CHAPITRE VI
CORPS COMMUTATIFS

Rédaction n° 046

Nombre de pages: 141

Nombre de feuilles: 141

M. Deheuvels

COMMENTAIRES SUR LE SUPPLEMENT AU CHAP. V et le CHAP.VI

Supplément à l'Appendice du chap.V. On y a défini les valuations additives discrètes, en relation avec la théorie des corps $\mathfrak{p}$-adiques faite dans cet Appendice. La question se pose de savoir s'il n'y aurait pas lieu de définir les valuations additives plus générales (elles sont définies en tout cas en Exercices) ; les valuations réelles tout au moins semblent prendre une grande importance en Géomètrie algèbrique (cf. Zariski, p.ex.) ; il faudrait que les spécialistes de ces questions donnent là-dessus leur avis. Y aurait-il lieu également de définir ici les valuations multiplicatives dites "archimédiennes"? On peut songer aussi à placer ces dernières, soit en Topologie, avec les Espaces métriques, soit dans les Espaces vectoriels topologiques, avec la théorie des anneaux normés (non rédigés pour le moment, mais qui semble prendre une grande importance en Analyse fonctionnelle, si on en juge d'après les travaux récents des Russes (Krein, Gelfand, Raikov, etc..)). Une discussion sur cette question s'impose.

Chapitre VI. Sommaire du chapitre :

§1. Caractéristique. Corps premiers.
§2. Extensions simples. Eléments algèbriques et éléments transcendants.
§3. Extensions algèbriques et extensions transcendantes.
§4. Extensions algèbriquement stables.
§5. Isomorphismes d'extensions algèbriques.
§6. Extensions galoisiennes.
§7. Racines de l'unité. Corps finis.
§8. Corps ordonnés et corps quasi-réels.
§9. Divisibilité dans les extensions algèbriques.

Appendice I. Extensions galoisiennes infinies.

Appendice II. Extensions algèbriques des corps $\mathfrak{p}$-adiques.

L'essentiel du chapitre (étude des corps commutatifs) est fait dans les 6 premiers paragraphes ; les 3 derniers sont consacrés à des questions plus particulières. La théorie des corps commutatifs est prise conformément aux principes Bourbaki, en procédans du général au particulier, ce qui donne exactement l'ordre inverse de celui suivi, par exemple, par v.der Waerden. Après 2 §§ introductifs, où on donne les définitions et outils essentiels pour ce qui suit, on donne au § 3 la classification des extensions en algèbriques et transcendance, qui permettent ensuite de ne plus considérer, dans les reste du chap., que des extensions algèbriques (finies ou non).

Au § 4, on établit tout de suite le th. de Steinitz sur l'existence de l'extension algèbriquement stable d'un corps K , et le fait que toute extension algèbrique de K peut (à un isomorphisme près) y être considérée comme plongée. C'est ce point de vue qu'on adopte systématiquement par la suite, sauf cas exceptionnels, ce qui donne la même commodité de langage et de pensée que dans l'ancienne Algèbre qui ne considérait que des sous-corps de $\mathbb{C}$; qu'on compare, par ex., avec les contorsions verbales auxquelles doit toujours avoir recours v.d.W. pour éviter de se servir de l'extension algèbrique maximale (il doit constamment introduire un sur-corps fini convenable, chaque fois différent suivant les démonstrations). Bien entendu, le rédacteur

est tout à fait conscient du fait que l'axiome de Zermelo est ainsi introduit dans des questions où il n'est pas nécessaire, et que soit que les malheureux atteints de Zermelophobie aigue pousseront des hauts cris ; pour son compte, il n'en a cure, et espère que, malgré quelques symptômes fâcheux, les membres de Bourbaki sont restés indemnes de cette maladie ridicule, qui devrait être exclusivement réservée aux philosophes en mal de copie. On notera que la démonstration du th. de Steinitz est celle de Zorn, d'une remarquable élégance (son "théorème" a été introduit par lui à cette occasion).

Les §§5 et 6 sont consacrés à l'étude des isomorphismes des extensions algèbriques, culminant au §6 avec la théorie de Galois. Le §5 sert en somme d'introduction à cette théorie, en donnant les définitions et outils indispensables ; l'accent y est mis dès le début sur la notion d'isomorphisme, et c'est de ce point de vue que sont définis les conjugués d'un élément, et les notions d'éléments séparables et inséparables. On définit aussi au §5 la norme et la trace d'un élément ; pour le cas des éléments inséparables, cette définition n'est pas identique à celle de v.d.W. : il semble au rédacteur que la définition de la trace donnée par v.d.W. dans ce dernier cas n'est guère intéressante, puisqu'avec cette définition, la trace d'un élément inséparable est toujours nulle ! Dans ce même §5 , on signale que la prop.8 (théorème de l'"élément primitif") n'est démontrée (comme dans v.d.W.) que pour un corps de base infini ; le rédacteur a vainement cherché une démonstration valable dans tous les cas, et propose de mettre la question au concours (il y a bien une démonstration, due à Deuring (Math. Ann.,t.107,p.140), mais elle utilise les systèmes hypercomplexes).

La théorie de Galois est traitée au §6 dans le cas le plus général possible, à l'exception de la théorie de Krull pour les extensions infinies, rejetée en Appendice I à cause des notions topologiques qu'elle suppose. En ce qui concerne ce §6 , le rédacteur signale que, dans la démonstration du 2è th. fondamental (th.2), il a dû utiliser le th. de l'"élément primitif" démontré seulement pour les corps infinis dans le §5 ; il y a là une lacune fâcheuse. Dans leur supplément au livre de Steinitz, Hasse et Baer signalent en Note que, dans la démonstration de ce théorème, on peut se passer du th. de l'élément primitif ; mais le rédacteur n'a pu comprendre comment ils procèdent, d'après les maigres indications qu'ils donnent. Il suggère un autre moyen d'esquiver la difficulté : c'est d'utiliser la prop.8 (qui vu son importance, mériterait d'ailleurs de passer théorème et devrait être fait plus tôt) : si $N_0 = E_0\langle a_1, a_2, \ldots, a_p\rangle$ (avec les notations du th.2), on considère l'extension transcendante $F = E_0(u_1, u_2, \ldots, u_p)$ et l'extension $M = F\langle a_1, a_2, \ldots, a_p\rangle$; si on pose $\theta = a_1u_1 + a_2u_2 + \ldots + a_pu_p$, il est immédiat que $M = F\langle\theta\rangle$, ce qui permet de faire sur M et F le raisonnement du th.2 sur N_0 et E_0 , auxquels on revient ensuite à l'aide de la prop.8 ; c'est un peu détourné, mais permet de se passer entièrement du théorème sur l'élément primitif.

Le rédacteur s'est conformé à la tradition en donnant, dans le §6, la méthode "pratique" de détermination du groupe de Galois d'une équation ; mais c'est bien à contre-coeur, et il profite de cette occasion pour poser nettement la question de l'intérêt de ces méthodes soi-disant "pratiques", mais qui dès qu'on veut les appliquer, conduisent à des calculs inextricables. Ce sont des vieux résidus des préjugés "constructifs" en Mathématique, et ils fourmillent en Algèbre plus qu'ailleurs ; exemples : calcul des fonctions symétriques, algorithme d'Euclide pour le p.g.c.d., crible d'Eratosthène, procédé de Kronecker pour la décomposition d'un polynome en facteurs irréductibles, détermination effective d'un groupe de Galois, théorème de Sturm, etc.. L'avis du rédacteur serait de balancer impitoyablement tous ceux de ces procédés qui ne sont pas des outils utiles dans les recherches théoriques, ou tout au moins de les rejeter au Calcul numérique.

Au §8, la théorie des corps quasi-réels est exposée suivant une méthode légèrement différente de celle d'Artin-Schreier ; alors que, pour démontrer le th.1, ces derniers passent par l'intermédiaire de l'extension quasi-réelle maximale, on a donné une démonstration qui est plus "interne" en quelque sorte, et s'inspire davantage de la théorie moderne des groupes ordonnés (cf.chap.V, §1). Dans la démonstration du th.2, on a suivi l'astuce classique de Gauss, mais la variante signalée par Artin-Schreier, et qui consiste à utiliser le th. de Sylow et les p-groupes (pour p=2) est bien préférable, parce qu'elle montre bien mieux l'origine du théorème : si on adoptait ce point de vue, il faudrait faire quelque part les théorèmes de Sylow (le rédacteur suggère en Appendice II au chap.V, ce qui lui semble l'endroit le plus indiqué). A propos de ce §, le rédacteur signale enfin qu'il manque le théorème d'unicité (à un isomorphisme près) de l'extension quasi-réelle maximale <u>algèbrique</u> d'un corps quasi-réel ; la démonstration d'Artin-Schreier utilise le th. de Sturm, et le rédacteur a vainement essayé de trouver une autre démonstration qui s'en passât ; comme ledit théorème lui inspire la plus vive répulsion (voir ci-dessus) il a préféré tout laisser tomber et met au concours la recherche d'une astuce idoine pour tourner la difficulté.

Les fondements de la théorie des entiers algèbriques sont traités au §9 en suivant Dedekind-Prüfer plutôt que E.Noether, comme on l'a déjà signalé dans les commentaires au chap.V ; en particulier on n'y fait pas des anneaux <u>clos</u> ("ganz-abgeschlossen") le pivot de la théorie ; il est curieux de noter, en suivant cette méthode, que le th.1 (extension algèbrique d'un anneau de Prüfer) est beaucoup plus simple que le th.2 (extension algèbrique <u>finie</u> d'un anneau de Dedekind) ; la dissociation de ces deux théorèmes a d'ailleurs l'avantage de mettre en lumière l'intervention des conditions de "finitude".

L'Appendice II est assez long ; on a cru utile d'y insérer ce qui, dans la théorie arithmétique des corps galoisiens de Hilbert est valable sans hypothèses particulières sur le corps de base.

Chapitre V

A 46

(Ancien CHAPITRE VI.)

Etat 1

CORPS COMMUTATIFS.

§ 1. Caractéristique. Corps premiers.

Caractéristique d'un corps. Rappelons la définition donnée au chap.II (§ 1) de la caractéristique d'un anneau A : l'annihilateur du groupe additif de A , considéré comme $\mathbb{Z}$-module, est un idéal principal (n) de $\mathbb{Z}$, où n est un entier $\geqslant 0$; n est appelé la caractéristique de A .

Proposition 1. La caractéristique d'un corps K (commutatif ou non) est égale à 0 ou à un nombre premier p .

Pour un entier m et un élément $x \neq 0$ de K , la condition $m.x=0$ qui s'écrit encore $(m.\varepsilon)x=0$, où ε est l'élément unité de K , équivaut à $m.\varepsilon=0$. La caractéristique n de K peut donc être définie comme égale au plus petit entier $m>0$ tel que $m.\varepsilon=0$ si un tel entier existe, à 0 dans le cas contraire. Si n était $\neq 0$ et non premier, il existerait deux entiers $p<n, q<n$ tels que $n=pq$; comme $n.\varepsilon=(p.\varepsilon)(q.\varepsilon)$, on aurait $(p.\varepsilon)(q.\varepsilon)=0$, avec $p.\varepsilon\neq 0$ et $q.\varepsilon\neq 0$, ce qui est absurde.

Dans un corps commutatif K de caractéristique $p\neq 0$, on a les identités

$$(1) \qquad (a+b)^p = a^p+b^p$$

$$(2) \qquad (a-b)^p = a^p-b^p$$

En effet, d'après la formule du binome

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

Or, pour $0<k<p$, le coefficient binomial $\binom{p}{k}$ est divisible par p , car $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k}$, et dans cette fraction le numérateur est divisible par p , et le dénominateur premier avec p puisque p est premier ;

d'où la formule (1) ; (2) s'en déduit en remplaçant a par a-b. Par récurrence, on a de même

$$(3) \qquad \Big(\sum_{i=1}^{n} a_i\Big)^{p^f} = \sum_{i=1}^{n} a_i^{p^f}$$

quels que soient les entiers f et $n > 0$.

On en conclut que l'application $x \to x^p$ est un <u>isomorphisme</u> de K <u>dans</u> K (c'est-à-dire <u>sur</u> un sous-corps de K).

<u>Corps premiers</u>. On sait (chap.I, §) que l'intersection d'une famille quelconque de <u>sous-corps</u> d'un corps K (commutatif ou non) est un <u>sous-corps</u> de K ; en particulier, l'intersection P de <u>tous</u> les sous-corps de K est <u>le plus petit</u> sous-corps de K . Le corps P ne contient donc <u>aucun sous-corps</u> distinct de lui-même ; un corps ayant cette propriété est dit <u>premier</u>. Nous allons déterminer la structure des corps premiers.

Si ε est l'unité d'un corps premier P , P contient l'anneau commutatif A formé des multiples entiers $n.\varepsilon$, où n parcourt $\mathbb{Z}$; l'application $n \to n.\varepsilon$ est une <u>représentation</u> de $\mathbb{Z}$ sur A , et l'ensemble des entiers n tels que $n.\varepsilon = 0$ est l'idéal (p), où p est la <u>caractéristique</u> de P ; donc :

1° si p=0 , A est <u>isomorphe</u> à $\mathbb{Z}$; donc P contient le corps des quotients de A , qui est isomorphe à $\mathbb{Q}$; P étant un corps premier, il est <u>isomorphe au corps $\mathbb{Q}$ des nombres rationnels</u>.

2° si $p > 0$, A est isomorphe à l'anneau $\mathbb{Z}/(p)$ des entiers modulo p ; comme p est un nombre premier, cet anneau quotient est un <u>corps</u>, donc P est <u>isomorphe à</u> $\mathbb{Z}/(p)$.

Tout sous-corps d'un corps K a évidemment même caractéristique que K ; en identifiant le plus petit sous-corps de K avec $\mathbb{Q}$ ou $\mathbb{Z}/(p)$ suivant les cas, on voit donc qu'un corps de caractéristique 0 peut toujours être considéré comme une <u>extension du corps $\mathbb{Q}$</u> ; un corps de caractéristique p 0 , comme une <u>extension du corps</u> $\mathbb{Z}/(p)$.

Ce résultat légitime l'étude générale des extensions commutatives d'nn corps commutatif, que nous allons maintenant entreprendre.

Au chap.VII, nous aborderons l'étude des extensions non-commutatives d'un corps commutatif.

Exercices. 1) Si A est un anneau d'intégrité, commutatif ou non, ayant ou non un élément unité, la caractéristique de A est 0 ou un nombre premier.

2) Soit A un anneau d'intégrité commutatif, $\mathfrak{P}$ un idéal premier de A . Si la caractéristique de A est un nombre premier $p>0$, 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 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 simples.

Eléments algèbriques et éléments transcendants.

Extensions finies et extensions infinies. Soit E un corps commutatif, extension d'un corps K ; E est donc une algèbre sur K ; son rang par rapport à K s'appelle plus souvent le degré du corps E par rapport à K , et se note $[E:K]$ s'il est fini ; on dit que E est une extension finie (resp.infinie) de K si son degré par rapport à K est fini (resp. infini).

On aura soin de ne pas confondre les notions de "corps fini" et d'"extension finie" ; une extension finie d'un corps K n'est un corps fini que si K est lui-même un corps fini.

Proposition 1. Si E est une extension finie de K et F une extension finie de E , F est une extension finie de K , et on a

$$[F : K] = [F : E] \cdot [E : K]$$

C'est un cas particulier de la proposition correspondante pour les algèbres sur un corps commutatif (chap.III, § 1).

Corollaire 1. Le degré par rapport à K d'un sous-corps E d'une extension finie F de K, tel que $K \subset E$, est un diviseur du degré $[F:K]$.

Corollaire 2. Si $[F:K] = [E:K]$, on a $E=F$; si $[F:K] = [F:E]$, $K=E$.

Le degré d'une extension d'un corps K ne peut en effet être égal à 1 que si cette extension est identique à K.

Adjonction. Soit E une extension commutative d'un corps commutatif K, et soit M une partie quelconque de E ; le sous-corps de E engendré par $K \cup M$, c'est-à-dire (chap.I, §) le plus petit sous-corps de E contenant à la fois K et M, se note $K\langle M\rangle$, et on dit que c'est le corps obtenu par adjonction de M à K. Il est immédiat que, si M et N sont deux parties de E, on a $K\langle M \cup N\rangle = K\langle M\rangle\langle N\rangle$, car $K\langle M \cup N\rangle$ contient $K\langle M\rangle$, donc $K\langle M\rangle\langle N\rangle$, et comme c'est le plus petit sous-corps contenant $K \cup M \cup N$, il est identique à $K\langle M\rangle\langle N\rangle$. Lorsque M est l'ensemble des éléments d'une suite finie $(a_i)_{1 \leqslant i \leqslant n}$ d'éléments de E, on écrit encore $K\langle a_1,\dots,a_n\rangle$ au lieu de $K\langle M\rangle$.

Il est immédiat que l'ensemble des expressions rationnelles à coefficients dans K, par rapport aux éléments de $K \cup M$ (ou simplement des éléments de $M \cup \{\varepsilon\}$, où ε est l'élément unité de K) est un sous-corps de E contenant $K \cup M$ (chap.IV, §2), et est contenu dans tout corps contenant $K \cup M$, donc dans $K\langle M\rangle$; il lui est donc identique. Autrement dit, pour tout élément $x \in K\langle M\rangle$, il existe un nombre fini d'éléments $a_1, a_2, \dots, a_n$ de M, et une fraction rationnelle $f \in K(e_1,\dots,e_n$ telle que la valeur $f(a_1,a_2,\dots,a_n)$ de la fonction rationnelle correspondante soit définie et égale à x. On voit donc que x appartient à l'extension $K\langle a_1,a_2,\dots,a_n\rangle$; on peut encore dire que $K\langle M\rangle$ est la réunion des extensions $K\langle X\rangle$, où X parcourt l'ensemble des parties finie de M.

On notera que si F est une extension finie de K , contenue dans E , F s'obtient par adjonction à K d'un nombre fini d'éléments (par exemple, les éléments d'une base vectorielle de F par rapport à K).

Extensions simples. Une extension E d'un corps K est dite simple si elle s'obtient par adjonction à K d'un seul élément θ ; nous allons étudier la structure d'une telle extension $E = K\langle\theta\rangle$.

Le corps E contient l'anneau A des expressions algèbriques entières à coefficients dans K , par rapport à θ et à l'élément unité ε de K ; tout élément de A est, comme on sait (chap.IV, § 2) de la forme $\dot{f}(\theta)$, où f est un polynome de $K[e]$, et $\dot{f}$ la fonction polynome correspondante définie dans E ($\dot{f}(x)=\sum_{k=0}^{n} a_k x^k$ si $f = \sum_{k=0}^{n} a_k e^k$). Il est clair en outre que l'application $f \longrightarrow \dot{f}(\theta)$ est une représentation de $K[e]$ sur A ; il en résulte que A est isomorphe à un anneau quotient $K[e]/\mathfrak{P}$, où $\mathfrak{P}$ est un idéal de $K[e]$; comme A est un anneau d'intégrité, $\mathfrak{P}$ ne peut être égal qu'à l'idéal nul (0), ou à un idéal premier de $K[e]$; nous allons examiner successivement ces deux cas.

1° $\mathfrak{P}=(0)$; cela signifie que la relation $f\neq 0$ entraîne $\dot{f}(\theta)\neq 0$, autrement dit, que θ ne satisfait à aucune équation algèbrique à coefficients dans K ; on dit alors que θ est un élément transcendant par rapport à K , et que $K\langle\theta\rangle$ est une extension transcendante simple de K. L'anneau A est alors isomorphe à $K[e]$; son corps des quotients est donc isomorphe au corps K(e) des fractions rationnelles d'une lettre sur K ; comme il contient K et θ et est contenu dans $K\langle\theta\rangle$, il est identique à $K\langle\theta\rangle$; autrement dit :

Proposition 2. Toute extension transcendante simple d'un corps K est isomorphe au corps K(e) des fractions rationnelles d'une lettre sur K .

A tout élément $x \in K\langle\theta\rangle$ correspond donc une fraction rationnelle irréductible g et une seule, telle que $x=\dot{g}(\theta)$.

Corollaire. Une extension transcendante simple est infinie.

2° $\mathfrak{P} = (\varphi)$, où φ est un polynome irréductible et $\neq 0$ de $K[e]$ (chap.V, § 4). On a alors $\dot{\varphi}(\theta)=0$, et, pour un polynome $f \in K[e]$, la relation $\dot{f}(\theta)=0$ est équivalente à $f \equiv 0 \pmod{\varphi}$; on dit que θ est un élément algèbrique par rapport à K , et $K\langle\theta\rangle$ une extension algèbrique simple de K ; l'équation algèbrique $\dot{\varphi}(x)=0$ (bien déterminée) est dite l'équation irréductible dont θ est une racine, et son degré n est appelé le degré de θ par rapport à K . L'anneau A est alors un corps ; comme il contient K et θ et est contenu dans $K\langle\theta\rangle$, il est identique à $K\langle\theta\rangle$; tout élément x de $K\langle\theta\rangle$ peut donc s'écrire $\dot{f}(\theta)$, où $f \in K[e]$; en outre, il existe un polynome g de degré $\leqslant n-1$, et un seul, tel que $f \equiv g \pmod{\varphi}$, donc x peut s'écrire d'une seule manière sous la forme $\dot{g}(\theta)$, où g est un polynome de degré $\leqslant n-1$.

En résumé :

Proposition 3. Une extension algèbrique simple $K\langle\theta\rangle$ d'un corps K , est isomorphe au corps quotient $K[e]/(\varphi)$, où φ est le polynome de plus petit degré (irréductible, et bien déterminé à un facteur constant près) tel que $\dot{\varphi}(\theta)=0$. Tout polynome $f \in K[e]$ tel que $\dot{f}(\theta)=0$ est un multiple de φ . Le degré $[K\langle\theta\rangle : K]$ est égal au degré n de θ par rapport à K , c'est-à-dire au degré de φ ; et les éléments ε , θ, $\theta^2, \ldots, \theta^{n-1}$ forment une base de $K\langle\theta\rangle$ par rapport à K .

On notera qu'en général, si E est une extension algèbrique simple du corps K , il existe plusieurs éléments θ de E (en général une infinité) tels que $E=K\langle\theta\rangle$ (cf. § 5, prop.8).

Corollaire 1. Une extension algèbrique simple est finie.

Ce corollaire, et celui de la prop.2, permettent de caractériser les éléments algèbriques et les éléments transcendants par rapport à K ;

pour que θ soit algèbrique (resp. transcendant) par rapport à K , il faut et il suffit que l'extension simple $K\langle\theta\rangle$ soit finie (resp. infinie) .

Corollaire 2. Si E est une extension de K obtenue par adjonction de m éléments a_i $(1 \leqslant i \leqslant m)$ tels que a_1 soit algèbrique de degré n_1 par rapport à K , a_i $(2 \leqslant i \leqslant m)$ algèbrique et de degré n_i par rapport à $K\langle a_1, a_2, \ldots, a_{i-1}\rangle$, E est une extension finie de K , de degré $n_1 n_2 \ldots n_m$.

Cela résulte aussitôt des prop.1 et 3 .

De la prop.3 et du cor.1 de la prop.1 (ou du cor.2 précédent), il résulte en particulier que le degré par rapport à K d'un élément θ d'une extension finie E de K , est un diviseur du degré $[E:K]$.

Proposition 4. Si θ est un élément algèbrique par rapport à K , appartenant à une extension E de K , et si F est un sous-corps quelconque de E , contenant K , θ est algèbrique par rapport à F .

En effet, θ est racine d'un polynome dont les coefficients appartiennent à K (donc à F) et sont $\neq 0$.

On peut ajouter que, si φ est le polynome irréductible de $K[e]$ dont φ est racine, φ n'est pas nécessairement irréductible dans $F[e]$; si $\varphi = \varphi_1 \varphi_2 \ldots \varphi_k$ est sa décomposition en polynomes irréductibles dans $F[e]$, on a $\varphi_i(\theta)=0$ pour une valeur de i au moins ; on a donc l'inégalité $[F\langle\theta\rangle : F] \leqslant [K\langle\theta\rangle : K]$.

Les prop.2 et 3 déterminent la structure possible des extensions simples de K ; réciproquement, il est immédiat que le corps $K(e)$ est une extension transcendante simple de K , et le corps $K[e]/(\varphi)$, où φ est irréductible dans $K[e]$, une extension algèbrique du corps K' isomorphe à K formé des classes (mod.(φ)) des éléments de K ; cette extension est engendrée en effet par la classe (mod. φ) de l'élémen
e ;

si on désigne cette classe par θ , et qu'on identifie K et K' , $\dot{\varphi}(x)=0$ est l'équation irréductible dont θ est racine. C'est de ce corps $K[\theta]/(\varphi)$ qu'il sera question dans le § 4 lorsqu'on parlera du corps obtenu par adjonction à K d'une racine du polynome irréductible φ .

Soit f un isomorphisme de K sur un corps K' , E une extension de K contenant une racine θ d'un polynome irréductible φ de $K[\theta]$, E' une extension de K' contenant une racine θ' du polynome φ' de $K'[\theta]$ correspondant à φ (par l'isomorphisme f prolongé à $K[\theta]$, voir chap.III et IV) ; il existe alors un isomorphisme et un seul $\overline{f}$ de $K<\theta>$ sur $K'<\theta'>$, prolongeant f , et tel que $\overline{f}(\theta)=\theta'$; cette condition définit en effet $\overline{f}(x)$ pour tout $x\in K<\theta>$, d'après la prop.3, et il est immédiat que cette application est un isomorphisme.

Exercices. 1) Soit E une extension finie d'un corps K . Montrer que le corps des fractions rationnelles $E(\theta)$ est une extension finie de $K(\theta)$, et que $[E(\theta):K(\theta)] = [E:K]$. Si E est une extension algèbrique simple de K , $E(\theta)$ est une extension algèbrique simple de $K(\theta)$, et tout élément θ engendrant E engendre aussi $E(\theta)$.

2) Si θ est un élément transcendant par rapport au corps K , il existe une infinité d'extensions distinctes E de K telles que $K \subset E \subset K<\theta>$ (considérer les extensions $K<\theta^p>$ pour tous les entiers $p>0$).

3) Soit E une extension de K telle qu'il n'existe qu'un nombre fini d'extensions distinctes de K contenues dans E ; montrer que E est une extension finie de K (en utilisant l'exerc.2, prouver d'abord que tout élément de E est algèbrique par rapport à K ; montrer ensuite que E est obtenu par adjonction d'un nombre fini d'éléments à K).

§ 3. Extensions algèbriques et extensions transcendantes.

Extensions algèbriques. Définition 1. On dit qu'une extension E d'un corps K est algèbrique, si tout élément de E est algèbrique par rapport à K . Une extension non algèbrique de K est dite transcendante.

Il est clair que, si F est un sous-corps d'une extension algèbrique E de K , contenant K , F est aussi une extension algèbrique de K , et E une extension algèbrique de F (§ 2, prop.4). Inversement :

Proposition 1. Si E est une extension algèbrique de K , et F une extension algèbrique de E , F est une extension algèbrique de K .

En effet, soit θ un élément de F , qui est algèbrique par rapport à E ; soit $\sum_{k=0}^{n} a_k x^k = 0$ l'équation irréductible à coefficients dans E , dont θ est racine ; si on pose $K' = K\langle a_0, a_1, \ldots, a_n \rangle$, θ est algèbrique par rapport à K' , autrement dit, $K'\langle\theta\rangle$ est une extension finie de K' ; comme K' est une extension finie de K , puisque les a_k sont algèbriques par rapport à K , $K'\langle\theta\rangle$ est une extension finie de K , et à fortiori $K\langle\theta\rangle$ est une extension finie de K , d'où la proposition.

Proposition 2. Toute extension finie d'un corps K est une extension algèbrique.

En effet, si E est une extension finie de degré n du corps K , et $\theta \in E$, les n+1 éléments ε (unité de K), $\theta, \theta^2, \ldots, \theta^n$ forment un système lié dans E (considéré comme algèbre sur K), autrement dit, il existe n+1 éléments a_k $(0 \leqslant k \leqslant n)$ non tous nuls de K tels que $\sum_{k=0}^{n} a_k \theta^k = 0$, ce qui prouve que θ est algèbrique par rapport à K .

Corollaire. Si E est une extension de K , l'ensemble des éléments de E , algèbriques par rapport à K , est un sous-corps de E .

En effet, si α et β sont deux éléments de E , algèbriques par rapport à K , $\alpha+\beta$, $\alpha\beta$ et α^{-1} (si $\alpha\neq 0$) sont des éléments de l'extension $K\langle\alpha,\beta\rangle$, qui est finie (§ 2, cor.2 de la prop.3), donc algèbrique ; ces éléments sont donc aussi algèbriques par rapport à K .

2 La prop.2 n'admet pas de réciproque ; une extension algèbrique d'un corps K peut fort bien être <u>infinie</u>.

<u>Extensions transcendantes pures</u>. <u>Définition 2. Soit E une extension d'un corps K. Une partie M de E est dite former un système algèbriquement lié par rapport à K , s'il existe une partie finie</u> $F=\{\theta_1,\theta_2,\dots,\theta_n\}$ <u>de M , et un polynome non nul</u> $f\in K[e_1,e_2,\dots,e_n]$ <u>tels que</u> $f(\theta_1,\theta_2,\dots,\theta_n)=0$. <u>Une partie de E qui n'est pas un système algèbriquement lié par rapport à K est dite système algèbriquement libre par rapport à K</u> .

Ces notions généralisent celles d'élément algèbrique et d'élément transcendant, qui sont respectivement les systèmes algèbriquement liés et les systèmes algèbriquement libres à <u>un</u> élément.

Si $M\subset E$ est <u>algèbriquement libre</u>, la condition pour qu'un élément $\theta\in E$ soit tel que $M\cup\{\theta\}$ soit encore algèbriquement libre, est que θ soit <u>transcendant par rapport à</u> $K\langle M\rangle$. En effet, si θ est algèbrique par rapport à $K\langle M\rangle$, il existe un polynome non nul $\varphi\in K\langle M\rangle[e]$, tel que $\varphi(\theta)=0$; en exprimant les coefficients de φ en fonctions rationnelles d'éléments de M , à coefficients dans K , et en chassant les dénominateurs, on en déduit aussitôt que $M\cup\{\theta\}$ est algèbriquement lié. Réciproquement, si $M\cup\{\theta\}$ est algèbriquement lié, il existe n éléments $\theta_1,\dots,\theta_n$ de M et un polynome non nul $f\in K[e_1,e_2,\dots,e_n,e]$ tel que $f(\theta_1,\theta_2,\dots,\theta_n,\theta)=0$; comme M est algèbriquement libre, le degré de f par rapport à e ne peut être nul,

et les coefficients du polynome en e obtenus en remplaçant les e_i par les θ_i dans f sont tous $\neq 0$; donc θ est algèbrique par rapport à $K\langle\theta_1,\ldots,\theta_n\rangle$, et a fortioti par rapport à $K\langle M\rangle$.

Définition 3. Une extension E d'un corps K est dite extension transcendante pure de K s'il existe un système algèbrique libre $M \subset E$ tel que $E = K\langle M\rangle$.

Théorème 1. Une extension transcendante pure d'un corps K est isomorphe à un corps de fractions rationnelles K(I) sur K (où I est un ensemble d'indices fini ou infini).

Soit en effet E une extension transcendante pure de K , M un système algèbriquement libre d'éléments de E tel que $E=K\langle M\rangle$. Soit I un ensemble d'indices en correspondance biunivoque avec M , ce qui permet d'écrire tout élément de M sous la forme x_ι ($\iota \in I$) ; si, à tout polynome $f \in K\left[e_{\iota_1}, e_{\iota_2},\ldots,e_{\iota_n}\right] \subset K\left[I\right]$ on fait correspondre l'élément $\mathring{f}(x_{\iota_1},x_{\iota_2},\ldots,x_{\iota_n})$ de E , on définit un isomorphisme de $K\left[I\right]$ sur un sous-anneau A de E contenant M , puisque M est algèbriquement libre ; cet isomorphisme se prolonge en un isomorphisme du corps des quotients K(I) sur le corps des quotients de A ; mais ce dernier, contenant $K\langle M\rangle$, est identique à E , d'où le théorème.

La prop.2 du §2 est un cas particulier de ce théorème.

La dénomination d'"extension transcendante pure" est justifiée par la proposition suivante :

Proposition 5. Si E est une extension transcendante pure de K , tout élément de E n'appartenant pas à K est transcendant par rapport à K .

Soit $E=K\langle M\rangle$ où M est un système algèbriquement libre, et soit $x \in E \cap \complement K$; désignons par $\mathfrak{F}$ l'ensemble des parties N et M telles que x n'appartienne pas à $K\langle N\rangle$; $\mathfrak{F}$ n'est pas vide (car $\emptyset \in \mathfrak{F}$)

et il est immédiat que, si on l'ordonne par inclusion, c'est un ensemble inductif ; il a donc un élément maximal N_0 ; posons $F=K\langle N_0\rangle$; on a $N_0 \neq M$, et si $\theta \in M \cap \complement N_0$, $x \in F\langle\theta\rangle$; l'extension $F\langle\theta\rangle$ est transcendante, sans quoi M ne serait pas algèbriquement libre ; on a donc $x=\dot{f}(\theta)/\dot{g}(\theta)$, où f et g sont deux polynomes non nuls et premiers entre eux de $F[e]$. Comme $x \in F\langle\theta\rangle$, $F\langle\theta\rangle$ est une extension de $F\langle x\rangle$, et cette extension est algèbrique, car θ satisfait à l'équation $x\dot{g}(\theta)-\dot{f}(\theta)=0$, non identiquement nulle et à coefficients dans $F\langle x\rangle$; donc x ne peut être algèbrique par rapport à K , car il serait algèbrique par rapport à F , et θ serait donc également algèbrique par rapport à F , d'après la prop.1 ; d'où la proposition.

Remarques. 1) L'application du théorème de Zorn dans cette démonstration est superflue, si on se souvient que, pour tout élément $x \in K\langle M\rangle$, il existe une partie finie P de M telle que $x \in K\langle P\rangle$.

2) La réciproque de la prop.3 est inexacte ; tous les éléments d'une extension E de K peuvent être transcendants par rapport à K sans que E soit une extension transcendante pure de K .

Bases de transcendance d'une extension. Théorème 2 (Steinitz). Une extension quelconque d'un corps K est une extension algèbrique d'une extension transcendante pure de K .

(Dans cet énoncé l'extension transcendante pure ou l'extension algèbrique peut se réduire à l'extension identique) .

En effet, soit E une extension de K , et soit $\mathcal{F}$ l'ensemble des systèmes algèbriquement libres par rapport à K et contenus dans E ; $\mathcal{F}$ n'est pas vide, car $\emptyset \in \mathcal{F}$, et $\mathcal{F}$ est évidemment inductif quand on l'ordonne par inclusion ; il a donc un élément maximal M .

Soit $F=K\langle M\rangle$, qui est une extension transcendante pure de K ; soit x un élément de E n'appartenant pas à F (si $F\neq E$) ; il est algèbrique par rapport à F , car dans le cas contraire, $M\cup\{x\}$ serait un système algèbriquement libre par rapport à K . Donc E est une extension algèbrique de F .

Une partie M de E telle que M soit algèbriquement libre par rapport à K , et que E soit une extension algèbrique de l'extension transcendante pure $K\langle M\rangle$, est appelée base de transcendance de E par rapport à K .

Proposition 4. Soit E une extension de K , M une base de transcendance de E par rapport à K , $N\subset E$ un système algèbriquement libre par rapport à K . Il existe une partie $P\subset M$ telle que $N\cup P$ soit une base de transcendance de E par rapport à K .

En effet, soit $\mathscr{E}$ l'ensemble des parties Q de M telles que $N\cup Q$ soit algèbriquement libre ; $\mathscr{E}$ n'est pas vide (il contient $\emptyset$) et est inductif ; soit P un élément maximal de $\mathscr{E}$. Tout élément x de $M\cap\complement P$ est algèbrique par rapport à $K\langle N\cup P\rangle$, sans quoi $N\cup P\cup\{x\}$ serait algèbriquement libre, contrairement au fait que P est maximal dans $\mathscr{E}$; donc $K\langle M\rangle$ est une extension algèbrique de $K\langle N\cup P\rangle$; comme E est une extension algèbrique de $K\langle M\rangle$, la proposition résulte de la prop1

Il existe en général une infinité de bases de transcendance d'une extension transcendante E d'un corps K (lorsque K est infini) ; mais on a le théorème suivant :

Théorème 3. Si l'extension E de K a, par rapport à K , une base de transcendance finie M , toute autre base de transcendance de E par rapport à K est finie et a le même nombre d'éléments que M .

Soit $M=\{x_1,x_2,\ldots,x_n\}$, et soit N une autre base de transcendance de E par rapport à K. Supposons d'abord que N ait au moins n éléments. Comme x_1 n'est pas algèbrique par rapport à $K\langle x_2,\ldots,x_n\rangle$ il existe un élément $y_1 \in N$ qui n'est pas algèbrique par rapport à $K\langle x_2,\ldots,x_n\rangle$, sans quoi $K\langle N\rangle$ serait une extension algèbrique de $K\langle x_2,\ldots,x_n\rangle$, et il en serait de même de E d'après la prop.1, ce qui est absurde ; donc $M_1=\{y_1,x_2,\ldots,x_n\}$ est un système algèbriquement libre. En outre M_1 est une base de transcendance de E, car le système $\{x_1\}\cup M_1$ est algèbriquement lié, sans quoi y_1 ne serait pas algèbrique par rapport à $K\langle M\rangle$, contrairement à l'hypothèse ; donc x_1 est algèbrique par rapport à $K\langle M_1\rangle$, ce qui montre que $K\langle M\rangle$, et par suite E, est une extension algèbrique de $K\langle M_1\rangle$, donc que M_1 est une base de transcendance de E. Par récurrence, on voit qu'il existe n éléments $y_1,\ldots,y_n$ de N formant une base de transcendance de E ; donc $N=\{y_1,y_2,\ldots,y_n\}$. Raisonnement analogue, en échangeant les rôles de M et N, si N a au plus n éléments.

Si une extension E de K a une base de transcendance <u>finie</u> par rapport à K, le nombre d'éléments de cette base est appelé le <u>degré de transcendance</u> de E par rapport à K (ne pas confondre avec le <u>degré</u> de E par rapport à K, qui est <u>infini</u> lorsque le degré de transcendance est >0) ; il résulte du th.5 que ce nombre ne dépend que de E, et non de la base de transcendance particulière considérée.

<u>Proposition 5</u>. <u>Soit E une extension de K, de degré de transcendance fini</u> r, <u>et F une extension de E, de degré de transcendance fini</u> s <u>par rapport à E ; le degré de transcendance de F par rapport à K est égal à</u> r+s.

En effet, soit M une base de transcendance de E par rapport à K , N une base de transcendance de F par rapport à E ; il suffit de prouver que $M \cup N$ est une base de transcendance de F par rapport à K .

Tout élément de E est algèbrique par rapport à $K\langle M\rangle$, donc aussi par rapport à $K\langle M \cup N\rangle$; il en résulte que tout élément de $E\langle N\rangle$ est algèbrique par rapport à $K\langle M \cup N\rangle$ (cor. de la prop. 2) ; comme F est une extension algèbrique de $E\langle N\rangle$, c'est aussi une extension algèbrique de $K\langle M \cup N\rangle$ (prop. 1).

Reste à voir que $M \cup N$ est algèbriquement libre par rapport à K . Si $M = \{x_1, \ldots, x_r\}$ et $N = \{y_1, \ldots, y_s\}$, et s'il existait un polynome $f \in K[e_1, e_2, \ldots, e_{r+s}]$ tel que $f(x_1, \ldots, x_r, y_1, \ldots, y_s) = 0$, on voit d'abord, en considérant f comme un polynome en $e_{r+1}, \ldots, e_{r+s}$, que les coefficients $g_i \in K[e_1, \ldots, e_r]$ de ce polynome sont tels que $g_i(x_1, \ldots, x_r) = 0$, N étant algèbriquement libre par rapport à E ; mais M étant algèbriquement libre par rapport à K , on a nécessairement $g_i = 0$, donc $f = 0$, ce qui achève la démonstration.

Remarques. 1) Cette démonstration prouve, plus généralement, que si M est une base de transcendance (finie ou non) de E par rapport à K , et N une base de transcendance (finie ou non) de F par rapport à E , $M \cup N$ est une base de transcendance de F par rapport à K .

On peut démontrer également que, si M et M' sont deux bases de transcendance infinies d'une même extension E de K , M et M' sont équipotentes (généralisation du th. 3).

2) Si E est une extension transcendante pure de K , et F une extension algèbrique de E , F peut encore être une extension transcendante pure de K . Par exemple, soit $E = K(e)$ (extension transcendante simple de K), et F l'extension algèbrique simple $E\langle u\rangle$,

où u est une racine de l'équation (irréductible dans K(e)) $u^2-e=0$. Il est immédiat que tout élément de F est égal à une fraction rationnelle en u , à coefficients dans K , donc $F=K\langle u\rangle$, et comme u est transcendant par rapport à K (sans quoi $E \subset F$ serait une extension algèbrique de K), F est une extension transcendante simple de K (donc isomorphe à E).

Exercices. 1) Dans une extension transcendante simple $K\langle\theta\rangle$ d'un corps K , tout élément $\eta \in K\langle\theta\rangle$ s'écrit sous la forme $f(\theta)/g(\theta)$, où f et g sont deux polynomes de $K[e]$ premiers entre eux (et bien déterminés à un facteur de K près) ; on appelle degré de η par rapport à $K\langle\theta\rangle$ le plus grand des degrés de f et g .

a) Montrer que $K\langle\theta\rangle$ est une extension algèbrique de degré n par rapport à $K\langle\eta\rangle$, si η est de degré n (montrer que le polynome $g\eta-f$ est irréductible dans $K\langle\eta\rangle[e]$, en remarquant que η est transcendant par rapport à K , et en se ramenant à montrer que le polynome ug-f est irréductible dans $K[e,u]$ (utiliser le lemme de Gauss, chap. V, § 4)).

b) En déduire que tout élément θ' de $K\langle\theta\rangle$ tel que $K\langle\theta'\rangle = K\langle\theta\rangle$ est de la forme $(a\theta+b)/(c\theta+d)$, avec a,b,c,d éléments de K tels que $ad-bc\neq 0$; réciproque. Trouver tous les automorphismes de $K\langle\theta\rangle$ laissant invariants les éléments de K .

c) Si η est de degré n par rapport à $K\langle\theta\rangle$ et ζ de degré m par rapport à $K\langle\eta\rangle$, ζ est de degré mn par rapport à $K\langle\theta\rangle$ (utiliser la prop. 1 du § 2) .

2) Si K est infini, toute extension algèbrique de K est équipotente à K . Si M est une base de transcendance d'une extension E de K , E est équipotent à $K\times M$. En déduire que toute extension E de K ,

autre que K , contient une extension F de K , distincte de E et équipotente à E .

3) Soit E une extension algèbrique d'un corps K . Si A est un anneau tel que $K \subset A \subset E$, montrer que A est un corps.

§ 4. Extensions algèbriquement stables.

Le th.2 du § 3 ramène l'étude d'une extension quelconque d'un corps commutatif K à celle des extensions algèbriques, d'une part et à celle des extensions transcendantes pures de l'autre. Le th. 1 du § 3 élucidant, en principe, la structure de ces dernières, il reste à faire l'étude des extensions algèbriques ; il ne sera plus question que de celles-ci dans le reste de ce chapitre.

Il y a une catégorie particulière de corps pour lesquels la détermination de leurs extensions algèbriques est immédiate ; ce sont les corps algèbriquement stables définis au chap.IV (§ 4) par la condition que, si K est un tel corps, tout polynome de $K[e]$ soit égal à un produit de polynomes du premier degré ; autrement dit, les seuls polynomes irréductibles de $K[e]$ sont les polynomes du premier degré. Tout élément algèbrique par rapport à K appartient donc nécessairement à K (§ 2, prop.3) ; en d'autres termes, il n'existe pas d'extension algèbrique d'un corps algèbriquement stable K , qui soit distincte de K ; la réciproque est évidente d'après la prop.3 du § 2, ce qui justifie la dénomination de "corps algèbriquement stable" .

* Comme on l'a déjà signalé, le corps $\mathbb{C}$ des nombres complexes est algèbriquement stable. *

Si E est une extension algèbriquement stable d'un corps K , l'ensemble F des éléments de E algèbriques par rapport à K forme encore une extension algèbriquement stable (et algèbrique) de K .

En effet, F est un corps (§ 3, cor. de la prop.2) ; et tout élément θ algèbrique par rapport à F est algèbrique par rapport à E , donc appartient à E ; mais comme F est une extension algèbrique de K , θ est aussi algèbrique par rapport à K , donc appartient à F .

Le but de ce paragraphe va être de construire, pour un corps quelconque K , une extension algèbrique de K qui soit algèbriquement stable. Nous aurons besoin de la proposition suivante :

Proposition 1. Soit E une extension algèbrique d'un corps K . Pour que E soit algèbriquement stable, il suffit que les seuls polynomes de $K[e]$ qui soient irréductibles dans $E[e]$ soient les polynomes du premier degré.

En effet, supposons cette condition remplie, et soit θ un élément algèbrique par rapport à E ; il est alors aussi algèbrique par rapport à K (§ 5, prop.1), donc racine d'un polynome à coefficients dans K . Ce polynome pouvant s'écrire, par hypothèse, $a(e-\alpha_1)(e-\alpha_2)\ldots(e-\alpha_n)$, où $a \in K$, $\alpha_i \in E$, on a nécessairement $\theta = \alpha_i$ pour un des indices i , donc $\theta \in E$, ce qui prouve que E est algèbriquement stable.

Théorème 1 (Steinitz). Etant donné un corps commutatif K , on peut définir une extension algèbrique Ω de K , ayant les propriétés suivantes :

1° Ω est algèbriquement stable.

2° Si K' est un corps isomorphe à K , E' une extension algèbrique de K' , φ un isomorphisme de K' sur K , il existe un prolongement de φ à E' , qui est un isomorphisme de E' sur un sous-corps de Ω .

Nous commencerons par établir la proposition suivante : étant donné un polynome $f \in K[e]$, on peut définir une extension finie L de K telle que, dans $E[e]$, f se décompose en facteurs irréductibles du premier degré (un tel corps est appelé corps de décomposition du polynome f).

Il suffit de le démontrer par récurrence sur le degré n de f . Soit g un facteur irréductible de f de degré >1 (s'il n'existe pas de tel facteur, K est déjà un corps de décomposition de f) ; soit K_1 le corps obtenu par adjonction à K d'une racine θ de g ; dans $K_1[e]$, on a donc $f=(e-\theta)f_1$, où f_1 est un polynome de degré $< n$; il existe par hypothèse une extension finie E de K_1 telle que, dans $E[e]$, f_1 soit un produit de polynomes du premier degré ; a fortiori, f est un produit de polynomes du premier degré dans $E[e]$.

Cette proposition étant démontrée, considérons l'ensemble des polynomes de degré >0 de $K[e]$, dont le coefficient du terme de plus haut degré est 1 , et écrivons cet ensemble sous forme d'une famille $(f_\alpha)_{\alpha\in A}$, où A est un ensemble d'indices en correspondance biunivoque avec l'ensemble considéré ; nous désignerons par n_α le degré de f_α . Soit I un ensemble en correspondance biunivoque avec $A \times \mathbb{N}$; nous désignerons par $y_{\alpha,p}$ $(\alpha \in A, p \in \mathbb{N})$ ses éléments. Pour chaque polynome f_α , considérons le polynome de $K[I][e]$:

$$g_\alpha = f_\alpha - (e-y_{\alpha,1})(e-y_{\alpha,2})\dots(e-y_{\alpha,n})$$

et soient $g_{\alpha,i}$ $(1 \leqslant i \leqslant n_\alpha)$ les coefficients de ce polynome (qui sont des polynomes de $K[I]$). Soit $\mathfrak{a}$ l'<u>idéal</u> de l'anneau $K[I]$ engendré par les $g_{\alpha,i}$ $(\alpha \in A , 1 \leqslant i \leqslant n_\alpha)$; nous allons voir d'abord que $\mathfrak{a} \neq K[I]$, c'est-à-dire que $1 \notin \mathfrak{a}$, ou encore qu'il ne peut y avoir d'identité de la forme

$$1 = \sum_{\alpha,i} h_{\alpha,i} g_{\alpha,i} \tag{1}$$

où les $h_{\alpha,i}$ sont des polynomes de $K[I]$ (les indices α qui figurent dans (1) étant bien entendu en nombre <u>fini</u>). Or, une telle identité donne encore lieu à une identité si on y remplace certains des $y_{\alpha,i}$ qui y figurent par des éléments quelconques d'une extension quelconque E de K

(chap.IV, § 2). Prenons E de sorte que tous les f_α correspondant aux indices α qui figurent dans (1) se décomposent en facteurs du premier degré dans $E[e]$, et soient $\theta_{\alpha,i}$ $(1 \leqslant i \leqslant n_\alpha)$ les racines de f_α dans E ; si on remplace les $y_{\alpha,i}$ par $\theta_{\alpha,i}$ dans $g_{\alpha,k}$ on obtient 0, donc par cette substitution le second membre de (1) s'annulerait, ce qui est absurde.

Comme $\mathfrak{a} \neq K[I]$, il existe un idéal <u>maximal</u> $\mathfrak{P}$ de $K[I]$ tel que $\mathfrak{a} \subset \mathfrak{P}$. L'anneau $K[I]/\mathfrak{P}$ est un <u>corps</u> ; comme $1 \notin \mathfrak{P}$, l'ensemble des classes (mod. $\mathfrak{P}$) des éléments de K forme un sous-corps de $K[I]/\mathfrak{P}$ isomorphe à K, et que nous <u>identifierons</u> à K. Nous désignerons enfin par Ω le sous-corps de $K[I]/\mathfrak{P}$ engendré par K et par les classes (mod. $\mathfrak{P}$) des éléments $y_{\alpha,p}$ $(\alpha \in A, 1 \leqslant p \leqslant n_\alpha)$. Nous allons montrer que Ω satisfait aux conditions du théorème.

1) <u>Ω est une extension algébrique et algébriquement stable de K</u>. En effet, on a

$$f_\alpha \equiv (e-y_{\alpha,1})\ldots(e-y_{\alpha,n_\alpha}) \pmod{\mathfrak{a}}$$

et a fortiori, cette congruence a lieu mod. $\mathfrak{P}$; cela signifie que, si $u_{\alpha,p}$ est la classe (mod. $\mathfrak{P}$) de $y_{\alpha,p}$, on a

$$f_\alpha = (e-u_{\alpha,1})\ldots(e-u_{\alpha,n_\alpha}) \tag{2}$$

dans l'anneau $\Omega[e]$; donc chacun des $u_{\alpha,p}$ est racine de f_α donc est algébrique par rapport à K, et par suite Ω est une extension algébrique de K (§ 5, cor. de la prop.2). En outre, la relation (2) et la prop. 1 montrent que Ω est algébriquement stable.

2) <u>L'isomorphisme φ de K' sur K se prolonge en un isomorphisme de E' sur un sous-corps de Ω</u>. Soit $\mathfrak{F}$ l'ensemble des isomorphismes Ψ d'un sous-corps de E' dans Ω qui sont des prolongements de φ, et <u>ordonnons $\mathfrak{F}$ par prolongement</u> (c'est-à-dire que $\Psi \leqslant \Psi'$ signifie

" ψ' est un prolongement de ψ ") ; comme la réunion d'une famille totalement ordonnée de sous-corps de E' est un sous-corps de E', il est immédiat que $\mathfrak{F}$ est un ensemble <u>inductif</u>. Il possède donc un élément <u>maximal</u> φ_0 , isomorphisme d'un sous-corps M' de E' sur un sous-corps $M = \varphi_0(M')$ de Ω ; montrons que M'=E' . En effet, si $\theta' \in E'$ n'appartenait pas à M' , θ' serait algèbrique par rapport à M' ; soit f le polynome irréductible de $M'[e]$ dont θ' est racine, et $\overline{f}$ le polynome qui lui correspond dans $M[e]$ (c'est-a-dire dont les coefficients sont transformés par φ_0 de ceux de f) ; soit θ une racine de $\overline{f}$ dans Ω ($\overline{f}$ étant décomposé en facteurs linéaires) ; le prolongement φ_1 de φ_0 à l'ensemble $M' \cup \{\theta'\}$ tel que $\varphi_1(\theta')=\theta$ définit un isomorphisme de $M'\langle\theta'\rangle$ sur $M\langle\theta\rangle$, donc φ_0 ne serait pas maximal dans $\mathfrak{F}$, contrairement à l'hypothèse. Le théorème est ainsi complètement démontré.

<u>Corollaire</u>. <u>Si E est une extension algèbrique et algèbriquement stable de K , E est isomorphe au corps Ω définie dans le th. 1</u> .

En effet, d'après ce théorème, E est isomorphe à un sous-corps G de Ω , qui est une extension algèbriquement stable de K ; mais comme Ω est une extension algèbrique de G , on a $\Omega = G$.

Le corps Ω possèdant les propriétés du th.1 est donc bien déterminé par ces propriétés <u>à une isomorphie près</u> ; nous l'appellerons l'<u>extension algèbrique maximale</u> de K . Toute extension algèbrique de K est isomorphe à un sous-corps de Ω ; désormais, sauf mention expresse du contraire, lorsque nous parlerons d'une extension algèbrique de K , nous la supposerons <u>identifiée avec un sous-corps de</u> Ω .

On notera que la démonstration du th.1 fait intervenir (à deux endroits) l'axiome de Zermelo. Dans beaucoup des questions traitées aux §§ suivants, on pourrait se dispenser d'appliquer le théorème 1, et se borner à utiliser des <u>corps de décomposition convenables</u> ;

mais la simplicité des raisonnements en souffre.

Exercice. Soit Ω l'extension algèbrique maximale d'un corps K. Quel que soit l'élément $x \in \Omega$ n'appartenant pas à K, il existe un sous-corps maximal E parmi les extensions algèbriques de K ne contenant pas x. Soit $r>1$ le degré de x par rapport à E. Montrer que le degré d'un polynome irréductible de $E[e]$ est égal à 1 ou à un multiple de r ; en particulier, tout polynome de $E[e]$ dont le degré n'est pas multiple de r a une racine dans E. Montrer aussi qu'il n'existe qu'une seule extension de E dont le degré par rapport à E soit égal à r, et cette extension est identique à $E\langle x\rangle$.

§ 5. Isomorphismes d'extensions algèbriques.

Soient K et K' deux sous-corps isomorphes d'un corps E. Si f est un isomorphisme de K sur K', la restriction de f au corps premier P contenu dans E (donc dans $K \cap K'$) est un automorphisme de P. Or, le seul automorphisme de P est l'application identique ; car si g est un tel automorphisme, on a $g(\varepsilon)=\varepsilon$ si ε est l'unité de P ; on en déduit $g(n.\varepsilon)=n.g(\varepsilon)=n.\varepsilon$ quel que soit $n \in \mathbb{Z}$, d'où résulte aisément que $g(x)=x$ quel que soit $x \in P$, que P soit de caractéristique nulle ou non.

Cette propriété des corps premiers ne leur est nullement particulière.* Par exemple, le corps $\mathbb{R}$ des nombres réels n'a pas d'autre automorphisme que l'automorphhisme identique .*

Tout isomorphisme de K sur un autre corps contenu dans E laisse donc fixes les éléments d'un sous-corps de K. En général, nous dirons qu'un isomorphisme de K dans E est un isomorphisme relatif au sous-corps S de K s'il laisse invariants tous les éléments de S.

Dans ce qui suit, nous considérerons les extensions algèbriques E d'un corps K , contenues dans l'extension algèbrique maximale Ω de K , et les isomorphismes de E dans Ω (donc sur un sous-corps de Ω) relatifs à K (donc laissant fixes tous les éléments de K). Si le nombre de ces isomorphismes est fini, on l'appelle degré réduit de E par rapport à K ; nous le désignerons par $\partial_K(E)$.

Proposition 1. Tout isomorphisme de E relatif à K peut être prolongé en un automorphisme de Ω relatif à K .

C'est une conséquence immédiate de la 2è partie du th.1 du § 4 : si f est un isomorphisme de E sur $E' \subset \Omega$, il peut être prolongé à l'extension algèbrique Ω de E , qu'il applique sur un sous-corps G de Ω ; G étant une extension algèbriquement stable de E', et Ω une extension algèbrique de G , $G = \Omega$, d'où la proposition.

Proposition 2. Soit E une extension algèbrique de K , F une extension algèbrique de E . Soit $(f_\alpha)_{\alpha \in A}$ la famille des isomorphismes distincts de E relatifs à K , prolongés en des automorphismes de Ω ; soit de même $(g_\beta)_{\beta \in B}$ la famille des isomorphismes distincts de F relatifs à E (prolongés à Ω) ; tout isomorphisme de F relatif à K se prolonge d'une manière et d'une seule en un isomorphisme de la forme $f_\alpha \circ g_\beta$.

Soit h un isomorphisme de F relatif à K ; sur E , il coïncide avec un f_α , donc $f_\alpha^{-1} \circ h$ est un isomorphisme de F relatif à E , donc égal sur F à un g_β ; autrement dit, on a $h = f_\alpha \circ g_\beta$ dans F' , et il est clair que réciproquement tout composé $f_\alpha \circ g_\beta$ est un isomorphisme de F relatif à K ; en outre, on ne peut avoir $f_\alpha \circ g_\beta = f_{\alpha_1} \circ g_{\beta_1}$ sur F que si $\alpha=\alpha_1$, $\beta=\beta_1$; en effet, on en tire que f_α et f_{α_1} sont identiques sur E, donc $\alpha=\alpha_1$, et en composant les deux isomorphismes avec f_α^{-1} , on a $g_\beta=g_{\beta_1}$, donc $\beta=\beta_1$. Ainsi, l'ensemble des isomorphismes de F par rapport

à K est en correspondance biunivoque avec $A \times B$, ce qui donne, dans le cas particulier où A et B sont finis, le corollaire :

Corollaire. Si les degrés réduits de E par rapport à K et de F par rapport à E sont finis, il en est de même du degré réduit de F par rapport à K, et on a $\vartheta_K(F) = \vartheta_K(E)\ \vartheta_E(F)$.

Conjugués d'un élément. Eléments séparables. Soit θ un élément quelconque de Ω, E une extension de K contenant θ ; si φ est le polynome irréductible de $K[e]$ dont θ est racine (§ 2), et f un isomorphisme quelconque de E relatif à K, on a évidemment $\varphi(f(\theta))=f(\varphi(\theta)) = 0$, donc $f(\theta)$ est une racine de φ dans Ω. On appelle éléments conjugués de θ par rapport à K les racines distinctes $\theta_1=\theta, \theta_2,\ldots,\theta_\rho$ de φ dans Ω. On peut donc énoncer la proposition suivante :

Proposition 3. Si θ est un élément d'une extension E de K, tout isomorphisme de E relatif à K applique θ sur un de ses conjugués relatifs à K.

Définition 1. On dit qu'un élément $\theta \in \Omega$ est séparable par rapport à K si le nombre de ses conjugués est égal à son degré par rapport à K ; dans le cas contraire, θ est dit inséparable par rapport à K.

Cherchons à caractériser un élément θ inséparable par rapport à K. Soit φ le polynome irréductible de $K[e]$ dont θ est racine ; le nombre de racines distinctes de φ étant strictement inférieur à son degré n, φ a au moins une racine multiple dans Ω, donc cette racine est aussi racine de la dérivée φ'. Or, si le polynome φ' n'a pas tous ses coefficients nuls, il est de degré $< n$, donc le p.g.c.d de φ et φ' dans $K[e]$ est égal à 1 ; il est donc aussi égal à 1 dans $\Omega[e]$, ce qui prouve que φ et φ' ne peuvent alors avoir de racine commune dans Ω. Ainsi, si θ est inséparable par rapport à K,

et si $\varphi = \sum_{k=0}^{n} a_k e^k$, on doit nécessairement avoir $ka_k=0$ pour $1 \leqslant k \leqslant n$. Si K est de caractéristique 0 , cela entraîne $a_k=0$ pour $1 \leqslant k \leqslant n$, ce qui est absurde ; il n'y a pas dans ce cas d'élément inséparable par rapport à K . Si K est de caractéristique $p>0$, les relations $ka_k=0$ donnent $a_k=0$ pour k <u>non multiple de</u> p .

Réciproquement, supposons cette condition remplie, et soit p^r la plus haute puissance de p telle que $a_k=0$ pour k non multiple de p^r ; il en résulte que φ s'obtient en remplaçant e par e^{p^r} dans un polynome $\psi = \sum_{h=0}^{\nu} b_h e^h$ de $K[e]$; en outre, on a $\psi' \neq 0$, sans quoi on aurait $a_k=0$ pour k non multiple de p^{r+1} ; donc ψ , qui est évidemment irréductible dans $K[e]$, n'a que des racines simples dans Ω , autrement dit on peut l'écrire $\psi = \prod_{h=1}^{\nu} (e-\alpha_h)$ d'où $\varphi = \prod_{h=1}^{\nu} (e^{p^r}-\alpha_h)$. Si θ_h est une racine de $e^{p^r}-\alpha_h$, on a $\theta_h^{p^r} = \alpha_h$, donc, en vertu de la formule (3) du § 1 ,

$$e^{p^r} - \alpha_h = (e-\theta_h)^{p^r}$$

d'où $\varphi = \prod_{h=1}^{\nu} (e-\theta_h)^{p^r}$; les racines θ_h sont évidemment distinctes et chacune d'elles est de multiplicité p^r . En résumé :

<u>Proposition 4. Pour qu'un élément</u> θ <u>soit inséparable par rapport à K , il faut et il suffit que K soit de caractéristique</u> $p>0$, <u>et que, si</u> $\varphi = \sum_{k=0}^{n} a_k e^k$ <u>est le polynome irréductible de</u> $K[e]$ <u>dont</u> θ <u>est racine, on ait</u> $a_k=0$ <u>pour k non multiple de</u> p .

Un polynome irréductible de $K[e]$ est dit <u>séparable</u> si ses racines sont séparables par rapport à K , <u>inséparable</u> dans le cas contraire ; la prop.4 donne donc une condition nécessaire et suffisante pour qu'un polynome irréductible soit inséparable. Le nombre ν des conjugués de θ s'appelle encore le <u>degré réduit</u> de θ par rapport à K ; la démonstration de la prop.4 prouve qu'on a,

entre le degré n et le degré réduit ϑ de θ , la relation

(1) $$n = \vartheta p^r$$

avec $r \geqslant 1$ (si θ est inséparable) ; r s'appelle l'exposant de θ par rapport à K .

Proposition 5 . Le degré réduit par rapport à K d'un élément θ est égal au degré réduit par rapport à K de l'extension $K\langle\theta\rangle$.

En effet, tout isomorphisme f de $K\langle\theta\rangle$ relatif à K est entièrement caractérisé par la donnée de $f(\theta)$; comme le nombre des valeurs distinctes de $f(\theta)$ est d'après la prop.3 le degré réduit de θ , la proposition est démontrée.

Proposition 6. Si θ est un élément séparable par rapport à K , il est séparable par rapport à toute extension E de K .

En effet, soit φ le polynome irréductible de $K[e]$ dont θ est racine ; dans $E[e]$, φ se décompose en un produit de polynomes irréductibles φ_i $(1 \leqslant i \leqslant q)$; comme, dans l'extension algèbrique maximale Ω' de E , φ n'a que des racines simples, il en est de même des φ_i , donc en particulier de celui des φ_i dont θ est racine.

Extensions séparables. Définition 2. On dit qu'une extension algèbrique E d'un corps K est séparable par rapport à K si tout élément de E est séparable par rapport à K ; dans le cas contraire, E est dite inséparable par rapport à K .

On peut caractériser d'une autre manière les extensions séparables finies :

Proposition 7. Pour toute extension finie E de K , on a $\vartheta_K(E) \leqslant [E:K]$ Pour que $\vartheta_K(E) = [E:K]$, il faut et il suffit que E soit une extension séparable de K .

La première partie résulte de la prop.5 pour une extension simple $K\langle\theta\rangle$; pour une extension finie E quelconque, il suffit d'observer que E est obtenu par adjonction à K d'un nombre fini d'éléments $a_1, a_2, \ldots, a_m$, de calculer $[E:K]$ en appliquant le cor.2 de la prop.3 du §2, et $\gamma_K(E)$ en appliquant la prop.2 de ce paragraphe par récurrence : si n_i est le degré de a_i par rapport à $K\langle a_1, a_2, \ldots, a_{i-1}\rangle$, et γ_i son degré réduit, on a $[E:K] = n_1 n_2 \ldots n_m$;
$\gamma_K(E) = \gamma_1 \gamma_2 \ldots \gamma_m \leqslant [E:K]$.

Si E est séparable, a_i , qui est séparable par rapport à K , l'est aussi par rapport à $K\langle a_1, a_2, \ldots, a_{i-1}\rangle$, donc $\gamma_i = n_i$, et par suite $\gamma_K(E) = [E:K]$. Inversement, cette relation entraîne que tout élément de E est séparable, car dans le cas contraire, on pourrait toujours supposer que a_1 est un élément inséparable de E , donc que $\gamma_1 < n_1$, ce qui entraînerait $\gamma_K(E) < [E:K]$, contrairement à l'hypothèse.

Corollaire 1. Une extension E de K , obtenue par adjonction à K d'un ensemble M d'éléments séparables par rapport à K , est une extension séparable par rapport à K .

Cela résulte de la démonstration précédente si E est une extension finie de K ; dans le cas contraire, tout élément de E appartient à un corps $K\langle N\rangle$, où N est une partie finie de M , donc est séparable.

Corollaire 2. Si E est une extension séparable de K , et F une extension séparable de E , F est une extension séparable de K .

En effet, la proposition résulte de la prop.2 de ce § , et de la prop.1 du §2, lorsque E et F sont des extensions finies. Dans le cas contraire, il suffit de remarquer que tout élément θ de F, étant séparable par rapport à E , est aussi séparable par rapport à l'extension K' de K obtenue par adjonction des coefficients du polynome irréductible

de $E[\theta]$ qui a θ pour racine ; K' étant séparable par rapport à K , θ est séparable par rapport à K d'après ce qui précède.

Proposition 8. Toute extension séparable finie E d'un corps infini K est une extension simple de K .

Il suffit de le démontrer pour une extension $K\langle a,b\rangle$ obtenue par adjonction de deux éléments, la proposition générale s'en déduisant aussitôt par récurrence sur le nombre d'éléments adjoints.

Soient a_i $(1 \leqslant i \leqslant m)$ les conjugués de a par rapport à K , et b_j $(1 \leqslant j \leqslant n)$ les conjugués de b par rapport à K $(a_1=a\ ,\ b_1=b)$. Montrons qu'on peut déterminer $\lambda \in K$ tel que, lorsque f parcourt l'ensemble des isomorphismes de $K\langle a,b\rangle$ relatifs à K , les éléments $f(a+\lambda b)$ soient tous distincts ; comme le degré de $K\langle a,b\rangle$ est égal à son degré réduit, il en résultera que $c=a+\lambda b$ a un degré par rapport à K égal à celui de $K\langle a,b\rangle$, autrement dit que $K\langle a,b\rangle = K\langle c\rangle$. Or, les éléments $f(a+\lambda b)$ sont de la forme $a_i+\lambda b_j$; comme on ne peut avoir $f(a)=g(a)$ et $f(b)=g(b)$ que si les isomorphismes f et g sont identiques, on sera certain que les éléments $f(a+\lambda b)$ sont tous distincts si $a_i+\lambda b_j \neq a_h+\lambda b_k$ pour $j \neq k$, i et h quelconques. Mais chacune des équations en λ : $a_i+\lambda b_j = a_h+\lambda b_k$ a au plus une solution dans K ; comme ces équations sont en nombre fini, et que K est supposé infini, on peut prendre $\lambda \in K$ ne satisfaisant à aucune d'entre elles, d'où la proposition.

Au § 7, nous verrons que cette proposition est encore exacte lorsque K est un corps fini.

Corps parfaits. Définition 3. On dit qu'un corps K est parfait si toute extension algébrique de K est séparable par rapport à K ; sinon, K est dit imparfait.

Il est immédiat, d'après ce qui précède, que tout corps de caractéristique 0 est parfait. Pour les corps de caractéristique $p>0$, le critère suivant caractèrise les corps parfaits :

Proposition 9. Pour qu'un corps K de caractéristique $p>0$ soit parfait, il faut et il suffit que l'isomorphisme $x \to x^p$ applique K sur lui-même (autrement dit, que tout élément de K soit une puissance $p^{ème}$ d'un élément de K).

La condition est nécessaire, car s'il existe un élément $a \in K$ qui ne soit pas puissance $p^{ème}$ d'un élément de K, le polynome e^p-a est irréductible dans $K[e]$: en effet, si $b \notin K$ est une racine de ce polynome, on a $e^p-a=(e-b)^p$, donc tout facteur de e^p-a ne peut avoir que la seule racine b, et on a vu plus haut qu'un polynome irréductible de $K[e]$ ne peut avoir que des racines simples ou dont l'ordre de multiplicité est une puissance de p ; comme e-b n'appartient pas à $K[e]$, e^p-a est bien irréductible. Il est clair alors, d'après la prop.4 que b est inséparable par rapport à K, donc K imparfait.

La condition est suffisante, car si elle est remplie, tout polynome $\sum_{k=0}^{n} a_{kp}e^{kp}$ ne contenant que des puissances multiples de p, peut s'écrire $(\sum_{k=0}^{n} b_k e^k)^p$, où b_k est un élément de K tel que $b_k^p=a_{kp}$; un tel polynome ne peut donc être irréductible dans $K[e]$, et la prop.4 prouve que K est parfait.

Cette proposition montre entre autres que les corps premiers $\mathbb{Z}/(p)$ sont parfaits ; plus généralement, tout corps fini est parfait, car l'isomorphisme $x \to x^p$ étant une application biunivoque de K dans lui-même, applique nécessairement alors K sur K.

Notons aussi que, d'après la prop.6, toute extension algèbrique d'un corps parfait est un corps parfait.

Il n'en est pas de même des extensions transcendantes. Par exemple, si K est un corps de caractéristique $p > 0$, l'extension transcendante simple K(e) est un corps imparfait ; en effet, e n'est pas puissance $p^{ème}$ d'un élément de K(e), sans quoi on aurait une identité de la forme $f^p e = g^p$, où f et g sont deux polynomes de $K[e]$, et une telle identité est absurde, comme on le voit en comparant les degrés des deux membres.

Extensions inséparables. Remarquons d'abord que, si K est un corps de caractéristique $p > 0$, le polynome $e^p - a$ a ses p racines confondues dans l'extension algèbrique maximale Ω de K, car, si β est une de ces racines, on a $a = \beta^p$, d'où $e^p - a = (e-\beta)^p$. La valeur commune de ces p racines se note $a^{1/p}$; l'application $x \to x^{1/p}$ est donc définie dans K, et c'est un isomorphisme de K sur une extension algèbrique de K, qu'on note $K^{1/p}$; en effet, il suffit de vérifier les identités

$$(2) \qquad (x+y)^{1/p} = x^{1/p} + y^{1/p}$$

$$(3) \qquad (xy)^{1/p} = x^{1/p} y^{1/p}$$

ce qui se fait immédiatement en élevant les deux membres de ces relations à la puissance p, et tenant compte de la formule (1) du § 1.

En itérant l'application $x \to x^{1/p}$, on définit, pour tout entier $n > 0$, un isomorphisme $x \to x^{p^{-n}}$ de K sur une extension algèbrique $K^{p^{-n}}$ de K. Si K est parfait, tous les corps $K^{p^{-n}}$ sont identiques à K d'après la prop. 9. Dans le cas contraire, la réunion K_∞ des corps $K^{p^{-n}}$ pour toutes les valeurs de n, est encore une extension algèbrique de K ; il résulte de la prop. 9 que K_∞ est un corps parfait, et que toute extension algèbrique parfaite de K contient K_∞ ; K_∞ est donc la plus petite extension algèbrique parfaite de K. Les éléments de K_∞ sont appelés éléments radiciels par rapport à K ; ils sont caractérisés

par la propriété que, pour tout $x \in K_\infty$, il existe un entier $n \geqslant 0$ tel que $x^{p^n} \in K$. Le plus petit entier $r \geqslant 0$ ayant cette propriété n'est autre que l'exposant de x par rapport à K. En effet, si $x^{p^r} = a \in K$, mais $x^{p^{r-1}} \notin K$, le polynome $e^{p^r} - a$ est irréductible dans $K[e]$; car il est égal à $(e-x)^{p^r}$, et tout facteur irréductible de ce polynome devrait être de la forme $(e-x)^{p^s}$, avec $s < r$; mais un tel polynome, égal à $e^{p^s} - x^{p^s}$, n'appartient pas à $K[e]$, d'après l'hypothèse. Le degré de x par rapport à K est donc p^r ; comme son degré réduit est 1, la formule (1) montre bien que r est l'exposant de x par rapport à K.

Les extensions E de K telles que $K \subset E \subset K_\infty$ sont donc formées d'éléments radiciels par rapport à K ; on les appelle extensions radicielles de K.

Ces notions permettent de préciser la structure des extensions inséparables d'un corps imparfait K.

Proposition 10. Si E est une extension inséparable d'un corps K, l'ensemble des éléments $x \in E$ séparables par rapport à K forme une extension séparable E_0 de K, et E est une extension radicielle de E_0.

La première partie de la proposition résulte du cor.1 de la prop.7 ; quand à la seconde, elle résulte de la démonstration de la prop.4 : on y a vu que, si θ est un élément inséparable par rapport à K, et si r est l'exposant de θ par rapport à K, θ^{p^r} est séparable par rapport à K, donc si $\theta \in E$, $\theta^{p^r} \in E_0$.

L'extension E_0 est appelée l'extension séparable de K associée à E ; si r est l'exposant par rapport à K d'un élément $\theta \in E$, p^r n'est autre que le degré de θ par rapport à E_0. Tout isomorphisme de E_0 par rapport à K se prolonge d'une seule manière à E, car si x est un élément de E, r son exposant par rapport à K, f un isomorphisme

de E_0 par rapport à K (prolongé à Ω), on a $f(x)=(f(x^{p^r}))^{1/p^r}$.

En particulier, le <u>degré réduit</u> $\varphi_{E_0}(E)=1$, donc (prop.2), si E_0 est une extension <u>finie</u> de K, de degré n_0 le degré réduit $\varphi_K(E)$ est égal à n_0 (ce qui signifie l'appellation de "degré réduit"). Si en outre, E est une extension finie de E_0, son degré par rapport à E_0 est une puissance p^f de la caractéristique p (§ 3, cor.2 de la prop.3) si $n=[E:K]$, on a donc

$$n = n_0 p^f \tag{4}$$

L'entier $f \geqslant 0$ est encore appelé l'<u>exposant</u> de E par rapport à K ; il est clair que, pour tout élément θ de E, l'exposant de θ est $\leqslant f$ (il peut être $< f$ pour tout $\theta \in E$; voir exerc. 8).

<u>Norme et trace d'un élément</u>. Soit E une extension algèbrique de K, dont le degré réduit $\varphi_K(E)=\varphi$ soit <u>fini</u> ; soient s_i $(1 \leqslant i \leqslant \varphi)$ les isomorphismes distincts de E, relatifs à K. Si θ est un élément quelconque de E, on appelle <u>norme</u> et <u>trace</u> de θ <u>relatives à E et K</u>, et on note respectivement $N_{E|K}(\theta)$ et $Tr_{E|K}(\theta)$ (ou simplement $N_E(\theta)$, $Tr_E(\theta)$, et même $N(\theta)$ et $Tr(\theta)$ si aucune confusion ne peut en résulter), les éléments

$$N_{E|K}(\theta) = s_1(\theta)s_2(\theta)\dots s_\varphi(\theta) \tag{5}$$

$$Tr_{E|K}(\theta) = s_1(\theta)+\dots+s_\varphi(\theta) . \tag{6}$$

Il résulte immédiatement de ces définitions les identités

$$N_{E|K}(\alpha\beta) = N_{E|K}(\alpha)N_{E|K}(\beta) \tag{7}$$

$$Tr_{E|K}(\alpha+\beta) = Tr_{E|K}(\alpha)+Tr_{E|K}(\beta)$$

Si $\alpha \in K$, on a $N_{E|K}(\alpha) = \alpha^\varphi$, $Tr_{E|K}(\alpha) = \varphi.\alpha$. Quel que soit $\theta \neq 0$ dans E, $N_{E|K}(1/\theta)=1/N_{E|K}(\theta)$, $Tr_{E|K}(-\theta) = -Tr_{E|K}(\theta)$.

Soit φ le polynome irréductible de $K[\theta]$ dont θ est racine ; nous allons exprimer $N_{E|K}(\theta)$ et $Tr_{E|K}(\theta)$ en fonction des coefficients de φ

Soient $\theta=\theta_1,\theta_2,\ldots,\theta_n$ les conjugués distincts de θ, et $r \geqslant 0$ l'exposant de θ par rapport à K (en supposant la caractéristique p de K strictement positive ; si p=0, il faut remplacer, dans ce qui suit, p^r par 1). On a $\varphi = \prod_{i=1}^{n}(e-\theta_i)^{p^r} = \sum_{k=0}^{n} a_k e^{kp^r}$ où les a_k appartiennent à K. D'autre part, soit μ le degré réduit de E par rapport à $K\langle\theta\rangle$; d'après la prop.2, il y a exactement μ isomorphismes de E par rapport à K dont la valeur pour θ soit égale à un des θ_i ; donc, on a

$$N_{E|K}(\theta) = (\theta_1\theta_2\ldots\theta_n)^{\mu}$$
$$Tr_{E|K}(\theta) = \mu(\theta_1+\theta_2+\ldots+\theta_n)$$

d'où résultent les relations

$$(N_{E|K}(\theta))^{p^r} = (-1)^{n\mu p^r} a_0^{\mu}$$
$$(Tr_{E|K}(\theta))^{p^r} = -\mu . a_{n-1}$$

(on utilise ici l'identité $\mu^{p^r} = \mu$, valable pour tout entier μ dans un corps de caractéristique p, d'après la formule (3) du § 1).

On voit en particulier que, si θ est séparable par rapport à K, sa norme et sa trace sont des éléments de K.

En outre, le calcul précédent montre que, si F est une extension de E, dont le degré réduit $\vartheta_E(F) = \lambda$ soit fini, on a

$$N_{F|K}(\theta) = (N_{E|K}(\theta))^{\lambda} \tag{9}$$
$$Tr_{F|K}(\theta) = \lambda . Tr_{E|K}(\theta). \tag{10}$$

La définition de la norme s'étend à un polynome quelconque f de $E[e]$; si $f = \sum_{k=0}^{n} a_k e^k$, on appelle norme de f relative à E et K, et on désigne encore par $N_{E|K}(f)$, le polynome

$$N_{E|K}(f) = \prod_{i=1}^{\vartheta}\left(\sum_{k=0}^{n} s_i(a_k)e^k\right)$$

En particulier, si on considère le polynome $e-\theta$, et si on pose $N_{E|K}(e-\theta) = \sum_{k=0}^{\vartheta} b_k e^k$, on a $N_{E|K}(\theta) = (-1)^{\vartheta} b_0$, $Tr_{E|K}(\theta) = -b_{\vartheta-1}$; en outre, avec les mêmes notations que ci-dessus, on a

$$(N_{E|K}(e-\theta))^{p^r} = \varphi^{\mu}$$

On définit de même la norme d'un polynome d'un nombre quelconque de lettres.

Exercices. 1) Si K est un corps de caractéristique $p>0$, pour quels polynomes $f \in K[e]$ a-t-on $f''=0$? Pour quelles fractions rationnelles $g \in K(e)$ a-t-on $g'=0$? (mettre g sous forme irréductible).

2) Pour que le polynome e^2-a dans $K[e]$ (K corps quelconque) soit irréductible, il faut et il suffit que a ne soit pas le carré d'un élément de K . S'il existe un tel élément a , soit $\sqrt{a}$ une racine de e^2-a ; si K n'est pas de caractéristique 2 , les seuls éléments de $K\langle\sqrt{a}\rangle$ dont le carré appartienne à K sont les éléments de K et ceux de la forme $a\sqrt{a}$, avec $a \in K$; pour quels éléments $\beta \in K$ a-t-on $K\langle\sqrt{\beta}\rangle = K\langle\sqrt{a}\rangle$?

3) Soit K un corps de caractéristique $\neq 2$, a et β deux éléments de K qui ne sont pas carrés d'éléments de K , et tels que $K\langle\sqrt{a}\rangle \neq K\langle\sqrt{\beta}\rangle$; montrer que, si on pose $\theta = \sqrt{a} + \sqrt{\beta}$, on a $K\langle\sqrt{a}, \sqrt{\beta}\rangle = K\langle\theta\rangle$. Dans les mêmes hypothèses sur a et β , si on suppose que K est de caractéristique 2 , montrer que $K\langle\sqrt{a}, \sqrt{\beta}\rangle$ n'est pas une extension simple de K (calculer le degré de $K\langle\sqrt{a}, \sqrt{\beta}\rangle$ par rapport à K , et le degré de chacun des éléments de $K\langle\sqrt{a}, \sqrt{\beta}\rangle$ par rapport à K).

4) Soit K un corps parfait de caractéristique 2 . Toute extension du second degré de K est de la forme $K\langle a\rangle$, où a est racine d'un polynome irréductible de la forme e^2+e+a , où $a \in K$. Si a et β sont des racines respectives des polynomes irréductibles e^2+e+a et e^2+e+b , à quelle condition a-t-on $K\langle a\rangle = K\langle\beta\rangle$?

5) Soit K un corps de caractéristique $p>0$. Si on pose $E=K(e_1, e_2)$ $E\langle e_1^{1/p}, e_2^{1/p}\rangle$ est une extension finie non simple de E .

6) Si K est un corps imparfait de caractéristique $p>0$, et E une extension de K telle que $K \subset E \subset K^{1/p}$, mais que le degré $[E:K]$ soit $>p$, montrer que E n'est pas une extension simple de K, et qu'il existe une infinité de corps distincts F tels que $K \subset F \subset E$ (montrer qu'il existe deux éléments α, β de E tels que les corps $K\langle\alpha\rangle$, $K\langle\beta\rangle$ soient distincts, et distincts de E et K ; en conclure que, pour $\lambda \in K$, les corps $K\langle\alpha+\lambda\beta\rangle$ sont tous distincts).

7) Soit E une extension finie inséparable d'un corps imparfait K, E_0 l'extension séparable de K, associée à E. Si α est un élément quelconque de E, montrer que le corps $E_0\langle\alpha\rangle$ est une extension simple de K. (E_0 est une extension simple de K ; si $E_0 = K\langle\beta\rangle$, montrer que $\alpha+\beta\lambda$ a même exposant que α par rapport à K quel que soit $\lambda \in K$).

8) Pour qu'une extension finie inséparable E d'un corps imparfait K soit simple, il faut et il suffit que l'exposant de E par rapport à K soit égal au plus grand des exposants par rapport à K, des éléments de E (pour montrer que la condition est suffisante, utiliser l'exerc. 7).

9) Soit E une extension finie inséparable d'un corps imparfait K ; on désigne par E_0 l'extension séparable associée à E, par E_r le sous-corps de E formé des éléments d'exposant r par rapport à K ($0 \leqslant r \leqslant f$, où f est le plus grand des exposants des éléments de E). On a $E_{r-1} \subset E_r \subset E_{r-1}^{1/p}$ et $E_r \neq E_{r-1}$ pour $0 < r \leqslant f$. Montrer que

$$\left[E_{r-1}^{1/p} : E_{r-1}\right] = \left[K^{1/p} : K\right]$$

(remarquer que l'isomorphisme $x \to x^{1/p}$ de E_{r-1} sur $E_{r-1}^{1/p}$ applique K sur $K^{1/p}$). Si E est une extension simple de K, on a $[E_r : E_{r-1}] = p$ pour $0 < r \leqslant f$.

10) a) Soit K un corps imparfait de caractéristique p , E une extension radicielle finie de K . Montrer que si $[E:K\langle E^p\rangle] = p^r$, r est le plus petit nombre d'éléments de E dont l'adjonction à K donne E (remarquer que, si $E=K\langle E^p\rangle\langle a_1,a_2,\ldots,a_r\rangle$, on a $K\langle E^p\rangle = K\langle E^{p^2}\rangle\langle a_1^p,a_2^p,\ldots,a_r^p\rangle$, et procéder par récurrence pour montrer que $E=K\langle a_1,\ldots,a_r\rangle$).

b) Soit E une extension inséparable de K , E_o l'extension séparable associée ; si $[E:E_o\langle E^p\rangle] = p^r$, r est le plus petit nombre d'éléments de E dont l'adjonction à K donne E (utiliser a) et l'exerc.7).

c) Si $[K:K^p] = p^s$, montrer que toute extension inséparable finie E de K s'obtient par adjonction à K de s éléments au plus (utiliser b), en remarquant que $[E:E^p] = [K:K^p]$). Pour que <u>toute</u> extension finie de K soit simple, il faut et il suffit que s=1(pour la nécessité de cette condition, utiliser l'exerc.6).

d) Montrer qu'il existe une partie M de K telle que $K=K^p\langle M\rangle$ et que, pour toute partie N de M distincte de M , $K^p\langle N\rangle$ soit distinct de K (utiliser le th. de Zorn, en considérant l'ensemble des parties M' de K telles que, pour toute partie N' de M' distincte de M' , $K^p\langle N'\rangle$ soit distinct de $K^p\langle M'\rangle$). Pour tout entier n , on a $K=Kp^n\langle M\rangle$. Une partie M de K ayant les propriétés précédentes est dite une p-<u>base</u> de K .

e) Si M est une p-base de K , et H le plus grand sous-corps parfait de K (intersection des corps K^{p^n} , où n parcourt l'ensemble des entiers >0), montrer que M est un système algèbriquement libre par rapport à H (si $a_1,a_2,\ldots,a_r$ sont r éléments distincts de M , montrer que a_r est de degré p^n par rapport à $K^{p^n}\langle a_1,a_2,\ldots,a_{r-1}\rangle$).

10 bis) Soit P le corps premier de caractéristique $p > 2$, et $K=P(e_1,e_2)\langle u\rangle$, où u est racine de l'équation $u^2-(e_1+e_2)^p=0$. Montrer que P est le plus grand sous-corps parfait contenu dans K, et que e_1 et e_2 forment une p-base de K.

11) Si E est une extension d'un corps K telle qu'il n'existe qu'un nombre fini de corps distincts F tels que $K \subset F \subset E$, E est une extension algèbrique simple de K (E est une extension finie de K d'après l'exerc.3 du § 2 ; si E est inséparable, utiliser les exerc. 6 et 9 pour montrer que $\left[E_r:E_{r-1}\right]=p$, puis l'exerc. 8).

12) Soit K un corps imparfait, θ un élément séparable par rapport à K. Montrer que le degré de θ par rapport à $K^{1/p}$ est égal au degré de θ par rapport à K (si $E=K\langle\theta\rangle$, montrer que le degré réduit de $E^{1/p}$ par rapport à K est égal au degré de θ par rapport à K, puis que le degré réduit de $E^{1/p}$ par rapport à $K^{1/p}$ est encore égal au degré de θ par rapport à K, en utilisant la prop.2).

13) Soit E une extension finie d'un corps imparfait K, F une extension de K telle que $K \subset F \subset E$; soit h le plus petit des nombres r tels que $F \subset E_r$; on pose $F_r=F \cap E_r$.

a) Si $E_o=F_o\langle\gamma\rangle$, montrer que

$$\left[F\langle\gamma\rangle : K\right] = \left[E_o:F_o\right] \cdot \left[F:K\right]$$

(utiliser l'exerc. 12).

b) En déduire que, si E est une extension simple de K, on a $F\langle\gamma\rangle=E_h$ (comparer les degrés de $F\langle\gamma\rangle$ et de E_h par rapport à K, en utilisant l'exerc. 9) et que F est une extension simple de K.

14) Toute extension finie d'un corps imparfait est un corps imparfait.

15) Soit E une extension algèbrique d'un corps imparfait K , E_o l'extension séparable associée à E , R le corps formé des éléments radiciels par rapport à K , contenus dans E . Montrer que le corps formé des éléments de E séparables par rapport à R est le plus petit corps F contenant R et E_o (remarquer qu'un élément radiciel par rapport à E_o appartient à F ou est élément radiciel par rapport à F , et dans ce dernier cas, qu'il est inséparable par rapport à R).

16) Soit K un corps imparfait de caractéristique p , f un polynome irréductible inséparable de $K[e]$; si E est une extension radicielle de K , montrer que, dans $E[e]$, f reste irréductible, ou est égal à une puissance d'exposant p^k d'un polynome irréductible (si θ est une racine de f, remarquer que le degré réduit de θ par rapport à K est égal à son degré réduit par rapport à E).

17) Soit P un corps de caractéristique $p > 0$, et K l'extension transcendante pure $P(e_1,e_2,\ldots,e_n)$; soit f le polynome $f = e^{np}+e_1e^{(n-1)p}+\ldots+e_{n-1}e^p+e_n$ de $K[e]$; montrer que f est un polynome irréductible et inséparable dans $K[e]$ (établir d'abord que $e^n+e_1e^{n-1}+\ldots+e_n$ est irréductible dans $K[e]$, en utilisant le lemme de Gauss (chap.V, § 4) ; en déduire ensuite la proposition en remarquant que les e_i ne sont pas des puissances p-ièmes d'éléments de K). Soit θ une racine de f ; montrer qu'il n'existe, dans le corps $K\langle\theta\rangle$ aucun élément radiciel par rapport à K autre que ceux de K (s'il existait un élément β tel que $\beta \notin K$, $\beta^p \notin K$, montrer, à l'aide de l'exerc.16 , que f serait une puissance p-ième dans $K\langle\beta\rangle[e]$; en conclure que les e_i seraient des puissances p-ièmes d'éléments de K).

§ 6. Extensions galoisiennes.

Définition 1. On dit qu'une extension algèbrique E d'un corps K est une extension galoisienne (ou extension normale) de K , si tout isomorphisme de E relatif à K est un automorphisme de E relatif à K .

K est évidemment une extension galoisienne de lui-même ; on a remarqué aussi (§ 4, cor. du th.1) que l'extension algèbrique maximale Ω de K est une extension galoisienne de K .

Proposition 1. Pour qu'une extension E de K soit galoisienne, il suffit que tout isomorphisme de E relatif à K soit un endomorphisme de E .

En effet, soit f un isomorphisme de E relatif à K prolongé à l'extension algèbrique maximale Ω (§ 5, prop.1) ; f est un automorphisme de Ω , soit g l'automorphisme réciproque. On a par hypothèse $f(E) \subset E$; s'il existait un élément $x \in E$ n'appartenant pas à $f(E)$, $g(x)$ ne pourrait appartenir à E ; or la restriction de g à E est un isomorphisme de E , et par hypothèse $g(E) \subset E$. Donc $f(E)=E$, ce qui prouve que E est une extension galoisienne.

Corollaire. Pour qu'une extension E de K soit galoisienne, il faut et il suffit que tous les conjugués par rapport à K d'un élément quelconque de E appartiennent à E .

En effet, si f est un isomorphisme de E relatif à K , et x un élément quelconque de E , $f(x)$ est conjugué de x par rapport à K (§ 5,prop.5), donc $f(x) \in E$, c'est-à-dire $f(E) \subset E$.

De la proposition 1, on déduit que, si (E_ι) est une famille d'extensions galoisiennes de K , l'intersection E des corps E_ι est encore une extension galoisienne de K ; en effet, si f est un isomorphisme de E , prolongé en un automorphisme de Ω , on a $f(E) \subset f(E_\iota) \subset E_\iota$, quel que soit ι , donc $f(E) \subset E$, ce qui établit la proposition.

Parmi toutes les extensions galoisiennes de K qui contiennent une extension donnée E (non galoisienne) de K , il en existe donc une contenue dans toutes les autres.

De même, le plus petit corps F contenant les E_ι est galoisien ; en effet, $F=K\langle \bigcup_\iota E_\iota \rangle$, donc tout élément de F est égal à une fonction rationnelle d'éléments (en nombre fini) des E_ι , à coefficients dans K . Tout isomorphisme de F a pour restriction à E_ι un isomorphisme de E_ι , donc un automorphisme de E_ι ; il transforme donc tout élément de F en un élément de F .

Proposition 2. Si (f_ι) est une famille de polynomes de $K[e]$, le plus petit corps contenant toutes les racines des f_ι est une extension galoisienne de K .

En effet, tout élément de ce corps E étant une fonction rationnelle de racines (en nombre fini) des f_ι , à coefficients dans K , tout isomorphisme de E transforme un élément de E en un élément de E , d'où la proposition, d'après la prop. 1 .

Proposition 3. Si N est une extension galoisienne de K , et E une extension de K telle que $K \subset E \subset N$, tout isomorphisme de E relatif à K peut être prolongé en un automorphisme de N (relatif à K).

En effet, si f est un tel isomorphisme, on peut le prolonger en un automorphisme $\bar{f}$ de Ω , et la restriction de $\bar{f}$ à N est un isomorphisme de N , donc un automorphisme de N .

La théorie de Galois. Définition 2. On appelle groupe de Galois (ou simplement groupe) relatif à K , d'une extension galoisienne N d'un corps K , le groupe des automorphismes de N relatifs à K .

La théorie de Galois est l'étude de deux fonctions : l'une g qui, à tout sous-corps E de N tel que $K \subset E \subset N$ (quand nous parlerons de

sous-corps de N dans ce paragraphe, il ne s'agira jamais que de sous-corps de cette nature), fait correspondre un sous-groupe $g(E)$ du groupe Γ de N ; l'autre k qui, à tout sous-groupe Δ du groupe Γ , fait correspondre un sous-corps $k(\Delta)$ de N . Ces applications sont définies comme suit : $g(E)$ est l'ensemble des automorphismes de N qui laissent invariants tous les éléments de E (autrement dit, l'ensemble des automorphismes de N relatifs à E , ou encore le groupe de N , considéré comme extension galoisienne de E) ; $k(\Delta)$ est le sous-corps formé des éléments de N qui sont invariants par tous les automorphismes appartenant à Δ (il est immédiat que cet ensemble est un corps et qu'il contient K).

Nous étudierons d'abord les propriétés de ces applications relatives à la relation d'inclusion entre sous-groupes de Γ d'une part, sous-corps de N de l'autre :

Proposition 4. Soit (E_ι) une famille de sous-corps de N , E le plus petit sous-corps de N contenant $\bigcup_\iota E_\iota$; $g(E)$ est l'intersection des sous-groupes $g(E_\iota)$.

En effet, si un automorphisme de N laisse invariants tous les éléments de E , il laisse invariants a fortiori tous ceux des E_ι , donc appartient à chacun des $g(E_\iota)$; réciproquement, s'il appartient à $\bigcap_\iota g(E_\iota)$, il laisse invariant toute fonction rationnelle d'éléments de $\bigcup_\iota E_\iota$ à coefficients dans K , donc tout élément de E .

Proposition 5. Soit (Δ_ι) une famille de sous-groupes de Γ , le plus petit sous-groupe de Γ contenant $\bigcup_\iota \Delta_\iota$; $k(\Delta)$ est l'intersection des sous-corps $k(\Delta_\iota)$.

En effet, si un élément de N est invariant par tout automorphisme de Δ , il l'est en particulier par tout ceux des Δ_ι , donc appartient

à chacun des $k(\Delta_\iota)$; réciproquement, s'il appartient à $\bigcap_\iota k(\Delta_\iota)$, il est invariant par tout automorphisme de $\bigcup_\iota \Delta_\iota$, donc par tout composé d'un nombre fini de ces automorphismes, c'est-à-dire par tout automorphisme de Δ.

Comme cas particuliers de ces propositions, on voit que la relation $E \subset E'$ entraîne $g(E) \supset g(E')$, et que la relation $\Delta \subset \Delta'$ entraîne $k(\Delta) \supset k(\Delta')$ (on peut encore dire que g et k sont des fonctions décroissantes).

Remarque. Si F est l'intersection d'une famille (E_ι) de sous-corps de N, $g(F)$ contient tous les groupes $g(E_\iota)$, donc aussi le plus petit sous-groupe de Γ contenant $\bigcup_\iota g(E_\iota)$, mais il n'est pas nécessairement identique à ce sous-groupe ; on peut faire une remarque analogue pour $k(\Delta)$ lorsque Δ est l'intersection d'une famille de sous-groupes de Γ (voir exerc. 9).

Si E est un sous-corps de N, on désignera par E_0 l'extension séparable associée à E (§ 5) par $\tilde{E}$ le corps des éléments radiciels par rapport à E et contenus dans N (autrement dit, $\tilde{E}=E_\infty \cap N$; si N est une extension séparable de K, $E_0=\tilde{E}=E$ pour tout sous-corps de N).

Théorème 1. Quel que soit le sous-corps E de N, on a $k(g(E))=\tilde{E}$.

En effet, tout automorphisme de N qui laisse invariants tous les éléments de E laisse aussi invariants les éléments radiciels par rapport à E, contenus dans N. Inversement, supposons que $x \notin \tilde{E}$; le polynome irréductible φ de $E[e]$, qui a x pour racine, a alors au moins une racine $y \neq x$ $(y \in N)$; l'isomorphisme u de $E\langle x \rangle$, relatif à E, qui transforme x en y, se prolonge en un automorphisme de N qui laisse invariants tous les éléments de E, mais non x.

Corollaire 1. Si un élément de N est invariant par tous les automorphismes du groupe de N par rapport à K, c'est un élément radiciel par rapport à K.

En particulier, les coefficients de la norme par rapport à K d'un polynome de $N[e]$ (§ 5) sont des éléments radiciels par rapport à K .

Corollaire 2. Le corps N est une extension séparable du corps $\tilde{K}$ des éléments radiciels par rapport à K contenus dans N .

En effet, soient $\theta_1=\theta$, $\theta_2,\dots,\theta_m$ les conjugués distincts d'un élément $\theta \in N$. Les coefficients du polynome $\prod_{i=1}^{m}(e-\theta_i)=f$ sont invariants par tous les automorphismes du groupe Γ , donc (cor.1) appartiennent à $\tilde{K}$; comme f a toutes ses racines distinctes, et est le polynome irréductible de $\tilde{K}[e]$ dont θ est racine, θ est séparable par rapport à $\tilde{K}$.

Corollaire 3. Pour qu'on ait $k(g(E))=E$ quel que soit le sous-corps E de N , il faut et il suffit que N soit une extension séparable de K .

La condition est évidemment suffisante, puisqu'alors $\tilde{E}=E$ quel que soit le sous-corps E . Elle est aussi nécessaire, car si N est une extension inséparable de K , on a $N_0 \neq N$ et $\tilde{N}_0=N$, donc $k(g(N_0))=N \neq N_0$.

Théorème 2. Pour qu'on ait $g(k(\Delta))=\Delta$ quel que soit le sous-groupe Δ de Γ , il faut et il suffit que N_0 soit une extension finie de K .

a) La condition est suffisante. Posons $E=k(\Delta)$; N_0 , qui contient E_0 , en est une extension séparable finie ; donc le degré $[N_0:E_0]$ est aussi l'ordre du groupe de N_0 par rapport à E_0 , c'est-à-dire l'ordre du groupe $g(k(\Delta))$; nous allons montrer que, si n est l'ordre de Δ , on a $[N_0:E_0] \leqslant n$; comme Δ est évidemment un sous-groupe de $g(k(\Delta))$, et que ce dernier est fini, l'ordre de Δ ne peut être supérieur à celui de $g(k(\Delta))$ que si $g(k(\Delta))=\Delta$, ce qui établira la proposition.

Or, N_0 est une extension simple de E_0 , autrement dit, il existe $\theta \in N_0$ tel que $N_0=E_0\langle\theta\rangle$ (nous n'avons démontré cette proposition au § 5 (prop.8) que lorsque E_0 est infini ; elle sera établie au § 7

pour les corps finis, indépendamment de la théorie de Galois).

Soient $\sigma_1, \sigma_2, \ldots, \sigma_n$ les éléments distincts de Δ ; les coefficients du polynome $\varphi = \prod_{h=1}^{n} (e - \sigma_h(\theta))$ sont invariants par tout automorphisme de Δ, donc appartiennent à E_0 ; comme θ est racine de φ, son degré est $\leqslant n$, d'où la proposition.

b) La condition est <u>nécessaire</u>. Pour le voir, nous allons d'abord montrer que, si N_0 est une extension <u>infinie</u> de K, le groupe Γ <u>n'est pas dénombrable</u>. En effet, il existe alors une suite (a_n) d'éléments de N telle que, si on pose $K_n = K\langle a_1, a_2, \ldots, a_n \rangle$, on ait $a_{n+1} \notin K_n$; si q_n est le degré de a_n par rapport à K_{n-1}, on a donc $q_n > 1$ quel que soit n. Soient $u_{n,i}$ $(1 \leqslant i \leqslant q_n)$ les isomorphismes distincts de K_n relatifs à K_{n-1} (prolongés en des automorphismes de N). A toute suite $s=(k_n)$ d'entiers tels que $1 \leqslant k_n \leqslant q_n$, faisons correspondre la suite des isomorphismes $f_n = u_{1,k_1} \circ u_{2,k_2} \circ \ldots \circ u_{n,k_n}$; f_n est un isomorphisme de K_n relatif à K, et la restriction de f_{n+1} à K_{n+1} prolonge celle de f_n à K_n ; si E est la réunion des corps K_n, on définit donc un isomorphisme g_s de E, en posant $g_s(x) = f_n(x)$ si $x \in K_n$; cet isomorphisme se prolonge ensuite en un automorphisme de N, que nous désignerons encore par g_s. Cela posé, deux automorphismes g_s correspondant à des suites s distinctes sont distincts (§ 5, prop.2) ; donc la puissance de Γ est au moins égale à celle de l'ensemble des suites s, c'est-à-dire à celle de $\mathfrak{P}(N)$, ce qui prouve que Γ n'est pas dénombrable.

Cela étant, soit Δ un sous-groupe infini dénombrable de Γ (par exemple, le sous-groupe engendré par une partie dénombrable de Γ). Si on pose $E = k(\Delta)$, N_0 est une extension infinie de E_0, car son groupe $g(E) = g(k(\Delta))$ par rapport à E contient Δ, et ne peut donc être fini.

Ce qui précède montre alors que $g(E)$ est non dénombrable, donc $\Delta \neq g(k(\Delta))$.

Ce théorème correspond au corollaire 3 du th.1, et ne caractèrise pas les sous-groupes Δ tels que $g(k(\Delta))=\Delta$; on verra dans l'Appendice I comment on peut faire cette caractérisation par l'emploi d'un langage emprunté à la Topologie.

Les résultats précédents se résument dans le théorème suivant :

Théorème 3 (théorème fondamental des extensions galoisiennes). Pour que les applications g et k soient réciproques, il faut et il suffit que N soit une extension (galoisienne) séparable et finie de K ; g est alors une application biunivoque et décroissante (pour la relation $\subset$) de l'ensemble des sous-corps de N sur l'ensemble des sous-groupes de Γ ; et pour tout sous-corps E de N , l'ordre de $g(E)$ est égal au degré $[N:E]$, l'indice $(\Gamma : g(E))$ au degré $[E:K]$.

Le dernier point résulte de l'égalité du degré réduit et du degré d'une extension séparable et finie, ainsi que de la formule $[N:K] = [N:E] \cdot [E:K]$.

Corollaire 1. Si E est une extension séparable et finie de K , il n'y a qu'un nombre fini de corps distincts F tels que $K \subset F \subset E$.

En effet, d'après la prop.2 , la plus petite extension galoisienne N de K contenant E est une extension séparable et finie ; d'après le th.3 , il n'y a qu'un nombre fini de corps F tels que $K \subset F \subset N$, d'où a fortiori le corollaire.

Corollaire 2. Si N est une extension séparable et finie de K , E_1 et E_2 deux sous-corps de N , $g(E_1 \cap E_2)$ est le plus petit sous-groupe de Γ contenant $g(E_1)$ et $g(E_2)$; de même, si Δ_1 et Δ_2 sont deux sous-groupes de Γ , $k(\Delta_1 \cap \Delta_2)$ est le plus petit sous-corps de N contenant $k(\Delta_1)$ et $k(\Delta_2)$.

Cette conséquence immédiate du fait que g est biunivoque et décroissante, complète, dans le cas envisagé, les prop.4 et 5 .

Sous-corps conjugués. Sous-corps galoisiens. Soit N une extension galoisienne quelconque de K , E un sous-corps de N , σ un automorphisme du groupe Γ ; il est facile de déterminer la relation entre les groupes $g(E)$ et $g(\sigma(E))$; en effet, pour qu'un automorphisme τ laisse invariant tous les éléments de $\sigma(E)$, il faut et il suffit que $\sigma^{-1}\tau\sigma$ laisse invariant tous les éléments de E , donc

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

De la même manière, on voit que

$$(2) \qquad k(\sigma\Delta\sigma^{-1}) = \sigma(k(\Delta)) .$$

Pour que E soit une extension galoisienne de K , il faut et il suffit que $\sigma(E)=E$ quel que soit $\sigma \in \Gamma$. Les formules (1) et (2) et le th.1 montrent donc que :

Proposition 6 . Si E est un sous-corps galoisien de N , $g(E)$ est un sous-groupe distingué de Γ . Réciproquement, si $g(E)$ est un sous-groupe distingué de Γ , $\tilde{E}$ est une extension galoisienne de K .

On notera que lorsque $\tilde{E}$ est une extension galoisienne de K , il en est de même de l'extension séparable E_0 associée à E .

Proposition 7 . Si E est une extension galoisienne de K contenue dans N , le groupe de Galois de E relatif à K est isomorphe au groupe quotient $\Gamma / g(E)$.

En effet, tout automorphisme de E est alors la restriction σ_E à E d'un automorphisme σ de N ; donc $\sigma \to \sigma_E$ est une représentation du groupe de Galois de N sur celui de E ; en outre, pour que σ_E soit l'automorphisme identique, il faut et il suffit que $\sigma \in g(E)$ d'après la définition de $g(E)$.

2

Remarque. La proposition 6 montre que si E est une extension galoisienne de K , et F une extension galoisienne de E , F n'est pas nécessairement une extension galoisienne de K . En effet, soit N une extension galoisienne de K contenant F , Γ son groupe par rapport à K , Δ son groupe par rapport à E , Θ son groupe par rapport à F . La prop.6 montre que Δ est sous-groupe distingué de Γ , et Θ sous-groupe distingué de Δ , mais on sait qu'il n'en résulte pas nécessairement que Θ soit sous-groupe distingué de Γ (voir exerc. 2).

Extension du corps de base. Soit N une extension galoisienne de K , et S un corps contenant N (extension algèbrique ou transcendante de N). Soit K' une extension de K contenue dans S , et N' l'extension $K'\langle N\rangle$ de K' . N' est une extension algèbrique de K', puisque tous les éléments de N sont algèbriques par rapport à K , donc aussi par rapport à K' . En outre, comme tout isomorphisme de N' relatif à K' transforme un élément x de N en un élément conjugué de x par rapport à K' , donc a fortiori conjugué de x par rapport à K , N' est une extension galoisienne de K' . Il est évident en outre que tout automorphisme de N' relatif à N' est bien déterminé par sa restriction à N , qui est un automorphisme σ de N relatif à K laissant invariants les éléments de $K'\cap N$. Réciproquement, tout automorphisme σ de N laissant tous les éléments de $K'\cap N$ invariants, peut être prolongé en un automorphisme de N' relatif à K' . En effet, soit $\mathfrak{F}$ l'ensemble des applications φ ayant les propriétés suivantes : 1) φ est un isomorphisme relatif à K' d'un sous-corps H de N' ; 2) φ coïncide avec σ sur $H\cap N$. Il est immédiat que $\mathfrak{F}$, ordonné par la relation de prolongement, est industif, donc a un élément maximal φ_0 , isomorphisme relatif à K' d'un sous-corps H_0 .

H_o contient N ; sans quoi, il existerait un élément θ de N , n'appartenant pas à H_o , donc algèbrique par rapport à H_o ; on pourrait alors prolonger φ_o en un isomorphisme $\bar{\varphi}_o$ de $H_o\langle\theta\rangle$, en posant $\bar{\varphi}_o(\theta)=\sigma(\theta)$, donc $\bar{\varphi}_o$ appartiendrait encore à $\mathfrak{F}$, contrairement à l'hypothèse ; comme $N\subset H_o$, on a $H_o=N'$, ce qui établit la proposition, et par suite l'énoncé suivant :

Proposition 8. Le groupe de Galois de N' par rapport à K' est isomorphe au sous-groupe $g(K'\cap N)$ du groupe de Galois de N par rapport à K .

Groupe de Galois d'une équation algèbrique. Soit f un polynome (irréductible ou non) de $K[\theta]$, $a_1, a_2, \ldots, a_n$ ses racines distinctes dans l'extension algèbrique maximale de K . Le corps $N=K\langle a_1, a_2, \ldots, a_n\rangle$ est une extension galoisienne de K (prop.2) qu'on appelle le corps des racines du polynome f (ou de l'équation $f(x)=0$) ; son groupe Γ par rapport à K est appelé le groupe de Galois (ou simplement le groupe) de l'équation $f(x)=0$ (ou du polynome f). Tout automorphisme σ appartenant à Γ , restreint à l'ensemble $\{a_1, \ldots, a_n\}$ est une permutation de cet ensemble ; et réciproquement la donnée de $\sigma(a_i)$ pour tous les indices i détermine la valeur de σ pour tout élément de $K\langle a_1, a_2, \ldots, a_n\rangle$; donc Γ peut être identifié au groupe des permutations correspondantes des a_i , donc à un sous-groupe du groupe symétrique $\mathfrak{S}_n$.

On notera qu'en général, le corps $K\langle a_i\rangle$ obtenu par adjonction à K d'une racine de f , n'est pas identique au corps des racines de f. S'il l'est, on dit que $f(x)=0$ est une équation galoisienne (ou normale). L'équation $f(x)=0$ est appelée abélienne (resp. cyclique) si son groupe de Galois est abélien (resp. cyclique).

La détermination explicite du groupe de Galois d'une équation explicitée lorsque N est séparable peut se faire par la méthode suivante :

Considérons le corps $N'=N(e_1,e_2,\dots,e_n)$ des fractions rationnelles de n lettres sur N ; si K' est le corps $K(e_1,e_2,\dots,e_n)$, on a $N'=K'\langle a_1,a_2,\dots,a_n\rangle$, et d'après la prop.8 N' est une extension galoisienne séparable de K' , et son groupe par rapport à K' est isomorphe à Γ ; on l'identifiera à Γ . Si on considère l'élément

$$\theta = e_1a_1 + e_2a_2 + \dots + e_na_n$$

de N', ses conjugués par rapport à K' sont les éléments

$$\sigma(\theta)=e_1\sigma(a_1)+e_2\sigma(a_2)+\dots+e_n\sigma(a_n)$$

où σ parcourt le groupe Γ ; ces éléments sont tous distincts, donc le degré de θ est égal à l'ordre de Γ , c'est-à-dire à $[N':K']$, et il en résulte que $N'=K'\langle\theta\rangle$. Nous allons former le polynome irréductible φ de $K'[e]$ dont θ est racine, et en déduire le groupe Γ . Soit π^{-1} la permutation du groupe $\mathfrak{S}_n$ telle que $\sigma(a_i)=a_{\pi^{-1}(i)}$; on a $\sigma(\theta) = \sum_{i=1}^{n} e_i a_{\pi^{-1}(i)} = \sum_{i=1}^{n} e_{\pi(i)}a_i$; si, pour <u>toutes</u> les permutations π du groupe $\mathfrak{S}_n$, on pose $\pi(\theta) = \sum_{i=1}^{n} e_{\pi(i)}a_i$, on voit que φ est un facteur irréductible du polynome $g = \prod_{\pi\in\mathfrak{S}_n} (e-\pi(\theta))$ de $N[e_1,e_2,\dots,e_n,e]$. Or, les coefficients de ce polynome sont des <u>fonctions symétriques</u> des a_i , donc appartiennent à K ; autrement dit g est un polynome de $K[e_1,e_2,\dots,e_n,e]$, qu'on peut déterminer explicitement lorsque f est donné. Soit alors $g=g_1g_2\dots g_r$ la décomposition de g en facteurs irréductibles ; si $\varphi=g_1$ par exemple, et si, pour tout polynome de h de $K[e_1,\dots,e_n,e]$ on désigne par $\pi(h)$ ce que devient h lorsqu'on y remplace e_i par $e_{\pi(i)}$ $(1\leqslant i\leqslant n)$, on voit que les permutations π du groupe Γ sont les permutations telles que $\pi(g_1)=g_1$. D'ailleurs, d'après la formation de g , il existe r-1 permutations π_k $(2\leqslant k\leqslant r)$

telles que $g_k=\pi_k(g_1)$; car pour toute permutation π , $\pi(g_1)$ est un facteur irréductible de g , et on peut toujours choisir π de sorte que $\pi(g_1)$ ait un facteur commun $e-\pi(\theta)$ avec g_k , donc coïncide avec g_k ; le groupe des permutations π telles que $g_k=\pi(g_k)$ est donc identique à $\pi_k^{-1}\Gamma\pi_k$, et est par suite isomorphe à Γ . Ainsi, pour avoir le groupe Γ , il suffit de décomposer g en facteurs irréductibles, et de déterminer le sous-groupe de $\mathfrak{S}_n$ laissant invariant un de ces facteurs.

Fonctions symétriques des racines d'un polynome. Nous venons de nous appuyer, pour déterminer explicitement le groupe de Galois d'une équation, sur le théorème des fonctions symétriques (chap.IV, § 5, th.1) ; nous allons voir que ce théorème lui-même peut être établi comme conséquence du théorème fondamental des extensions galoisiennes (dans la démonstration duquel on observera que le théorème des fonctions symétriques n'a pas été utilisé.)

Soit en effet K un corps quelconque, $N=K(e_1,e_2,\ldots,e_n)$ le corps des fractions rationnelles de n lettres sur K . Considérons dans $N[e]$ le polynome $\varphi=\prod_{i=1}^{n}(e-e_i)=e^n+\sum_{k=1}^{n}(-1)^k s_k e^{n-k}$, où les s_k $(1\leqslant k\leqslant n)$ sont les n fonctions symétriques élémentaires des e_i . Si on pose $E=K\langle s_1,s_2,\ldots,s_n\rangle$, E est une extension de K contenue dans N , et φ appartient à $E[e]$. Comme $N=E\langle e_1,e_2,\ldots,e_n\rangle$, et que les e_i sont les n racines distinctes de φ , N est une extension séparable, finie et galoisienne (prop.2) de E . Soit alors f une fraction rationnelle symétrique de N ; tout automorphisme de N relatif à E permute les e_i , donc laisse invariant f ; donc(cor.1 ou th.1), f appartient à E , et est par suite égale à une fonction rationnelle des s_i , à coefficients dans K .

On peut en outre prouver aussi de cette manière l'unicité de l'expression d'une fonction symétrique à l'aide des s_i (chap.IV, § 5, prop.3) ; tout revient à prouver que les s_i forment un système algèbriquement libre par rapport à K . Or, s'il n'en était pas ainsi, le degré de transcendance de E par rapport à K serait $< n$; comme N est une extension algèbrique de E , le degré de transcendance de N par rapport à K serait aussi $< n$, ce qui est absurde, les e_i formant un système algèbriquement libre de n éléments par rapport à K .

Remarques. Il est immédiat que toute permutation des e_i définit un automorphisme de N qui laisse invariant E ; donc le groupe de Galois de N par rapport à E est le groupe symétrique $\mathfrak{S}_n$. En outre, comme il existe une permutation de ce groupe transformant e_1 en l'un quelconque des e_i , les e_i sont tous conjugués par rapport à E, ce qui prouve que φ est irréductible dans E .

Enfin, comme les s_k forment un système algèbriquement libre, E est une extension transcendante pure de K , isomorphe à N .

Exercices. 1) Toute extension de degré 2 d'un corps K , et toute extension de K engendrée par une famille d'éléments de degré 2 par rapport à K , est galoisienne.

2) Le polynome $e^2 - \sqrt{2}$ est irréductible dans $K = Q(\sqrt{2})$ ($\sqrt{2}$ étant une racine de l'équation $x^2-2=0$) ; si E est l'extension de K obtenue par adjonction d'une racine de ce polynome, montrer que E n'est pas une extension galoisienne de Q (établir que $i = \sqrt{-1}$ n'appartient pas à E , soit directement, soit à l'aide des propriétés du corps des nombres réels). Quel est la plus petite extension galoisienne de Q qui contient E ? Déterminer la structure de son groupe par rapport à Q , ainsi que celle des groupes g(E) et g(K).

3) Soit Ω l'extension algèbrique maximale d'un corps K , x un élément de Ω n'appartenant pas à K , E une extension maximale de K ne contenant pas x (exerc. du § 4) ; montrer que $E\langle x\rangle$ est une extension galoisienne de E dont le groupe est cyclique et d'ordre premier r . Montrer que toute extension galoisienne séparable et finie de E est de degré r^m (utiliser le th. de Sylon (chap.V, § 4, exerc. 24)).

4) Soient E_1, E_2 deux extensions galoisiennes d'un corps K , E_0 leur intersection, E le plus petit corps contenant E_1 et E_2 ("composé" de E_1 et E_2) . On désigne par Γ_1 , Γ_2 , Γ les groupes de E_1, E_2 et E respectivement, relatifs à K , par Δ_1 , Δ_2 les sous-groupes de Γ_1 , Γ_2 correspondant au sous-corps de E_0 de E_1 et E_2 respectivement. A toute classe (mod. Δ_1) de Γ_1 , soit $\overline{\sigma}_1$, correspond la classe (mod. Δ_2) de Γ_2 , soit $\overline{\sigma}_2$, formée des automorphismes de Γ_2 dont la restriction à E_0 est identique à la restriction de tout automorphisme de $\overline{\sigma}_1$; 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 Θ du produit $\Gamma_1 \times \Gamma_2$, formé des couples (σ_1, σ_2) tels que, si $\overline{\sigma}_1$ et $\overline{\sigma}_2$ sont les classes de σ_1 et σ_2 respectivement dans Γ_1/Δ_1 et Γ_2/Δ_2 , on ait $\overline{\sigma}_2 = \varphi(\overline{\sigma}_1)$ (raisonner comme dans la prop.8).

5) Soit N une extension galoisienne séparable et finie d'un corps K. On dit que N est le "composé direct" de n sous-corps galoisiens $E_1, E_2, \ldots, E_n$ si N est le composé des E_i , et si l'intersection de chacun des E_i avec le corps composé des E_j pour $j \neq i$, se réduit à K Montrer que, pour que N soit composé direct des E_i , il faut et il suffit que le groupe Γ de N par rapport à K soit le produit direct de ses sous-groupes $g(E_1)$.

6) Pour que le groupe de Galois du corps des racines d'un polynome séparable $f \in K[e]$ soit transitif (considéré comme groupe de permutations des racines de f), il faut et il suffit que f soit irréductible dans $K[e]$.

7) Soit $f \in K[e]$ un polynome irréductible et séparable de degré n, dont le groupe de Galois soit <u>abélien</u> ; montrer que ce groupe est d'ordre n, et que, si θ est une racine quelconque de f, le corps des racines de f est identique à $K\langle\theta\rangle$ (si un automorphisme du groupe de Galois laisse invariant θ, montrer qu'il laisse invariant toutes les racines de f, en utilisant le fait que le groupe est abélien et transitif).

8) Soient f et g deux polynomes irréductibles et séparables de $K[e]$, m le degré de f, n le degré de g, α une racine de f, β une racine de g. Soit $f=f_1 f_2 \cdots f_r$ la décomposition en facteurs irréductibles de f dans $K\langle\beta\rangle$, $g=g_1 g_2 \cdots g_s$ celle de g dans $K\langle\alpha\rangle$. Montrer que $r=s$, et qu'on peut permuter les g_i de sorte que, si m_i est le degré de f_i, n_i celui de g_i, on ait $m/n = m_i/n_i$. (Soit N le corps des racines du polynome fg, Γ son groupe de Galois, Δ le sous-groupe de Γ correspondant au sous-corps $K\langle\beta\rangle$. Soit α_i une des racines de f_i, h_i le polynome de $K\langle\alpha_i\rangle[e]$ dont β est racine. A l'aide de l'exerc.4, montrer qu'il existe un automorphisme σ_i de Γ tel que $\sigma_i(\alpha_i)=\alpha$, et en déduire que, pour $i \neq j$, les polynomes $\sigma_i(h_i)$ et $\sigma_j(h_j)$ sont des facteurs distincts de g dans $K\langle\alpha\rangle$. Etablir ensuite la relation $m_i/n_i=m/n$ en évaluant de deux manières différentes le degré du corps $K\langle\alpha_i,\beta\rangle$ par rapport à K).

9) Soit $N=K(e_1,e_2)$, $E=K\langle e_1+e_2, e_1 e_2\rangle$, où K est un corps de caractéristique $p>0$; on a vu que N est une extension galoisienne de E.

Soit F le corps $N\langle e_1^{1/p}, e_2^{1/p}, (e_1+e_2)^{1/p^2}\rangle$; F est une extension galoisienne de E ; soient F_1, F_2 les sous-corps $N\langle e_1^{1/p}\rangle$, $N\langle e_2^{1/p}\rangle$ de F ; montrer que l'intersection des sous-groupes $g(F_1)$, $g(F_2)$ du groupe de Galois Γ de F par rapport à E , se réduit à l'élément neutre de Γ , mais que le plus petit sous-corps contenant F_1 et F_2 est distinct de F .

10) Pour une extension algèbrique quelconque E d'un corps K , on désigne par Γ le groupe des automorphismes de E relatifs à K ; pour tout sous-corps F de E (contenant K), g(F) est le sous-groupe de Γ formé des automorphismes de E laissant invariants tous les éléments de F ; pour tout sous-groupe Δ de Γ , $k(\Delta)$ est le sous-corps de E formé des éléments invariants par tous les automorphismes de Δ .

Montrer que le sous-corps $S = k(g(K)) = k(\Gamma)$ est le plus petit sous-corps F de E tel que E soit une extension galoisienne et séparable de F (utiliser le th.1 pour montrer que tout corps F ayant cette propriété contient S ; pour montrer que E est une extension galoisienne et séparable de S , prouver que, si a est un élément quelconque de E , $a_1=a, a_2, \ldots, a_r$ ses transformés distincts par les automorphismes de Γ , le polynome $\prod_{i=1}^{r}(e-a_i)$ appartient à $S[e]$).

11) Avec les notations de l'exercice 10, montrer que, pour que E soit une extension galoisienne de K , il faut et il suffit que S soit une extension radicielle de K (pour voir que la condition est suffisante, remarquer que, si elle est remplie, pour tout polynome φ de $S[e]$, il existe une puissance de φ qui soit un polynome de $K[e]$).
S est alors le corps formé de tous les éléments radiciels par rapport à K contenus dans E .

12) Avec les notations de l'exerc.10, soit S_0 l'extension séparable de K associée à S . Montrer que S_0 est le plus petit sous-corps F de E

tel que E soit une extension galoisienne de F (utiliser le th.1 pour montrer que, si F' possède cette propriété, S est une extension radicielle de F , et par suite que $S_0 \subset F$; utiliser l'exerc.11 pour montrer que E est une extension galoisienne de S_0).

13) Avec les notations de l'exerc.10, montrer que, pour que $g(k(\Delta))=\Delta$ pour tout sous-groupe Δ de Γ , il faut et il suffit que le groupe Γ soit fini (remarquer que Γ est le groupe de Galois de E par rapport à S , et appliquer le th. 2).

14) Soit E une extension algèbrique de K , E_0 l'extension séparable associée, R le sous-corps de E formé des éléments radiciels par rappor à K , contenus dans E . Si N est la plus petite extension galoisienne de K contenant E , N_0 l'extension séparable associée à N , montrer que N_0 est la plus petite extension galoisienne de K contenant E_0 .
Si E est une extension séparable de R , N est identique au plus petit corps contenant R et N_0 (cf. § 5, exerc.15) ; en déduire que tout élément radiciel par rapport à K , contenu dans N , est alors contenu dans R (remarquer que N est une extension séparable de R).

15) Avec les notations de l'exerc.10, montrer que E est le plus petit corps contenant S et l'extension séparable E_0 associée à E .

16) Soit A un anneau arithmétique, K son corps des quotients, $\mathfrak{P}$ un idéal premier de A , A' l'anneau quotient $A/\mathfrak{P}$, K' le corps des quotients de A'. Soit f un polynome de A [e] , g le polynome de A'[e] qui lui correspond par l'homomorphisme canonique de A sur A' . Si on suppose que f et g n'ont que des racines simples, montrer que le groupe de Galois du polynome g est isomorphe à un sous-groupe du groupe de Galois de f (utiliser la méthode de détermination du groupe de Galois d'un polynome, donnée dans le texte).

§ 7. Racines de l'unité. Corps finis.

Racines de l'unité. Soit K un corps commutatif quelconque, dont nous désignerons par 1 l'élément unité. On appelle racines n-ièmes de l'unité de K les racines du polynome e^n-1 ; ces racines sont algèbriques par rapport au corps premier P contenu dans K . Si K est de caractéristique $p>0$, on peut se borner à considérer le cas où n n'est pas divisible par p ; en effet, supposons que $n=p^k m$, où m n'est pas divisible par p ; on a alors $e^n-1=(e^m)^{p^k}-1=(e^m-1)^{p^k}$, donc les racines n-ièmes de l'unité sont alors identiques aux racines m-ièmes de l'unité. Nous supposons donc dans ce qui suit que $n \not\equiv 0$ (p). Il est clair que si $n \equiv 0$ (mod. m) toute racine m-ième de l'unité est aussi racine n-ième de l'unité.

La dérivée de e^n-1 étant ne^{n-1} , ne s'annule que pour $x=0$, qui n'est pas racine de e^n-1 ; donc e^n-1 n'a que des racines simples ; il y a exactement n racines n-ièmes distinctes de l'unité ; bien entendu 1 est une de ces racines ; les n-1 autres sont racines du polynome

$$(e^n-1)/(e-1) = e^{n-1}+e^{n-2}+\ldots+e+1 .$$

On désignera par $R_n(K)$ le corps des racines du polynome e^n-1 , autrement dit, le corps obtenu par adjonction à K de toutes les racines n-ièmes de l'unité ; on l'appelle le corps des racines n-ièmes de l'unité de K . Comme tout corps de racines, c'est une extension galoisienne finie de K ; elle est en outre séparable.

Les racines n-ièmes de l'unité forment évidemment un groupe multiplicatif G_n ; nous allons voir que :

Proposition 1. Le groupe multiplicatif G_n des racines n-ièmes de l'unité d'un corps K , est un groupe cyclique d'ordre n .

Démontrons-le par récurrence sur le nombre des facteurs premiers distincts de n .

1° $n=q^k$, où q est premier. Toute racine q^{k-1}-ième de l'unité est aussi racine q^k-ième ; comme il n'y a que q^{k-1} racines q^{k-1}-ièmes, il existe une racine n-ième ζ telle que $\zeta^{q^{k-1}} \neq 1$; comme l'ordre de ζ dans G_n est un diviseur de q^k et ne peut diviser q^{k-1} , il est égal à $q^k=n$, ce qui prouve que ζ engendre G_n .

2° supposons $n=rs$, où r et s sont premiers entre eux et >1 ; la proposition étant supposée vraie pour r et s , soit ξ une racine r-ième, η une racine s-ième, engendrant respectivement les groupes G_r et G_s . Le produit $\xi^h \eta^k$ est une racine n-ième de l'unité, et on ne peut avoir $\xi^h \eta^k=1$ que si $h \equiv 0\ (r)$ et $k \equiv 0\ (s)$: en effet, on en tire $\eta^{kr}=1$, donc $kr \equiv 0$ (mod.s), et comme r est premier avec s , $k \equiv 0$ (mod.s) ; on voit de même que $h \equiv 0$ (mod.r) . Il en résulte immédiatement, d'une part que G_n est le produit direct de G_r et G_s ; d'autre part, $\zeta = \xi\eta$ est un élément d'ordre n dans G_n , car on ne peut avoir $\zeta^m=1$ que si $m \equiv 0$ (mod.r) et $m \equiv 0$ (mod.s) , donc, comme r et s sont premiers entre eux, $m \equiv 0$ (mod. rs).

Les racines de l'unité qui engendrent le groupe G_n sont appelées racines primitives de l'unité ; si ζ est l'une d'elles, il est facile d'avoir toutes les autres ; en effet, toutes les racines de l'unité sont de la forme ζ^a , où $0 \leqslant a \leqslant n-1$; et la condition $(\zeta^a)^m=1$ est équivalente à $am \equiv 0$ (mod.n) ; pour que cette congruence soit équivalente à $m \equiv 0$ (mod.n) , il faut et il suffit que a soit premier avec n (chap.V, § 5, prop.8) ; le nombre $\varphi(n)$ des racines primitives distinctes est donc égal au nombre des entiers a premiers avec n et $< n$.

Si $n=rs$, où r et s sont premiers entre eux, il résulte de la démonstration de la prop.1, que toute racine n-ième primitive ζ peut s'écrire $\zeta = \xi\eta$, où ξ et η sont des racines r-ièmes et s-ièmes respectivement ; en outre, ξ et η sont des racines

primitives, sans quoi ζ serait d'ordre $< n$ dans G_n ; comme inversement, la démonstration de la prop.1 montre que $\zeta\eta$ est racine primitive si ζ et η le sont, on voit qu'on a $\varphi(n)=\varphi(rs)=\varphi(r)\varphi(s)$. La détermination de $\varphi(n)$ se ramène donc au cas où $n=q^k$, q premier ; mais la démonstration de la prop. prouve qu'il existe alors q^k-q^{k-1} racines primitives, donc $\varphi(q^k)=q^k-q^{k-1}=q^k(1-1/q)$.

Si $n=q_1^{n_1}q_2^{n_2}..q_h^{n_h}$ est la décomposition de n en facteurs premiers (les q_i étant distincts), on a par suite :

$$\varphi(n)=n(1-1/q_1)(1-1/q_2)...(1-1/q_h) .$$

La fonction $\varphi(n)$ est appelée indicateur d'Euler.

Si ζ est une racine n-ième primitive de l'unité, le corps $R_n(K)$ est donc identique à $K<\zeta>$. Soit Γ son groupe de Galois par rapport à K ; toute substitution de Γ transforme ζ en une racine primitive, donc de la forme ζ^a , où a est premier avec n , et est entièrement déterminée par la donnée de a (mod.n) ; nous la désignerons par σ_a . On a en outre $\sigma_a(\sigma_b(\zeta)) = \sigma_a(\zeta^b)= (\sigma_a(\zeta))^b = \zeta^{ab}$, autrement dit $\sigma_a\sigma_b=\sigma_{ab}$; donc :

Proposition 2. Le groupe de Galois du corps $R_n(K)$ des racines n-ièmes de l'unité, est isomorphe à un sous-groupe du groupe multiplicatif des $\varphi(n)$ classes (mod.n) premières avec n ; il est donc abélien.

Corollaire. Le degré du corps $R_n(K)$ par rapport à K est un diviseur de $\varphi(n)$.

La détermination du groupe de Galois Γ dépend essentiellement du corps K ; à l'aide de la prop.8 du §6 , on peut se limiter au cas où K est un corps premier ; la détermination de Γ dépend alors de la caractéristique de K (voir exerc. 3 et 7).

Posons $h=\varphi(n)$, et soient $\zeta_1, \zeta_2, \ldots, \zeta_h$ les racines n-ièmes primitives de l'unité ; si k est l'ordre du groupe Γ, le polynome $\Phi_n = \prod_{i=1}^{k}(e-\zeta_i)$ est égal à un produit de h/k polynomes irréductibles de degré k, appartenant à $K[e]$; donc Φ_n appartient lui-même à $K[e]$. Il est facile de le déterminer ; en effet, une racine n-ième quelconque de l'unité est racine d-ième primitive de l'unité pour un diviseur d de n bien déterminé : si ζ est une racine primitive n-ième, une racine n-ième ζ^a est racine primitive d'ordre n/b, où b est le p.g.c.d. de n et a. On a donc, quel que soit n, l'identité

$$(1) \qquad e^n-1 = \prod_{d|n} \Phi_d$$

qui permet de déterminer Φ_n par récurrence ; par exemple, si q est premier, on déduit de (1), appliquée pour $n=q^k$ et $n=q^{k-1}$, que

$$\Phi_{q^k} = 1+e^{q^{k-1}} + e^{2q^{k-1}} + \ldots + e^{(q-1)q^{k-1}}$$

(voir exerc. 2).

Corps finis. Comme nous le verrons au chap.VII, un corps fini K est nécessairement commutatif ; comme il est nécessairement de caractéristique $p>0$, c'est une extension finie de son corps premier $P = \mathbb{Z}/(p)$. Soit n le degré de K par rapport à P ; si $a_1, a_2, \ldots, a_n$ est une base vectorielle de K par rapport à P, tout élément de K se met d'une seule manière sous la forme $\sum_{i=1}^{n} \xi_i a_i$, où les $\xi_i \in P$, et réciproquement, toute expression de cette forme appartient à K ; il en résulte aussitôt que K est un ensemble à $q=p^n$ éléments.

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

(2) $$e^q - e = \prod_{i=1}^{q} (e - \zeta_i)$$

On voit donc que K est nécessairement identique au corps des racines du polynome $e^q - e$ de $P[e]$. Inversement, pour toute puissance $q = p^n$ de p, les racines de $e^q - e$ forment un corps, extension finie de P , en vertu de la formule (5) du §1 ; comme P est un corps parfait (comme tout corps fini), cette extension est séparable, donc a q éléments distincts. Ainsi :

Proposition 5. Un corps commutatif fini a nécessairement un nombre d'éléments q égal à une puissance p^n d'un nombre premier p . L'extension F_{p^n} du corps premier $F_p = Z/(p)$, obtenue par adjonction à F_p des racines du polynome $e^{p^n} - e$, est un corps à $q = p^n$ éléments, identique à l'ensemble de ces racines et de degré n par rapport à F_p ; et tout corps fini à q éléments est isomorphe à F_{p^n} .

Si $K = F_q$ $(q = p^n)$, le groupe multiplicatif K^* des éléments $\neq 0$ de K est identique au groupe des racines (q-1)-ièmes de l'unité de F_p ; comme q-1 est premier avec p , la prop. 1 montre que :

Proposition 4. Le groupe multiplicatif des éléments $\neq 0$ d'un corps fini est un groupe cyclique.

Corollaire. Le corps fini F_q est une extension simple de son corps premier F_p .

Il est obtenu en effet par adjonction d'une racine primitive (q-1)-ième de l'unité.

Tout automorphisme de F_q laisse invariant le corps premier F_p ; le groupe Γ de ces automorphisme est donc le groupe de Galois de F_q par rapport à F_p . Or, il est facile de déterminer ces automorphismes : comme pour tout corps parfait de caractéristique p , chacun des isomorphismes $x \to x^{p^k}$ est un automorphisme de F_q ; d'autre part, si ζ est une racine (q-1)-ième primitive de l'unité, les n éléments

$\zeta, \zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{n-1}}$ sont tous distincts, donc, si σ_k désigne l'automorphisme $x \to x^{p^k}$, les n automorphismes σ_k correspondant à $0 \leqslant k \leqslant n-1$ sont distincts. Comme Γ est d'ordre n, il est identique à l'ensemble des σ_k ; en outre, on a $\sigma_h(\sigma_k(x)) = \sigma_h(x^{p^k}) = (\sigma_h(x))^{p^k} = x^{p^{h+k}} = \sigma_{h+k}(x)$, donc $\sigma_h \sigma_k = \sigma_{h+k}$; par suite :

Proposition 5. Le groupe Γ des automorphismes de F_q, qui est aussi le groupe de Galois de F_q par rapport à F_p, est un groupe cyclique d'ordre n.

Exercices. 1) Si d est le p.g.c.d. de m et n, montrer que le p.g.c.d. des polynomes $e^n - 1$ et $e^m - 1$ est $e^d - 1$.

2) Démontrer que l'on a

$$\Phi_n = \prod_{d|n} (e^d - 1)^{\mu(n/d)}$$

où $\mu(n)$ est la fonction de Möbius (chap. V, § 5, exerc. 8) dans l'anneau $\mathbb{Z}$. (Etablir que cette expression satisfait à l'identité (1) en utilisant l'exerc. 12 du § 3 du chap. V).

3) a) Si ζ est une racine n-ième de l'unité du corps $F_p = \mathbb{Z}/(p)$, avec $n \not\equiv 0 \ (p)$, ζ et ζ^p sont racines du même polynome irréductible de $F_p[e]$ (remarquer que $x \to x^p$ est un automorphisme de toute extension algèbrique de F_p).

b) Si ζ est une racine n-ième primitive de l'unité du corps Q, et p un nombre premier ne divisant pas n, montrer que ζ et ζ^p sont racines du même polynome irréductible de $Q[e]$ (raisonner par l'absurde, en montrant, à l'aide de a), que dans le cas contraire, $e^n - 1$ serait divisible par le carré d'un polynome irréductible de $F_p[e]$).

c) En déduire que, dans $Q[e]$, le polynome Φ_n est irréductible (montrer que, si ζ est une racine n-ième primitive de l'unité

du corps Q, ζ et ζ^a sont racines du même polynome irréductible de $Q[e]$, quel que soit a premier avec n, en raisonnant par récurrence sur le nombre de facteurs premiers (distincts ou non) de a).

4) Le groupe de Galois Γ_n du corps $R_n(Q)$ par rapport à Q est isomorphe au groupe multiplicatif des $\varphi(n)$ classes (mod.n) premières avec n (exerc.3). Montrer que si $n=n_1 n_2,..,n_p$, où les n_i sont premiers entre eux deux à deux, Γ_n est isomorphe au produit des Γ_{n_i} (chap.V, §5, prop.9). En déduire que le corps $R_n(Q)$ est le "composé direct" de ses sous-corps $R_{n_i}(Q)$ (§6, exerc.5).

5) Montrer que, si p est un nombre premier $\neq 2$, le groupe Γ_{p^k} ($k>0$) est cyclique, et que le groupe Γ_{2^k} est cyclique pour $k=1$ et $k=2$, et le produit d'un groupe cyclique d'ordre 2 et d'un groupe cyclique d'ordre 2^{k-2} si $k \geqslant 3$ (considérer l'ordre de la classe de $1+p$ dans le groupe multiplicatif des classes (mod.p^k) premières avec p, d'une part ; d'autre part, en utilisant la prop.4 appliquée à $Z/(p)$, montrer qu'il existe dans ce groupe un élément d'ordre $p-1$; conclure à l'aide de l'expression de $\varphi(p^k)$, dans le cas où $p\neq 2$; dans le cas où $p=2$ et $k \geqslant 3$, considérer aussi le sous-groupe d'ordre 2 engendré par la classe de -1). En déduire que Γ_n n'est cyclique que si n est égal à 2,4, p^k ou $2p^k$ (p nombre premier impair).

6) Quels sont les sous-corps de F_q ($q=p^n$, p premier) ? Montrer que le polynome e^q-e est le produit des polynomes irréductibles de $F_p[e]$, dont le degré est un diviseur de n, et le terme de plus haut degré a pour coefficient 1. En déduire le nombre de ces polynomes ayant un degré donné (utiliser la formule d'inversion de Möbius (chap.V, §3, exerc. 12)).

7) Montrer que le degré du corps $R_n(\mathbf{F}_p)$ des racines n-ièmes de l'unité, par rapport à $\mathbf{F}_p$ ($n \not\equiv 0(p)$), est égal au plus petit nombre m tel que p^m-1 soit multiple de n .

8) Déduire de l'exerc.7 que le polynome $\Phi_{12}=e^4-e^2+1$, est réductible dans tous les anneaux $\mathbf{F}_p[e]$ correspondant aux nombres premiers p non diviseurs de 12.

9) Soient x et y deux éléments algèbriques par rapport à $\mathbf{F}_p$, de degrés respectifs m et n ; si m et n sont premiers entre eux, le degré de $x+y$ par rapport à $\mathbf{F}_p$ est mn .

10) Soient s_i ($1 \leqslant i \leqslant p$) les fonctions symétriques élémentaires des nombres 1,2,...,p-1 (p premier) ; démontrer les congruences $s_i \equiv 0$ ($1 \leqslant i \leqslant p-1$) , $(p-1)! \equiv -1$ (mod.p) (appliquer l'identité (2) au corps $\mathbf{F}_p = \mathbf{Z}/(p)$).

11) Soit p un nombre premier impair, $n \not\equiv 0$ (mod.p), et a un entier tel que $\Phi_n(a) \equiv 0$ (mod.p) ; n divise p-1 (exerc. 7), et est le plus petit entier tel que $a^n-1 \equiv 0$ (mod.p) (dans le cas contraire, montrer en utilisant la formule (1), que e^n-1 aurait une racine multiple dans $\mathbf{F}_p$).

12) Soit K un corps contenant les n racines n-ièmes de son unité et dont la caractéristique ne divise pas n . Montrer que le corps des racines W du polynome e^n-a est cyclique par rapport à K , et engendré par une quelconque des racines θ de ce polynome (si σ est un automorphisme du groupe de Galois de W , on a $\sigma(\theta)= \zeta_\sigma \theta$, où ζ_σ est une racine n-ième de l'unité, et l'application $\sigma \to \zeta_\sigma$ est une représentation du groupe de Galois de W dans le groupe multiplicatif des racines n-ièmes de l'unité). Soit $G_n(K)$ le groupe multiplicatif des puissances n-ièmes des éléments $\neq 0$ de K ; si H(a) est le sous-groupe

du groupe multiplicatif K^*, engendré par la réunion de $G_n(K)$ et $\{a\}$, montrer que le degré d de W par rapport à K est égal à l'indice $(H(a):G_n(K))$, ou encore au plus petit des entiers r tels que a^r soit une puissance n-ième d'un élément de K ; montrer que d divise n (remarquer que si σ est un automorphisme engendrant le groupe de Galois de W, d est l'ordre de la racine ζ_σ).

Comment se modifient ces résultats lorsqu'on suppose que la caractéristique de K divise n, les racines n-ièmes de l'unité appartenant encore à K ?

13) On fait sur K les mêmes hypothèses que dans l'exerc. 12. Si W est le corps des racines de e^n-a, tout élément b de W tel que $b^n \in K$, est de la forme $b=c\theta^r$, avec $c \in K$ (montrer qu'on a $\sigma(b)=\omega b$, ω étant une racine n-ième de l'unité, puisque ω est de la forme ζ_σ^r).

14) Soit K un corps satisfaisant aux conditions de l'exerc.12, G un groupe multiplicatif d'éléments $\neq 0$ de K, contenant $G_n(K)$, W le corps obtenu par adjonction à K des racines de toutes les équations $x^n-a=0$, où a parcourt G. Montrer que $[W:K]=(G:G_n(K))$ (décomposer le groupe abélien $G/G_n(K)$ en un produit direct de groupes cycliques, puis raisonner par récurrence sur le nombre des groupes facteurs, en utilisant l'exerc. 13).

15) Soit K un corps satisfaisant aux conditions de l'exerc.12, K_0 un sous-corps de K tel que K soit une extension galoisienne de K_0. Soit a un élément de K tel que le corps des racines W de e^n-a soit de degré n par rapport à K. Pour que W soit une extension galoisienne de K_0, il faut et il suffit que, pour tout automorphisme σ du groupe de K par rapport à K_0, on ait $\sigma(a)=b^n a^r$, avec $b \in K$ (utiliser l'exerc. 13).

16) a) Soit E une extension cyclique séparable de degré n d'un corps K , σ un automorphisme engendrant le groupe de E par rapport à K . Si a est un élément de E tel que $N_{E/K}(a)=1$, montrer qu'il existe un élément $b \in E$ tel que $a=b(\sigma(b))^{-1}$ (si $E=K\langle\theta\rangle$, considérer les éléments

$$b_k=\theta^k+a^{-1}\sigma(\theta^k)+a^{-1}\sigma(a^{-1})\sigma^2(\theta^k)+\ldots+a^{-1}\sigma(a^{-1})\ldots\sigma^{n-2}(a^{-1}).\sigma^{n-1}(\theta^k)$$

("résolvantes de Lagrange-Hilbert"), et prouver qu'un au moins de ces éléments, pour $1 \leqslant k \leqslant n-1$, est $\neq 0$ et répond à la question).

b) En déduire que, si K contient les racines n-ièmes de l'unité, et si la caractéristique de K ne divise pas n , E est le corps des racines d'un polynome θ^n-a , où $a \in K$ (appliquer a) au cas où $a=\zeta$ est une racine n-ième primitive de l'unité).

16 bis) a) Avec les mêmes notations que dans l'exerc. 16a), soit a un élément de E tel que $Tr_{E/K}(a)=0$; montrer qu'il existe un élément $b \in E$ tel que $a=b-\sigma(b)$ (considérer les éléments

$$b_k = \frac{a\sigma(\theta^k)+(a+\sigma(a))\sigma^2(\theta^k)+\ldots+(a+\sigma(a)+\ldots+\sigma^{n-2}(a))\sigma^{n-1}(\theta^k)}{\theta^k+\sigma(\theta^k)+\ldots+\sigma^{n-1}(\theta^k)}$$

et prouver qu'un de ces éléments est défini et répond à la question).

b) En déduire que si K de caractéristique p , et si n=p , E est le corps des racines d'un polynome irréductible de la forme $\theta^p-\theta-a$, où $a \in K$ (appliquer a) au cas où $a=\varepsilon$, ε élément unité de K).

17) Soit K un corps de caractéristique $p > 0$; pour que le polynome $\theta^p-\theta-a$ de $K[\theta]$ soit irréductible, il faut et il suffit qu'il n'ait aucune racine dans K (remarquer que, si θ est une de ses racines, les autres sont $\theta+k\varepsilon$, où ε est l'unité de K , et k prend les valeurs entières $1,2,\ldots,p-1$).

18) Soit K un corps de caractéristique $p>0$; montrer que, s'il existe une extension cyclique séparable de degré p de K , il existe une

extension de degré p^r de K , quel que soit l'entier $r>0$ (si e^p-e-a est irréductible dans $K[e]$ et θ une de ses racines, montrer que $e^p-e-a\theta^{p-1}$ est irréductible dans $K<\theta>$, en utilisant l'exerc. 17 ; conclure à l'aide de l'exerc. 16 bis).

19) Soit K un corps tel qu'une extension E de degré premier q de K soit algèbriquement stable.

a) Montrer que K est parfait.

b) Montrer que la caractéristique de K est $\neq q$ (utiliser l'exerc.18).

c) Montrer que $E=K<\xi>$, où ξ est une racine primitive q^2-ième de l'unité (montrer qu'on peut appliquer à K et E l'exerc.16 ; si $E=K<\theta>$, où θ est racine de e^q-a , $a\in K$, remarquer que le polynome $e^{q^2}-a$ de $K[e]$ a un facteur de degré q (irréductible ou non) appartenant à $K[e]$, et examiner la forme du terme constant de ce facteur).

d) En supposant que K est de caractéristique 0 , soit ζ une racine q^3-ième primitive de l'unité. Montrer que $Q<\zeta>$ est de degré q par rapport aux deux sous-corps distincts $K\cap Q<\zeta>$, et $Q<\xi>$; en déduire que le groupe de $Q<\zeta>$ par rapport à Q n'est pas cyclique, et conclure de l'exerc. 5 que $q=2$.

e) Montrer que K ne peut avoir une caractéristique $\neq 0$ (même méthode que dans d) ; si q^γ est la plus haute puissance de q telle que toutes les racines q^γ-ièmes de l'unité appartiennent à $P<\xi>$, où P est le corps premier de K , prendre pour ζ une racine primitive $q^{\gamma+1}$-ième de l'unité).

20) Déduire de l'exerc.19 que, si K est un corps dont une extension <u>finie</u> E est algèbriquement stable, K est de caractéristique 0 , et $E=K<i>$, où i est racine du polynome e^2+1 (raisonner par l'absurde; si on avait $E\neq K<i>$, prouver, à l'aide du théorème fondamental

des extensions galoisiennes et du théorème de Sylow, qu'il existerait un corps F tel que $K<i>\subset F\subset E$, et que E soit de degré premier par rapport à F ; déduire alors de l'exerc. 19 que cette conclusion est absurde).

§ 8. Corps ordonnés et corps quasi-réels.

Corps ordonnés. Définition 1. On appelle corps ordonné un corps commutatif K, totalement ordonné par une relation d'ordre $x \leqslant y$, qui satisfait aux deux axiomes suivants :

(KO_I) La relation $x \leqslant y$ entraîne $x+z \leqslant y+z$ quel que soit z.

(KO_{II}) Les relations $x \leqslant y$ et $z \geqslant 0$ entraînent $xz \leqslant yz$.

Une structure de corps et une structure d'ensemble totalement ordonné sur un ensemble K sont dites compatibles si elles satisfont aux axiomes (KO_I) et (KO_{II}).

Exemples. Le corps $\mathbb{Q}$ des nombres rationnels est un corps ordonné (pour la relation d'ordre définie au chap. I, §). *Il en est de même du corps des nombres réels $\mathbb{R}$.*

Remarque. Une structure d'ordre sur un corps K, pour laquelle K n'est pas totalement ordonné, peut cependant satisfaire aux axiomes (KO_I) et (KO_{II}) (exerc. 1) ; il semble donc que c'est aux corps munis d'une telle structure qu'il aurait fallu réserver le nom de "corps ordonnés", en appelant "corps totalement ordonnés" ceux que nous avons appelés simplement "corps ordonnés" ci-dessus. Toutefois, une telle structure d'ordre sur un corps K ne serait vraiment intéressante dans les applications que si K, muni de cette structure, était un ensemble réticulé ; or on peut montrer que, dans ce cas, K est nécessairement totalement ordonné si $x>0$ entraîne $\frac{1}{x}>0$ (exerc. 2).

L'axiome (KO_I) n'est autre que l'axiome (GO) des groupes ordonnés ; muni de sa seule structure de groupe additif, K est donc un groupe <u>totalement ordonné</u> (chap.V, § 1) ; toutes les propriétés de ces groupes lui sont donc applicables (cf.chap.V, § 1). Examinons maintenant les conséquences de (KO_{II}). Tout d'abord, les relations $x \geqslant 0$, $y \geqslant 0$ entraînent $xy \geqslant 0$; comme K n'a pas de diviseurs de 0 , les relations $x > 0$, $y > 0$ entraînent donc $xy > 0$.

Comme $(-x)y = -xy$, $(-x)(-y) = xy$, on voit que les relations $x \leqslant 0$, $y \geqslant 0$ (resp. $x < 0$, $y > 0$; $x \leqslant 0$, $y \leqslant 0$; $x < 0$, $y < 0$) entraînent $xy \leqslant 0$ (resp. $xy < 0$; $xy \geqslant 0$; $xy > 0$). On en conclut l'identité

$$|xy| = |x| \cdot |y| \tag{1}$$

Comme K est totalement ordonné, les règles précédentes montrent que $x \neq 0$ entraîne $x^2 > 0$; comme d'autre part, une somme d'éléments $\geqslant 0$ de K ne peut être nulle que si chacun d'eux l'est (chap.V, § 1), on a la proposition suivante :

<u>Proposition 1.</u> <u>Dans un corps ordonné</u> K , <u>la relation</u> $x_1^2 + x_2^2 + \ldots + x_n^2 = 0$ <u>entraîne</u> $x_1 = x_2 = \ldots = x_n = 0$.

En particulier, l'élément $1 = 1^2$ est > 0 ; il en est donc de même de la somme $n.1$, quel que soit l'entier $n > 0$; donc :

<u>Proposition 2.</u> <u>Un corps ordonné est de caractéristique nulle</u>.

Un peut donc toujours supposer que le corps premier contenu dans K est identique à $\mathbb{Q}$. On remarquera en outre que la structure d'ordre <u>induite</u> sur $\mathbb{Q}$ par celle de K est nécessairement identique à celle définie au chap.I, § ; en effet, comme $1 > 0$ dans cette structure, on a aussi $n > 0$ pour tout entier naturel n , puis $1/n > 0$, sans quoi, on aurait $n.(1/n) = 1 \leqslant 0$; enfin, de $1/q > 0$, on déduit $p.(1/q) = p/q > 0$ pour tout couple d'entiers naturels

non nuls p,q. Autrement dit, il n'y a qu'une seule structure d'ordre compatible avec la structure de corps de $\mathbb{Q}$.

De (KO_{II}), on déduit aussi que $x \leqslant y$ et $z \leqslant 0$ entraînent $xz \geqslant yz$; on peut dire que, dans K, une homothétie de rapport >0 conserve l'ordre, une homothétie de rapport <0 change l'ordre en l'ordre opposé.

Si $x>0$, on a $x^{-1}>0$, car $x.x^{-1}=1>0$, ce qui prouve qu'on ne peut avoir $x^{-1} \leqslant 0$; on en conclut que, si $0<x<y$, on a $y^{-1}<x^{-1}$ car on a $x^{-1}>0$, $y^{-1}>0$, donc $x^{-1}y^{-1}>0$, et par suite $x(x^{-1}y^{-1})<y(x^{-1}y^{-1})$; si on désigne par K_+^* l'ensemble des éléments >0 de K, on voit que l'application $x \to x^{-1}$ est une permutation involutive de K_+^*, strictement décroissante. Ce fait prouve que K_+^* est un sous-groupe du groupe multiplicatif K^* des éléments $\neq 0$ de K, et que la structure d'ordre est compatible avec la structure de ce groupe, autrement dit que K_+^* est un groupe multiplicatif totalement ordonné.

Semi-corps. L'ensemble K_+ des éléments positifs d'un corps ordonné K vérifie évidemment les relations suivantes :

(2) $K_+ + K_+ \subset K_+$;

(3) $K_+ . K_+ \subset K_+$;

(4) $K_+ \cap (-K_+) = \{0\}$;

(5) $K_+ \cup (-K_+) = K$.

Ces propriétés sont caractéristiques ; de façon précise :

Proposition 3. Soit P une partie d'un corps commutatif K, satisfaisant aux conditions suivantes :

(KP_I) $P+P \subset P$; (KP_{II}) $P.P \subset P$; (KP_{III}) $P \cap (-P) = \{0\}$;

(KP_{IV}) $P \cup (-P) = K$.

Il existe une structure d'ordre et une seule, compatible avec la structure de corps de K, et telle que $K_+ = P$.

En effet, (KP_I), (KP_{III}) et (KP_{IV}) prouvent qu'il existe une et une seule structure d'ensemble totalement ordonné compatible avec la structure de groupe additif de K et telle que $P=K_+$ (cf. chap.V, § 1) ; si on munit K de cette structure, (KP_{II}) signifie que $x\geqslant 0$ et $y\geqslant 0$ entraînent $xy\geqslant 0$; si $x\leqslant y$ et $z\geqslant 0$, on a donc $y-x\geqslant 0$, $z(y-x)\geqslant 0$, d'où $xz\leqslant yz$, ce qui établit (KO_{II}).

On voit donc que les axiomes (KP_I) à (KP_{IV}) entraînent que, si P^* désigne l'ensemble des éléments $\neq 0$ de P, on a (KP_V) $(P^*)^{-1}\subset P$.

Pour abréger, nous dirons qu'une partie P d'un corps K qui satisfait aux axiomes (KP_I), (KP_{II}), (KP_{III}) et (KP_V) est un semi-corps.

Si P satisfait seulement aux axiomes (KP_I), (KP_{II}) et (KP_{III}) il est facile d'en déduire un semi-corps Q contenant P : il suffit de prendre l'ensemble des xy^{-1}, où x et y sont des éléments de P et $y\neq 0$; cet ensemble vérifie en effet (KP_V), et, comme on le voit aussitôt, (KP_I) et (KP_{II}) ; en outre, si $xy^{-1}=-x'y'^{-1}$, on en tire $xy'=-x'y$ et d'après (KP_{II}) et (KP_{III}), $xy'=x'y=0$; comme y et y' sont $\neq 0$, cela entraîne $x=x'=0$, donc $xy^{-1}=x'y'^{-1}=0$, et prouve que Q satisfait à (KP_{III}).

Corps quasi-réels. Nous allons caractériser les corps K tels qu'il existe une structure d'ordre compatible avec la structure de corps de K :

Théorème 1 (Artin-Schreier). *Pour qu'il existe une structure d'ordre compatible avec la structure de corps d'un corps* K, *il faut et il suffit que* K *vérifie l'axiome suivant* :

(QR) *La relation* $x_1^2+x_2^2+\ldots+x_n^2=0$ *entraîne* $x_1=x_2=\ldots=x_n=0$.

(Il est immédiat que cet axiome est équivalent au suivant : -1 *n'est pas égal à une somme de carrés d'éléments de* K).

Un corps ne peut évidemment satisfaire à (QR) que s'il est de caractéristique 0 ; mais il y a des corps de caractéristique 0 qui ne satisfont pas à (QR) : un exemple est fourni par le corps $\mathbb{Q}\langle i\rangle$, où i est une racine de e^2+1 ; dans ce corps on a en effet $i^2+1^2=0$.

La proposition 1 montre que la condition est nécessaire. Pour voir qu'elle est suffisante, il nous suffira de former un semi-corps contenu dans K , et satisfaisant à (KP_{IV}).

Remarquons pour cela que, s'il existe une structure d'ordre compatible avec la structure de corps de K , le semi-corps K_+ contient l'ensemble des carrés des éléments de K . Considérons donc l'ensemble $\mathfrak{M}$ des semi-corps contenus dans K et contenant l'ensemble des carrés des éléments de K . Nous allons tout d'abord prouver, à l'aide de (QR), que $\mathfrak{M}$ n'est pas vide.

Considérons à cet effet, l'ensemble P_o des éléments de la forme $(x_1^2+x_2^2+\ldots+x_p^2)/(y_1^2+\ldots+y_q^2)$, où p et q sont quelconques, les x_i et x_j quelconques dans K sous la seule condition que les y_j ne soient pas tous nuls, ce qui entraîne, d'après (QR), que les éléments de la forme précédente sont bien définis. Il est immédiat que P_o satisfait aux axiomes (KP_I),(KP_{II}) et (KP_V) ; il satisfait aussi à (KP_{III}) en vertu de (QR) ; donc P_o est un semi-corps, et comme il contient évidemment les carrés des éléments de K , il appartient à $\mathfrak{M}$.

Remarquons maintenant que $\mathfrak{M}$, ordonné par inclusion, est un ensemble inductif ; il possède donc un élément maximal Q ; nous allons montrer que Q est un semi-corps satisfaisant à (KP_{IV}).

En effet, soit $x\neq 0$ un élément de K n'appartenant pas à Q . Si on considère l'ensemble Q' des expressions rationnelles de la forme

$(a_o+a_1x+\ldots+a_px^p)/(b_o+b_1x+\ldots+b_qx^q)$, où les a_i et b_j appartiennent à Q, et dont le dénominateur n'est pas nul, il est clair que Q' satisfait aux axiomes (KP_I), (KP_{II}) et (KP_V) ; comme il contient Q et en est distinct, il ne peut satisfaire à (KP_{III}) d'après la définition de Q. Donc il existe p+1 éléments non tous nuls a_i de Q tels que $a_o+a_1x+\ldots+a_px^p=0$, ce qui peut s'écrire $(a_o+a_2x^2+\ldots)+(a_1+a_3x^2+..)x=0$; comme $x^2 \in P_o \subset Q$, on peut écrire cette relation $b+cx=0$, où b et c appartiennent à Q ; d'ailleurs, on ne peut avoir $b=0$, car, comme $x\neq 0$, on en tirerait $c=0$, et tous les a_i seraient nuls ; de même, on ne peut avoir $c=0$. Donc, $x=-b/c$ appartient à -Q, ce qui achève la démonstration.

Un corps K satisfaisant à l'axiome (QR) est dit corps <u>quasi-réel</u> (ou encore corps <u>ordonnable</u>) ; il est évident que tout sous-corps d'un corps quasi-réel est quasi-réel.

<u>Remarque</u>. L'ensemble P_o considéré dans la démonstration du th.1 est visiblement le <u>plus petit</u> semi-corps contenu dans K et contenant l'ensemble des carrés des éléments de K. Si on remarque que le quotient a/b s'écrit $a.b(b^{-1})^2$, on voit que P_o est identique à l'ensemble des <u>sommes de carrés</u> d'éléments de K.

En outre, P_o est l'<u>intersection</u> des semi-corps de K satisfaisant à (KP_{IV}) ; autrement dit :

<u>Propcsition 4</u>. <u>Pour qu'un élément d'un corps quasi-réel</u> K <u>soit positif pour toute structure d'ordre compatible avec la structure de corps de</u> K, <u>il faut et il suffit qu'il soit égal à une somme de carrés d'éléments de</u> K.

Il n'y a à démontrer que la <u>nécessité</u> de cette condition. Remarquons pour cela que, si y est un élément positif pour une structure d'ordre sur K, l'ensemble des fractions rationnelles $(a_o+a_1y+..+a_py^p)/$
$/(b_o+b_1y+..+b_qy^q)$,

où les a_i et b_j appartiennent à P_0 , est contenu dans un semi-corps satisfaisant à (KP_{IV}) donc est un semi-corps ; et réciproquement, le raisonnement du th.1 montre que si cet ensemble est un semi-corps, il existe une structure d'ordre sur K pour laquelle $y \geqslant 0$. Cela étant, soit x un élément strictement positif pour <u>toute</u> structure d'ordre sur K ; -x ne peut donc être positif pour <u>aucune</u> de ces structures ; il existe donc p+1 éléments non tous nuls a_i de P_0 tels que $a_0-a_1x+\ldots+(-1)^p a_p x^p=0$, ce qui s'écrit $b-cx=0$, avec $b=a_0+a_2x^2\ldots$, $c=a_1+a_3x^2+\ldots$. Comme $x\neq 0$, une des relations $b=0$, $c=0$ entraînerait l'autre, donc aussi $b+cx=0$, et la remarque ci-dessus montrerait que x ne peut être positif pour aucune structure d'ordre sur K , ce qui est absurde. Donc $bc\neq 0$, d'où $x=b/c$, et comme b et c appartiennent à P_0 , $x\in P_0$.

<u>Extensions d'un corps quasi-réel</u>. <u>Proposition 5</u>. <u>Une extension transcendante pure d'un corps quasi-réel est un corps quasi-réel</u>.

Il suffit évidemment de le démontrer pour $K(e_1,e_2,\ldots,e_n)$; or, supposons qu'il y ait un nombre fini de fractions rationnelles f_i $(1 \leqslant i \leqslant m)$ telles que $-1=\sum_{i=1}^{m} f_i^2$; comme K est de caractéristique nulle, donc infini, il existe un point $(x_k) \in K^n$ pour lequel les m fonctions rationnelles $\dot{f}_i$ sont définies ; on aurait par suite $-1 = \sum_{i=1}^{m} (\dot{f}_i(x_1,x_2,\ldots,x_n))^2$, contrairement à l'hypothèse.

<u>Proposition 6</u>. <u>Une extension algèbrique finie de degré impair</u> n <u>d'un corps quasi-réel est un corps quasi-réel</u>.

La proposition étant évidente pour n=1 , nous la démontrerons par récurrence sur n . Comme K est de caractéristique nulle, il est parfait ; une extension algèbrique de K est séparable, donc une extension finie est de la forme $K\langle\theta\rangle$, où θ est de degré n par rapport à K (§ 5, prop8).

Soit f le polynome irréductible de $K[e]$ dont θ est racine ; si $K\langle\theta\rangle$ n'était pas quasi-réel, on aurait une relation de la forme $-1=\sum_{k=1}^{m}(\varphi_k(\theta))^2$, où les φ_k sont des polynomes de degré $\leqslant n-1$, relation qui équivaut donc à une identité

$$(6) \qquad -1 = \sum_{k=1}^{m} \varphi_k^2 + fg$$

où g est un polynome de $K[e]$; la comparaison des degrés des deux membres de (6) montre que g est un polynome de degré <u>impair</u> et $\leqslant n-2$; il existe donc au moins un facteur irréductible h de g qui soit de degré impair et $<n$. Soit α une racine de h ; on déduit de (6) l'identité $-1 = \sum_{k=1}^{m} (\varphi_k(\alpha))^2$; mais comme par hypothèse, $K\langle\alpha\rangle$ est quasi-réel, cette relation est contradictoire, d'où la proposition.

<u>Proposition 7. Soit K un corps quasi-réel, (a_ι) une famille d'éléments de K ; si $\sqrt{a_\iota}$ désigne une racine du polynome e^2-a_ι , pour que le corps E obtenu par adjonction à K des éléments $\sqrt{a_\iota}$ soit quasi-réel, il faut et il suffit que, pour une structure d'ordre compatible avec la structure de corps de K , tous les a_ι soient positifs.</u>

La condition est évidemment <u>nécessaire</u>, car $a_\iota = (\sqrt{a_\iota})^2$ est positif pour toute structure d'ordre compatible avec la structure de corps de E , donc pour la structure qu'elle induit sur K .

Pour montrer que la condition est <u>suffisante</u>, il suffit évidemment d'établir l'impossibilité d'une relation de la forme

$$(7) \qquad -1 = \sum_{i=1}^{n} c_i x_i^2$$

où les c_i sont des éléments <u>positifs</u> de K pour la structure d'ordre considérée, et les x_i des éléments de E ; comme les x_i appartiennent à un corps obtenu par adjonction à K d'un nombre <u>fini</u> de racines $\sqrt{a_\iota}$, on peut se restreindre au cas où E s'obtient en adjoignant à K une famille finie $(\sqrt{a_k})_{1\leqslant k\leqslant r}$ de racines carrées d'éléments positifs de K.

Pour démontrer dans ce cas l'impossibilité de la relation (7), nous procéderons par récurrence sur r , la proposition résultant de l'hypothèse sur K pour r=0. Soit F le corps obtenu par adjonction à K de $\sqrt{a_1}$, $\sqrt{a_2}$,..., $\sqrt{a_{r-1}}$; on a $E=F\langle\sqrt{a_r}\rangle$; si $\sqrt{a_r}\in F$, la relation (7) est impossible par hypothèse ; sinon, on peut écrire $x_i=y_i+z_i\sqrt{a_r}$, où les y_i et z_i appartiennent à F ; (7) s'écrit donc

$$-1=\sum_{i=1}^{n} c_i y_i^2+\sum_{i=1}^{n} c_i a_r z_i^2+2\sqrt{a_r}\sum_{i=1}^{n} c_i y_i z_i$$

ce qui entraîne d'abord $\sum_{i=1}^{n} c_i y_i z_i=0$, sans quoi on aurait $\sqrt{a_r}\in F$ contrairement à l'hypothèse ; mais alors, il reste une relation de la même forme que (7), mais où les éléments élevés au carré appartiendraient à F , ce qui est encore contraire à l'hypothèse ; la proposition est ainsi démontrée.

Corps quasi-réels maximaux. Définition 2. On dit qu'un corps quasi-réel K est maximal si toute extension algèbrique quasi-réelle de K est identique à K .

Théorème 2. Pour qu'un corps quasi-réel K soit maximal, il faut et il suffit qu'il satisfasse aux conditions suivantes :

a) tout élément de K positif pour une structure d'ordre compatible avec la structure de corps de K , est le carré d'un élément de K ;

b) tout polynome de $K[e]$ de degré impair a une racine dans K .

En outre, si K est maximal, le corps $K\langle i\rangle$, obtenu par adjonction à K d'une racine i du polynome e^2+1 , est algèbriquement stable.

La nécessité des conditions a) et b) résulte des prop.6 et 7 . Pour voir qu'elles sont suffisantes, nous allons montrer que, si elles sont remplies, $K\langle i\rangle$ est algèbriquement stable. Comme $K\langle i\rangle$ n'est pas quasi-réel (car $i^2=-1$), et qu'il n'y a pas d'autre extension algèbrique de K que K et $K\langle i\rangle$, le théorème sera démontré.

Pour établir que $K\langle i\rangle$ est algèbriquement stable, il suffit de prouver que tout polynome f de $K[e]$ a une racine dans $K\langle i\rangle$ (§ 3, prop.1). La proposition résulte de la condition b) si le degré de f est impair ; supposons que ce degré soit $n=2^m q$, où q est impair. Nous allons démontrer la proposition par récurrence sur m . On peut évidemment supposer f irréductible ; comme K est parfait, les n racines $a_1, a_2, .., a_n$ de f sont distinctes. Considérons les $n(n-1)/2 = 2^{m-1}q(2^m q-1)$ éléments $a_j a_k + c(a_j + a_k)$, pour $1 \leqslant j < k \leqslant n$, c étant un élément de K ; elles satisfont à une équation à coefficients dans K de degré $n(n-1)/2$ d'après le théorème des fonctions symétriques), donc une au moins, soit $\theta = a_1 a_2 + c(a_1 + a_2)$ appartient à $K\langle i\rangle$ par hypothèse. Or, comme K est infini, on peut supposer que c a été choisi de sorte que les $n(n-1)/2$ éléments $a_j a_k + c(a_j + a_k)$ soient distincts. Il en résulte (§ 5, prop.8) que le corps $K\langle a_1 a_2, a_1 + a_2\rangle$ est contenu dans $K\langle\theta\rangle$, c'est-à-dire dans $K\langle i\rangle$. Autrement dit, a_1 et a_2 sont racines d'une équation du second degré $x^2+px+q=0$, à coefficients dans $K\langle i\rangle$. Tout revient à prouver que les racines d'une telle équation appartiennent à $K\langle i\rangle$, et comme on a $x^2+px+q=(x+\frac{p}{2})^2 + (q-p^2/4)$, il suffit de prouver que tout élément $a=b+ci$ de $K\langle i\rangle$ ($b \in K$, $c \in K$) est le carré d'un élément $u+vi$ de $K\langle i\rangle$. Or, l'équation $(u+vi)^2=b+ci$ équivaut à $u^2-v^2=b$, $2uv=c$, d'où $(u^2+v^2)^2=b^2+c^2$; comme b^2+c^2 est positif pour toute structure d'ordre sur K compatible avec sa structure de corps, la condition a) montre qu'il existe $d \in K$ tel que $d^2=b^2+c^2$, et on peut évidemment supposer $d>0$ pour une structure d'ordre sur K (sinon on remplacerait d par -d). On a donc $u^2=(b+d)/2$, $v^2=(d-b)/2$. L'un au moins des éléments d+b , d-b est $\geqslant 0$ dans K , et comme $(d-b)(d+b)=d^2-b^2=c^2 \geqslant 0$, ils sont $\geqslant 0$ tous deux. D'après a), il existe donc des éléments u et v de K satisfaisant aux équations précédentes.

C.Q.F.D.

Corollaire 1. Il existe une seule structure d'ordre compatible avec la structure de corps d'un corps quasi-réel maximal.

En effet, si, dans un corps quasi-réel maximal K , un élément a est positif pour une structure d'ordre compatible avec la structure de corps de K , il est le carré d'un élément de K , d'après la condition a) du th. 2 . Comme inversement, un carré est positif dans toute structure d'ordre, on voit que pour toute structure d'ordre, K_+ est identique à l'ensemble des carrés des éléments de K , d'où le corollaire.

Corollaire 2. Si K est un corps quasi-réel maximal, les polynomes irréductibles dans $K[e]$ sont les polynomes linéaires, et les polynomes du second degré e^2+pe+q tels que $q-p^2/4 > 0$.

En effet, toute extension algèbrique de K est au plus du second degré, et si $q-p^2/4 \leqslant 0$, le polynome e^2+pe+q a ses racines dans K , d'après la condition a) du th. 2 .

Proposition 8. Soit f une fonction polynome à coefficients dans un corps quasi-réel maximal K , définie dans K . Si a et b sont deux éléments de K tels que $a < b$, $f(a) < 0$, $f(b) > 0$, il existe $c \in K$ tel que $a < c < b$ et $f(c) = 0$.

Le théorème est immédiat lorsque f est du premier degré. Dans le cas général, f est le produit de polynomes du premier degré et de polynomes de la forme $(x+a)^2+b^2$ (cor.2 du th.2), avec $b \neq 0$, et un tel polynome est > 0 quel que soit x ; il y a donc au moins un facteur du premier degré g de f tel que $g(a)g(b) < 0$, d'où la proposition.

Extensions quasi-réelles maximales d'un corps quasi-réel. Théorème 3. *Soit K un corps quasi-réel, S une extension algèbriquement stable de K . Pour toute structure d'ordre sur K compatible avec sa structure de corps, il existe une extension quasi-réelle maximale R de K , contenue dans S , telle que $S=R\langle i\rangle$, et que la structure d'ordre de R induise sur K la structure d'ordre donnée.*

Soit $\mathfrak{M}$ l'ensemble des extensions quasi-réelles de K contenues dans S (S peut être une extension transcendante de K) ; il est immédiat que $\mathfrak{M}$ est un ensemble inductif quand on l'ordonne par inclusion; il a donc un élément maximal R_0 . Il ne peut exister d'extension transcendante pure de R_0 contenue dans S , sans quoi, d'après la prop.5, R_0 ne serait pas maximal dans $\mathfrak{M}$; donc S est une extension algèbrique de R_0 . D'autre part, R_0 satisfait, pour la même raison, aux conditions a) et b) du th.2, en vertu des prop.6 et 7 . Donc, d'après le th.2, R_0 est un corps quasi-réel maximal, et $R_0\langle i\rangle$ est une extension algèbtiquement stable de R_0 ; comme elle est contenue dans S , et que S est une extension algèbrique de $R_0\langle i\rangle$, $S=R_0\langle i\rangle$.

Considérons maintenant le corps K' obtenu par adjonction à K des racines carrées de tous les éléments positifs de K dans l'ordre considéré sur K . D'après la prop.7 , K' est un corps quasi-réel contenu dans S ; en lui appliquant ce qui précède, on définit une extension quasi-réelle maximale R de K' , contenue dans S et telle que $S=R\langle i\rangle$; or, pour l'ordre de R , les éléments positifs de K sont encore positifs, puisqu'ils sont des carrés d'éléments de R . Le théorème est donc complètement démontré.

Il existera en général une infinité d'extensions R possédant les propriétés énoncées dans le th.3 .

Notations. Si K est un corps quasi-réel maximal, tout élément $a \geqslant 0$ de K (pour l'unique structure d'ordre sur K), est le carré d'un élément positif unique b (l'autre racine de l'équation $x^2=a$ étant -b) ; on réserve la notation $\sqrt{a}$ à cet élément b .

De même, comme la fonction x^{2n} est strictement croissante pour $x \geqslant 0$, l'équation $x^{2n}=a$ admet, d'après la prop.8 , une racine positive et une seule, qu'on désigne par $\sqrt[2n]{a}$ (elle admet aussi la racine négative $-\sqrt[2n]{a}$). La fonction x^{2n+1} est strictement croissante dans K ; quel que soit $a \in K$ (positif ou non), l'équation $x^{2n+1}=a$ admet donc une seule racine dans K , qu'on note $\sqrt[2n+1]{a}$, et qui a le signe de a .

Si K est un corps ordonné quelconque (maximal ou non), l'extension $K\langle i\rangle$, où i est une racine de e^2+1 , est une extension galoisienne séparable de degré 2 ; tout élément $z \in K\langle i\rangle$ s'écrit d'une seule manière sous la forme $z=x+iy$, où x et y appartiennent à K ; on pose $x = \mathcal{R}(z)$, $y = \mathcal{I}(z)$; $\mathcal{R}$ et $\mathcal{I}$ sont des applications linéaires de $K\langle i\rangle$ dans K .

Le seul conjugué de i (relatif à K) distinct de i est -i ; le groupe de Galois de $K\langle i\rangle$ par rapport à K se compose donc de l'automorphisme identique et de l'automorphisme qui fait correspondre à $z=x+iy$ son conjugué $x-iy$, qu'on désigne par $\bar{z}$; on notera qu'on a $\mathcal{R}(z) = (z+\bar{z})/2$, $\mathcal{I}(z)=(z-\bar{z})/2i$. La norme N(z) de z relative à K est égale à $z\bar{z} = x^2+y^2$; elle est positive pour toute structure d'ordre sur K (compatible avec la structure de corps de K), et ne peut être nulle que si $z=0$.

Si tout élément $\geqslant 0$ de K a une racine carrée (en particulier si K est maximal), l'élément positif $\sqrt{N(z)} = \sqrt{z\bar{z}}$ se réduit à la valeur absolue de z lorsque $z \in K$; aussi, pour tout $z \in K\langle i \rangle$ le note-t-on encore $|z|$ et l'appelle-t-on <u>valeur absolue</u> de z ; on a $|zz'| = |z| \cdot |z'|$ d'après la propriété correspondante des normes ; en outre, on a l'<u>inégalité du triangle</u>

(8) $$|z+z'| \leqslant |z| + |z'|$$

En effet, les deux membres étant positifs, cela revient à montrer que, si $z=x+iy$, $z'=x'+iy'$

$$(x+x')^2+(y+y')^2 \leqslant x^2+y^2+x'^2+y'^2+2\sqrt{(x^2+y^2)(x'^2+y'^2)}$$

c'est-à-dire

$$(xx'+yy')^2 \leqslant (x^2+y^2)(x'^2+y'^2)$$

ou encore $$(xy'-yx')^2 \geqslant 0 .$$

<u>Exercices</u>. 1) a) Sur le corps $\mathbb{Q}$ des nombres rationnels, montrer qu'il n'existe aucune structure d'ensemble ordonné (totalement ordonné ou non) satisfaisant à (KO_I), (KO_{II}), et telle que $x > 0$ entraîne $1/x > 0$, autre que la structure d'ordre ordinaire de $\mathbb{Q}$.

b) Montrer que, sur $\mathbb{Q}$, il n'existe aucune structure d'ordre compatible avec la structure de groupe additif de $\mathbb{Q}$ telle que $n.x \geqslant 0$ entraîne $x \geqslant 0$, et qu'il existe un $x > 0$, autre que la structure d'ordre ordinaire et son opposée.

c) Dans $\mathbb{Q}$, on désigne par P l'ensemble formé de 0 et des nombres rationnels $\geqslant 1$ (pour l'ordre habituel) . Montrer que la structure de groupe ordonné définie sur le groupe additif de $\mathbb{Q}$ par la condition que P soit l'ensemble des éléments positifs de ce groupe, est une structure de groupe filtrant, et satisfait à (KO_{II}).

2) On considère, sur un corps K , une structure d'ensemble réticulé satisfaisant à (KO_I) et (KO_{II}).

a) Montrer que, si $x \neq 0$ est tel que $(x^+)^{-1} > 0$, on a $(x^+.x)^+ = (x^+)^2$, et $x^+x^- = 0$.

b) En déduire que, si la relation $x > 0$ entraîne $x^{-1} > 0$, K est totalement ordonné par la relation considérée.

3) Soit K un corps quasi-réel maximal, $a_1, a_2, \ldots, a_n, b_1, \ldots, b_n$ et c , $2n+1$ éléments de K tels que $b_1 < b_2 < \ldots < b_n$. Montrer que, si a_k et a_{k+1} sont de même signe, la fonction rationnelle

$$c + \frac{a_1}{x-b_1} + \frac{a_2}{x-b_2} + \ldots + \frac{a_n}{x-b_n}$$

a au moins une racine x telle que $b_k < x < b_{k+1}$, et en tout cas un nombre impair de racines satisfaisant à cette condition (utiliser la prop. 8).

4) Soit K un corps quasi-réel maximal, f(x) une fonction polynome définie dans K , a et b deux racines de f dans K , telles que $a < b$ et que f(x) n'ait aucune racine dans l'intervalle $]a,b[$. Montrer que, si g(x) est une fonction rationnelle définie dans K , dont le dénominateur ne s'annule pas dans l'intervalle $[a,b]$, l'équation $f(x)g(x)+f'(x)=0$ a un nombre impair de racines dans l'intervalle $]a,b[$ (même méthode que dans l'exerc.3). En déduire que, si h(x) est une fonction rationnelle définie dans K , ayant a et b pour racines, et dont le dénominateur ne s'annule pas dans $]a,b[$, l'équation $h'(x)=0$ a au moins une racine dans $]a,b[$ ("théorème de Rolle").

5) Soit K un corps quasi-réel maximal, h(x) une fonction rationnelle définie dans l'intervalle $[a,b]$. Montrer qu'il existe c tel que $a < c < b$, et $h(b)-h(a)=(b-a)h'(c)$ ("théorème de la moyenne" ;

appliquer le théorème de Rolle à la fonction rationnelle $h(x)-h(a) - \frac{h(b)-h(a)}{b-a}(x-a)$.) En déduire que, pour que h soit croissante dans l'intervalle $\left[a,b\right[$, il faut et il suffit que $h'(x) \geqslant 0$ dans cet intervalle (pour montrer que la condition est nécessaire, décomposer l'intervalle par les racines éventuelles de $h'(x)=0$).

6) Soit K un corps quasi-réel maximal, $a_0+a_1x+\ldots+a_nx^n=0$ une équation ayant toutes ses racines dans K . Si f(x) est une fonction polynome définie dans K , montrer que le nombre des racines de l'équation

$$a_0f(x)+a_1f'(x)+a_2f''(x)+\ldots+a_nf^{(n)}(x) = 0$$

qui n'appartiennent pas à K est au plus égal au nombre des racines de $f(x)=0$ qui n'appartiennent pas à K (appliquer l'exerc.4 pour le cas où $n=1$, puis procéder par récurrence). En déduire que l'équation $a_0 + \frac{a_1}{1!}x + \frac{a_2}{2!}x^2+\ldots+\frac{a_n}{n!}x^n = 0$ a toutes ses racines dans K .

7) Soit K un corps quasi-réel maximal, g(x) une fonction polynome définie dans K , ayant toutes ses racines dans K , et n'appartenant pas à l'intervalle $\left[0,n\right]$ de K . Montrer que si $f(x)=a_0+a_1x+\ldots+a_nx^n$ est une fonction polynome de degré n définie dans K , le nombre des racines de l'équation

$$a_0g(0)+a_1g(1)x+a_2g(2)x^2+\ldots+a_ng(n)x^n = 0$$

qui n'appartiennent pas à K est au plus égal au nombre des racines de f qui n'appartiennent pas à K (utiliser l'exercice 4 quand g est de degré 1, puis procéder par récurrence).

8) Soit K un corps quasi-réel maximal, f(x) une fonction polynome de degré n définie dans K , et ayant toutes ses racines dans K .

Quel que soit $c \neq 0$ dans K , le polynome f^2+cf' a au moins n-1 ~~et au moins n-1~~ et au plus n+1 racines dans K (étudier les variations de $f'(x)/(f(x))^2$ en utilisant l'exerc. 5).

9) Soit K un corps quasi-réel maximal, f(x) une fonction polynome définie dans K . Pour que, quelle que soit la fonction polynome g(x) définie dans K , le nombre des racines de $f(x)g(x)+g'(x)=0$ qui n'appartiennent pas à K soit au plus égal au nombre des racines de $g(x)=0$ n'appartenant pas à K , il faut et il suffit que $f(x)=a-bx$, où a est arbitraire dans K , et $b \geqslant 0$ (Pour montrer que la condition est suffisante, utiliser l'exerc.4 ; pour montrer qu'elle est nécessaire, appliquer à $g(x)=1$ et $g(x)=f(x)$, en utilisant l'exerc. 8).

10) Soit K un corps quasi-réel maximal,

$$f(x) = a_0+\binom{n}{1}a_1x+\binom{n}{2}a_2x^2+\ldots+a_nx^n$$

une fonction polynome définie dans K . Quels que soient les entiers p,q tels que $0 \leqslant p < p+q \leqslant n$, le nombre de racines du polynome

$$a_p+\binom{q}{1}a_{p+1}x+\binom{q}{2}a_{p+2}x^2+\ldots+a_{p+q}x^q$$

qui n'appartiennent pas à K est au plus égal au nombre des racines de f(x) qui n'appartiennent pas à K (utiliser le th. de Rolle).

En déduire que, si $b_1,b_2,\ldots,b_n$ sont n éléments distincts positifs de K , et si on pose

$$(x+b_1)\ldots(x+b_n) = x^n+\binom{n}{1}m_1x^{n-1}+\ldots+m_n$$

on a

$$\sqrt[k]{m_k} > \sqrt[k+1]{m_{k+1}} \qquad (1 \leqslant k \leqslant n-1)$$

(considérer le cas où q=2) .

11) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une suite finie de n éléments d'un corps ordonné K ; soit $(a_{i_k})_{1 \leqslant k \leqslant p}$ $(p \leqslant n)$ la suite extraite de (a_i) formée des a_i non nuls $(i_1 < i_2 < \ldots < i_p)$; on appelle <u>nombre de variations</u>

de la suite (a_i) le nombre des indices $k \leqslant p-1$ tels que a_{i_k} et $a_{i_{k+1}}$ soient de signes contraires.

Soit K un corps quasi-réel maximal, f(x) une fonction polynome définie dans K , et de degré n ; pour tout $a \in K$, on désigne par w(a) le nombre de variations de la suite $(f^{(i)}(a))_{0 \leqslant i \leqslant n}$. Si ν est le nombre de racines de f(x) dans l'intervalle $]a,b]$ $(a<b)$, montrer que $\nu \leqslant w(a)-w(b)$ et que la différence $w(a)-w(b)-\nu$ est paire ("règle de Budan-Fourier" ; décomposer l'intervalle $]a,b]$ par les racines des dérivées de f , et évaluer la quantité dont varie w(x) lorsque x traverse une de ces racines).

En déduire que, si $f(x)=a_0+a_1x+\ldots+a_nx^n$, le nombre de racines >0 de f(x) est au plus égal au nombre de variations de la suite $(a_i)_{0 \leqslant i \leqslant n}$, et que la différence de ces deux nombres est paire ("règle de Descartes").

12) Soit K un corps quasi-réel maximal, $f(x)=a_0+a_1x+\ldots+a_nx^n$ une fonction polynome définie dans K , telle que $a_0 \neq 0$, $a_n \neq 0$, et $a_p=a_{p+1}=\ldots=a_{p+2m-1}=0$ pour $1 \leqslant p < p+2m-1 \leqslant n-1$; montrer que f(x) a au plus $n-2m$ racines dans K (utiliser la règle de Descartes).

En déduire que, si $g(x)=1+a_1x+\ldots+a_nx^n$ a toutes ses racines dans K , et si $1+b_1x+\ldots+b_{2m}x^{2m}=f(x)$ est le polynome formé par les $2m+1$ premiers termes du développement de $1/g$ en série de puissances ascendantes (chap. IV, § 1), f(x) n'a aucune racine dans K .

13) Soit K un corps quasi-réel maximal, $a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_n$, 2n éléments de K tels que $b_1<b_2<\ldots<b_n$. Si on considère la fonction polynome

$$f(x) = a_1(x-b_1)^m + a_2(x-b_2)^m+\ldots+a_n(x-b_n)^m$$

(m entier $\geqslant 1$), montrer que le nombre ν de racines de f(x) dans K est au plus égal au nombre de variations w de la suite $(a_1, a_2, .., a_n, (-1)^m a_1)$, et que la différence $w-\nu$ est paire (raisonner par récurrence sur w , en étudiant, à l'aide de l'exerc.5, les variations de la fonction rationnelle $f(x)/(x-c)^m$, où c est un élément convenablement choisi).

14) Etant donnée une fonction polynome irréductible f(x) définie dans un corps quasi-réel maximal K , on appelle <u>suite de Sturm</u> relative à f et à un intervalle $]\alpha,\beta[$, une suite $(f_i(x))_{0 \leqslant i \leqslant p}$ de polynomes ayant les propriétés suivantes : a) deux termes consécutifs de la suite n'ont aucune racine commune dans $[\alpha,\beta]$; b) si $f_k(a)=0$ pour $1 \leqslant k < p$ et $a \in [\alpha,\beta]$, $f_{k-1}(a)$ et $f_{k+1}(a)$ sont de signes contraires ; c) $f_n(x)$ ne s'annule pas dans $[\alpha,\beta]$; d) $f_0(x)=f(x)$. Si w(x) désigne le nombre de variations de la suite $(f_i(x))$, montrer que le nombre de racines de f(x) appartenant à $]\alpha,\beta[$ est <u>égal</u> à $w(\alpha)-w(\beta)$ (méthode de l'exerc. 11).

Soit $(g_i(x))_{1 \leqslant i \leqslant r}$ la suite des restes successifs dans la recherche du p.g.c.d. de f et f' par l'algorithme d'Euclide (g_r étant le dernier reste $\neq 0$). Si on pose $f_1=f'$, $f_2=-g_1$, et en général $f_{2k}=(-1)^k g_{2k-1}$, $f_{2k+1}=(-1)^k g_{2k}$, montrer que la suite $(f_i)_{0 \leqslant i \leqslant r+1}$ est une suite de Sturm.

Si on ne suppose plus f irréductible, et qu'on détermine encore les f_i à partir des restes successifs g_i comme ci-dessus, le nombre $w(\alpha)-w(\beta)$ est égal au nombre des racines <u>distinctes</u> de f(x) appartenant à $]\alpha,\beta[$ ("théorème de Sturm").

15) Soit K un corps ordonné, G un sous-corps de K ; un élément x de K est dit <u>infiniment grand</u> par rapport à G si $|x|$ n'est majoré par

aucun élément de G ; un élément x de K est dit <u>infiniment petit</u> par rapport à G s'il n'existe aucun élément y de G tel que $0<y<|x|$. Pour que $x \neq 0$ soit infiniment petit par rapport à G, il faut et il suffit que x^{-1} soit infiniment grand par rapport à G. Une extension E de G, contenue dans K, est dite <u>comparable</u> à G s'il n'existe aucun élément de E infiniment grand par rapport à G ; en particulier, E est dit <u>archimédien</u> s'il est comparable à son sous-corps premier $\mathbb{Q}$.

Montrer que l'ensemble des éléments x de K qui ne sont pas infiniment grands par rapport à G forment un <u>anneau</u> F(G), et l'ensemble des éléments de K infiniment petits par rapport à G un <u>idéal maximal</u> $\mathfrak{P}(G)$ de F(G). Si une classe (mod. $\mathfrak{P}(G)$) contient un élément >0 de K et ne contient pas 0, elle ne contient que des éléments >0 de K.

En déduire qu'on définit, sur le corps quotient $K(G)=F(G)/\mathfrak{P}(G)$ une structure d'ordre compatible avec sa structure de corps en prenant comme éléments positifs les classes (mod. $\mathfrak{P}$) qui contiennent un élément $\geqslant 0$ de K.

Montrer qu'une classe (mod. $\mathfrak{P}$) ne peut contenir qu'un seul élément de G ; en déduire que l'application canonique de K dans K(G), restreinte à G, est un isomorphisme du corps ordonné G sur un sous-corps G' de K(G), et que K(G) est <u>comparable</u> à G'.

Montrer enfin que, si K est un corps quasi-réel maximal, il en est de même de K(G) (utiliser le th. 2).

16) Soit K un corps quasi-réel maximal, E un sous-corps de K, $f=e^n+a_1e^{n-1}+\ldots+a_n$ un polynome de $E[e]$; montrer que, si on pose

$$m = \mathrm{Max}(1, |a_1|+|a_2|+\ldots+|a_n|)$$

toutes les racines de f dans K appartiennent à l'intervalle $[-m,+m]$.

En déduire que, si E est une extension d'un corps G , comparable à G (exerc.15), l'ensemble R des éléments de K algèbriques par rapport à E est un corps quasi-réel maximal, comparable à G .

Montrer que f(t), pour une valeur $t \in K$, ne peut être infiniment petit par rapport à G que si t est congru (mod. $\mathfrak{P}(G)$) à une racine de f dans K (décomposer K en intervalles par les racines de f et f' ; remarquer que, si $x<t$, où $x \in R$ n'est pas congru (mod. $\mathfrak{P}(G)$) à t , il existe $y \in R$ tel que $x<y<t$; appliquer l'exerc.5).

17) On appelle <u>coupure</u> d'un ensemble totalement ordonné E une <u>partition</u> (A,B) de E en deux ensembles tels que, quels que soient $x \in A$, $y \in B$, on ait $x<y$, et que, si A admet une borne supérieure dans E , cette borne appartient à A . Soit K un corps quasi-réel maximal ; montrer qu'il existe une correspondance biunivoque entre les structures d'ordre sur K(e), prolongeant celle de K , et pour lesquelles K(e) est comparable à K , et les coupures (A,B) de K telles que A n'ait pas de borne supérieure dans K (montrer, à l'aide de l'exerc.5 , que la connaissance de l'ensemble des éléments $x \in K$ tels que $x<e$ détermine le signe de h(e) , quelle que soit la fraction rationnelle $h \in K(e)$; on décomposera une extension quasi-réelle maximale algèbrique de K(e) en intervalles par les racines du numérateur et du dénominateur de h , ainsi que les racines de h'). A toute coupure (A,B) de K telle que A ait une borne supérieure dans K correspondent deux structures d'ordre sur K(e) pour lesquelles K(e) n'est pas comparable à K ; enfin, il existe deux structures d'ordre sur K(e) pour lesquelles e est infiniment grand par rapport à K . Montrer qu'on obtient de cette manière <u>toutes</u> les structures d'ordre sur K(e) prolongeant celle de K .

18) On ordonne l'ensemble C(E) des coupures d'un ensemble totalement ordonné E , en posant $(A,B) \leqslant (A',B')$ si $A' \supset A$; dans C(E), qui est ainsi totalement ordonné, tout ensemble majoré admet une borne supérieure. Montrer que, si (A,B), (A',B') sont deux coupures dans $\mathbb{Q}$, il en est de même de $(A+A', B+B')$, et que $C(\mathbb{Q})$, muni de la loi de composition ainsi définie, est un <u>groupe</u> totalement ordonné contenant un sous-groupe isomorphe à $\mathbb{Q}$. Définir de la même manière (à l'aide de coupures sur l'ensemble des nombres rationnels > 0) une multiplication dans $C(\mathbb{Q})$, et montrer qu'on définit ainsi sur $C(\mathbb{Q})$ une structure de corps ordonné archimédien, prolongeant celle de $\mathbb{Q}$; le corps ordonné $C(\mathbb{Q})$ se note $\mathbb{R}$ et s'appelle <u>corps des nombres réels</u> (cf. <u>Top. gén.</u>, chap. IV).

Si K est un corps archimédien, et $x<y$ deux éléments de K , montrer qu'il existe un nombre rationnel r tel que $x<r<y$. En déduire que K est isomorphe à un sous-corps ordonné unique de $\mathbb{R}$ (faire correspondre à tout $x \in K$ la borne supérieure, dans $\mathbb{R}$, de l'ensemble des nombres rationnels r tels que $r \leqslant x$).

19) Pour que, dans un corps ordonné K , tout ensemble majoré ait une borne supérieure, il faut et il suffit que K soit isomorphe à $\mathbb{R}$ (montrer d'abord que, dans un corps non archimédien, l'ensemble $\mathbb{Q}$ n'a pas de borne supérieure ; utiliser ensuite l'exerc. 18).

20) Dans le corps des fractions rationnelles $K = \mathbb{Q}(e)$, on considère la structure d'ordre non archimédien pour laquelle e est >0 et infiniment grand par rapport à $\mathbb{Q}$ (exerc. 17). Montrer que $\mathbb{Q}(e)$ est comparable à son sous-corps $\mathbb{Q}\langle e^2 \rangle$, et donner un exemple de deux éléments x,y de $\mathbb{Q}(e)$, tels que $x < y$ et qu'il n'existe aucun élément de $\mathbb{Q}\langle e^2 \rangle$ dans l'intervalle $\left]x,y\right[$.

Montrer que le polynome $(u^2-e)(u^2-4e)-1$ de $K[u]$ est irréductible dans K , qu'il admet des racines dans toute extension quasi-réelle maximale de K , et que la fonction polynome correspondante est strictement positive dans K .

21) Soit K un corps ordonné, K(I) une extension transcendante pure de K . Montrer que :

a) si K est archimédien, pour qu'il existe une structure d'ordre sur K(I), prolongeant celle de K , et telle que K(I) soit comparable à K , il faut et il suffit que la puissance de I soit au plus égale à celle d'une base de transcendance M de $\mathbb{R}$ par rapport à K (K étant plongé dans $\mathbb{R}$, conformément à l'exerc.18) ; l'ensemble de ces structures d'ordre est alors équipotent à l'ensemble des applications biunivoques f de I dans $\mathbb{R}$, telles que f(I) forme un système algébriquement libre par rapport à K .

b) Si K n'est pas archimédien, il existe toujours (au moins) une structure d'ordre sur K(I), prolongeant celle de K , et telle que K(I) soit comparable à K (le cas où I n'a qu'un élément résulte des exerc.17 et 19 ; passer ensuite au cas général à l'aide du théorème de Zorn).

22) Soit K un sous-corps de $\mathbb{R}$, θ un nombre réel algèbrique par rapport à K . Montrer que le nombre de structures d'ordre distinctes de $K\langle\theta\rangle$, prolongeant celle de K , est égal au nombre des conjugués réels de θ (utiliser le th.3 et les exerc. 16 et 18).

23) Soit K un corps quasi-réel maximal, G un sous-corps de K . Montrer que l'ensemble des extensions E de G , contenues dans K et comparables avec G , est inductif ; si E_0 est un élément maximal de cet ensemble, montrer que E_0 est un corps isomorphe au corps K(G)

défini dans l'exerc.15 (prouver que l'application canonique de F(G) sur K(G) applique E_0 sur K(G) , en montrant d'abord, à l'aide de l'exerc. 16, que E_0 est un corps quasi-réel maximal, puis, à l'aide de l'exerc. 17, qu'il n'existe aucun élément de K(G) transcendant par rapport à l'image canonique de E_0).

24) Soit K un corps non algèbriquement stable, mais tel que $K\langle i\rangle$ soit algèbriquement stable. Montrer que K est un corps quasi-réel maximal (il suffit d'établir que toute somme de n carrés d'éléments de K est le carré d'un élément de K , car on en tire que K est quasi-réel maximal. Pour démontrer cette proposition, procéder par récurrence sur n ; dans le cas n=2 , pour prouver que a^2+b^2 est un carré, considérer la décomposition en facteurs irréductibles dans $K[e]$, du polynome $(e^2-a)^2+b^2$).

25) Déduire de l'exerc.24, et de l'exerc.20 du § 7, que, si un corps K est tel que son extension algèbrique maximale soit une extension finie de K , K est un corps quasi-réel maximal.

26) Soit K un corps ordonné, $E=S_1(K)$ le corps des séries formelles d'une lettre e sur K (chap.IV, § 1) : montrer qu'on définit une structure d'ordre compatible avec la structure de corps de E en prenant pour éléments strictement positifs de E les séries formelles dont le coefficient du terme de plus petit degré est >0 dans K .

Sur l'ensemble $H=S_1(E)$ des séries formelles $\sum_n a_n u^n$ d'une lettre u sur E , on définit comme d'ordinaire l'addition de deux éléments, mais on définit une multiplication non commutative, de la façon suivante : on pose $u^q e^p = 2^{pq} e^p u^q$, quels que soient les entiers rationnels p et q ; si $a = \sum_n \alpha_n e^n$, $b = \sum_n \beta_n e^n$ sont deux éléments de E , on pose

$$(au^p)(bu^q)=\sum_{m,n} a_m\beta_n e^m u^p e^n u^q = \sum_{m,n} a_m\beta_n 2^{pn} e^{m+n} u^{p+q} =$$

$$= \Big(\sum_{m,n} a_m\beta_n 2^{pn} e^{m+n}\Big)u^{p+q}$$

Enfin, on pose

$$\Big(\sum_n a_n u^n\Big)\Big(\sum_n b_n u^n\Big) = \sum_{m,n} (a_m u^m)(b_n u^n)$$

chacun des produits étant développé suivant la règle précédente, et les puissances de u mises en facteur dans les sommes obtenues.

a) Montrer que la multiplication ainsi définie sur H est associative et doublement distributive, et définit sur H une structure de corps non commutatif.

b) Si on prend pour éléments strictement positifs de H les séries dont le coefficient du terme de plus petit degré en u est strictement positif dans E , on définit sur H une structure d'ordre compatible avec sa structure de groupe additif, faisant de H un ensemble totalement ordonné, et telle que, si $z \geqslant 0$, la relation $x \leqslant y$ entraîne $xz \leqslant yz$ et $zx \leqslant zy$ ("corps ordonné non commutatif de Hilbert").

§ 9. Divisibilité dans les extensions algèbriques. Entiers algèbriques.

Soit A un anneau d'intégrité commutatif ayant un élément unité, K son corps des quotients, E une extension du corps K ; si x désigne un élément de E , le plus petit sous-anneau de E contenant A et x est évidemment l'ensemble $A[x]$ des expressions algèbriques entières (chap.IV, § 2) par rapport à x et aux éléments de A , c'est-à-dire l'ensemble des éléments de la forme $a_0+a_1x+\ldots+a_nx^n$, où les a_i sont des éléments arbitraires de A .

Cet anneau contient A , donc est en particulier un A-module ; nous allons chercher dans quel cas ce module est de type fini (chap.V, § 5).

Proposition 1. Pour que le plus petit sous-anneau $A[x]$ de E contenant A et x soit un A-module de type fini, il faut et il suffit que x satisfasse à une équation de la forme

$$x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_n = 0 \qquad (1)$$

où les coefficients b_i appartiennent à A .

La condition est évidemment suffisante, car si elle est remplie, tout élément de $A[x]$ est égal à une combinaison linéaire, à coefficients dans A , des éléments $1, x, x^2, \ldots, x^{n-1}$.

Pour voir que la condition est nécessaire, remarquons que, si $A[x]$ a , en tant que A-module, un système fini de générateurs $c_1, c_2, \ldots, c_m$, les éléments xc_i $(1 \leqslant i \leqslant m)$ appartiennent à $A[x]$, donc il existe m^2 éléments a_{ij} $(1 \leqslant i, j \leqslant m)$ de A tels que

$$xc_i = \sum_{j=1}^{m} a_{ij} c_j \qquad (1 \leqslant i \leqslant m) \qquad (2)$$

Comme les c_i ne sont pas tous nuls et vérifient le système (2) de m équations homogènes à m inconnues, le déterminant de ce système est nul, autrement dit, si $\underline{B}$ est la matrice (a_{ij}) , on a

$$\boxed{x\underline{I} - \underline{B}} = 0 \qquad (3)$$

équation qui, développée, est évidemment du type (1) .

Définition 1. On dit qu'un élément x de E est un entier algèbrique de E , relativement à l'anneau A , s'il satisfait à une équation de la forme (1), où n est un entier naturel >0 , et les coefficients b_i des éléments de A .

On dira souvent "entier algèbrique de E " ou même "entier algèbrique" au lieu de "entier algèbrique de E relativement à A " lorsqu'aucune confusion n'en peut résulter.

La dénomination d'"entier algèbrique" est justifiée par le fait qu'un entier algèbrique relativement à A est évidemment un élément de E algèbrique par rapport au corps K .

En outre, si x satisfait à (1), le polynome irréductible de $K[e]$ dont x est racine divise le polynome $e^n+b_1e^{n-1}+\ldots+b_n$, donc les conjugués par rapport à K d'un entier algèbrique sont des entiers algèbriques (dans toute extension de K les contenant).

Proposition 2. Si un sous-anneau B de E , contenant A , est un A-module de type fini, tous ses éléments sont des entiers algèbriques relativement à A . Réciproquement, le plus petit sous-anneau de E contenant A et un nombre fini d'entiers algèbriques relativement à A , est un A-module de type fini.

La première partie est une conséquence du raisonnement de la seconde partie de la démonstration de la prop.1 . D'autre part, le plus petit anneau contenant A et n éléments $x_1,x_2,\ldots,x_n$ de E est l'anneau $A[x_1,x_2,\ldots,x_n]$ des expressions entières par rapport à ces éléments ; si $A[x_i]$ est engendré par les puissances x_i^q $(0\leqslant q\leqslant m_i)$ en nombre fini, $A[x_1,x_2,\ldots,x_n]$ est un A-module engendré par les monomes $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ où $0\leqslant a_i\leqslant m_i$, qui sont en nombre fini.

De cette proposition, on déduit en particulier les deux suivantes :

Proposition 3. L'ensemble des entiers algèbriques par rapport à A , contenus dans E , est un anneau.

En effet, si x et y sont deux entiers algèbriques contenus dans E , x+y et xy appartiennent au plus petit sous-anneau de E contenant x et y , qui est un A-module de type fini, et dont tous les éléments sont donc des entiers algèbriques.

Proposition 4. Soit B l'anneau des entiers algèbriques par rapport à A , contenus dans E , et soit F une extension de E ; tout entier algèbrique par rapport à B , contenu dans F , est un entier algèbrique par rapport à A .

En effet, soit x un entier algèbrique par rapport à B ; il satisfait à une équation de la forme (1), où les b_i appartiennent à B ; x est donc entier algèbrique par rapport à l'anneau $A[b_1, b_2, \ldots, b_n] = C$, autrement dit, $C[x]$ est un C-module de type fini. Mais, d'après la définition de B et la prop.2 , C est un A-module de type fini, donc $C[x]$ est aussi un A-module de type fini, ce qui prouve (d'après la prop.2) que x est entier algèbrique par rapport à A .

Supposons maintenant que E soit une extension algèbrique de K . Alors

Proposition 5. Si B est l'anneau des entiers algèbriques par rapport à A , contenus dans E , E est le corps des quotients de B .

En effet, soit x un élément de E ; il est algèbrique par rapport à K , donc satisfait à une équation algèbrique à coefficients dans K ; en mettant ces coefficients sous forme de rapports d'éléments de A , et multipliant par le produit des dénominateurs, on peut supposer que l'équation est de la forme

$$a_0 x^m + a_1 x^{m-1} + \ldots + a_m = 0 \tag{4}$$

où les $a_i \in A$. Si on pose $y = a_0 x$, et qu'on multiplie l'équation (4) par a_0^{m-1} , il vient

$$y^m + a_1 y^{m-1} + a_0 a_2 y^{m-2} + \ldots + a_0^{m-1} a_m = 0$$

ce qui prouve que y est entier, d'où $x = y/a_0$, ce qui établit l'énoncé sous une forme plus précise, puisqu'on peut toujours supposer que x est égal à une fraction dont le numérateur appartient à B et le dénominateur à A .

Il est essentiel de remarquer que, si x est un entier algèbriqu par rapport à A , $A[x]$ n'est pas nécessairement identique à l'anneau des entiers algèbriques contenus dans son corps des quotients. Par exemple, si $A = \mathbb{Z}$, $x = \sqrt{-3}$, l'élément $y = (1 + \sqrt{-3})/2$

n'appartient pas à $A[x]$, mais vérifie l'équation $y^2-y+1=0$, donc est un entier algèbrique du corps des quotients de $A[x]$.

Divisibilité dans les anneaux d'entiers algèbriques. La théorie de la divisibilité des entiers algèbriques est l'étude de la divisibilité dans l'anneau B des entiers algèbriques par rapport à un anneau d'intégrité A qui appartiennent à une extension algèbrique E du corps des quotients K de A, connaissant la théorie de la divisibilité dans A.

Comme B est un A-module, à tout A-module $\mathfrak{m}$ contenu dans K, on peut faire correspondre le produit $B\mathfrak{m}$ des A-modules B et $\mathfrak{m}$ (chap.V, §3) qui est évidemment le B-module contenu dans E et engendré par $\mathfrak{m}$; en particulier, si $\mathfrak{a}$ est un idéal fractionnaire de K, $B\mathfrak{a}$ est un idéal fractionnaire de E, car il existe $c \in A$ tel que $c\mathfrak{a} \subset A$, d'où $c(B\mathfrak{a}) \subset B$. On définit ainsi une application de l'ensemble des A-modules contenus dans K dans l'ensemble des B-modules contenus dans E ; en outre, on a immédiatement, d'après les règles du produit des A-modules, $(B\mathfrak{m})+(B\mathfrak{n})=B(\mathfrak{m}+\mathfrak{n})$ et $(B\mathfrak{m})(B\mathfrak{n})=B(\mathfrak{m}\mathfrak{n})$; en particulier, si $\mathfrak{a}$ est un idéal inversible de K, on a $(B\mathfrak{a})(B\mathfrak{a}^{-1})=B(\mathfrak{a}\mathfrak{a}^{-1})=B$, autrement dit, $B\mathfrak{a}$ est un idéal inversible de E, dont l'inverse est $B\mathfrak{a}^{-1}$.

Nous allons maintenant nous borner au cas où A est un anneau de Prüfer (chap.V, § 5) ; on a alors le théorème suivant :

Théorème 1 (Dédekind). L'anneau B des entiers algèbriques par rapport à un anneau de Prüfer A, appartenant à une extension algèbrique E du corps des quotients K de A, est un anneau de Prüfer.

Soit α un élément quelconque du corps des quotients E de B ; il suffit de montrer que l'idéal fractionnaire $(1)+(\alpha)$ de E est inversible (chap.V, § 5, cor. de la prop. 3).

Soit $f=c_0e^n+c_1e^{n-1}+\ldots+c_n$ un polynome à coefficients dans A dont a est racine ; on peut donc écrire, dans $E[e]$

$$c_0e^n+\ldots+c_n=(e-a)(b_0e^{n-1}+b_1e^{n-2}+\ldots+b_{n-1})$$

Nous allons montrer que les b_i sont des entiers algèbriques, donc appartiennent à B . En effet, on a

$$b_k = c_k+c_{k-1}a + c_{k-2}a^2+\ldots+ c_0a^k \qquad (0\leqslant k\leqslant n-1)$$

d'où on tire

$$b_ka^p = c_ka^p+\ldots+ c_0a^{k+p} \quad \text{pour} \quad 0\leqslant p\leqslant n-k-1$$

$$b_ka^p = -c_{k+1}a^{p-1}-c_{k+2}a^{p-2}-\ldots-c_na^{p-(n-k)} \quad \text{pour} \quad n-k\leqslant p\leqslant n-1 .$$

On obtient ainsi un système de n équations linéaires homogènes satisfaites par les n éléments $1,a,a^2,\ldots,a^{n-1}$; on en conclut que son déterminant est nul, et comme les c_k sont des éléments de A , il en résulte que b_k satisfait à une équation de la forme (1).

Comme on a

$$(5) \qquad c_k=b_k-b_{k-1}a \quad (1\leqslant k\leqslant n-1) , \qquad c_n=-b_{n-1}a$$

on voit que les éléments b_ka $(0\leqslant k\leqslant n-1)$ sont également des entiers algèbriques. Si d est un élément de K tel que les c_kd appartiennent à A, on en conclut que les b_kd et b_kad appartiennent à B , par le même raisonnement appliqué au polynome df .

Considérons alors, dans A , l'idéal $\mathfrak{c}$ engendré par les c_k ; comme A est un anneau de Prüfer, $\mathfrak{c}$ admet un inverse $\mathfrak{c}^{-1}=\mathfrak{a}$, engendré par un nombre fini d'éléments $a_i \in A$ $(1\leqslant i\leqslant m)$; comme, pour tout indice i , les éléments c_ka_i sont entiers dans K $(0\leqslant k\leqslant n)$, les éléments b_ka_i et b_kaa_i appartiennent à B . Autrement dit, si $\mathfrak{b}$ est l'idéal de B engendré par les b_k $(0\leqslant k\leqslant n-1)$, on a

$$\mathfrak{b}((1)+(a))(B\mathfrak{a})\subset B$$

Mais, d'après (5), $B\mathfrak{r} \subset \mathfrak{b}((1)+(a))$

donc $B = (B\mathfrak{r})(B\mathfrak{a}) \subset \mathfrak{b}((1)+(a))(B\mathfrak{a}) \subset B$

ce qui prouve que l'idéal $\mathfrak{b}(B\mathfrak{a})$ est l'inverse de $(1)+(a)$.

C. Q. F. D.

Nous allons voir en outre que l'application qui, à tout idéal de type fini $\mathfrak{a}$ de A , fait correspondre l'idéal $B\mathfrak{a}$ de B est une application biunivoque de l'ensemble des idéaux de type fini de A dans l'ensemble des idéaux de type fini de B . Nous démontrerons tout d'abord la proposition suivante :

Proposition 6. Si A est un anneau de Prüfer K son corps des quotients, B un anneau d'entiers algèbriques par rapport à A , on a $B \cap K = A$. (Autrement dit, un élément fractionnaire de K ne peut être entier algèbrique par rapport à A).

En effet, soit x un élément de K tel que

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \tag{6}$$

où les a_i appartiennent à A . Si $\mathfrak{a}$ est l'idéal de type fini de K engendré par $1, x, x^2, \ldots, x^{n-1}$, l'équation (6) montre que $x^n \in \mathfrak{a}$, autrement dit que $(x)\mathfrak{a} \subset \mathfrak{a}$, d'où en multipliant par $\mathfrak{a}^{-1}$, $(x) \subset (1)$, c'est-à-dire $x \in A$.

Comme le montre l'exemple donné ci-dessus, cette proposition n'est pas exacte pour un anneau d'intégrité quelconque ; les anneaux d'intégrité pour lesquels elle est vraie sont appelés anneaux clos. L'exemple donné ci-dessus montre que, si x est un entier algèbrique par rapport à un anneau de Prüfer A , l'anneau $A[x]$ n'est pas nécessairement clos, et a fortiori n'est pas nécessairement un anneau de Prüfer ; il faut donc se garder d'étendre inconsidérément le th.1 à un anneau B quelconque formé d'entiers algèbriques par rapport à A .

Corollaire. Si α est un entier algèbrique par rapport à A , les coefficients du polynome irréductible $f \in K[e]$, dont le terme de plus haut degré a pour coefficient 1 , et dont α est racine, sont des éléments de A

En effet, ce sont des fonctions symétriques entières par rapport aux conjugués de α , donc des entiers algèbriques par rapport à A ; comme ils appartiennent à K , ce sont des éléments de A .

En particulier, si α est séparable par rapport à K , sa trace et sa norme par rapport à K (dans toute extension finie de K le contenant) sont des éléments de A .

Proposition 7. Si $\mathfrak{a}$ est un idéal de type fini de K , on a $(B\mathfrak{a}) \cap K = \mathfrak{a}$

En effet, soit b un élément de $(B\mathfrak{a}) \cap K$; on a donc $b = \sum_{i=1}^{n} \beta_i a_i$ où les a_i appartiennent à $\mathfrak{a}$, et les β_i à B . Soit E la plus petite extension galoisienne de K contenant les β_i , et soient σ_k $(1 \leqslant k \leqslant m)$ les automorphismes de son groupe par rapport à K . Si on forme la norme $\prod_{k=1}^{m} \left(\sum_{i=1}^{n} \sigma_k(\beta_i) e_i \right)$ du polynome $\sum_{i=1}^{n} \beta_i e_i$, (§ 5), ses coefficients sont invariants par tous les σ_k donc (§ 6, cor.1 du th.1) sont des éléments radiciels par rapport à K ; il existe donc une puissance de cette norme dont les coefficients appartiennent à K (ce sera la norme elle-même si E est séparable par rapport à K) ; en outre, ces coefficients sont évidemment des entiers algèbriques par rapport à A donc (prop.6) appartiennent à A . Comme par hypothèse, $b \in K$, on a $b = \sum_{i=1}^{n} \sigma_k(\beta_i) a_i$; donc il existe une puissance b^q qui est égale à une combinaison linéaire, à coefficients dans A , de monômes de degré q par rapport à $a_1, a_2, \ldots, a_n$; il en résulte que $b^q \in \mathfrak{a}^q$, ou encore $((b)\mathfrak{a}^{-1})^q \subset (1)$. Par suite, comme le groupe des idéaux de type fini de K est réticulé, on a $(b)\mathfrak{a}^{-1} \subset (1)$ (chap.V, § 1, cor.2 de la prop.5), c'est-à-dire $b \in \mathfrak{a}$.

Cette proposition établit donc bien ce que nous avions annoncé ci-dessus, à savoir que l'application $\mathfrak{a} \longrightarrow B\mathfrak{a}$ est biunivoque ;

en outre, d'après ce qui a été vu plus haut, elle fait correspondre à la somme et au produit de deux idéaux de K la somme et le produit, respectivement, des idéaux correspondants dans le corps des quotients de B ; c'est donc un <u>isomorphisme</u> du <u>groupe réticulé</u> $\mathfrak{J}_f(A)$ des idéaux fractionnaires de type fini de K <u>dans</u> le groupe réticulé $\mathfrak{J}_f(B)$ des idéaux fractionnaires de type fini de E .

En raison de cette isomorphie, on <u>identifie</u> souvent par abus de langage un idéal $\mathfrak{a}$ de K avec l'idéal correspondant $B\mathfrak{a}$ de E ; on écrit par exemple des relations de la forme $\mathfrak{a} = \mathfrak{b}\mathfrak{k}$, où $\mathfrak{a}$ est un idéal de K , $\mathfrak{b}$ et $\mathfrak{k}$ des idéaux de E , au lieu d'écrire $B\mathfrak{a} = \mathfrak{b}\mathfrak{k}$.

On notera que l'isomorphisme précédent n'applique pas, en général, $\mathfrak{J}_f(A)$ sur $\mathfrak{J}_f(B)$.

Supposons maintenant que A soit un <u>anneau de Dedekind</u> ; on peut alors compléter le résultat du th.1 par le suivant :

<u>Théorème 2</u>. <u>Soit</u> A <u>un anneau de Dedekind</u>, K <u>son corps des quotients</u>, <u>E une extension finie de K</u> . <u>Si B est l'anneau des entiers algèbriques par rapport à</u> A , <u>appartenant à E</u> , B <u>est un anneau de Dedekind</u>.

Comme, d'après le th.1, B est un anneau de Prüfer, il suffit de prouver que B est un <u>anneau de Noether</u>, c'est-à-dire (chap.V, § 5) que toute suite croissante (pour la relation $\subset$) d'<u>idéaux</u> de B n'a qu'un nombre <u>fini</u> de termes distincts.

Si $\mathfrak{b}$ est un idéal de B , sa trace $\mathfrak{b} \cap A$ est un idéal de A ; si $(\mathfrak{b}_n)$ est une suite croissante d'idéaux de B , la suite $(\mathfrak{b}_n \cap A)$ est une suite croissante d'idéaux de A , donc on a $\mathfrak{b}_n \cap A = \mathfrak{b}_{n+1} \cap A$ à partir d'un certain rang ; on peut donc se borner à considérer une suite $(\mathfrak{b}_n)$ dont tous les idéaux ont même trace $\mathfrak{a}$ sur A .

On a alors $B\mathfrak{a} \subset \mathfrak{b}_n$ quel que soit n ; le théorème sera établi si on prouve que, dans B , l'idéal $B\mathfrak{a}$ n'a qu'un nombre <u>fini</u> de diviseurs distincts, ou encore que l'anneau $B/B\mathfrak{a}$ ne possède qu'un nombre <u>fini</u> d'idéaux. Si $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{P}_i^{r_i}$ est la décomposition de $\mathfrak{a}$ en facteurs premiers dans A , on a $B\mathfrak{a} = \prod_{i=1}^{k} (B\mathfrak{P}_i)^{r_i}$, et les idéaux $B\mathfrak{P}_i$ sont premiers entre eux deux à deux dans B ; donc, comme B est un anneau de Prüfer, $B/B\mathfrak{a}$ est isomorphe au produit des anneaux $B/(B\mathfrak{P}_i)^{r_i} = B/B(\mathfrak{P}_i)^{r_i}$; tout idéal de $B/B\mathfrak{a}$ est égal au produit de ses composantes dans les anneaux facteurs ; donc, pour démontrer le théorème, on peut finalement se restreindre à démontrer que, si $\mathfrak{P}$ est un idéal <u>premier</u> de A , $B\mathfrak{P}^r$ n'a qu'un nombre fini de diviseurs distincts dans B , ou encore, que toute suite croissante de diviseurs de $B\mathfrak{P}^r$ n'a qu'un nombre fini de termes distincts.

Or, dans $B/B\mathfrak{P}^r$, tout idéal est un B-module, et a fortiori un A-module ; le résultat sera obtenu si nous prouvons que $B/B\mathfrak{P}^r$ est un <u>A-module de type fini</u> (chap.V, § 6, prop.1).

Considérons d'abord le cas où r=1 . $B/B\mathfrak{P}$ contient alors l'anneau $(A+B\mathfrak{P})/B\mathfrak{P}$, isomorphe à $A/A \cap B\mathfrak{P} = A/\mathfrak{P}$ (prop.7), et qui est par suite un <u>corps</u> ; on va prouver que $B/B\mathfrak{P}$, en tant qu'<u>algèbre</u> sur $A/\mathfrak{P}$, a un <u>rang fini</u> . En effet, soit n le degré $[E:K]$, et soient ω_i $(1 \leqslant i \leqslant n+1)$ n+1 éléments de B ; il suffit d'établir qu'il existe n+1 éléments $b_i \in A$ tels que $\sum_{i=1}^{n+1} b_i\omega_i \equiv 0 \pmod{B\mathfrak{P}}$, les b_i n'appartenant pas tous à $\mathfrak{P}$. Or, il existe par hypothèse n+1 éléments $a_i \in A$, non tous nuls, tels que $\sum_{i=1}^{n+1} a_i\omega_i = 0$; posons $(a_i) = \mathfrak{P}^{k_i}\mathfrak{a}_i$; on peut (chap.V, § 5, prop.10), trouver un $\pi \in A$ tel que $(\pi) = \mathfrak{P}\vartheta$, où ϑ est premier avec $\mathfrak{P}$, puis $c \in A$ tel que $(c) = \vartheta\mathfrak{c}$,

où $\varkappa$ est premier avec $\mathfrak{P}$; par suite $(a_i) = (\frac{\pi}{c})^{k_i} \omega_i \varkappa^{k_i}$, $a_i = b_i(\pi/c)^{k_i}$, où b_i est premier avec $\mathfrak{P}$; si on multiplie la relation $\sum_{i=1}^{n+1} a_i \omega_i = 0$ par c^k/π^k où k est le plus grand des k_i et h le plus petit, on obtient bien une relation du type voulu.

Il en résulte que $B/B\mathfrak{P}$ admet une <u>base finie</u> $(\dot{u}_i)$ par rapport à $A/\mathfrak{P}$; si u_i est un élément de la classe $\dot{u}_i$ dans B, tout élément de B est congru (mod. $B\mathfrak{P}$) à une combinaison linéaire des u_i, à coefficients <u>dans</u> A, ce qui prouve que $B/B\mathfrak{P}$ est un A-module de type fini.

Passons au cas général, et raisonnons par récurrence sur r ; on a $\mathfrak{P}^{r-1} = (\pi^{r-1}) + \mathfrak{P}^r$, d'où $B\mathfrak{P}^{r-1} = B(\pi^{r-1}) + B\mathfrak{P}^r$; tout élément de $B\mathfrak{P}^{r-1}$ est donc congru (mod. $B\mathfrak{P}^r$) à une combinaison linéaire, à coefficients <u>dans</u> A, des éléments $u_i \pi^{r-1}$, d'où

C. Q. F. D.

La démonstration du th.2 est beaucoup plus rapide dans le cas où l'anneau B, en tant que <u>A-module</u>, est <u>de type fini</u> ; car alors, c'est un module de Noether par rapport à A, et a fortiori un anneau de Noether. Toutefois, cette propriété n'est pas exacte si on ne soumet l'anneau de Dedekind A à aucune restriction supplémentaire(*) ; mais on a la proposition suivante :

<u>Proposition 8</u>. <u>Soit</u> A <u>un anneau de Dedekind</u>, K <u>son corps des quotients</u>, E <u>une extension séparable et finie de</u> K . <u>Si</u> B <u>est l'anneau des entiers algèbriques par rapport à</u> A , <u>appartenant à</u> E , B <u>est un A-module de type fini</u>.

En effet, on a alors $E = K\langle\theta\rangle$ (§ 5, prop.8), où θ est un élément séparable par rapport à K ; soit n son degré, θ_i ses conjugués ($1 \leqslant i \leqslant n$, $\theta_1 = \theta$) ;

(*) voir F.K. SCHMIDT, Math. Zeitschr., t. 41 (1936), p. 443

on peut supposer en outre que θ est un entier algèbrique, car dans le cas contraire, on a $\theta=a/r$, où a est un entier algèbrique, et $r\in A$, et il est clair que $E=K<a>$. Si x est un élément quelconque de E , on a (§ 2, prop.3)

$$(7) \qquad x = \sum_{k=0}^{n-1} a_k \theta^k ,$$

où les a_k appartiennent à K et sont uniquement déterminés en fonction de x . Il est facile d'ailleurs d'obtenir leur expression en fonction de x : si x_i $(1\leqslant i\leqslant n$, $x_1=x)$ sont les conjugués de x par rapport à K , on a aussi

$$x_i = \sum_{k=0}^{n-1} a_k \theta_i^k \qquad (1\leqslant i\leqslant n)$$

et le déterminant $\Delta = \begin{vmatrix} \theta_i^k \end{vmatrix}$ de ce système de n équations linéaires par rapport aux a_k , n'est autre que le déterminant de Vandermonde des θ_i , donc est $\neq 0$ par hypothèse ; on peut par suite écrire

$$(8) \qquad \Delta\, a_k = \sum_{i=1}^{n} r_{ki} x_i \qquad (0\leqslant k\leqslant n-1)$$

où les r_{ki} sont, d'après les formules de Cramer, des polynomes par rapport aux θ_i , à coefficients entiers rationnels ; comme les θ_i sont entiers algèbriques par rapport à A , il en est de même de Δ et des r_{ki} . Remarquons en outre que $\Delta^2 = \prod_{i<j} (\theta_j-\theta_i)^2$ est une fonction symétrique des θ_i , donc appartient à K (et même à A , d'après la prop. 7).

Supposons maintenant que x soit entier algèbrique par rapport à A ; alors les seconds membres des équations (8) sont entiers par rapport à A , donc il en est de même des éléments $\Delta\, a_k$, et aussi des éléments $\Delta^2 a_k$; mais $\Delta^2 a_k \in K$, donc (prop.7) , $\Delta^2 a_k \in A$. Autrement dit, on peut écrire

$$x = \sum_{k=0}^{n-1} b_k u_k$$

où $b_k \in A$, et $u_k = \theta^k / \Delta^2$; cela signifie que B est contenu dans le A-module engendré par les u_k ; comme A est un anneau de Dedekind, ce module est un module de Noether (chap.V, § 6, prop.1), donc B est un A-module de type fini.

Remarques. 1) Dans le cas considéré dans la prop.8, B est un module régulier de type fini par rapport à l'anneau de Dedekind A ; la théorie générale de ces modules, faite au chap.V, § 6, lui est donc applicable ; en particulier, la prop.5 prouve que l'espace vectoriel (par rapport à K) associé à B , est isomorphe à E . Autrement dit, si E est une extension séparable de degré n par rapport à K , B est un A-module régulier de rang n ; en particulier, si A est un anneau principal, B admet, en tant que A-module, une base de n éléments. Ces considérations s'appliquent aussi aux idéaux (fractionnaires) de E , et plus généralement aux sous-anneaux de B contenant A .

2) En général, si $\mathfrak{p}$ est un idéal premier de A , l'idéal correspondant $B\mathfrak{p}$ dans B ne sera plus premier, mais se décomposera en un produit d'idéaux premiers de B ; l'étude de cette décomposition, dans le cas où A est l'anneau des entiers algèbriques par rapport à $\mathbb{Z}$ d'une extension finie du corps $\mathbb{Q}$ des rationnels, est un des problèmes fondamentaux de la théorie des nombres algèbriques.

3) Si $\mathfrak{P}$ est un idéal premier de B , $\mathfrak{p} = \mathfrak{P} \cap A$ est un idéal premier de A ; en effet, si $x \in A$, $y \in A$ et $xy \equiv 0 \pmod{\mathfrak{p}}$, on a par hypothèse, $x \equiv 0$ ou $y \equiv 0 \pmod{\mathfrak{P}}$, donc x ou y appartient à $A \cap \mathfrak{P} = \mathfrak{p}$. On a en outre $B\mathfrak{p} \subset \mathfrak{P}$, donc $\mathfrak{P}/B\mathfrak{p}$ est un idéal stable de l'algèbre $B/B\mathfrak{p}$ par rapport au corps $A/\mathfrak{p}$; il résulte alors de la démonstration du th.2 que le corps $B/\mathfrak{P} = (B/B\mathfrak{p})/(\mathfrak{P}/B\mathfrak{p})$ est une extension finie du corps $A/\mathfrak{p}$; le degré de cette extension se nomme degré de l'idéal premier $\mathfrak{P}$.

Soit f le degré de $\mathfrak{P}$; si $\mathfrak{P}^k$ est une puissance de $\mathfrak{P}$ qui divise $B\mathfrak{P}$, le résultat précédent se généralise de la façon suivante : l'algèbre $B/\mathfrak{P}^k=(B/B\mathfrak{P})/(\mathfrak{P}^k/B\mathfrak{P})$ est <u>de rang</u> kf par rapport au corps $A/\mathfrak{P}$. En effet, soit $\dot{u}_i$ $(1\leqslant i\leqslant f)$ une base de $B/\mathfrak{P}$ par rapport à $A/\mathfrak{P}$; si u_i est un élément de la classe $\dot{u}_i$ dans B , tout élément de B est congru (mod. $\mathfrak{P}$) à une combinaison linéaire $\sum_{i=1}^{f} a_i u_i$, où les éléments a_i sont des éléments de A , qui sont <u>bien déterminés</u> (mod. $\mathfrak{P}$). Soit π un élément de $\mathfrak{P}$ n'appartenant pas à $\mathfrak{P}^2$; comme $\mathfrak{P}^{r-1}=(\pi^{r-1})+\mathfrak{P}^r$, on voit par récurrence sur r que tout élément de B est congru (mod. $\mathfrak{P}^k$) à une combinaison linéaire des éléments $\pi^h u_i$ $(0\leqslant h\leqslant k-1$; $1\leqslant i\leqslant f)$ à coefficients dans A , déterminés (mod. $\mathfrak{P}$) ; en outre, supposons qu'on ait $\sum_{h,i} a_{hi}\pi^h u_i \equiv 0$ (mod. $\mathfrak{P}^k$), et soit m le plus petit entier tel qu'il existe un $a_{mi}\not\equiv 0$ (mod. $\mathfrak{P}$) ; on aurait alors, d'après le choix de π , $\sum_{i=1}^{f} a_{mi}u_i \equiv 0$ (mod. $\mathfrak{P}$), donc, d'après la définition des u_i , $a_{mi}\equiv 0$ (mod. $\mathfrak{P}$) quel que soit i , ce qui est contradictoire. Les classes (mod. $\mathfrak{P}^k$) des kf éléments $\pi^h u_i$ forment donc bien une <u>base</u> de $B/\mathfrak{P}^k$ par rapport à $A/\mathfrak{P}$.

Soit alors $B\mathfrak{P}=\prod_{i=1}^{t}\mathfrak{P}_i^{e_i}$ la décomposition de $B\mathfrak{P}$ en facteurs premiers dans B . L'algèbre $B/B\mathfrak{P}$ est somme directe des algèbres $B/\mathfrak{P}_i^{e_i}$, donc son <u>rang</u> (chap.III, §1) par rapport au corps $A/\mathfrak{P}$ est égal à $\sum_{i=1}^{t} e_i f_i$, où f_i désigne le <u>degré</u> de l'idéal premier $\mathfrak{P}_i$. Or, on a vu dans la démonstration du th.2, que ce rang est $\leqslant n$, si n désigne le degré de l'extension E de K ; on a donc l'inégalité

$$\sum_{i=1}^{t} e_i f_i \leqslant n \quad . \tag{9}$$

Dans le cas où B est de <u>type fini</u> par rapport à A (ce qui est toujours le cas lorsque E est une extension séparable de K , d'après la prop.8), on a, de façon plus précise, l'<u>égalité</u>

$$\sum_{i=1}^{t} e_i f_i = n \quad . \tag{10}$$

En effet, on sait alors (chap.V, § 6, prop.4) que B est somme directe de n modules de la forme $\mathfrak{a}_i u_i$, où les $\mathfrak{a}_i$ sont des idéaux de A ; donc $B/B\mathfrak{p}$ est somme directe des n modules $\mathfrak{a}_i u_i/\mathfrak{p}\mathfrak{a}_i u_i$, qui sont tous isomorphes à $A/\mathfrak{p}$ (cf. chap.V, § 6, prop.7) ; autrement dit, $B/B\mathfrak{p}$ est <u>de rang n</u> par rapport au corps $A/\mathfrak{p}$.

<u>Exercices</u>. 1) On dit qu'un anneau d'intégrité A est <u>clos</u> si tout entier algèbrique par rapport à A , qui appartient au corps des quotients K de A , appartient nécessairement à A . Si A est un anneau d'intégrité quelconque, E une extension de son corps des quotients K , B l'anneau des entiers algèbriques par rapport à K , appartenant à E , montrer que B est un anneau clos.

2) Montrer que tout anneau arithmétique (chap.V, § 3) est clos (écrire qu'un élément de K , mis sous forme irréductible, satisfait à une équation de la forme (1)).

3) Pour qu'un anneau A soit clos, il faut et il suffit que, pour tout idéal fractionnaire de type fini $\mathfrak{a}$ de A , la relation $x\mathfrak{a} \subset \mathfrak{a}$ $(x \in K)$ entraîne $x \in A$ (pour voir que la condition est suffisante, raisonner comme dans la prop.6 ; pour voir qu'elle est nécessaire, raisonner comme dans la prop.1).

4) a) Soit A un anneau d'intégrité, a un élément de A non diviseur de 1 ; montrer que a^{-1} n'est pas un entier algèbrique par rapport à A .

b) Soit K le corps des quotients de A ; montrer qu'il existe un sous-anneau maximal A_0 de K ne contenant pas a^{-1} (appliquer le th. de Zorn).

c) Montrer, à l'aide de a), que l'anneau A_0 est clos (remarquer que, dans le cas contraire, a^{-1} serait entier algèbrique par rapport à A_0).

En déduire que A_o est un anneau de valuation (chap.V,Appendice,exerc2; montrer que, si $x^{-1} \notin A_o$, x est entier algèbrique par rapport à A_o).

5) a) Soit A un anneau clos, K son corps des quotients ; montrer que A est l'intersection des anneaux de valuation contenus dans K et contenant A (si $x \in \complement A$, appliquer l'exerc.4 à l'anneau $A[x^{-1}]$ des expressions entières en x^{-1}, à coefficients dans A, pour prouver qu'il existe un anneau de valuation contenant A, et auquel x n'appartient pas).

b) Réciproquement, montrer que, dans un corps K, toute intersection d'anneaux de valuation est un anneau clos (si $x^n = -\sum_{k=0}^{n-1} a_k x^k$, comparer les valuations des deux membres). En déduire que, si A est un anneau d'intégrité quelconque, K son corps des quotients, l'anneau des entiers algèbriques par rapport à A, contenus dans K, est l'intersection des anneaux de valuation contenant A et contenus dans K.

6) Soit A un anneau d'intégrité, $\mathfrak{a}$ un idéal entier de A, $A(\mathfrak{a})$ l'anneau des éléments a/b, où a parcourt A, et b l'ensemble des éléments de A tels que $(b) + \mathfrak{a} = A$. Montrer que si A est clos, $A(\mathfrak{a})$ est clos.

7) a) Soit A un anneau clos, $\mathfrak{P}$ un idéal maximal de A, $\mathfrak{M}$ l'ensemble des anneaux B clos, contenant A et contenus dans le corps des quotients K de A, et tels qu'il existe un idéal maximal $\mathfrak{m}$ de B tel que $\mathfrak{m} \cap A = \mathfrak{P}$. Montrer que $\mathfrak{M}$ a un élément maximal A_o (soit H un ensemble d'indices totalement ordonné, (B_α) une famille d'anneaux de $\mathfrak{M}$ telle que $\alpha \leqslant \beta$ entraîne $B_\alpha \subset B_\beta$, et que, si $\mathfrak{m}_\alpha$ est un idéal maximal de B_α tel que $\mathfrak{m}_\alpha \cap A = \mathfrak{P}$, $\alpha \leqslant \beta$ entraîne $\mathfrak{m}_\alpha \subset \mathfrak{m}_\beta$; montrer que $B = \bigcup_\alpha B_\alpha$ est un anneau clos, et

et $\mathfrak{m} = \bigcup_\alpha \mathfrak{m}_\alpha$ un idéal maximal dans B tel que $\mathfrak{m} \cap A = \mathfrak{p}$; conclure à l'aide du th. de Zorn).

b) Si $\mathfrak{m}_0$ est un idéal maximal de A_0 tel que $\mathfrak{m}_0 \cap A = \mathfrak{p}$, montrer que $A_0(\mathfrak{m}_0) = A_0$, puis en déduire que A_0 est un anneau de valuation (remarquer que, si $x \notin A_0$, et qu'on pose $B = A_0[x]$, on a nécessairement $1 \in B.\mathfrak{m}_0$, et en conclure que $x^{-1} \in A_0$).

c) Soit $\mathfrak{q}$ un idéal premier quelconque de A ; déduire de b) qu'il existe un anneau de valuation B contenant A et contenu dans K, tel que, si $\mathfrak{m}$ est l'unique idéal maximal de B, on ait $\mathfrak{m} \cap A = \mathfrak{q}$ (appliquer b) à l'anneau $A(\mathfrak{q})$).

8) Soit A un anneau clos, K son corps des quotients ; si $f = \sum_k a_k e^k$, $g = \sum_h b_h e^h$ sont deux polynomes de $K[e]$ tels que le produit fg ait tous ses coefficients dans A, tous les produits $a_k b_h$ appartiennent à A (utiliser l'exerc.5 ; w étant une valuation de K, considérer le plus petit indice i tel que $w(a_i)$ soit égal au minimum des $w(a_k)$, le plus petit indice j tel que $w(b_j)$ soit égal au minimum des $w(b_h)$, et calculer la valuation du coefficient de e^{i+j} dans le produit fg).

9) Soit A un anneau d'intégrité, K son corps des quotients ; si A est un sous-anneau maximal de K (c'est-à-dire qu'il n'existe aucun sous-anneau B de K, autre que A et K, tel que $A \subset B \subset K$), montrer que A est un anneau de valuation dont le groupe des idéaux principaux est archimédien (chap.V, § 2 : utiliser l'exerc.4, puis montrer que le groupe totalement ordonné des idéaux principaux de A ne peut contenir aucun sous-groupe épais). Réciproque.

10) On dit qu'un anneau d'intégrité A est <u>complètement clos</u> si le groupe ordonné de ses idéaux principaux est <u>archimédien</u>

(chap.V, § 2 ; c'est-à-dire si, pour un $x \in K$, la relation "il existe $c \in A$ tel que, pour tout entier $n \geqslant 0$, $cx^n \in A$", entraîne $x \in A$). Montrer que tout anneau complètement clos est clos. Réciproquement, si A est un anneau de Noether clos, il est complètement clos (remarquer que si $cx^n \in A$ quel que soit $n \geqslant 0$, le A-module engendré par les x^n est de type fini). Donner un exemple d'anneau de valuation non complètement clos.

11) Si A est un anneau complètement clos, montrer que l'anneau de polynomes $A[e]$ est complètement clos (soit K le corps des quotients de A, f,g,h trois polynomes de $A[e]$ tels que $hf^n/g^n \in A[e]$ quel que soit $n \geqslant 0$; montrer que $f/g = \varphi \in K[e]$; si on pose $\varphi = a_0 e^p + a_1 e^{p-1} + \ldots + a_p$, établir ensuite, par récurrence sur k, que $a_k \in A$).

12) Soit A un anneau complètement clos, K son corps des quotients, E une extension algèbrique de K, B l'anneau des entiers algèbriques par rapport à A, appartenant à E ; montrer que B est complètement clos (soient $\xi \in E$, $\gamma \in B$ tels que $\gamma \xi^n \in B$ quel que soit $n \geqslant 0$; si $e^p + a_1 e^{p-1} + \ldots + a_p$ est le polynome irréductible de $K[e]$ qui a ξ pour racine, et si c est le produit de γ et de ses conjugués, montrer que $ca_i^n \in A$ quel que soit $n \geqslant 0$).

13) Si A est un anneau clos, l'anneau de polynomes $A[e]$ est clos (même méthode que dans l'exerc.11).

14) Soit A un anneau d'intégrité, B un anneau contenant A, dont tous les éléments sont entiers algèbriques par rapport à A. Si $\mathfrak{P}$ est un idéal premier de B tel que $\mathfrak{P} \cap A$ soit un idéal maximal de A, $\mathfrak{P}$ est un idéal maximal de B (raisonner par l'absurde ;

s'il existait un idéal $\mathfrak{a}$ distinct de $\mathfrak{P}$ et de B , et contenant $\mathfrak{P}$, soit x un élément de $\mathfrak{a}$ n'appartenant pas à $\mathfrak{P}$; montrer que x satisfait à une congruence de la forme $x^m+a_1x^{m-1}+\ldots+a_m \equiv 0 \pmod{\mathfrak{P}}$, où les a_i sont des éléments de A tels que $a_m \not\equiv 0 \pmod{\mathfrak{P}}$, et en conclure que $\mathfrak{a} \cap A$ est un idéal distinct de $\mathfrak{P} \cap A$, donc égal à A , d'où contradiction).

15) Montrer que si A est un anneau de Noether clos, K son corps des quotients, E une extension séparable finie de K , B l'anneau des entiers algèbriques par rapport à A , appartenant à E , B est un A-module de type fini, et par suite un anneau de Noether (même raisonnement que dans la prop.8).

16) Etendre le résultat de l'exerc.15 au cas où l'extension E n'est pas séparable, mais où, si on désigne par $A^{1/p}$ l'anneau des racines p-ièmes (p caractéristique de K) des éléments de A , $A^{1/p}$ est un A-module de type fini (considérer l'extension séparable associée à E).

17) Soit A un anneau principal, K son corps des quotients, B un anneau contenant A, formé d'éléments entiers algèbriques par rapport à A , et dont le corps des quotients E soit une extension séparable et finie, de degré n , de K . B admet alors une base (ω_i) $(1 \leqslant i \leqslant n)$ par rapport à A ; si $\omega_i^{(j)}$ $(1 \leqslant j \leqslant n)$ sont les images de ω_i par les n isomorphismes de E par rapport à K , montrer que le déterminant $\boxed{\omega_i^{(j)}}$ n'est pas nul et que son carré appartient à A (remarquer que les ω_i forment une base de E par rapport à K , et les exprimer en fonction d'un élément $\theta \in E$ tel que $E = K\langle\theta\rangle$).

Appendice I

Extensions galoisiennes infinies.

Soit N une extension galoisienne infinie d'un corps K , Γ son groupe de Galois par rapport à K . Nous conserverons les notations introduites au §6 ; en outre, nous désignerons par $\mathfrak{F}$ l'ensemble des extensions finies 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 ; le groupe Γ étant noté multiplicativement, il est clair qu'on a $(\sigma\tau)_F=\sigma_F\tau_F$, et $(\sigma^{-1})_F = (\sigma_F)^{-1}$; si Δ est un sous-groupe quelconque de Γ , on désignera par Δ_F le groupe formé par les σ_F lorsque σ parcourt Δ .

Nous allons définir sur Γ une topologie de groupe (Top.gén., chap.III) qui nous permettra de compléter les résultats du §6 , en donnant la caractérisation du groupe $g(k(\Delta))$ pour tout sous-groupe Δ de Γ .

Proposition 1. Si, pour toute extension finie $F \in \mathfrak{F}$, 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), pour voir qu'ils forment un système fondamental de voisinages de ϵ dans une topologie compatible avec la structure de groupe, de montrer que $\mathfrak{V}$ est une base de filtre, et que pour tout $\sigma \in \Gamma$, $\sigma V_F \sigma^{-1}$ appartient à $\mathfrak{V}$. Or (§6,prop.4), si F_1 et F_2 sont deux extensions finies de K , $V_{F_1} \cap V_{F_2}$ est le sous-groupe $g(F)$, où F est le plus petit sous-corps contenant $F_1 \cup F_2$, qui est évidemment une extension finie. D'autre part (§6,formule (1)), on a $\sigma V_F \sigma^{-1} = V_{\sigma(F)}$, et $\sigma(F) \in \mathfrak{F}$.

Pour montrer que la topologie ainsi définie est séparée, il suffit (Top.gén., chap.III, § 1) de montrer que, pour tout $\sigma \neq \varepsilon$ il existe $F \in \mathfrak{F}$ tel que $\sigma \notin V_F$; or, il existe un $a \in N$ tel que $\sigma(a) \neq a$; si on prend $F = K\langle a \rangle$, on aura donc $\sigma \notin g(F) = V_F$.

Quand nous parlerons, dans ce qui suit, de la topologie de Γ, il s'agira toujours de celle qui est définie par $\mathfrak{V}$.

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 $\gamma \in V_F = g(F)$ tel que $\sigma\gamma \in g(E)$; pour tout $a \in E \cap F$, on a donc $a = \sigma(\gamma(a)) = \sigma(a)$. Or, pour tout $a \in E$, il existe $F \in \mathfrak{F}$ tel que $a \in E \cap F$ (il suffit de prendre $F = K\langle a \rangle$), donc on a $\sigma(a) = a$, ce qui prouve que $\sigma \in g(E)$.

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 finie quelconque, G la plus petite extension galoisienne (finie) contenant F ; σ laissant invariant tout élément de $k(\Delta)$, laisse invariant tout élément de $k(\Delta) \cap G$; or, par rapport à Γ_G, qui n'est autre que le groupe de Galois de G par rapport à K, le corps $k(\Delta) \cap G$ n'est autre que $k(\Delta_G)$; donc, d'après le th. 2 du § 6, on a $\sigma_G \in g(k(\Delta_G)) = \Delta_G$; autrement dit, il existe $\tau \in \Delta$ tel que $\sigma_G = \tau_G$, ou encore que $(\sigma\tau^{-1})_G = \varepsilon_G$, c'est-à-dire $\sigma\tau^{-1} \in g(G) \subset V_F$. On peut écrire $\sigma \in V_F \Delta$, d'où, comme V_F est symétrique, $(\sigma V_F) \cap \Delta \neq \emptyset$, ce qui prouve que σ est adhérent à Δ.

Proposition 4. *Le groupe topologique* Γ *est compact*.

Montrons d'abord que Γ est <u>complet</u>. Pour cela, soit $\mathfrak{F}$ un filtre de Cauchy sur Γ ; pour tout $F \in \mathfrak{F}$, il existe un ensemble H_F de $\mathfrak{F}$ qui soit petit d'ordre V_F ; donc, si $\sigma \in H_F$, $\tau \in H_F$, on a $\sigma\tau^{-1} \in V_F$, autrement dit, quel que soit $x \in F$, $\sigma(x) = \tau(x)$.

Soit alors x un élément quelconque de N ; si on désigne par H_x la réunion des H_F pour toutes les extensions finies telles que $x \in F$, la valeur de $\sigma(x)$ est <u>la même</u> pour tous les $\sigma \in H_x$; désignons cette valeur par $\sigma_0(x)$. Si x et y sont deux éléments quelconques de N , il existe une extension finie F contenant à la fois x et y , donc $\sigma(x+y)=\sigma(x)+\sigma(y)$, $\sigma(xy)=\sigma(x)\sigma(y)$ pour tout $\sigma \in H_F$, ce qui prouve que σ_0 est un endomorphisme de N , et par suite un <u>automorphisme</u> (§ 6,prop.1) ; il est clair par ailleurs que σ_0 , d'après sa définition, est point limite du filtre $\mathfrak{F}$.

Montrons maintenant que Γ est <u>précompact</u>. Soit F une extension finie quelconque de K ; si F_0 est l'extension séparable associée, on a $V_F = V_{F_0}$ (§ 6), donc on peut se borner à considérer le cas où F est séparable. Prouvons alors qu'on peut recouvrir Γ avec un nombre fini d'ensembles petits d'ordre V_F^2 ; d'après l'hypothèse F est une extension simple $K\langle\theta\rangle$; soient θ_i $(1 \leqslant i \leqslant n$, $\theta_1=\theta)$ ses conjugués ; pour tout i , il existe $\sigma_i \in \Gamma$ tel que $\sigma_i(\theta)=\theta_i$. Or, quel que soit $\sigma \in \Gamma$, on a $\sigma(\theta)=\theta_i$ pour un indice i ; donc $\sigma_i^{-1}\sigma \in g(F)=V_F$, ce qui prouve que les n ensembles $\sigma_i V_F$ forment un recouvrement de Γ .

Appendice II.

Extensions algèbriques des corps $\mathfrak{P}$-adiques.

Nous nous proposons d'étudier comment la valuation d'un corps $\mathfrak{P}$-adique K peut se prolonger en une valuation d'une extension algèbrique finie de K . On rappelle (chap.V, Appendice) que K est le corps des quotients d'un anneau principal A , ne possédant qu'un seul idéal premier $\mathfrak{P}=(\pi)$; tout élément $x \in K$ peut s'écrire $x=\varepsilon.\pi^h$, où ε est un diviseur de 1 dans A , et la valuation de K est définie par $w(x)=h$.

Tout polynome de $K[e]$ peut s'écrire sous la forme $\pi^k\varphi$, où φ est un polynome primitif de $A[e]$ (chap.V, § 4). Pour tout polynome $f \in A[e]$, nous désignerons par $\overline{f}$ le polynome qui lui correspond par l'homomorphisme canonique de A sur le corps quotient $A/\mathfrak{P}$.

L'étude des extensions algèbriques de K repose sur le théorème fondamental suivant :

Théorème 1 (critère de réductibilité de Hensel). Soit K un corps $\mathfrak{P}$-adique, f un polynome primitif de $A[e]$; s'il existe deux polynomes g_o, h_o de $A[e]$ tels que $\overline{f}=\overline{g}_o\overline{h}_o$, et que $\overline{g}_o$ et $\overline{h}_o$ soient premiers entre eux, il existe deux polynomes g,h de $A[e]$ tels que $f=gh$, $\overline{g}=\overline{g}_o$, $\overline{h}=\overline{h}_o$.

On peut évidemment toujours supposer que les coefficients de g_o et h_o sont des diviseurs de 1 dans A ; soient m,r,s les degrés respectifs de f, g_o et h_o ; on a donc $r+s \leqslant m$. Nous allons montrer qu'on peut définir par récurrence deux suites $(g_n),(h_n)$ de polynomes de $A[e]$, telles que le degré de g_n soit $\leqslant r$, que celui de h_n soit $\leqslant m-r$, et qu'on ait pour tout $n \geqslant 0$, les congruences $g_{n+1} \equiv g_n \pmod{\mathfrak{P}^{n+1}}$, $h_{n+1} \equiv h_n \pmod{\mathfrak{P}^{n+1}}$, $f \equiv g_n h_n \pmod{\mathfrak{P}^{n+1}}$.

Il est clair alors (chap.V, Appendice) qu'il existe deux polynomes g,h de $A[e]$ tels que $g \equiv g_n \pmod{\mathfrak{P}^n}$, $h \equiv h_n \pmod{\mathfrak{P}^n}$ quel que soit n ; donc $f-gh \equiv 0 \pmod{\mathfrak{P}^n}$ quel que soit n, c'est-à-dire $f=gh$.

Supposons g_n et h_n définis, et cherchons à définir deux polynomes u et v, de degrés respectifs $\leqslant r$ et $\leqslant m-r$, tels que, si on pose $g_{n+1}=g_n+\pi^{n+1}u$, $h_{n+1}=h_n+\pi^{n+1}v$, on ait $f \equiv g_{n+1}h_{n+1} \pmod{\mathfrak{P}^{n+2}}$. Par hypothèse, on peut écrire $g_nh_n-f = \pi^{n+1}r$, où r est un polynome de degré $\leqslant m$; on a donc

$$g_{n+1}h_{n+1}-f \equiv \pi^{n+1}(g_nv+h_nu-r) \pmod{\mathfrak{P}^{n+2}}$$

Il suffit donc que l'on ait

$$\bar{g}_n\bar{v} + \bar{h}_n\bar{u} = \bar{r}$$

ou, comme $\bar{g}_n=\bar{g}_o$, $\bar{h}_n=\bar{h}_o$ par hypothèse, $\bar{g}_o\bar{v} + \bar{h}_o\bar{u} = \bar{r}$. Comme $\bar{g}_o$ et $\bar{h}_o$ sont premiers entre eux par hypothèse, il existe bien deux polynomes $\bar{u}$ et $\bar{v}$, de degrés respectifs $< r$ et $\leqslant m-r$, à coefficients dans le corps $A/\mathfrak{P}$, et satisfaisant à la relation précédente, d'après l'identité de Bezout (chap.V, § 4) ; comme on peut toujours supposer que u et v ont même degré que $\bar{u}$ et $\bar{v}$ respectivement, le théorème est démontré.

Corollaire. Si

$$f = a_oe^n + a_1e^{n-1} + \ldots + a_n$$

est un polynome irréductible de $K[e]$, on a

$$\mathrm{Min}(w(a_o),w(a_1)\ldots,w(a_n)) = \mathrm{Min}(w(a_o),w(a_n)).$$

On peut se borner au cas où f est primitif, donc $\mathrm{Min}(w(a_i))_{1 \leqslant i \leqslant n}=0$. Supposons qu'on ait $w(a_o)>0$, $w(a_n)>0$; il existerait alors un indice k tel que $0<k<n$, et que $w(a_k)=0$, $w(a_i)>0$ pour $i>k$; on aurait donc $f \equiv e^k(a_oe^{n-k} + \ldots + a_k) \pmod{\mathfrak{P}}$, ce qui, d'après le th.1, entraîne la réductibilité de f, contrairement à l'hypothèse.

Théorème 2. Soit E une extension algèbrique finie du corps $\mathfrak{p}$-adique K . Il existe une valuation de E prolongeant la valuation de K .

Soit x un élément quelconque de E , $x^n+a_1x^{n-1}+\ldots+a_n=0$ l'équation irréductible à coefficients dans K dont x est racine ; posons $\overline{w}(x)=(w(a_n))/n$; nous allons montrer que $\overline{w}$ est une valuation de E prolongeant w . Le dernier point étant évident, il suffit d'établir que, si x et y sont deux éléments de E , on a

$$(1) \qquad \overline{w}(xy) = \overline{w}(x) + \overline{w}(y)$$

$$(2) \qquad \overline{w}(x+y) \geqslant \mathrm{Min}(\overline{w}(x),\overline{w}(y))$$

Considérons l'extension $F=K\langle x,y\rangle$ de K ; si m est son degré réduit par rapport à K , on a $\overline{w}(x) = \frac{1}{m} w(N_{F|K}(x))$, $\overline{w}(y) = \frac{1}{m} w(N_{F|K}(y))$, (§ 5), d'où résulte aussitôt l'identité (1). D'autre part, comme $\overline{w}(x+y) = \overline{w}(y)+\overline{w}(1+x/y)$, $\mathrm{Min}(\overline{w}(x),\overline{w}(y)) = \overline{w}(y)+\mathrm{Min}(0,\overline{w}(x/y))$, on peut, pour démontrer (2), se limiter au cas où $y=1$. Mais alors $x+1$ satisfait à une équation irréductible de la forme $(x+1)^n+\ldots+c_n=0$, avec $c_n=a_n-a_{n-1}+\ldots+(-1)^{n-1}a_1+(-1)^n$; donc, d'après le corollaire du th.1

$$\overline{w}(x+1)=w(c_n)/n \geqslant \frac{1}{n}\mathrm{Min}(w(a_n),w(a_{n-1})\ldots,w(a_1),w(1))= \frac{1}{n}\mathrm{Min}(w(a_n),0)$$
$$= \mathrm{Min}(\overline{w}(x),0)$$

ce qui achève la démonstration.

Nous pouvons en déduire le complément suivant au corollaire du th.1 :

Proposition 1. Si $f = e^n+a_1e^{n-1}+\ldots+a_n$ est un polynome irréductible de $K[e]$, on a $w(a_k) \geqslant \frac{k}{n} w(a_n)$.

En effet, soient θ_i $(1 \leqslant i \leqslant n)$ les racines (distinctes ou non) de f ; dans l'extension finie de K qu'elles engendrent, il existe d'après le th.2 une valuation $\overline{w}$ prolongeant w , et telle que $\overline{w}(\theta_i)= \frac{1}{n} w(a_n)$ pour $1 \leqslant i \leqslant n$. Comme a_k est une fonction symétrique homogène de degré k des θ_i , la proposition résulte aussitôt des relations (1) et (2).

Théorème 3. Si E est une extension algèbrique finie d'un corps $\mathfrak{P}$-adique K, il existe une seule valuation de E prolongeant celle de K.

En effet, soit v une valuation de E prolongeant w, et soit x un élément quelconque de E, $x^n+a_1x^{n-1}+\ldots+a_n=0$ l'équation irréductible à coefficients dans K dont x est racine. Si on avait $v(x)>w(a_n)/n$, on en déduirait, d'après la prop.1 $v(a_kx^{n-k})=(n-k)v(x)+w(a_k)>w(a_n)$ pour $0\leqslant k\leqslant n-1$, donc $w(a_n)<\mathrm{Min}(v(a_kx^{n-k}))\leqslant v(x^n+a_1x^{n-1}+\ldots+a_{n-1}x)$, ce qui est absurde. De même, si $v(x)<w(a_n)/n$, on aurait $v(a_kx^{n-k})>v(x^n)$ pour $1\leqslant k\leqslant n$, d'où $v(x^n)<v(a_1x^{n-1}+\ldots+a_n)$, et on obtient encore une contradiction. La valuation de E dont l'existence a été démontrée dans le th.2 est donc unique.

Nous désignerons encore par w la valuation de E prolongeant la valuation w de K ; on notera que w prend ses valeurs dans le groupe $\frac{1}{n}\mathbb{Z}$ si n est le degré de E par rapport à K. L'anneau B des éléments de E tels que $w(x)\geqslant 0$ est identique à l'anneau des entiers algèbriques par rapport à A contenus dans E ; en effet, si x est racine de l'équation irréductible $x^n+a_1x^{n-1}+\ldots+a_n=0$, la condition $w(x)\geqslant 0$ équivaut à $w(a_n)\geqslant 0$, et par suite, d'après le corollaire du th.1, à $w(a_k)\geqslant 0$ pour $1\leqslant k\leqslant n$: autrement dit pour que x appartienne à B, il faut et il suffit que tous les a_k appartiennent à A, d'où la proposition.

On sait (chap.V, Appendice) que B est un anneau principal ne possédant qu'un seul idéal premier $\mathfrak{P}$, ensemble des x tels que $w(x)\geqslant 1/n$. En outre :

Proposition 2. Le corps E est un corps $\mathfrak{P}$-adique.

E, en tant qu'espace vectoriel sur K, a n dimensions. Nous allons montrer que, muni de la structure de groupe additif et de la topologie

définie par w , il est isomorphe au produit de n groupes topologiques identiques au groupe additif de K ce qui établira qu'il est complet, d'où la proposition. Plus généralement, si H est un sous-espace vectoriel à p dimensions de E , nous montrerons que le groupe topologique H est isomorphe à K^p pour $1 \leqslant p \leqslant n$. La proposition est évidente pour p=1 ; nous l'établirons par récurrence sur p . Soit H" un sous-espace vectoriel à p-1 dimensions de H , H' un sous-espace à une dimension supplémentaire de H" dans H ; pour tout $x \in H$, on peut écrire d'une seule manière $x=x'+x"$, avec $x' \in H'$, $x" \in H"$; nous poserons $x'=f(x)$, $x"=g(x)$; tout revient à prouver que f est continue dans H , car il en résulte la continuité de $g(x)=x-f(x)$, puis celle de l'application $x \to (f(x),g(x))$ de H sur le produit $H' \times H"$; l'application réciproque de cette dernière étant $(x',x") \to x'+x"$, donc continue, il en résultera l'isomorphisme annoncé.

Or, soit a un élément $\neq 0$ de H' ; tout $x' \in H'$ s'écrit $x'=\lambda a$, avec $\lambda \in K$. Si f n'était pas continue, il existerait un nombre h tel que, pour tout entier $m > 0$, il existe $x_m \in H$ satisfaisant à $w(x_m) \geqslant m$, $f(x_m) = \lambda_m a$, avec $w(\lambda_m) \leqslant h$; d'où $w(x_m/\lambda_m) \geqslant m-h$, ce qui prouve que la suite (x_m/λ_m) tend vers 0 , donc la suite $(-a+x_m/\lambda_m)$ tend vers -a ; mais cette suite de points appartient à H" , qui est complet par hypothèse, donc fermé dans H ; sa limite ne peut donc être -a , qui n'appartient pas à H" , d'où la contradiction cherchée.

Dans l'annéau B , l'idéal $B_{\mathfrak{P}}$ est égal à une puissance $\mathfrak{P}^e$ de l'idéal premier $\mathfrak{P}$; en outre, si f désigne le degré de $\mathfrak{P}$, c'est-à-dire (§9) le degré du corps $\overline{E}=B/\mathfrak{P}$ par rapport à $\overline{K} = A/\mathfrak{p}$, on a l'inégalité $ef \leqslant n$; si de plus B est un A-module de type fini, ce qui est toujours le cas lorsque E est une extension séparable de K ,

on a $ef=n$. Dans le cas général, on peut préciser un peu les relations entre e,f et n ; tout d'abord $\frac{1}{e}Z$ est le groupe des valeurs de w dans E , donc c'est un sous-groupe de $\frac{1}{n}Z$, ce qui prouve que e *divise* n . D'autre part, soit x un élément quelconque de B , $\bar{x}$ sa classe (mod. $\mathfrak{P}$); soit $f=e^m+a_1e^{m-1}+\ldots+a_m$ le polynome irréductible de $A[e]$ dont x est racine ; $\bar{x}$ est racine du polynome $\bar{f}\in\bar{K}[e]$; comme f est irréductible, $\bar{f}$ est nécessairement une puissance d'un polynome irréductible de $\bar{K}[e]$, en vertu du th.1 ; donc, le degré de $\bar{x}$ par rapport à $\bar{K}$ *divise* le degré de x par rapport à K .

Soit alors E_o l'extension séparable *associée* à E (§ 5), B_o l'anneau des entiers algèbriques contenus dans E_o , $\mathfrak{P}_o$ l'unique idéal premier de B_o (qui est un anneau $\mathfrak{P}_o$-adique d'après la prop.2) ; si n_o est le degré $[E_o:K]$, d l'exposant de E (§ 5), p la caractéristique de K , on a $n=n_op^d$ (§ 5) ; d'autre part, si $\mathfrak{P}=\mathfrak{P}_o^{e_o}$, et si $\mathfrak{P}_o=\mathfrak{P}^{e'}$ on a $e=e_oe'$; enfin, si f_o est le degré de $\mathfrak{P}_o$ par rapport à $\mathfrak{P}$, f' le degré de $\mathfrak{P}$ par rapport à $\mathfrak{P}_o$, on a $f=f_of'$ d'après la définition de ces degrés. En vertu de ce qui précède, on a $n_o=e_of_o$, et le degré d'un élément quelconque de $\bar{E}$ par rapport à $\bar{E}_o=B_o/\mathfrak{P}_o$ divise p^d ; donc f' est une puissance de p divisant p^d ; on en conclut que f *divise* n . Il est immédiat, d'ailleurs que $\bar{E}$ est une extension *radicielle* (§ 5) de $\bar{E}_o$, comme le montre le raisonnement fait ci-dessus pour déterminer le polynome irréductible de $\bar{E}_o[e]$ dont un élément de $\bar{E}$ est racine.

2 Il ne faudrait pas croire, par contre, que $\bar{E}_o$ soit nécessairement une extension séparable de $\bar{K}$, bien que E_o soit une extension séparable de K ; en particulier, il peut se faire que K soit de caractéristique 0, mais $\bar{K}$ de caractéristique $p>0$, et que $\bar{E}_o$ soit une extension inséparable de $\bar{K}$ (voir exerc. 16) .

Extensions galoisiennes d'un corps $\mathfrak{P}$-adique. Bornons-nous à présent au cas où E est une extension galoisienne finie et séparable de K ; soit Γ son groupe de Galois par rapport à K . Il est immédiat alors, d'après les relations entre les polynomes irréductibles dont sont racines un élément $x \in B$ et sa classe $\bar{x} \in \bar{E}$, que $\bar{E}$ est une extension galoisienne de $\bar{K}$; son groupe est déterminé par la proposition suivante:

Proposition 3. Le groupe de Galois de $\bar{E}=B/\mathfrak{P}$ par rapport à $\bar{K}=A/\mathfrak{p}$ est isomorphe au groupe quotient $\Gamma/\mathcal{H}$, où $\mathcal{H}$ est le sous-groupe distingué de Γ formé des automorphismes σ tels que, pour tout $x \in B$, $\sigma(x) \equiv x \pmod{\mathfrak{P}}$.

Soit $\bar{\Gamma}$ le groupe de Galois de $\bar{E}$ par rapport à $\bar{K}$; si σ est un automorphisme de Γ, la relation $x \equiv y \pmod{\mathfrak{P}}$ entraîne $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{P}}$, puisque les valuations de deux éléments conjugués de E sont égales ; donc, à toute classe $\bar{x} \in \bar{E}$ correspond une classe $\bar{\sigma}(\bar{x}) \in \bar{E}$ formée des transformés par σ des éléments de $\bar{x}$; et il est immédiat que $\bar{\sigma}$ est un automorphisme de $\bar{E}$ relatif à $\bar{K}$. On définit ainsi une représentation $\sigma \to \bar{\sigma}$ de Γ dans $\bar{\Gamma}$; en outre, pour que $\bar{\sigma}$ soit l'automorphisme identique de $\bar{\Gamma}$, il faut et il suffit évidemment que $\sigma \in \mathcal{H}$.

Reste à prouver que $\sigma \to \bar{\sigma}$ applique Γ sur $\bar{\Gamma}$; or, soit $K_1=k(\bar{\Gamma})$ le sous-corps de $\bar{E}$ formé des éléments invariants par $\bar{\Gamma}$ (sous-corps qui est distinct de $\bar{K}$, lorsque $\bar{E}$ est une extension inséparable de $\bar{K}$); $\bar{E}$ est alors une extension séparable de K_1 (§ 6, cor.2 du th.1), et $\bar{\Gamma}$ est son groupe de Galois par rapport à K_1. Il existe alors $\bar{\alpha} \in \bar{E}$ tel que $\bar{E}=K_1\langle\bar{\alpha}\rangle$; soit α un élément de la classe $\bar{\alpha}$, f le polynome irréductible dans $A[e]$ dont α est racine, g le polynome irréductible dans $K_1[e]$ dont $\bar{\alpha}$ est racine ; g est un diviseur de $\bar{f}$, donc,

pour tout automorphisme $\sigma' \in \overline{\Gamma}$, il existe un automorphisme $\sigma \in \Gamma$ tel que $\sigma'(\overline{a}) = \overline{\sigma}(\overline{a})$, ce qui entraîne $\sigma' = \overline{\sigma}$, et achève la démonstration.

Le groupe Θ est appelé <u>groupe d'inertie</u> de l'idéal premier $\mathfrak{P}$ par rapport à $\mathfrak{p}$; le sous-corps $T = k(\Theta)$ qui lui correspond dans E est dit <u>corps d'inertie</u> de $\mathfrak{P}$. Comme Θ est un sous-groupe distingué de Γ , T est une extension galoisienne de K , dont le groupe de Galois par rapport à K est isomorphe à Γ/Θ . Si f est le degré de $\overline{E}$ par rapport à $\overline{K}$, f_0 son degré réduit, Γ/Θ est d'ordre f_0 d'après la prop.3, donc $[T:K] = f_0$, puisque E (et a fortiori T) est une extension séparable de K . Soit B_t l'anneau des entiers algèbriques par rapport à A contenus dans T , $\mathfrak{P}_t$ l'unique idéal premier de B_t ; T est un corps $\mathfrak{P}_t$-adique d'après la prop.2 . Si on pose $\overline{T} = B_t/\mathfrak{P}_t$, on a en outre la proposition suivante :

<u>Proposition 4. Dans le corps d'inertie T de $\mathfrak{P}$, on a $B_t\mathfrak{p} = \mathfrak{P}_t$, $\overline{T}$ est l'extension séparable de $\overline{K}$ associée à $\overline{E}$</u> .

En effet, il est évident que le groupe d'inertie de $\mathfrak{P}$ par rapport à $\mathfrak{P}_t$ est identique à Θ ; d'après la prop.3, le groupe de Galois de $\overline{E}$ par rapport à $\overline{T}$ se réduit donc à l'automorphisme identique, ce qui prouve que $\overline{E}$ est une extension radicielle de $\overline{T}$; comme $\overline{T}$ est une extension galoisienne de $\overline{K}$, le groupe de Galois de $\overline{T}$ par rapport à $\overline{K}$ est isomorphe au groupe de $\overline{E}$ par rapport à $\overline{K}$, donc le degré de $\overline{T}$ par rapport à $\overline{K}$ est au moins égal à f_0 ; comme d'autre part, il est $\leqslant [T:K] = f_0$, on a $[\overline{T}:\overline{K}] = f_0$, ce qui prouve que $\overline{T}$ est séparable par rapport à $\overline{K}$, donc est l'extension séparable associée à $\overline{E}$. En outre, comme le degré de l'idéal $\mathfrak{P}_t$ est égal au degré $[T:K]$, $\mathfrak{P}_t$ figure à l'exposant 1 dans la décomposition de $B_t\mathfrak{p}$ dans B_t .

On conclut de cette proposition que $\mathfrak{P}_t = \mathfrak{p}^e$, et que, si $f=f_0 p^r$ (p caractéristique de $\overline{K}$), $\mathfrak{P}$ est de degré p^r par rapport à T ; en particulier, si $p^r=1$ (ce qui sera toujours le cas si $\overline{K}$ est un corps parfait, par exemple s'il est fini, ou de caractéristique 0 ; ou encore si n n'est pas divisible par p), le corps T possède la propriété que, dans T , l'idéal $\mathfrak{p}$ ne se décompose pas, mais devient un idéal premier $\mathfrak{P}_t$ de degré égal à celui de $\mathfrak{P}$; dans E , au contraire, l'idéal $\mathfrak{P}_t$ se décompose en un produit d'idéaux (tous égaux à $\mathfrak{P}$) du premier degré par rapport à T .

On peut se demander si, dans tous les cas, il n'existe pas un corps L ayant cette propriété, c'est-à-dire tel que $[E:L] = e$, $[L:K] = f$ (ou, ce qui revient au même, $\overline{E}=\overline{L}$) ; on peut donner des exemples où il n'en est pas ainsi (voir exerc. 16).

Nous allons nous restreindre dans ce qui suit au cas où $f=f_0$, c'est-à dire au cas où $\overline{E}$ est une extension séparable de $\overline{K}$. Le corps E est alors une extension galoisienne de degré e du corps d'inertie T ; or, si on pose $\mathfrak{P}=(\pi)$, on a $w(\pi)=1/e$, ce qui prouve que π est au moins de degré e par rapport à T ; il en résulte que $E=T\langle\pi\rangle$. Nous allons étudier dans ce cas la structure du groupe d'inertie $\mathfrak{H}$. Pour tout indice $i \geqslant 1$, nous appellerons groupe de ramification d'indice i de l'idéal $\mathfrak{P}$ le sous-groupe Φ_i de $\mathfrak{H}$ formé des automorphismes σ tels que, pour tout $x \in E$, on ait $\sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}}$; il est immédiat que tous ces groupes sont des sous-groupes distingués de Γ .

Proposition 5. Le groupe $\mathfrak{H}/\Phi_1$ est abélien et isomorphe à un sous-groupe du groupe multiplicatif $\overline{E}^*$ des éléments $\neq 0$ de $\overline{E}$.

Pour tout automorphisme $\sigma \in \Theta$, posons $\sigma(\pi)=c_\sigma \pi$; c_σ est un diviseur de 1 dans E , car π et $\sigma(\pi)$ ont même valuation ; montrons que $\sigma \to \bar{c}_\sigma$ ($\bar{c}_\sigma$ classe de c_σ dans $\bar{E}$) est une représentation de Θ dans le groupe multiplicatif $\bar{E}^*$. On a en effet, pour $\tau \in \Theta$, $\sigma(\tau(\pi))=\sigma(c_\tau \pi)=\sigma(c_\tau)c_\sigma \pi$ donc $\bar{c}_{\sigma\tau} = \overline{\sigma(c_\tau)}.\bar{c}_\sigma$; mais comme σ appartient au groupe d'inertie on a $\sigma(c_\tau) \equiv c_\tau \pmod{\mathfrak{P}}$, donc $\bar{c}_{\sigma\tau} = \bar{c}_\sigma.\bar{c}_\tau$. On définit donc un isomorphisme d'un groupe quotient Θ/Ψ de Θ , sur un sous-groupe de $\bar{E}^*$, Ψ étant le sous-groupe de Θ fermé des automorphismes σ tels que $c_\sigma \equiv 1 \pmod{\mathfrak{P}}$, c'est-à-dire $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$; montrons que $\Psi = \Phi_1$. On a évidemment $\Phi_1 \subset \Psi$; d'autre part, tout élément $x \in B$ peut s'écrire $x=a_0+a_1\pi+a_2\pi^2+\ldots+a_{e-1}\pi^{e-1}$, où les $a_i \in T$; comme $w(\pi)=1/e$ et que les $w(a_i)$ sont des entiers rationnels, tous les nombres $w(a_i\pi^i)$ sont distincts, et par suite $w(x)=\mathrm{Min}(w(a_i\pi^i))$, ce qui prouve que les a_i sont entiers algèbriques par rapport à A ; si $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$, on aura donc a fortiori $\sigma(a_i\pi^i)=a_i(\sigma(\pi))^i \equiv a_i\pi^i \pmod{\mathfrak{P}^2}$, d'où $\sigma(x) \equiv x \pmod{\mathfrak{P}^2}$ quel que soit $x \in B$, ce qui établit que $\Psi \subset \Phi_1$. La proposition est démontrée.

<u>Proposition 6</u>. <u>Pour</u> $i \geqslant 1$, <u>le groupe</u> Φ_i/Φ_{i+1} <u>est abélien, et isomorphe à un sous-groupe du groupe additif de</u> $\bar{E}$.

Pour tout automorphisme $\sigma \in \Phi_i$, on a $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$; on peut donc poser $\sigma(\pi)=\pi+b_\sigma.\pi^{i+1}$, où $b_\sigma \in B$; nous allons voir que $\sigma \to \bar{b}_\sigma$ ($\bar{b}_\sigma$ classe de b_σ dans $\bar{E}$) est une représentation de Φ_i dans le groupe additif $\bar{E}$. En effet, on a $\sigma(\tau(\pi)) = \sigma(\pi + b_\tau\pi^{i+1}) = \pi + b_\sigma\pi^{i+1} + \sigma(b_\tau \pi^{i+1})$; or, comme $\sigma \in \Theta$, $\sigma(b_\tau) \equiv b_\tau \pmod{\mathfrak{P}}$, donc $\sigma(\tau(\pi)) \equiv \pi + (b_\sigma+b_\tau)\pi^{i+1} \pmod{\mathfrak{P}^{i+2}}$, ce qui donne $b_\sigma+b_\tau \equiv b_\sigma \pmod{\mathfrak{P}}$, ou encore $\bar{b}_{\sigma\tau} = \bar{b}_\sigma+\bar{b}_\tau$. On montre comme dans la prop.5 que la condition $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+2}}$ est équivalente à $\sigma(x) \equiv x \pmod{\mathfrak{P}^{i+2}}$ pour tout $x \in B$, ce qui établit que le

le sous-groupe de Φ_i formé des σ tels que $b_\sigma \equiv 1 \pmod{\mathfrak{P}}$ est identique à Φ_{i+1}, d'où la proposition.

Il résulte en particulier de la prop.2 que, si $\overline{E}$ a pour caractéristique 0, tous les groupes Φ_i/Φ_{i+1} se réduisent à un seul élément, car il n'existe pas alors de sous-groupe du groupe additif de $\overline{E}$ qui soit fini et ait plus d'un élément ; pour tout automorphisme $\sigma \in \Phi_1$, on a donc $\sigma(x) \equiv x \pmod{\mathfrak{P}^k}$ quel que soit k, ce qui entraîne nécessairement $\sigma(x)=x$, et par suite montre que σ est l'élément neutre de Φ_1 ; autrement dit, dans ce cas, tous les groupes de ramification sont réduits à l'élément neutre.

Le même raisonnement montre d'ailleurs qu'en général, il existe un indice k tel que, pour $i > k$, le groupe Φ_i soit réduit à l'élément neutre.

Application à la divisibilité dans une extension algèbrique. Soit A un anneau de Dedekind, K son corps des quotients, E une extension algèbrique finie de K, B l'anneau des entiers algèbriques par rapport à A contenus dans E. Soit $\mathfrak{p}$ un idéal premier de A, $\mathfrak{P}$ un des diviseurs premiers de $B\mathfrak{p}$ dans B ; si $\mathfrak{P}^e$ est la plus haute puissance de $\mathfrak{P}$ qui divise $B\mathfrak{p}$, $\frac{1}{e} \cdot w_{\mathfrak{P}}$ est une valuation de E qui prolonge la valuation $w_{\mathfrak{p}}$ de K.

Réciproquement, soit v une valuation additive discrète de E qui prolonge $w_{\mathfrak{p}}$; d'après la définition des entiers algèbriques, il est immédiat qu'on ne peut avoir $v(x) < 0$ pour un $x \in B$; donc l'anneau de valuation V correspondant à v contient B, et si $\overline{\mathfrak{P}}$ est l'idéal premier de V, $B \cap \overline{\mathfrak{P}} = \mathfrak{P}$ est un idéal premier de B, et $\overline{\mathfrak{P}} \cap A = \mathfrak{P} \cap A$ est un idéal premier de A, identique à l'ensemble des $x \in A$ tels que $v(x) > 0$, donc identique à $\mathfrak{p}$, ce qui prouve que $\mathfrak{P}$ est un diviseur premier de $B\mathfrak{p}$, et par suite que $v = w_{\mathfrak{P}}/e$.

L'étude des diviseurs premiers de $B_{\mathfrak{P}}$ dans B est donc équivalente à celle des valuations de E qui prolongent la valuation $w_{\mathfrak{P}}$. On peut déterminer ces valuations de la façon suivante :

Soit N la plus petite extension galoisienne de K contenant E ; toute valuation v de E qui prolonge $w_{\mathfrak{P}}$ se prolonge en une valuation de N, et nous pouvons par suite ne considérer que les valuations v de N qui prolongent $w_{\mathfrak{P}}$. Soit N_v le complété de N pour la valuation v ; l'adhérence K_v de K dans N_v est isomorphe au corps $\mathfrak{P}$-adique $K_{\mathfrak{P}}$, d'après l'hypothèse sur v ; en outre, si $N=K\langle a_1,a_2,\dots,a_m\rangle$, on a $N_v=K_v\langle a_1,a_2,\dots,a_m\rangle$; en effet, la valuation induite par v sur $K'=K_v\langle a_1,a_2,\dots,a_m\rangle$ est la seule valuation sur ce corps qui prolonge w (th.3), et pour cette valuation, K' est complet (prop.2), donc fermé dans N_v ; comme il contient N, qui est partout dense dans N_v, $K'=N_v$. Considérons alors, dans l'extension algèbriquement stable Ω du corps $\mathfrak{P}$-adique $K_{\mathfrak{P}}$, l'unique extension galoisienne N' de K isomorphe à N ; si M' est l'extension galoisienne de $K_{\mathfrak{P}}$ égale à $K_{\mathfrak{P}}\langle N'\rangle$, il existe un isomorphisme φ de N_v sur M', laissant invariants tous les éléments de K, et tel que, si w est l'unique valuation de M' prolongeant la valuation $w_{\tilde{\mathfrak{P}}}$ de $K_{\mathfrak{P}}$, on ait $w(\varphi(x))=v(x)$ quel que soit $x\in N$, et en particulier pour tout $x\in E$. On obtient donc <u>toutes</u> les valuations cherchées en considérant les divers isomorphismes φ de N (relatifs à K) sur N', et en prenant $v(x)=w(\varphi(x))$.

Cherchons maintenant à quelle condition deux isomorphismes distincts φ, ψ de N sur N' donnent la <u>même</u> valuation sur E ; on peut écrire $\psi=\sigma'\circ\varphi$, où σ' est un automorphisme de N' (relatif à K) ; tout revient à voir à quelle condition on a $w(x)=w(\sigma'(x))$ pour tout $x\in\varphi(B)$. Soit $x^n+a_1x^{n-1}+\dots+a_n=0$ l'équation irréductible <u>dans</u> $K_{\mathfrak{P}}$ à laquelle

satisfait x ; pour tout $k>0$, il existe $b_{1k},b_{2k},\dots,b_{nk}$ appartenant à K et tels que $w(a_i-b_{ik})\geqslant k$, d'où $w(x^n+b_{1k}x^{n-1}+\dots+b_{nk})\geqslant k$. Si on pose $y=\sigma'(x)$, on a donc (puisque les b_{ik} qui appartiennent à K , sont invariants par σ'), $w(y^n+b_{1k}y^{n-1}+\dots+b_{nk})\geqslant k$; en faisant croître k indéfiniment, et passant à la limite, il vient $y^n+a_1y^{n-1}+\dots+a_n=0$, autrement dit x et $y=\sigma'(x)$ sont <u>conjugués par rapport à</u> $K_\wp$. Réciproquement, si un automorphisme σ' de N' transforme tout élément $x\in\varphi(B)$ en un conjugué de x par rapport à $K_\wp$, on a , avec les mêmes notations $w(x)=\frac{1}{n}w(a_n)=w(\sigma'(x))$, ce qui prouve que la condition obtenue est nécessaire et suffisante pour que φ et ψ donnent la même valuation sur E .

On déduit de là toutes les valuations distinctes de E qui prolongent $w_\wp$: supposons d'abord que E soit une extension séparable de K ; on a donc $E=K\langle\theta\rangle$; soit f le polynome irréductible de $K[e]$ dont θ est racine ; dans l'anneau $K_\wp[e]$, le polynome f se décompose en un produit de facteurs irréductibles distincts (E étant séparable), $f=f_1f_2\dots f_g$; pour qu'un automorphisme σ' de N' laisse invariante la valuation w sur l'image $\varphi(E)$ du corps E par un isomorphisme φ de N sur N', il faut, d'après ce qui précède, que $\theta'=\varphi(\theta)$ et $\sigma'(\theta')$ soient racines du même polynome f_i , et cette condition est évidemment suffisante, puisque θ' engendre $\varphi(E)$; donc le nombre des valuations distinctes de E qui prolongent $w_\wp$ est égal au <u>nombre des facteurs irréductibles</u> de f dans $K_\wp[e]$.

Il est clair, d'autre part, que toute valuation w d'un corps imparfait K se prolonge d'une seule manière à une extension <u>radicielle</u> E de K : tout élément $x\in E$ satisfait à une équation $x^{p^r}-a=0$, avec $a\in K$, donc $w(x)=p^{-r}w(a)$. Pour avoir toutes

les valuations (prolongeant $w_{\mathfrak{P}}$) d'une extension inséparable finie E de K ; il suffit donc d'avoir toutes les valuations (prolongeant $w_{\mathfrak{P}}$) de l'extension séparable associée E_0 ; la question est donc résolue par le résultat précédent, pour toute extension finie de K .

Considérons en particulier le cas où E=N est une extension galoisienne de K . Soit v une des valuations de N prolongeant $w_{\mathfrak{P}}$, φ un des isomorphismes de N sur N' qui donnent v ; si ψ est un autre isomorphisme de N sur N' donnant la valuation v , on peut écrire $\psi = \varphi \circ \sigma$, où σ est un automorphisme de N relatif à K ; d'après ce qui précède, σ laisse en particulier invariants tous les éléments du corps $D_v = \varphi^{-1}(N' \cap K_{\mathfrak{P}})$; réciproquement, si σ satisfait à cette condition, pour tout $x \in N$, $\sigma(x)$ est conjugué de x par rapport à D_v , donc $\varphi(x)$ et $\psi(x)$ sont conjugués par rapport à $K_{\mathfrak{P}}$, et par suite $w(\varphi(x))=w(\psi(x))$, ou encore $v(x)=v(\sigma(x))$. On voit donc que les automorphismes de N relatifs à K qui laissent invariante une valuation v de N (prolongeant $w_{\mathfrak{P}}$) sont les automorphismes du sous-groupe $\Delta_v = g(D_v)$ du groupe de Galois Γ de N , correspondant au sous-corps D_v de N . Par ailleurs, toute valuation v' de N prolongeant $w_{\mathfrak{P}}$ est, d'après ce qui précède, de la forme $v'(x)=v(\sigma(x))$, où σ est un automorphisme de Γ ; donc le nombre g des valuations distinctes de N prolongeant $w_{\mathfrak{P}}$ est égal à l'indice $(\Gamma : \Delta_v)$ du sous-groupe Δ_v . On sait que toute valuation de N prolongeant $w_{\mathfrak{P}}$ est une valuation $\mathfrak{P}$-adique, correspondant à un diviseur premier $\mathfrak{P}$ de $B\mathfrak{P}$ dans B ; deux valuations distinctes correspondent d'ailleurs à deux diviseurs premiers distincts, sans quoi elles seraient proportionnelles, et comme elles coïncident dans K , elles seraient identiques. Soient donc $v_1=v, v_2, \ldots, v_g$ les g valuations distinctes de N ,

correspondant aux g facteurs premiers distincts $\mathfrak{P}_1 = \mathfrak{P}, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ de $B\mathfrak{p}$. Les automorphismes du groupe Δ_v sont tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$ et, pour tout indice i , il existe un automorphisme σ_i du groupe Γ tel que $\sigma_i(\mathfrak{P}) = \mathfrak{P}_i$, les σ_i $(1 \leqslant i \leqslant g)$ formant un système de représentants des g classes à gauche de Γ suivant Δ_v ; le groupe Δ_v peut donc être défini comme formé des automorphismes σ tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$; on l'appelle <u>groupe de décomposition</u> de l'idéal $\mathfrak{P}$, le corps D_v s'appelant <u>corps de décomposition</u> de ; le groupe de décomposition de $\mathfrak{P}_i$ est alors $\sigma_i \Delta_v \sigma_i^{-1}$, et le corps de décomposition de $\mathfrak{P}_i$ est $\sigma_i(D_v)$; les groupes de décomposition (resp. corps de décomposition) des divers idéaux $\mathfrak{P}_i$ sont en général distincts.

Comme l'idéal $B\mathfrak{p}$ est invariant par tout automorphisme du groupe Γ, l'exposant auquel figure $\mathfrak{P}_i$ dans $B\mathfrak{p}$ est égal à l'exposant e auquel figure $\mathfrak{P}$; autrement dit, on a la formule

$$B\mathfrak{p} = (\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_g)^e \tag{3}$$

En outre, par passage aux quotients, l'isomorphisme σ_i donne un isomorphisme du corps $B/\mathfrak{P}$ sur le corps $B/\mathfrak{P}_i$, donc tous les idéaux premiers $\mathfrak{P}_i$ ont <u>même degré</u> f par rapport à K , et on a l'inégalité $efg \leqslant n$, avec $efg = n$ lorsque B est un A-module de type fini.

Le nom de "corps de décomposition" provient de l'étude de la décomposition de l'idéal $\mathfrak{p}$ dans le corps D_v ; bornons-nous pour l'étudier au cas où N (et par suite D_v) est une extension séparable de K . Alors D_v est de degré g par rapport à K , et on a $D_v = K\langle\theta\rangle$, où θ est racine d'un polynome irréductible f de degré g de $K[\theta]$; soit φ un des isomorphismes de N sur N' donnant la valuation v ; comme $\varphi(D_v) \subset K_{\mathfrak{p}}$, $\varphi(\theta)$ est racine d'un facteur du premier degré de f dans la décomposition de ce polynome dans l'anneau $K_{\mathfrak{p}}[\theta]$; il en résulte que les valuations

$v_2,\dots,v_g$ induisent sur D_v des valuations distinctes de v ; autrement dit, si E_v est l'anneau des entiers algèbriques contenus dans D_v, l'idéal $B_v\mathfrak{P}$ peut se mettre sous la forme $\mathfrak{P}_v^r\mathfrak{a}$, où $\mathfrak{P}_v$ est un idéal premier de B_v tel que $B\mathfrak{P}_v$ soit une puissance de $\mathfrak{P}$, et où $\mathfrak{a}$ est premier avec $\mathfrak{P}_v$. En outre, on a $r=1$, car le prolongement w de $w_{\mathfrak{P}}$ ne prend que des valeurs entières dans $K_{\mathfrak{P}}$. Enfin, le corps $B_v/\mathfrak{P}_v$ contient $A/\mathfrak{P}$ et est contenu dans $A_{\mathfrak{P}}/\tilde{\mathfrak{P}}$; comme des deux derniers corps sont identiques (chap.V Appendice), $B_v/\mathfrak{P}_v$ leur est identique, autrement dit, l'idéal $\mathfrak{P}_v$ est du premier degré par rapport à K. Ainsi le passage de K au corps de décomposition D_v a pour effet de faire apparaître, dans $\mathfrak{P}$, la puissance $\mathfrak{P}^e$ de l'idéal $\mathfrak{p}$ qui le divise, l'idéal $\mathfrak{P}^e\cap D_v$ étant un idéal premier de B_v, qui reste du premier degré par rapport à K.

Lorsque σ parcourt les automorphismes du groupe de décomposition Δ_v, $\sigma'=\varphi\circ\sigma\circ\varphi^{-1}$ parcourt les automorphismes du groupe de Galois de N' par rapport à $N'\cap K_{\mathfrak{P}}$; ces automorphismes ne sont autres que les restrictions à N' des automorphismes de M' par rapport à $K_{\mathfrak{P}}$ (§6,prop.8) ; le groupe Δ_v est donc isomorphe au groupe de Galois de M' par rapport à $K_{\mathfrak{P}}$. Soit $\tilde{\mathfrak{P}}$ l'idéal premier correspondant à la valuation w de M' ; aux automorphismes σ' du groupe d'inertie Θ de l'idéal $\tilde{\mathfrak{P}}$ par rapport à l'idéal premier $\tilde{\mathfrak{P}}$ de $K_{\mathfrak{P}}$ correspondent des automorphismes $\sigma\in\Delta_v$ tels que $\sigma(x)\equiv x \pmod{\mathfrak{P}}$ quel que soit $x\in N$; réciproquement, si σ a cette propriété on a $\sigma'(x)\equiv x \pmod{\tilde{\mathfrak{P}}}$ pour tout $x\in N'$, et, en vertu de la continuité de σ' pour la topologie $\tilde{\mathfrak{P}}$-adique, $\sigma'(x)\equiv x \pmod{\tilde{\mathfrak{P}}}$ pour tout $x\in M'$; donc les automorphismes σ ayant la propriété précédente forment un sous-groupe distingué Θ_v de Δ_v isomorphe à Θ, et qu'on appelle

encore <u>groupe d'inertie</u> de $\mathfrak{P}$ par rapport à $\mathfrak{p}$. Le sous-corps $T_v=k(\Theta_v)$ qui lui correspond dans N est encore appelé <u>corps d'inertie</u> de $\mathfrak{P}$ par rapport à $\mathfrak{p}$. L'étude de la décomposition de $\tilde{\mathfrak{p}}$ dans le corps d'inertie T de $\tilde{\mathfrak{P}}$ s'étend aussitôt à la décomposition de $\mathfrak{p}_v$ dans T_v : l'idéal $B_t\mathfrak{P}_v=\mathfrak{P}_t$ est un idéal premier dans B_t (anneau des entiers algèbriques appartenant à T_v) ; le corps $B_t/\mathfrak{P}_t$ est l'extension séparable de $B_v/\mathfrak{P}_v$ associée à $B/\mathfrak{P}$; on a $B\mathfrak{p}_t=\mathfrak{P}^e$; enfin, si $B/\mathfrak{P}$ est une extension séparable de $B_v/\mathfrak{p}_v$, $\mathfrak{P}$ est un idéal du premier degré par rapport au corps d'inertie T_v .

De même, aux automorphismes σ' du <u>groupe de ramification</u> Φ_i de l'idéal $\tilde{\mathfrak{P}}$ par rapport à $\tilde{\mathfrak{p}}$, correspondent les automorphismes $\sigma\in\Theta_v$ tels que $\sigma(x)\equiv x \pmod{\mathfrak{P}^{i+1}}$, et réciproquement ; les automorphismes σ ayant cette propriété forment un sous-groupe distingué $\Phi_i^{(v)}$ de Θ_v , isomorphe à Φ_i , et qu'on appelle encore <u>groupe de ramification d'indice i</u> de $\mathfrak{P}$ par rapport à $\mathfrak{p}$.

<u>Exercices</u>. 1) Soit K un corps complet pour la topologie définie par une valuation réelle quelconque v sur K (chap.V, Appendice, exerc.8) ; soit A l'anneau de valuation correspondant (ensemble formé des $x\neq 0$ tels que $v(x)\geqslant 0$, et de 0), $\mathfrak{p}$ l'idéal maximal ~~Kxkaxkh~~ de A formé de 0 et des x tels que $v(x)>0$.

a) Généraliser à K le th.1 (remplacer l'élément π qui figure dans la démonstration de ce théorème, par un élément dont la valuation soit >0 , mais assez petite).

b) Soient f_1, f_2 deux polynomes de $A[e]$ de la forme $f_1=x^n+a_{11}x^{n-1}+\ldots+a_{n1}$, $f_2=x^n+a_{12}x^{n-1}+\ldots+a_{n2}$, tels que $v(a_{i1}-a_{i2})\geqslant s>0$ pour $1\leqslant i\leqslant n$, et que $f_1=g_1h_1$, $f_2=g_2h_2$ avec $\bar{g}_1=\bar{g}_2$, $\bar{h}_1=\bar{h}_2$, $\bar{g}_1$ et $\bar{h}_1$ étant premiers entre eux dans $\bar{K}[e]$ ($\bar{K}=A/\mathfrak{p}$) : montrer que les coefficients des polynomes

g_1-g_2 , h_1-h_2 ont tous des valuations $\geqslant s$ (suivre le raisonnement du th.1, en utilisant l'unicité des polynomes figurant dans l'identité de Bezout, quand on suppose leurs degrés minimaux).

c) En déduire en particulier que, dans a), les polynomes g et h , facteurs de f , sont déterminés à des facteurs diviseurs de 1 près.

2) K étant un corps qui satisfait aux hypothèses de l'exerc.1, généraliser les th.2 et 3 à une extension algèbrique quelconque (finie ou non) E de K . Si E est une extension finie de K , E est complet pour la valuation (unique) qui prolonge v (et qu'on note encore v).

Soit B l'anneau de valuation correspondant à v dans E , $\mathfrak{P}$ l'idéal maximal de B. Le corps $\overline{E}=B/\mathfrak{P}$ est une extension de $\overline{K}=A/\mathfrak{p}$; si E est une extension de degré n de K , $\overline{E}$ est une extension finie de $\overline{K}$, et le degré de tout élément de $\overline{E}$ par rapport à $\overline{K}$ est un diviseur de n (utiliser 1a)).

Soit Λ_K le sous-groupe $v(K^*)$ de R , Λ_E le sous-groupe $v(E^*)$; l'ordre de tout élément du groupe quotient Λ_E/Λ_K est un diviseur de n .

Si $f=\left[\overline{E}:\overline{K}\right]$, $e=(\Lambda_E:\Lambda_K)$, on a $ef\leqslant n$ (soient $a_1,a_2,\ldots,a_f$ des éléments de B dont les classes (mod. $\mathfrak{P}$) forment une base vectorielle de $\overline{E}$ par rapport à $\overline{K}$; soient $b_1,b_2,\ldots,b_e$ des éléments de B dont les valuations appartiennent aux e classes distinctes de Λ_E (mod. Λ_K) ; prouver que les éléments a_ib_j de E forment un système libre par rapport à K).

3) Avec les notations de l'exerc.2, on suppose que E est une extension galoisienne finie et séparable de K ; généraliser les prop.3 et 4 (pour montrer que $\Lambda_T=\Lambda_K$, on utilisera

l'inégalité $ef \leqslant n$ démontrée dans l'exerc.2). Déduire de l'exerc.2 que, si n n'est pas divisible par la caractéristique p de $\overline{K}$, on a $\overline{T}=\overline{E}$.

4) Avec les notations de l'exerc.2, on suppose que E est une extension séparable de degré n de K, telle que $\overline{E}=\overline{K}$, et que n ne soit pas divisible par la caractéristique de $\overline{K}$.

a) Soit a un élément de B, m l'ordre de la classe de $v(a)$ dans le groupe quotient Λ_E/Λ_K ; montrer qu'il existe $a \in A$ tel que $mv(a)=v(a)$ et $v(a^m-a)>v(a)$. En déduire qu'il existe $x \in B$ tel que $x^m=a$ (raisonner comme dans l'exerc. 1a) en remarquant, d'après l'exerc.2, que m n'est pas divisible par la caractéristique de $\overline{K}$).

b) Si $\Lambda_E=\Lambda_K$, montrer que $n=1$ (raisonner par l'absurde, en prouvant qu'il ne peut alors y avoir d'élément de E satisfaisant à une équation irréductible de la forme $x^m+a_2x^{m-2}+\ldots+a_m=0$, à coefficients dans A, et tels que $v(a_m)=0$).

c) Déduire de a) et b) que l'indice $(\Lambda_E:\Lambda_K)$ est égal à n (décomposer Λ_E/Λ_K en produit direct de groupes cycliques, et à l'aide de a), former une extension F de K de degré égal à $(\Lambda_E:\Lambda_K)$, telle que $F \subset E$ et $\Lambda_F=\Lambda_E$; déduire de b) que $F=E$).

5) a) Soit E une extension galoisienne séparable et de degré n de K (les notations étant celles de l'exerc.2) ; montrer que, si n n'est pas divisible par la caractéristique p de $\overline{K}$, on a $ef=n$ (utiliser les exerc. 3 et 4c)).

b) Si E est une extension quelconque de degré n de K, ef divise n, et n/ef est une puissance de la caractéristique p de $\overline{K}$ (considérer d'abord le cas où n n'est pas divisible par p, et montrer qu'alors $ef=n$, en utilisant a) ; ensuite le cas où E est une extension galoisienne séparable de K ; former alors une extension F de K telle que

$E \supset F$, que $[F:K]$ soit premier avec p , et $[E:F]$ une puissance de p ; passer de là au cas où E est une extension séparable quelconque de K , et enfin au cas général, en étudiant le cas des extensions radicielles, à l'aide de l'exerc.2).

6) Soit E une extension galoisienne de degré n de K , telle que n ne soit pas divisible par la caractéristique de $\overline{K}$. Soit Φ le sous-groupe du groupe d'inertie Θ formé des automorphismes σ tels que $v(\sigma(x)-x) > v(x)$ quel que soit $x \in B$. Montrer que, si Λ_E/Λ_K est un groupe abélien de rang r (en tant que $\mathbb{Z}$ -module), le groupe Θ/Φ est isomorphe à un sous-groupe du groupe produit $(\overline{E}^*)^r$ (raisonner comme dans la prop.5, en utilisant l'exerc. 2 et l'ex.5a)).

7) Soit K' le corps obtenu par adjonction au corps 2-adique $\mathbb{Q}_2$ des racines de tous les polynomes $e^{2^n}-2$, v la valuation sur K' prolongeant la valuation 2-adique de $\mathbb{Q}_2$, K le complété de K' pour la valuation v . Montrer que le polynome e^2-3 est irréductible dans $K[e]$, et que, si E est le corps des racines de ce polynome, on a (avec les notations de l'exerc.2) $e=f=1$ et $n=2$, bien que E soit une extension séparable de K (pour prouver que $e=1$, remarquer que, si $z \in \Lambda_K$, $z/2 \in \Lambda_K$) .

8) a) Soit K un corps complet pour une valuation réelle v , et soit $f=e^n+a_1e^{n-1}+..+a_n$ un polynome de $A[e]$, dont toutes les racines sont distinctes. Montrer que, si α est un élément tel que $v(\alpha)>0$, et g un polynome quelconque de degré n de $A[e]$, on peut déterminer k assez grand pour que, si $x_1,x_2,..,x_n$ sont les racines de f , $y_1,y_2,\dots,y_n$ celles de $f+\alpha^k g$, $y_1,y_2,..,y_n$ soient distinctes et telles que $v(x_i-y_i)$ soit aussi grand qu'on veut pour $1 \leqslant i \leqslant n$ (raisonner en se plaçant dans l'extension finie de K déterminée par les x_i et y_i ; procéder par récurrence sur n , en faisant un changement de variable qui permette d'appliquer l'exerc. 1b)).

b) Etendre le résultat précédent au cas où les racines de f ne sont pas toutes distinctes (montrer que, dans ce cas pour toute valeur de k, on peut déterminer un polynome f_1 tel que $f+a^k f_1$ ait toutes ses racines distinctes).

c) Déduire de b) que, si K est un corps algèbriquement stable muni d'une valuation réelle v, le complété K_v de K correspondant à cette valuation est algèbriquement stable (dans l'extension finie de K_v déterminée par les racines d'un polynome de $K_v[e]$, montrer que ces racines sont adhérentes à K).

d) Si K est un corps de caractéristique p complet pour une valuation v, et tel que tout polynome séparable de $K[e]$ ait toutes ses racines dans K, K est algèbriquement stable (utiliser b)).

9) a) Avec les notations de l'exerc. 8a), montrer que, si f est séparable et irréductible dans $A[e]$, il en est de même de $f+a^k g$ pour k assez grand (en considérant l'extension galoisienne de K déterminée par les racines de f et $f+a^k g$, remarquer qu'un même automorphisme de cette extension permute de la même manière les x_i et les y_i dès que k est assez grand, en s'appuyant sur le fait qu'un tel automorphisme conserve la valuation et en utilisant 8a)). Plus généralement, si $f = \prod_{i=1}^{r} f_i$ est la décomposition de f en facteurs premiers dans $A[e]$ (facteurs distincts et séparables, puisque f est supposé séparable), la décomposition de $f+a^k g$ est de la forme $\prod_{i=1}^{r} g_i$, où g_i est de même degré que f_i (décomposition "du même type" que f).

b) Si $v(a) \leqslant 0$, et si k est tel que $f+a^k g$ ait une décomposition du même type que f dans $K[e]$, $a^n f(e/a)+a^k g$ a aussi une décomposition du même type que f, quel que soit le polynome $g \in A[e]$ de degré n.

c) Soient v_1, v_2 deux valuations réelles sur un corps K, K_1, K_2 les complétés de K pour les topologies correspondantes. Soit f un polynome séparable de degré n de $K_1[e]$, g un polynome séparable de degré n de $K_2[e]$. Si v_1 et v_2 ne sont pas des valuations équivalentes (c'est-à-dire si les anneaux de valuation correspondants sont distincts), il existe un polynome $h \in K[e]$ qui, dans $K_1[e]$, ait une décomposition du même type que f, et dans $K_2[e]$, une décomposition du même type que g (se ramener au cas où f et g ont leurs coefficients dans K et le coefficient de e^n égal à 1 ; considérer le polynome $a^n f(e/a)+b^n g(e/b)-e^n$, où a est un élément de K tel que $v_1(a) \leqslant 0$, $v_2(a)$ positif et arbitrairement grand, b un élément de K tel que $v_1(b)$ soit arbitrairement grand (cf. chap. V, Appendice, ex. 1); appliquer a) et b)).

d) Déduire de c) que, si K est complet pour la valuation v_1, K_2 est algèbriquement stable (prendre pour f un polynome irréductible, pour g un produit de n facteurs distincts du premier degré ; utiliser l'exerc. 8d)).

e) Si K est un corps $\mathfrak{o}$-adique, il n'existe aucune valuation réelle v sur K, non équivalente à la valuation $\mathfrak{o}$-adique, et telle que K soit complet pour v (remarquer que si $\mathfrak{o}=(\pi)$, l'équation $x^n-\pi=0$ est irréductible dans K, et par suite que K n'est pas algèbriquement stable).

10) Soit K un corps complet pour une valuation réelle v. Si E est une extension algèbrique infinie séparable de K, montrer que E n'est pas complet pour la valuation prolongeant v (former une suite (x_p) d'éléments de E, telle que le degré n_p de x_p par rapport à K

croisse indéfiniment, et que $v(x_{p+1}-x_p)$ soit supérieure aux valuations des différences de x_p et de tous ses conjugués par rapport à K ; montrer que la suite (x_p) ainsi formée est une suite de Cauchy non convergente dans E).

11) Soit K un corps muni d'une valuation réelle v (ou d'une valuation impropre v , c'est-à-dire une fonction prenant la valeur 0 en tout élément de K^*).

a) Soit $E=K\langle\theta\rangle$ une extension transcendante simple de K : on définit sur E une valuation réelle prolongeant v en posant $v(\theta)=a$, où a est un nombre réel quelconque, puis, si $x=f(\theta)=a_0+a_1\theta+\ldots+a_n\theta^n$ est un polynome en θ à coefficients dans K , $v(x)=\mathrm{Min}(v(a_k)+ka)_{0\leqslant k\leqslant n}$.

b) Réciproquement, si une valuation v sur E prolonge la valuation v sur K et est telle qu'aucun multiple entier de $v(\theta)=a$ n'appartienne au groupe $v(K^*)$, v est identique à la valuation définie dans a).

c) Déduire de a) que tout corps K possède au moins une valuation réelle, à l'exception des extensions algèbriques des corps premiers de caractéristique $\neq 0$. Si K est une extension algèbrique finie d'une extension transcendante pure du corps premier contenu dans K , K possède une valuation discrète au moins.

12) Soit E une extension algèbrique finie d'une extension transcendante pure, de degré de transcendance fini n , d'un corps quelconque K . Soit v une valuation réelle sur E , telle que $v(x)=0$ pour tout élément $x\in K^*$.

a) Montrer que le groupe $v(E^*)$ est un $\mathbb{Z}$-module de rang $\leqslant n$ (raisonner par l'absurde).

b) Si $v(E^*)$ est de rang n , il est isomorphe au groupe $\mathbb{Z}^n$ (considérer une base de transcendance $(x_i)_{1\leqslant i\leqslant n}$ de E , telle que les éléments $v(x_i)$ forment un système libre dans le $\mathbb{Z}$-module $v(E^*)$;

si $F=K\langle x_1,x_2,..,x_n\rangle$, montrer que $v(F^*)$ est isomorphe à $\mathbb{Z}^n$, et montrer que $v(E^*)$ est un $\mathbb{Z}$-module de type fini en utilisant le fait que E est une extension algèbrique finie de F).

13) Soit K un corps complet pour une valuation réelle v ; soit $\overline{K}$ le corps $A/\mathfrak{P}$, où A est l'anneau de valuation correspondant à v, $\mathfrak{P}$ son unique idéal maximal. On suppose que K et $\overline{K}$ ont <u>même caractéristique</u>.

a) Montrer qu'il existe un sous-corps K_0 de K contenu dans A, et tel que l'application canonique de A sur $\overline{K}$ soit un isomorphisme de K_0 sur $\overline{K}$ (montrer que si un sous-corps H de A est tel que l'application canonique de A sur $\overline{K}$ soit un isomorphisme de H sur un sous-corps $\overline{H}$ de $\overline{K}$ distinct de $\overline{K}$, il existe une extension simple de H contenue dans A et ayant la même propriété ; examiner séparément le cas où $\overline{K}$ est une extension transcendante ou une extension algèbrique de $\overline{H}$; dans ce dernier cas, utiliser l'exerc. 1a) ; conclure en utilisant le th. de Zorn).

b) Si K est un corps $\mathfrak{P}$-adique, montrer que K est isomorphe au corps des séries formelles d'une lettre $S_1(K_0)$ (cf.chap.V,Appendice).

14) Soit K un corps $\mathfrak{P}$-adique de caractéristique 0, tel que, si A est l'anneau des entiers $\mathfrak{P}$-adiques, $\overline{K}=A/\mathfrak{P}$ ait une caractéristique $p>0$; on a alors, dans K, $(p)=\mathfrak{P}^r$, où r est un entier >0.

a) Montrer que, dans K, la congruence $a\equiv b \pmod{\mathfrak{P}^h}$ entraîne $a^{p^n}\equiv b^{p^n} \pmod{\mathfrak{P}^{h+n}}$.

b) En déduire que, si $\overline{K}$ est un corps parfait, $\overline{x}$ un élément $\neq 0$ de $\overline{K}$, a_n un élément quelconque de la classe $\overline{x}^{p^{-n}}$, la suite $(a_n^{p^n})$ converge vers un élément $\varphi(\overline{x})$ de K, indépendant de l'élément a_n choisi dans $\overline{x}^{p^{-n}}$.

c) Montrer que φ est un isomorphisme du groupe multiplicatif $\overline{K}^*$ dans le groupe multiplicatif K^*, et que c'est le seul.

15) Soit K un corps $\mathfrak{P}$-adique, E une extension de degré n de K telle que $\overline{E}=\overline{K}$ (notations du texte) ; si $\mathfrak{P}=(\pi)$, $\mathfrak{p}=(\overline{\omega})$, montrer que l'équation irréductible à coefficients dans K à laquelle satisfait $\overline{\omega}$ est de la forme $x^n+\pi(a_{n-1}x^{n-1}+\dots+a_1x+a_0)=0$, où $w_{\mathfrak{P}}(a_i)\geqslant 0$ pour $1\leqslant i\leqslant n-1$, et $w_{\mathfrak{P}}(a_0)=0$ (on a nécessairement $\varepsilon\pi=\overline{\omega}^m$, où ε est diviseur de 1 dans E, et m un entier >0 ; déduire de la représentation de tout élément de E en série de puissances de $\overline{\omega}$ (chap.V, Appendice) que les puissances $\overline{\omega}^k$ pour $0\leqslant k\leqslant m-k$ forment une base vectorielle de E par rapport à K, donc que $m=n$ et $E=K\langle\overline{\omega}\rangle$; exprimer ensuite ε à l'aide de cette base vectorielle).

Réciproque.

16) Soit K' l'extension transcendante simple $Q_2(e)$ du corps 2-adique Q_2, dans lequel on prolonge la valuation 2-adique v de Q_2 suivant le procédé de l'exerc.11a), en posant $v(e)=0$; soit K le complété de K' pour cette valuation. Soit E la plus petite extension galoisienne de K contenant une racine de l'équation $(x^2-e)^2-2=0$. Montrer (avec les notations du texte) qu'on a pour cette extension, $n=8$, $e=4$, $f=2$, $f_0=1$, que $\overline{E}$ est une extension radicielle de $\overline{K}$ et qu'il n'existe aucune extension F de K telle que $[E:F]=e$ et $\overline{F}=\overline{E}$ (une telle extension serait nécessairementd de la forme $K\langle\sqrt{\alpha}\rangle$, où $\alpha\in K$ serait tel que $\alpha\equiv e \pmod 2$; déduire de là une contradiction, en exprimant $\sqrt{\alpha}$ à l'aide d'une base vectorielle de E par rapport à K, et en montrant que e n'est pas un carré dans $\overline{K}$).
