γ comme un groupe topologique, il sera sous-entendu qu'il s'agit de Γ muni de la topologie définie par l'ensemble $\mathfrak{V}$.

Proposition 2.- Pour toute extension E de K contenue dans N, le sous-groupe $g(E)$ est fermé dans Γ.

En effet, soit $\sigma \in \overline{g(E)}$, et soit $F \in \mathfrak{F}$; le voisinage σV_F de σ rencontre $g(E)$, donc il existe $\tau \in V_F = g(F)$ tel que $\sigma\tau \in g(E)$; pour tout $a \in E \cap F$, on a donc $a = \sigma(\tau(a)) = \sigma(a)$. Or, pour tout $a \in E$, il existe $F \in \mathfrak{F}$ tel que $a \in E \cap F$, par exemple $F = K(a)$; on a donc $\sigma(a) = a$ pour tout $a \in E$, c'est-à-dire $\sigma \in g(E)$.

Proposition 3.- Pour tout sous-groupe Δ de Γ, on a $g(k(\Delta)) = \overline{\Delta}$.

Comme $g(k(\Delta))$ est fermé d'après la prop. 2, on a $\overline{\Delta} \subset g(k(\Delta))$. Il suffit donc de prouver que si $\sigma \in g(k(\Delta))$, σ est adhérent à Δ. Or, soit F une extension quelconque de K de degré fini, contenue dans N ; soit G l'extension normale de K engendrée par F ; on sait (§ 6, cor. 1 de la prop. 4) que G est de degré fini sur K. Comme σ laisse invariant tout élément de $k(\Delta)$, il laisse a fortiori invariant tout élément de $k(\Delta) \cap G$; mais $k(\Delta) \cap G$ n'est autre que le sous-corps de G formé des éléments invariants par tous les automorphismes appartenant au groupe Δ_G ; donc (§ 6, cor. de la prop. 11), on a $\sigma_G \in \Delta_G$; autrement dit, il existe $\tau \in \Delta$ tel que $\sigma_G = \tau_G$, ou encore $(\sigma\tau^{-1})_G = \varepsilon_G$, c'est-à-dire $\sigma\tau^{-1} \in g(G) \subset V_F$; comme V_F est un voisinage symétrique, on a $(\sigma V_F) \cap \Delta \neq \emptyset$, ce qui montre que σ est adhérent à Δ.

Le th.2 du § 6 se généralise donc de la façon suivante :

Théorème 1.- Si M est une extension galoisienne de K, l'application $E \to g(E)$ est une application biunivoque strictement décroissante de l'ensemble $\mathcal{K}$ des sous-corps de M contenant K, sur l'ensemble $\mathcal{G}$ des sous-groupes fermés de Γ, et $\Delta \to h(\Delta)$ est l'application réciproque de g.

Il en résulte qu'à l'intersection d'une famille (E_ι) de sous-corps de M correspond, par l'application g, l'adhérence dans Γ du sous-groupe de Γ engendré par la réunion des sous-groupes $g(E_\iota)$.

Proposition 4.- Le groupe topologique Γ est un groupe compact totalement discontinu.

Montrons d'abord que Γ est complet. Pour cela, soit $\mathfrak{F}$ un filtre de Cauchy sur Γ ; pour tout $F \in \mathcal{F}$, il existe un ensemble H_F de $\mathfrak{F}$, petit d'ordre $(V_F)_d$: cela signifie que si $\sigma \in H_F$ et $\tau \in H_F$, on a $\sigma\tau^{-1} \in V_F$, autrement dit $\sigma(x) = \tau(x)$ pour tout $x \in F$.

Soit alors x un élément quelconque de M, et H_x la réunion des H_F pour toutes les extensions $F \in \mathcal{F}$ telles que $x \in F$; pour tous les éléments $\sigma \in H_x$, $\sigma(x)$ a la même valeur d'après ce qui précède ; nous désignerons cette valeur par $\sigma_0(x)$. Si x et y sont deux éléments quelconques de M, il existe une extension $F \in \mathcal{F}$ contenant à la fois x et y, donc $\sigma(x+y) = \sigma(x) + \sigma(y)$ et $\sigma(xy) = \sigma(x)\sigma(y)$ pour tout $\sigma \in H_F$, ce qui prouve que σ_0 est un endomorphisme de M relatif à K, et par suite (§ 6, prop. 1) un automorphisme de M relatif à K ; il est clair en outre que σ_0, d'après sa définition, est point limite du filtre $\mathfrak{F}$.

Montrons en second lieu que Γ est précompact. Soit F une extension quelconque de K, de degré fini et contenue dans M ; montrons qu'on peut recouvrir Γ par un nombre fini d'ensembles petits d'ordre

$(V_F^2)_d$; il n'existe qu'un nombre fini m d'isomorphismes distincts τ_i $(1 \leqslant i \leqslant m)$ de F dans N (relatifs à K) ; soient σ_i $(1 \leqslant i \leqslant m)$ m automorphismes de N tels que la restriction de σ_i à F soit identique à τ_i $(1 \leqslant i \leqslant m)$; pour tout automorphisme $\sigma \in \Gamma$, σ_F est identique à un des τ_i , donc on a, pour cet indice i , $\sigma_i^{-1}\sigma \in g(F)=V_F$, ce qui prouve que les m ensembles $\sigma_i V_F$ forment un recouvrement de Γ .

Enfin, tout voisinage de ε dans Γ contient un sous-groupe V_F de Γ , qui est à la fois ouvert et fermé, donc Γ est totalement discontinu.

Exercices.- 1) Soit E une extension normale de K contenue dans N ; montrer que l'application $\sigma \to \sigma_E$ de Γ sur le groupe Γ_E de E par rapport à N est continue, et en déduire que le groupe topologique Γ_E est isomorphe au groupe topologique $\Gamma/g(E)$.

2) Montrer que le plus petit sous-corps de N contenant toutes les extensions abéliennes de K contenues dans N , est une extension abélienne A de K (utiliser l'exerc.3 du § 6) ; le groupe $g(A)$ est l'adhérence du groupe des commutateurs de Γ .

3) Soit (N_λ) une famille de sous-corps de N , qui sont des extensions normales de K , ayant les propriétés suivantes :
a) pour chaque indice λ , si N'_λ est le corps engendré par la réunion des N_μ d'indice $\mu \neq \lambda$, on a $N_\lambda \cap N'_\lambda = K$;
b) N est engendré par la réunion des N_λ . Montrer que le groupe topologique Γ est isomorphe au groupe topologique produit des groupes $\Gamma/g(N_\lambda)$ (utiliser le cor.2 du th.1 du § 6).