Algèbres Étales et Théorie de Galois

---

par

Alexander Grothendieck

Transcription by

Edited by Mateo Carmona
mateo.carmona@csg.igrothendieck.org
Centre for Grothendieckian Studies (CSG)
Grothendieck Institute
Corso Statuto 24, 12084 Mondovì, Italy

This transcription is derived from an unpublished scan provided by the "Fonds du secrétariat Bourbaki (ENS-ULM)" with the reference Rédaction Bourbaki "No. 457". This project was carried out by researchers and volunteers of the CSG under the supervision of Mateo Carmona. More details are available at:
https://csg.igrothendieck.org/transcriptions/

How to cite:

Alexander Grothendieck. *Algèbres étales et théorie de Galois*. Rédaction Bourbaki No. 457. Unpublished note. 10.1965. Transcription by M. Carmona et al., CSG, Grothendieck Institute. Draft, February 2026.

SOMMAIRE

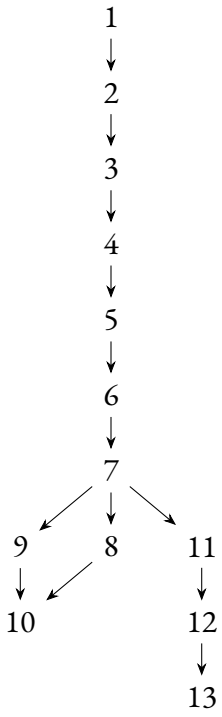
PROJET DE RÉÉDITION D'ALGÈBRE, CHAPITRE V, CORPS COMMUTATIFS

Plan

1. Corps premiers, caractéristique.
2. Extensions.
3. Algèbres entières et extensions algébriques.
4. Extensions algébriquement closes.
5. Extensions transcendantes.
6. Isomorphismes et automorphismes de corps. Extensions quasi-galoisiennes.
7. Algèbres entières séparables.
8. Théorie de Galois.
9. Normes et traces.
10. Racines de l'unité, corps finis, extensions kummériennes.
11. Algèbres et extensions radicielles.
12. Algèbres séparables. Produit tensoriels d'extensions.

13. Dérivations et différentielles dans les corps.

Leitfaden



COMMENTAIRES SUR LE PLAN

Le changement essentiel de la présente rédaction par rapport au texte publié est l'accent mis sur les *algèbres*, partout où il n'y avait pas lieu de se limiter à des *extensions* seulement, et sur le procédé de changement du corps de base, qui rend ce point de vue nécessaire, puisque une extension ne reste plus une extension après changement du corps de base.

La définition des algèbres séparables est donnée dans cet esprit au §7, où on traite surtout des phénomènes spéciaux au cas des algèbres séparables entières (comprenant les extensions algébriques séparables), qui sont mis en relation avec les notions d'algèbre diagonalisable, et d'algèbre étale (= qui devient diagonalisable après changement de base). Le §7 contient également la suite des corps parfaits et des extensions radicielles, et les notions de clôture parfaite et de clôture séparable, bien utiles et qui ne figuraient pas dans Bourbaki.

Dans la théorie de Galois proprement dite, au §8, n° 1 à 3, on a pratiquement suivi le texte publié, en augmentant simplement de quelques détails (notamment sur le cas quasi-galoisien). Comme innovation, on introduit la notion d'algèbre à groupes d'opérateurs galoisienne, pour pouvoir définir l'objet $\mathrm{H}^1(k, G)$, qui est un groupe commutatif si G l'est, qu'on utilisera pour donner une formulation plus satisfaisante de la théorie de Kummer au §10. On a étoffé un peu le n° des groupes de Galois topologiques (qui passe dans le texte du §) par des suites sur les groupes profinis, et on a introduit la notion de groupe fondamental d'un corps (= groupe de Galois topologique d'une clôture séparable), dont l'importance n'est apparue que dans les dernières années, ce qui explique son absence dans le texte publié.

Les normes et traces sont disjointes du § de Galois et forment un paragraphe à part

(§9) ; il a paru antibourbachique, en effet, de définir des notions aussi générales en commençant par le cas étriqué des extensions séparables finies, sous prétexte que dans ce cas le norme et la trace s'expriment en termes des isomorphismes de l'extension dans une clôture algébrique. Pratiquement, ce changement de plan consiste à remonter au Chap. V le par. 12, n° 1 et 2, du Chap. VIII. Une autre possibilité serait de remonter la suite des normes et traces au Chap. III ou IV (leur place semble en effet plutôt dans un Chapitre consacré à des algèbres générales, plutôt que dans un Chapitre sur les algèbres semi-simples). Si cette solution était adoptée, le §9 de la présente rédaction disparaîtrait, et serait remplacé par un nouveau n° au §7, indiquant le calcul de la norme et de la trace d'une algèbre étale au moyen des homomorphismes dans une clôture algébrique du corps de base, et le critère d'étalité par la forme trace.

Le paragraphe des corps finis, racines de l'unité, extensions cycliques, reste inchangé, sauf que la théorie de Kummer est réécrite dans l'esprit du H^1, et le théorème 90 énoncé dans le cas général, pas seulement cyclique. De plus, les théorèmes de l'élément primitif et de la base normale sont reportés à ce paragraphe. L'ordre des paragraphes a été pris de telle façon que les §7, 8, 9, 10 forment un "bloc galoisien" qui soit indépendant des §11, 12, 13 concernant des algèbres et extensions pas nécessairement entières séparables (voir le Leitfaden).

Le par. 11 est nouveau, et consiste à magnifier le fait que les extensions radicielles d'un corps k sont telles qui donnent des anneaux locaux (à idéal maximal un nilidéal) par toute extension du corps de base. Il peut être dégonflé à volonté, à l'exception de ce dernier résultat.

Le par. 12 contient le critère de Mac-Lane et ses variantes, et les propriétés essentielles des produits tensoriels de corps, traités très imparfaitement par Bourbaki. Le critère de Mac-Lane s'énonce ici en disant qu'une algèbre commutative A sur un corps k est séparable si et seulement si $A \otimes_k k^{p^{-1}}$ est réduite.

Enfin, le par. 13, en plus du critère différentiel de séparabilité d'une extension et du théorème sur les bases de transcendance séparantes, est étoffé par l'introduction des modules d'imperfection d'une algèbre et par l'égalité de Cartier sur les extensions de type fini, ainsi que par la suite des p-bases.

Le plan adopté, consistant à faire passer le bloc galoisien avant l'étude générale de la séparabilité et les questions différentielles, a pour conséquence que les résultats sur les

extensions séparables, et en particulier les critères de séparabilité, sont répartis dans trois paragraphes : par. 8 (cas des algèbres entières, i.e. des extensions algébriques), par. 12 (critère de Mac-Lane et variantes), par. 13 (critère différentiel, bases de transcendance séparantes). Cela était également le cas dans le texte publié, et ne me semble offrir aucun inconvénient sérieux.

COMMENTAIRES DE DÉTAIL

Le texte publié sera changé entièrement à partir du paragraphe 7. Pour les par. 1 à 6, nous signalons plus bas les modifications de détail qui semblent nécessaires. Nous avons groupé dans un appendice quelques résultats épars de théorie des anneaux, dont la place naturelle pour la plupart semblerait aux Chapitres I et IV, mais dont certains pourraient être insérés peut-être au cours du Chap. V. Bourbaki décidera. On référera aux énoncés de l'Appendice par des sigles tels que App 3.27.

Par 1.

N° 1. La notion de caractéristique introduite au Chap. I, à laquelle on réfère haut de p. 71, est canularesque et sera vidée dans la prochaine édition. Il faut donc rédiger sans utiliser cette terminologie. Dégager le raisonnement "deux cas peuvent se présenter" en un.

Lemme. — *Soit n un entier ≥ 0. Alors $\mathbf{Z}/n\mathbf{Z}$ est intègre sss on a $n = 0$ ou n est un nombre premier ; dans ce deuxième cas (et seulement dans celui-là) $\mathbf{Z}/n\mathbf{Z}$ est un corps.*

Énoncer le théorème 1 sans terminologie de caractéristique, en disant que les corps premiers sont ceux isomorphes aux corps $\mathbf{Q}$ ou $\mathbf{F}_p$ (p premier), ces corps-types étant d'ailleurs deux à deux non isomorphes. Les remarques 2 et 3 tombent ou sont reportées après la notion de caractéristique, que je propose d'introduire dans le même n° ainsi :

Proposition A. — *Soit A un anneau (pas nécessairement commutatif, mais associatif et unitaire comme il se doit), et soit p un nombre premier. Les conditions suivantes sont*

équivalentes :

(i) $p \cdot 1_A = 0_A$ *(où* 1_A *et* 0_A *sont resp. les élément unité et nul de* A*).*

(ii) $pA = 0$*, i.e. pour tout* $x \in A$*, on a* $px = 0$*.*

(iii) A *peut être muni d'une structure de* $\mathbf{F}_p$*-algèbre compatible avec sa structure d'anneau.*

De plus, si ces conditions sont vérifiées, la structure d'algèbre mentionnée dans (iii) est uniquement déterminée.

Proposition B. — *Soit* A *un anneau (pas néc comm). Les conditions suivantes sont équivalentes :*

(i) Pour tout entier $n > 0$*, l'application* $x \rightsquigarrow nx$ *dans* A *est bijective.*

(iii) A *peut être muni d'une structure de* $\mathbf{Q}$*-algèbre compatible avec sa structure d'anneau.*

De plus, si ces conditions sont vérifiées, la structure d'algèbre envisagée dans (iii) est uniquement déterminée.

Définition C. — *Soit* p *un entier* ≥ 0*, qui est soit nul, soit un nombre premier. On dit qu'un anneau* A *est de caractéristique* p*, si* A *satisfait aux conditions de la prop. A dans le cas où* p *est premier, resp. à celles de prop. B si* p *est nul.*

Proposition D. — *Un anneau* A *non nul a au plus une caractéristique, qui est aussi l'entier* $n \geq 0$ *caractérisée par la relation* $J = n\mathbf{Z}$*, où* J *est l'idéal annulateur de l'homomorphisme* $n \rightsquigarrow n.1_A$ *de* $\mathbf{Z}$ *dans* A*. L'anneau nul admet comme caractéristique tout entier premier ou nul.*

Proposition E. — *Un corps a une caractéristique bien déterminée, égale à celle de tout sous-corps et de tout sur-corps. Pour tout entier* p *comme dans déf. C, il existe des corps (en fait des corps premiers) de caractéristique* p*. Pour deux corps premiers de caractéristique* p*, il existe un isomorphisme unique de l'un sur l'autre.*

Remarque F. — Soit p comme dans déf. C, et soit P le corps premier type de caractéristique p (donc égal à $\mathbf{F}_p$ si $p \neq 0$, à $\mathbf{Q}$ si $p = 0$). Alors un anneau A est de caractéristique p si et seulement si il peut être muni d'une structure de P-algèbre compatible avec sa structure d'anneau, et alors cette structure de P-algèbre est unique. *La Mémère-catégorie des anneaux de caractéristique p est donc isomorphe, si on ose ainsi s'exprimer, à la Pépère-catégorie des P-algèbres associatives et unitaires.*

Remarque F'. — Si A est un anneau non nul de caractéristique p, il contient un sous-corps isomorphe au corps premier P. Si $p = 0$, donc $P = \mathbf{Q}$, alors P est infini, donc un anneau non nul de caractéristique nulle est infini. En particulier, tout corps fini est de caractéristique $p > 0$.

N° 2. Prendre des anneaux au lieu de corps.

Par 2.

Dans l'introduction de la notion d'extension, il faut dire qu'une extension d'un corps K est une K-algèbre L qui se trouve être un corps. En effet, il est contraire aux bons yogas de structure, et aussi à l'usage que Bourbaki lui-même fait de ce terme, de se borner au cas où L est vraiment un sur-corps de K, i.e. K une partie de L. Définir aussi l'extension triviale : $K \longrightarrow L$ est un isomorphisme (pas nécessairement une identité !).

N° 1. Il n'y a aucune raison de ne donner un sens au symbole $[E : K]$ que lorsqu'il est fini, au contraire il est parfois commode d'utiliser la notation en tous les cas. Ligne 12, la référence est canularesque, ligne suivante référence changée en Chap. II, par. 1, prop. 25. Dans le théorème 1, supprimer le passage "si l'un des nombres...est défini, il en est de même de l'autre", tout est toujours défini. On aura remarqué que pour des extensions de corps, le degré est un entier ≥ 1 ou $+\infty$, donc les deux membres de l'égalité du th. 1 sont toujours bien définis.

Dans la proposition 1, on peut supprimer les hypothèses de commutativité. Dans le corollaire de la proposition 1, supprimer l'assertion sur l'égalité des éléments unités, qui est canularesque. De même, le passage "nous ne considérons que des représentations non nulles, c'est-à-dire telles que $f(1) = 1$"...Il doit être entendu une bonne fois (au besoin dans le chapeau du chapitre) que les algèbres sont associatives et unitaires, les homomorphismes d'anneaux et d'algèbres respectent les unités. Il y a aussi deux références au Chap. II qui doivent être changées.

N° 2. Page 77, dans la note de bas de page, "les axiomes...ne font intervenir que des

parties finies...” ne veut rien dire. On aurait intérêt à vider cette brillante note. Page 78, 5ème ligne avant la fin du n°, lire “réunion *filtrante*”.

N° 3. Référence au Chap. III changée. Page 79, ligne 1, supprimer “(par exemple)”. Dans le texte précédant prop. 5, prendre pour A et B des parties (pas nécessairement des sous-anneaux) engendrant les extensions E resp. F.

Par 3.

Il faudrait rédiger systématiquement en termes d'algèbres entières (ou algébriques, si Bourbaki préfère — le rédacteur ne préfère pas), au lieu d'*extensions* algébriques. Ainsi, dès la définition 1, prendre pour E une algèbre (qu'on noterait plutôt A), pas même commutative, et introduire la notion “transcendant” et “entier = algébrique”, (la formulation de cette deuxième notion devrait être changée si on commence par ne pas supposer non plus que k soit un corps). Kif-kif pour définition 2, pour le théorème 1 (reformulé en conséquence, en supprimant le mot “corps” où il le faut) etc. Dans la remarque à la fin du n° 1, 4ème ligne avant la fin, lire “et si f est $\neq 0$ et qu'on désigne par n son degré”. Dans prop. 1, ajouter qu'alors *toutes* les racines de f sont simples, et $f(X) = (X - x_1) \dots (X - x_n)$, où les x_i sont les conjugués de x.

Par 4.

Remplacer le titre par : “Isomorphismes et automorphismes de corps. Extensions quasi-galoisiennes”.

N° 1. Remplacer l'exemple 2 en petits caractères, par une proposition en forme, sous la forme suivante : Un corps algébriquement clos est infini.

N° 2. Dans le th. 1 et son corollaire, lire “extension algébriquement close” au lieu de “clôture algébrique”. La démonstration du corollaire est amoureuse, et ce corollaire ne doit sa raison d'être qu'à la définition amoureuse adoptée par Bourbaki pour la notion d'extension.

Par 5.

Page 95, fin de la remarque, référence au Chap. II changée ; ligne - 13, au lieu de “algébriquement indépendants” il faudrait lire “mutuellement algébriquement indépendants”, ou ne rien dire du tout.

Page 98, supprimer la note en petits caractères après le th. 2.

N° 3. Énoncer le th. 3 et la déf. 4 sans hypothèse de finitude. Dans définition 4, supprimer la terminologie "dimension algébrique" et la notation dim al$_K E$, que personne n'a jamais employée, et la notation dim$_K E$, terriblement ambiguë ; introduire deg. tr$_K L$. Vider le noble laïus en petits caractères après déf. 4. Dans le théorème 4, supprimer "si l'un des nombres...est défini, il en est de même de l'autre".

Par 6.

N° 1. Page 109, lignes 7 et 8, la notion d'extension universelle, introduite fort légèrement et par la bande, est bonne pour le vidage. Dans le cor. à prop. 1, lire "degré de transcendance" ; le corollaire semble d'ailleurs bon à vider. Vider la remarque en petits caractères à la fin du n° 1.

N° 2. Dans déf. 1, prendre pour E et F des parties quelconques. Dans la note en petits caractères au bas de p. 110, vider la première phrase, et remplacer le mot "classes d'intransitivité" par "orbites". Dire que la même remarque s'applique pour la relation de conjugaison entre parties. Page 111, petits caractères, après "intrinsèque" ajouter "à K et E".

N° 3. Le titre devient : *Extensions quasi-galoisiennes.* Remplacer l'ensemble des propositions 5 et 6, qui font un bonnet blanc-blanc bonnet bien désagréable, par la

Proposition 5. — *Soient K un corps, E une extension algébrique de K, Ω une extension algébriquement close de E. Les conditions suivantes sont équivalentes :*

(i) Tout K-homomorphisme de E dans Ω applique E dans lui-même.

(ii) Tout K-automorphisme de Ω applique E dans lui-même (donc, en vertu de prop. 4, induit un K-automorphisme de E).

(iii) Pour tout élément x de E, tous les conjugués de x sur K (dans Ω) appartiennent à E.

(iv) Tout polynôme irréductible de $K[X]$, ayant une racine dans E, se décompose en facteurs linéaires (distincts ou non) dans $E[X]$.

Comme tout K-homomorphisme de E dans Ω ne prolonge un K-automorphisme de Ω (prop. 2, cor. 2), l'équivalence de (i) et (ii) est claire. D'autre part, les polynômes

irréductibles f de $K[X]$, ayant une racine dans E, sont exactement (à des constantes multiplicatives près) les polynômes minimaux des éléments x de E, les racines de f étant justement les conjugués de x (prop. 3). Comme f se décompose dans $E[X]$ en produit de facteurs linéaires si et seulement si toutes les racines dans Ω se trouvent dans E, cela montre l'équivalence de (iii) et (iv). Comme par définition les conjugués sur K (dans Ω) d'un élément x de E sont précisément les transformés par les K-automorphismes de Ω, l'équivalence de (ii) et (iii) est également claire, ce qui prouve la proposition.

Définition 2. — *Soient K un corps, E une extension de K. On dit que E est une extension quasi-galoisienne de K si elle est algébrique, et si elle satisfait à la condition (iv) de la prop. 5 (équivalente, une fois choisie une clôture algébrique Ω de E, aux autres conditions (i) à (iii) de la prop. 5).*

On peut encore dire qu'une sous-extension E d'une extension algébriquement close Ω de K est quasi-galoisienne si et seulement si elle est algébrique, et identique à toutes les extensions conjuguées (définition 1) de E dans Ω. Par exemple, toute clôture algébrique de K est une extension quasi-galoisienne de K.

Je ne pense pas qu'il y ait lieu de garder la prop. 7, qui constitue une simple redite. Il y a lieu par contre d'étoffer le corollaire des extensions quasi-galoisiennes. On peut garder les prop. 8 et 9 actuelles (elles deviennent 7 et 8), et les corollaires de cette dernière, tels quels, sauf qu'il faut remplacer partout "normale" par "quasi-galoisienne". Il faut enfin ajouter deux propositions.

Proposition 9. — *Soient K un corps, Ω une extension de K, E et K' deux sous-extensions de Ω. Si E est quasi-galoisienne sur K, alors $E' = K(E')$ est quasi-galoisienne sur K'.*

En effet, en vertu du théorème de Steinitz on peut supposer Ω algébriquement close, et comme tout K-automorphisme de Ω est un K-automorphisme, il applique E dans lui-même, donc $E' = K'(E)$ dans lui-même, ce qui prouve que E' est une extension quasi-galoisienne de K', compte tenu qu'elle est algébrique en vertu de par. 3, n° 2, prop. 7.

Proposition 10. — *Soient K un corps, E une extension de K, K' une sous-extension de E. Si E est quasi-galoisienne sur K, elle est quasi-galoisienne sur K'.*

En effet, soit Ω une extension algébriquement close de E, alors tout K'-automorphisme de Ω est un K-automorphisme, donc applique E dans lui-même, ce qui prouve que E est une extension quasi-galoisienne de K' (compte tenu qu'elle est algébrique sur K', l'étant sur K).

Pour d'autres commentaires au n° 3, cf. §6, n° 1, le N. B.

Je suggère de faire du th. d'Artin un n° 4 au §6 :

N° 4. **Le théorème d'Artin.**

Le résultat du présent numéro, de nature surtout technique, nous servira au §8 à prouver un résultat clef de la théorie de Galois, et au par. 12 à démontrer le critère de séparabilité de Mac Lane. Il ne sera pas utilisé directement à d'autres endroits du présent livre.

Théorème 1 (Artin). — *Soient K un corps, G un ensemble d'automorphismes de K, stable par multiplication et contenant l'automorphisme identique, k le corps des invariants de G, V une partie de K, n un entier ≥ 0. Munissons K comme structure d'espace vectoriel sur k, et l'ensemble des applications de V dans K de sa structure naturelle d'espace vectoriel sur K. Pour que l'ensemble des restrictions à V des $u \in G$ soit de rang n sur K, il faut et il suffit que la partie V de K soit de rang n sur k.*

N. B. — La démonstration est celle de la présente édition, où il faut simplement changer la référence à l'ancienne édition du Chap. II. On pourrait aussi, tant qu'à faire, mettre tout de suite la version non commutative, qui ne coûte pas plus cher. Le rédacteur pense qu'il ne faut pas expliciter ici la prop. 1 page 117 de la présente édition du Chap. V, trop triviale pour mériter un tel honneur. Je pense qu'il faut garder les quatre lignes de laïus préliminaires ci-dessus, qui seront bien utiles au lecteur pour l'encourager à oublier le théorème d'Artin. Vérifier s'il y a quelque part la justification du terme "*corps* des invariants", je ne l'ai trouvée nulle part.

Enfin, je suggère de faire un

N° 5. **Théorèmes d'indépendance linéaire et algébrique d'isomorphismes de corps.**

Le premier de ces deux théorèmes me semble sans doute qu'un rappel d'un énoncé plus général figurant au Chap. IV (cf. App. 5,6), il sera utilisé au §8 pour la théorie de Galois. Le théorème d'indépendance algébrique ne servira plus dans le livre d'Algèbre, et le rédacteur avait qu'il n'en est encore jamais servi lui-même. Aussi il propose de mettre ce théorème en petits caractères.

§ 7. — ALGÈBRES ENTIÈRES SÉPARABLES SUR UN CORPS. CLÔTURE SÉPARABLE ET CLÔTURE PARFAITE D'UN CORPS

---

1. — Algèbres diagonalisables

Définition 1. — *Soient k un anneau (le chapeau du Chapitre impliquera qu'il est commutatif), A une k-algèbre. On dit que A est diagonalisable s'il existe un entier $n \geq 0$ tel que A soit isomorphe à l'algèbre produit k^n.*

Par exemple, l'algèbre 0, ainsi que k muni de sa structure canonique de k-algèbre, sont diagonalisables ; tout produit fini d'algèbres diagonalisables est diagonalisable. Une algèbre diagonalisable sur k est de degré fini sur k.

Proposition 1. — *Soient k un corps, A une k-algèbre de degré fini n, $P(A)$ l'ensemble des k-homomorphismes de A dans k, Ω une extension algébriquement close de k. Les conditions suivantes sont équivalentes :*

(i) *A est diagonalisable (déf. 1).*

(ii) *A est réduit, et pour tout k-homomorphisme $u : A \longrightarrow \Omega$, on a $u(A) \subset k$.*

(ii bis) *A est réduit et ses extensions résiduelles (App. n° 5) sont triviales.*

(iii) *card$(P(A)) = n$.*

(iv) *A a exactement n idéaux maximaux.*

Ce n'est autre que App. 5.7.

Proposition 2. — *Soit k un corps.*

(i) Soit A une k-algèbre. Si A est diagonalisable, il en est de même de toute sous-algèbre et de toute algèbre quotient de A.

(ii) Soit $(A_i)_{i\in I}$ une famille finie de k-algèbres. Pour que le produit A de cette famille soit diagonalisable, il faut et il suffit que chacune des A_i le soit.

(iii) Soient A et B deux k-algèbres. Si A et B sont diagonalisables, il en est de même de $A \otimes_k B$. Inversement, si $A \otimes_k B$ est diagonalisable et $A \neq 0$, alors B est diagonalisable.

(iv) Soit A une k-algèbre, engendrée par une famille de sous-algèbres A_i $(i \in I)$. Pour que A soit diagonalisable, il faut et il suffit qu'elle soit commutative et de degré fini, et que chacune des A_i soit diagonalisable.

(v) Soit A une k-algèbre diagonalisable, alors pour toute extension k' de k, $A \otimes_k k'$ est une k'-algèbre diagonalisable.

Démonstration.

(i) Si A est diagonalisable, il résulte aussitôt du critère (ii bis) de prop. 1 que toute sous-algèbre l'est également. D'ailleurs la connaissance des idéaux d'un produit de corps (App. 1.14) montre aussitôt que toute algèbre quotient de k^n est isomorphe à une algèbre k^m $(m \leq n)$, ce qui prouve que si A est diagonalisable, il en est de même de toute algèbre quotient.

(ii) Si les A_i sont diagonalisables, il en est de même de leur produit, comme il résulte trivialement de la définition. Inversement, si le produit A est diagonalisable, comme les A_i sont isomorphes à des algèbres quotients de A, elles sont diagonalisables en vertu de (i).

(iii) Si A et B sont diagonalisables, il en est de même de $A \otimes_k B$, comme il résulte trivialement de la définition et du calcul du produit tensoriel d'algèbres produits. Inversement, si $A \otimes_k B$ est diagonalisable et $A \neq 0$, alors B est diagonalisable

en vertu de (i), car isomorphe à une sous-algèbre $1_A \otimes_k B$ de $A \otimes_k B$, qui est diagonalisable.

(iv) La nécessité de la condition résulte aussitôt de (i). Inversement, supposons les A_i diagonalisables et A commutative et de degré fini sur k, alors il existe une sous-famille finie de $(A_i)_{i\in I}$ qui engendre déjà A, donc A est isomorphe à une algèbre quotient du produit tensoriel d'une sous-famille finie de (A_i), donc diagonalisable en vertu de (iii), en utilisant une récurrence sur le cardinal de l'ensemble d'indices de cette sous-famille.

(v) Est triviale sur la définition.

Proposition 3. — *Soient k un corps, $f \in k[X]$ un polynôme en une indéterminée X, à coefficients dans k, non identiquement nul, $A = k[X]/fk[X]$. Alors A est diagonalisable si et seulement si f se décompose en facteurs linéaires tous distincts, i.e. peut s'écrire sous la forme*

$$f = c \prod_{1\leq i\leq n} (X - a_i),$$

où n est le degré de f, c et les a_i ($1 \leq i \leq n$) sont dans k, et les a_i sont tous distincts.

Cela résulte en effet aussitôt de App. 5.8, compte tenu que pour un polynôme unitaire irréductible f_i, le corps $k[X]/fk[X]$ est une extension triviale de k si et seulement si f_i est de la forme $X - a_i$, et que deux polynômes de la forme $X - a, X - b$ sont égaux si et seulement si a et b le sont.

Corollaire. — *Soient A une algèbre sur un corps k, $(x_i)_{i\in I}$ une famille génératrice d'éléments de A. Pour que A soit diagonalisable, il faut et il suffit que A soit de degré fini, et que pour tout $i \in I$, le polynôme minimal f_i de x_i sur k (§3, n°1, déf. 3) se décompose en facteurs linéaires tous distincts.*

En effet, A est engendré par ses sous-algèbres $A_i = k[x_i]$, isomorphes aux $k[X]/f_ik[X]$, et on conclut par Proposition 2 (iv) et Proposition 3.

Corollaire. — *Soient k un corps, V un espace vectoriel de dimension finie sur k. Soit u un endomorphisme de V; on dit que u est diagonal par rapport à une base $(e_s)_{s\in S}$ de V, si sa matrice par rapport à cette base est diagonale, i.e. si pour tout $s \in S$, il existe un*

$\lambda_s \in k$ *tel que* $u(e_s) = \lambda_s e_s$ *; on dit que* u *est diagonalisable si on peut trouver une base de* V *par rapport à laquelle* u *soit diagonal. Une famille* $(u_i)_{i\in I}$ *d'endomorphismes de* V *est dite diagonalisable si on peut trouver une base* $(e_s)_{s\in S}$ *de* V *telle que pour tout* $i \in I$*,* u_i *soit diagonal par rapport à cette base.*

On notera que si A est une partie de $\mathrm{End}_k(V)$, considérant A comme définissant la famille des endomorphismes $u \in A$ de V, la définition précédente donne un sens à la locution : "A est diagonalisable". Nous allons voir que lorsque A est une sous-algèbre de $\mathrm{End}_k(V)$, cette dernière définition est compatible avec la définition 1, i.e. A est diagonalisable, en tant que partie de $\mathrm{End}_k(V)$, si et seulement si elle est diagonalisable en tant que k-algèbre :

Proposition 4. — *Soient* k *un corps,* V *un espace vectoriel de dimension finie sur* k*,* $(u_i)_{i\in I}$ *une famille d'endomorphismes de* V*,* A *la sous-algèbre de* $\mathrm{End}_k(V)$ *qu'elle engendre. Les conditions suivantes sont équivalentes :*

(i) La k*-algèbre* A *est diagonalisable (cf. déf. 1).*

(ii) La partie A *de* $\mathrm{End}_k(V)$ *est diagonalisable (cf. déf. 2).*

(iii) La famille $(u_i)_{i\in I}$ *est diagonalisable (cf. déf. 2).*

(iv) Les u_i *sont diagonalisables et commutent deux à deux.*

(v) Les u_i *commutent deux à deux, et pour tout* $i \in I$ *le polynôme minimal (§3, n°*1*, déf. 3) de* u_i *se décompose en facteurs linéaires tous distincts.*

Comme A est commutative si et seulement si les u_i commutent deux à deux, l'équivalence de (i) et (v) est un cas particulier du corollaire à la prop. 3. D'autre part (i) implique (ii) en vertu de App. 1.24, et (ii) implique que A est isomorphe à une sous-algèbre d'une algèbre diagonalisable (l'algèbre des matrices diagonales, qu'on aurait pu donner en exemple dès après la définition 1), donc est diagonalisable en vertu de prop. 2 (i). Donc (i), (ii), (v) sont équivalentes. Appliquant ceci au cas d'une famille réduite à un seul élément, on conclut que si u est un endomorphisme de V, alors u est diagonalisable si et seulement si son polynôme minimal se décompose en facteurs linéaires tous distincts, ce qui prouve que (iv) équivalait à (v). L'équivalence de (ii) et (iii) est claire, car

pour une base donnée de V, les matrices des u_i sont toutes diagonales si et seulement si il en est ainsi des matrices de tous les $u \in A$. Cela achève la démonstration de prop. 4.

Corollaire. — *Soit A une algèbre sur un corps k. Pour que A soit diagonalisable, il faut et il suffit que pour toute représentation linéaire de A par des endomorphismes d'un espace vectoriel V de dimension finie sur k, la famille correspondante (indexée par A) d'endomorphismes de V soit diagonalisable, et il faut et suffit qu'on puisse trouver une représentation linéaire fidèle de A ayant cette propriété.*

Si A est diagonalisable, donc isomorphe à une algèbre k^n, alors la connaissance explicite de ses représentations linéaires (App. 1.24) montre la nécessité de la condition énoncée dans le corollaire. Inversement, si A admet une représentation linéaire fidèle satisfaisant à la condition de diagonalisabilité du corollaire, alors A est une algèbre diagonalisable en vertu de prop. 4, (ii) $\Rightarrow$ (i). Notant que toute algèbre de degré fini sur k admet une représentation linéaire fidèle (par exemple la représentation régulière), on achève la démonstration du corollaire.

Remarque. — On fera attention que sous les conditions préliminaires de la prop. 4, il est possible que tout élément de A soit un endomorphisme diagonalisable de V, sans que A soit commutatif, donc sans que A soit diagonalisable, cf. exerc....

2. — Algèbres étales sur un corps

Proposition 5. — *Soient k un corps, A une algèbre commutative de degré fini sur k, Ω une extension algébriquement close de k. Alors les deux conditions sont équivalentes :*

(i) $A \otimes_k \Omega$ *est une algèbre diagonalisable sur* Ω *(cf. déf. 1).*

(ii) $A \otimes_k \Omega$ *est un anneau réduit.*

De plus, ces conditions sont indépendantes de l'extension algébriquement close Ω envisagée de k. Si K est une sous-extension de Ω telle que pour tout k-homomorphisme $u : A \longrightarrow \Omega$, on ait $u(A) \subset K$, alors les conditions (i) et (ii) sont équivalentes aux conditions qu'on en déduit en y remplaçant Ω par K.

Notons que la condition envisagée sur K s'exprime en termes de la K-algèbre $B = A \otimes_k K$ par le fait que pour tout K-homomorphisme $v : B \longrightarrow \Omega$, on a $v(B) =$

K, ce qui en vertu de App. 5.4 et de §4, n°2, th. 1 équivaut au fait que les extensions résiduelles de la K-algèbre B sont triviales. D'après la prop. 1, on sait bien qu'alors B est diagonalisable si et seulement si elle est réduite ; en vertu de prop. 2 (v) la Ω-algèbre $B \otimes_K \Omega$, isomorphe à $A \otimes_k \Omega$, sera alors diagonalisable, et l'inverse est vrai, car B est isomorphe à un sous-anneau de $B \otimes_K \Omega$, donc réduit si ce dernier l'est. Il reste à prouver que les conditions (i) et (ii) ne dépendent pas de l'extension algébriquement close Ω choisie de k. Or si Ω' est une autre telle extension, on peut trouver une extension algébriquement close Ω'' de k et des k-isomorphismes de Ω, Ω' sur des sous-extensions de Ω'' (§4, prop. 2 et th. 2) ; il résulte alors de ce qui précède que les conditions envisagées pour Ω, Ω' sont équivalentes séparément aux conditions analogues pour Ω'', donc équivalentes entre elles. Cela achève la démonstration de la proposition.

Définition 3.— *Soient k un corps, A une algèbre sur k. On dit que A est étale (ou étale sur k, si une confusion est à craindre sur le corps de base), si A est commutative, de degré fini, et si elle satisfait aux conditions équivalentes de la prop. 5.*

Cette définition a un sens grâce au théorème de Steinitz, (§4, th. 2), assurant que k admet bien une extension algébriquement close.

Proposition 6.— *Soit A une algèbre commutative de degré fini sur le corps k. Pour que A soit étale, il faut et il suffit que pour toute extension K de k, $A \otimes_k K$ soit un anneau réduit. En particulier, si A est étale, A est un anneau réduit.*

C'est trivialement suffisant sur la forme (ii) des conditions de prop. 5. Inversement, si A est étale, prouvons que $A \otimes_k K$ est réduit pour toute extension K de k. En effet, prenons pour Ω une extension algébriquement close de K, alors par hypothèse $A \otimes_k \Omega$ est réduit, donc aussi $A \otimes_k K$ qui est isomorphe à un sous-anneau de celui-ci.

Proposition 7. — *Avec les notations de la prop. 5, les conditions (i) et (ii) équivalent aussi à la condition suivante :*

(iii) Le cardinal de l'ensemble des k-homomorphismes de A dans Ω est égal au degré n de A.

Quitte à remplacer A par la Ω-algèbre $A \otimes_k \Omega$, on peut supposer que $\Omega = k$, et on conclut par la prop. 1.

Proposition 8. — *Soit k un corps.*

(i) Soit A une k-algèbre. Si A est étale, il en est de même de toute sous-algèbre et de toute algèbre quotient de A.

(ii) Soit $(A_i)_{i\in I}$ une famille finie de k-algèbres. Pour que le produit A de cette famille soit étale, il faut et il suffit que chacun des A_i le soit.

(iii) Soient A et B des k-algèbres. Si A et B sont étales, il en est de $A\otimes_k B$. Inversement, si $A\otimes_k B$ est étale et si $A\neq 0$, B est étale.

(iv) Soit A une k-algèbre, engendrée par une famille (A_i) de sous-algèbres. Pour que A soit étale, il faut et il suffit qu'elle soit commutative, de degré fini, et que les A_i soient étales.

(v) Soit A une k-algèbre, k' une extension de k, $A'=A\otimes_k k'$ la k'-algèbre déduite par changement du corps de base. Pour que A soit étale, il faut et il suffit que A' le soit.

Démonstration. — Tout d'abord, (v) est immédiat sur le critère de la prop. 5, comme on voit en choisissant une extension algébriquement close Ω de K, et en la considérant également comme une extension de k. Ceci noté, pour prouver les énoncés (i) à (iv), on choisit une extension algébriquement close Ω de k, et on est ramené par changement de base à prouver les mêmes assertions sur un corps algébriquement clos. Or dans ce cas, une algèbre sur k est étale si et seulement si elle est diagonalisable, et nos assertions résultent des assertions analogues de la prop. 2.

Corollaire 1. — *Soit A une algèbre sur le corps k. Pour que A soit étale, il faut et il suffit que A soit isomorphe au produit d'une famille finie d'extensions étales de k.*

La suffisance résulte de (ii), et la nécessité également, compte tenu du fait qu'une algèbre commutative de degré fini sur k est isomorphe au produit d'une famille finie d'algèbres *locales* de degré fini sur k (App. 3.5), et que si ces dernières sont étales, elles sont réduites (prop. 6) donc des corps (App. 3.7).

Corollaire 2. — *Soient K une extension du corps k, A une K-algèbre. Pour que A soit étale en tant que k-algèbre, il suffit que l'extension K soit étale et que la K-algèbre A soit étale, et ces conditions sont également nécessaires lorsque $A\neq 0$.*

Supposons K étale sur k et A étale sur K, et prouvons que A est étale sur k. Soit k' une clôture algébrique de k, alors par hypothèse $K' = K \otimes_k k'$ est isomorphe au produit d'une famille finie de k'-algèbres K'_i isomorphes à k'. L'algèbre $A' = A \otimes_k k'$ sur K' se décompose alors en produit d'algèbres A'_i sur les facteurs K'_i (App. 1.25), ces dernières n'étant autres d'ailleurs que $A'_i = A \otimes_K K'_i$, donc diagonalisables puisque A est étale sur K et que K'_i est une extension algébriquement close de K. Il en résulte que A', en tant que k'-algèbre, est un produit fini d'algèbres diagonalisables A'_i sur k', donc diagonalisable, ce qui prouve que A est une k-algèbre étale. Inversement, supposons A étale sur k et $A \neq 0$. Comme alors K est isomorphe à une sous-algèbre de A, il résulte de prop. 8 (i) que K est étale sur k. Reste à prouver que A est étale sur K. Or si k' est une extension algébriquement close de k, alors $A \otimes_K K'$ est isomorphe à une algèbre quotient de $A \otimes_K K'$, et cette dernière est diagonalisable puisque A est étale sur k, donc il en est de même de $A \otimes_K K'$ en vertu de prop. 2 (i), ce qui prouve que A est étale sur K.

Remarque. — Le corollaire 1 montre que la classification des algèbres étales sur un corps donné k se ramène complètement à celle des *extensions* étales de k. Nous montrerons au §8 comment on peut effectuer cette classification en termes d'ensembles à groupes d'opérateurs, grâce à la théorie de Galois.

Proposition 9. — *Soient k un corps, $f \in k[X]$ un polynôme à une indéterminée X à coefficients dans K, non identiquement nul. Pour que l'algèbre $A = k[X]/(fk[X])$ sur k soit étale, il faut et il suffit que les racines de f (dans une extension algébriquement close donnée Ω de k) soient simples (réf.), ou encore que f se décompose en un produit de polynômes irréductibles distincts dont chacun n'a que des racines simples (réf.) dans Ω. Lorsque f est irréductible, ces conditions signifient aussi que l'on ait $f \notin k[X^p]$ (où p désigne l'exposant caractéristique de k).*

Le premier critère, qui s'énonce aussi en disant que f, considéré comme polynôme à coefficients dans Ω, se décompose en facteurs linéaires distincts, est une conséquence immédiate de la déf. 3 et de la prop. 3. Le deuxième critère résulte du premier, compte tenu de la décomposition de A en facteurs locaux correspondants à la décomposition de f en produit de puissances de polynômes irréductibles (App. 5.8) du fait que A est réduit si et seulement si les exposants dans la décomposition de f en facteurs sont tous égaux à 1 (App. 5.9), et que A étale implique A réduit (proposition 6). Enfin, lorsque f

est irréductible, ces conditions équivalent à $f \notin k[X^p]$ en vertu de §3, prop. 1.

Définition 4. — *Soit k un corps. On dit qu'un polynôme f, à coefficients dans k, est étale, ou encore séparable, s'il est non nul et s'il satisfait aux conditions équivalentes de la proposition 9. Un élément x d'une algèbre A sur k est dit étale sur k, si la sous-algèbre $k[x]$ de A engendrée par x est étale sur k.*

On notera que si K est une extension de k, alors pour que f soit étale en tant que polynôme à coefficients dans k, il faut et il suffit qu'il le soit en tant que polynôme à coefficients dans K, comme il résulte par exemple de prop. 8 (v). C'est pourquoi il est inutile dans la première partie de la définition 4 de préciser "étale sur k", comme il est parfois prudent de le faire pour la notion d'algèbre ou d'élément étale.

Corollaire 1. — *Soient k un corps, A une k-algèbre, $(x_i)_{i\in I}$ une famille génératrice d'éléments de A. Pour que A soit étale, il faut et il suffit qu'elle soit de degré fini, commutative (i.e. que les x_i commutent deux à deux), et que pour tout $i \in I$, x_i soit étale sur k. Pour qu'un élément x de A soit étale sur k, il faut et il suffit qu'il soit algébrique sur k (§3, n°1, déf. 1) et que son polynôme minimal (§3, n°1, déf. 3) soit séparable.*

La première assertion n'est autre que prop. 8 (iv), la deuxième n'est autre que la prop. 9, compte tenu de l'isomorphisme $k[x] \simeq k[X]/fk[X]$, où f désigne le polynôme minimal de x sur k (§3, n°1, th. 1).

Corollaire 2. — *Soient k un corps, K une extension de k, x un élément de K qui est racine simple d'un polynôme $f \in k[X]$, alors x est étale sur k.*

En effet, le polynôme minimal g de x divise f (§3, th. 1) donc x est racine simple de g, donc les racines de g dans une clôture algébrique de K (qui sont conjuguées de x) sont toutes simples, donc en vertu du corollaire 1, x est séparable sur k.

Corollaire 3. — *Soient k un corps, Ω une extension de k, K une sous-extension de Ω. Tout élément x de Ω qui est étale sur k est étale sur K.*

En effet, si f est le polynôme minimal de x sur k, les racines de f (dans une extension algébriquement close de Ω) sont simples, et on a $f(x) = 0$, d'où la conclusion en vertu du corollaire 2.

Proposition 10. — *Soient k un corps, V un espace vectoriel de dimension finie sur k, $(u_i)_{i\in I}$ une famille d'endomorphismes de V, A la sous-algèbre de $End_k(V)$ qu'elle engendre, Ω une extension algébriquement close de k. Alors les conditions suivantes sont équivalentes :*

(i) La famille des endomorphismes $u_i \otimes_k \Omega$ ($i \in I$) de $V \otimes_k \Omega$ est diagonalisable (déf. 2).

(ii) L'algèbre A est étale.

Comme par définition, A est étale si et seulement si $A \otimes_k \Omega$ est diagonalisable sur Ω, et que cette dernière algèbre n'est autre que la sous-algèbre de $\mathrm{End}_\Omega(V \otimes_k \Omega)$ engendrée par les $u_i \otimes_k \Omega$, la prop. 10 est un cas particulier de l'équivalence des conditions (i) et (iii) dans la prop. 4. — Lorsque les conditions équivalentes de prop. 10 sont vérifiées, on dira parfois que la famille $(u_i)_{i\in I}$ est *absolument diagonalisable* ; on fera attention qu'une famille diagonalisable est manifestement absolument diagonalisable, mais que l'inverse n'est pas vrai en général, cf. exerc. . . . Avec la terminologie qu'on vient d'introduire, on prouve comme pour le corollaire à prop. 4 :

Corollaire. — *Soient k un corps, A une algèbre sur k. Pour que A soit étale, il faut et il suffit que pour toute représentation linéaire de A par des endomorphismes d'un espace vectoriel de dimension finie V sur k, la famille correspondante (indexée par A) d'endomorphismes de V soit absolument diagonalisable, et il faut et il suffit qu'on puisse trouver une représentation linéaire fidèle de A ayant cette propriété.*

3. — Algèbres séparables sur un corps k

Définition 5. — *Soit A une algèbre commutative sur un corps k. On dit que A est séparable (ou séparable sur k, si une confusion sur le corps de base est à craindre) si pour toute extension K de k, $A \otimes_k K$ est réduit.*

Proposition 11. — *Soit A une algèbre sur un corps k. Pour que A soit séparable, il faut et il suffit que pour toute algèbre réduite B sur k, le produit tensoriel $A \otimes_k B$ soit un anneau réduit.*

La condition est manifestement suffisante, prouvons qu'elle est nécessaire, i.e. supposons A séparable, et prouvons que si B est une algèbre réduite sur k, $A \otimes_k B$ est réduit. En vertu de App. 2.12, dire que B est réduit signifie que l'intersection des idéaux premiers $\mathfrak{p}$ de B est réduite à zéro, ou encore, introduisant les corps des fractions K des anneaux intègres $A/\mathfrak{p}$, que B se plonge dans un produit de corps, soit $P = \prod_{i\in I} K_i$. Par suite, $A \otimes_k B$ se plonge dans $A \otimes_k P = A \otimes_k \left(\prod_{i\in I} K_i\right)$, donc en vertu du Lemme 1 ci-dessous, il se plonge dans l'algèbre produit $\prod_{i\in I}(A \otimes_k K_i)$. L'hypothèse sur A implique que les $A \otimes_k K_i$ sont réduits, donc il en est de même de leur produit (App. 2.11, remords), donc aussi de $A \otimes_k B$. Il reste à prouver le

Lemme 1. — *Soient k un anneau, A un k-module, $(K_i)_{i\in I}$ une famille de k-modules, considérons l'homomorphisme canonique (réf. ?)*

$$A \otimes_k \prod_{i\in I} K_i \longrightarrow \prod_{i\in I} A \otimes_k K_i.$$

Si A est libre, cet homomorphisme est injectif.

(N. B.— Devrait figurer au Chap. II, par exemple en respect avec l'hypothèse "I fini" au lieu de "A libre"). En effet, choisissant une base $(a_j)_{j\in J}$ dans A, la source de la flèche envisagée s'identifie à $\left(\prod_{i\in I} K_i\right)^{(J)}$, donc se plonge dans $\left(\prod_{i\in I} K_i\right)^J \simeq \prod_{i\in I} K_i^J$, tandis que le but s'identifie à $\prod_{i\in I}(K_i)^{(J)}$; or le terme général de ce produit se plonge dans K_i^J, donc le produit lui-même se plonge dans $\prod_{i\in I} K_i^J$ (réf.). Avec ces identifications, on vérifie immédiatement que l'homomorphisme envisagé dans le lemme est induit par l'application identique de $\prod_{i\in I} K_i^J$, ce qui prouve qu'il est injectif.

Proposition 12. — *Soit k un corps.*

(i) Soit A une k-algèbre commutative. Si A est séparable, il en est de même de toute sous-algèbre. Inversement, si A est réunion filtrante croissante de sous-algèbres qui sont séparables, alors A est séparable.

(ii) Soit $(A_i)_{i\in I}$ une famille de k-algèbres commutatives. Pour que l'algèbre produit A soit séparable, il faut et il suffit que chacune des A_i le soit.

(iii) Soient A et B deux k-algèbres commutatives. Si A et B sont séparables, il en est de même de $A \otimes_k B$. Inversement, si $A \neq 0$ et si $A \otimes_k B$ est séparable, alors B est séparable.

(iv) Soient A une k-algèbre, k' une extension de k. Pour que A soit une k-algèbre séparable, il faut et il suffit que $A' = A \otimes_k k'$ soit une k'-algèbre séparable.

(v) Soient E une extension de k, et A une E-algèbre. Si E est séparable sur k, et A séparable sur E, alors A est séparable sur k.

Démonstration. —

(i) La première assertion résulte de ce que pour toute sous-algèbre B de A, et toute extension K de k, $B \otimes_k K$ s'identifie à une sous-algèbre de $A \otimes_k K$, donc est réduite si cette dernière l'est. De même, si A est réunion filtrante croissante de sous-algèbres B_i, alors $A \otimes_k K$ est réunion filtrante croissante de sous-algèbres isomorphes aux $B_i \otimes_k K$ (réf.), donc est réduite si ces dernières le sont, ce qui prouve la deuxième assertion de (i).

(ii) Utilisant le lemme 1 ci-dessus, on voit que pour toute extension K de k, $A \otimes_k K$ s'identifie à une sous-algèbre de $\prod_{i\in I}(A_i \otimes_k K)$; donc si les A_i sont séparables, donc les $A_i \otimes_k K$ réduits, il en est de même de leur produit (App. 2.11), donc $A \otimes_k K$ est également réduit, ce qui prouve que A est séparable. Inversement, si A est séparable, les A_i qui sont isomorphes à des sous-algèbres de A, sont séparables en vertu de (i).

(iv) Pour toute extension K' de k', $A' \otimes_{k'} K'$ est k'-isomorphe à $A \otimes_k K'$ (réf.), donc est réduite si A est séparable, ce qui implique qu'alors A' est séparable. Pour prouver l'inverse, il suffit de noter que toute extension K de k se plonge dans une extension convenable K' de k' (§4, n° 2, prop. 2), or $A \otimes_k K \simeq A' \otimes_{k'} K'$ étant réduit, il en est de même de $A \otimes_k K$, isomorphe à un sous-anneau de celui-ci, ce qui prouve que A est séparable.

(iii) Supposons A et B séparables, prouvons que $A \otimes_k B$ l'est, i.e. que pour toute extension K de k, $(A \otimes_k B) \otimes_k K$ est réduit. Or cette algèbre est canoniquement isomorphe à $A_K \otimes_K B_K$, où $A_K = A \otimes_k K$, $B_K = B \otimes_k K$ (réf.), or en vertu de (iv) déjà prouvé, A_K est une K-algèbre séparable, d'autre part B_K est une K-algèbre réduite, donc $A_K \otimes_K B_K$ est réduite en vertu de prop. 11.

(v) Soit K une extension de k, alors on a un isomorphisme $A \otimes_k K \simeq A \otimes_E (E \otimes_k K)$ (réf.), or d'après l'hypothèse sur E, $E \otimes_k K$ est réduit, ce qui implique, grâce à prop. 11 qu'il en est de même de son produit tensoriel avec l'algèbre séparable A, donc $A \otimes_k K$ est réduit. Cela prouve que A est séparable sur k.

Corollaire. — *Soit A une algèbre commutative sur un corps k. Pour que A soit séparable, il faut et il suffit que toute sous-algèbre de type fini le soit. Lorsque A est une extension de k, pour que A soit séparable, il faut et il suffit que toute sous-extension de type fini le soit.*

Cela résulte aussitôt de prop. 12 (ii).

Proposition 13. — *Soient k un corps, A une k-algèbre intègre, E son corps des fractions. Pour que A soit séparable sur k, il faut et il suffit que E le soit.*

Si E est séparable, il en est de même de A en vertu de prop. 12 (i). Inversement, supposons que A soit séparable, et prouvons que E l'est. Compte tenu de la définition de E, c'est un cas particulier du résultat plus général suivant (N. B. qu'on pourrait élever au rang de proposition, prop. 13 devenant corollaire) :

Corollaire 1. — *Soit A une algèbre séparable sur un corps k, alors pour toute partie multiplicativement stable S de A, l'anneau des fractions AS^{-1} de A par rapport à S (Chap. I ...) est séparable sur k.*

Cela résulte aussitôt de la définition, et des deux lemmes suivants :

Lemme 2. — *Soient k un anneau commutatif, A une k-algèbre commutative, S une partie multiplicativement stable de A, k' une k-algèbre commutative, $A' = A \otimes_k k'$, S' l'image de S par l'homomorphisme canonique $A \longrightarrow A'$. Alors on a un isomorphisme canonique de k'-algèbres :*

$$(AS^{-1}) \otimes_k k' \simeq A'S'^{-1}.$$

C'est un remords au Chap. II, dont je laisse la démonstration au rédacteur définitif.

Lemme 3. — *Soient A un anneau, S une partie multiplicativement stable de A. Si A est réduit, il en est de même de l'anneau des fractions AS^{-1}.*

En effet, tout élément x de AS^{-1} s'écrivant sous la forme $\varphi(y)\varphi(s)^{-1}$ avec $y \in$

$A, s \in S$, où $\varphi : A \longrightarrow AS^{-1}$ est l'homomorphisme canonique, si x est nilpotent on doit avoir $\varphi(y^n)\varphi(s^n)^{-1} = 0$ pour un entier $n > 0$ convenable, donc il existe un $t \in S$ tel que $ty^n = 0$ et a fortiori $t^n y^n = (ty)^n = 0$, ce qui implique $\varphi(y) = 0$ et a fortiori $x = 0$.

Corollaire 2. — *Soient k un corps, $(X_i)_{i\in I}$ une famille d'indéterminées. Alors l'anneau des polynômes $k[(X_i)_{i\in I}]$, et le corps des fractions rationnelles $k((X_i)_{i\in I})$, sont séparables sur k. En particulier toute extension transcendante pure de k est séparable.*

En vertu de prop. 13, il suffit de prouver que l'algèbre de polynômes $A = k[(X_i)_{i\in I}]$ est séparable, or pour toute extension K de k, $A \otimes_k K$ est canoniquement isomorphe à l'algèbre de polynômes $K[(X_i)_{i\in I}]$ (réf.), qui est intègre (réf.), et a fortiori réduite, ce qui prouve que A est séparable sur k.

Remarque. — En plus des résultats du présent numéro, et du numéro suivant (ces derniers relatifs aux algèbres séparables *entières*), le lecteur trouvera des compléments importants sur les algèbres séparables aux §11 (critère de Mac-Lane et ses conséquences) et 12 (critères différentiels de séparabilité, et étude des bases de transcendance séparables).

N. B. — La prop. 13 est bien éculée, la forme satisfaisante est celle-ci : A est séparable sur k si et seulement si A est réduite, et pour tout idéal premier *minimal* $\mathfrak{p}$ de A, le corps des fractions de $A/\mathfrak{p}$ est une extension séparable de k.

Si on le veut ici, on doit pouvoir l'avoir sans mal ; si on juge que le lieu serait plutôt en Géométrie Algébrique, on peut du moins inclure ce résultat en exercice.

4. — Algèbres entières séparables sur un corps

N. B. — Conformément à ce qui a été dit dans les "commentaires", le sorite des algèbres entières est supposé fait au §3, n°1.

Proposition 14. — *Soient k un corps, A une algèbre commutative entière sur k, $(x_i)_{i\in I}$ une famille génératrice d'éléments de A, Ω une extension algébriquement close de k. Les conditions suivantes sont équivalentes :*

(i) A est séparable.

(i bis) L'anneau $A \otimes_k \Omega$ est réduit.

(ii) Toute sous-algèbre B de A qui est de degré fini sur k est étale.

(iii) Pour tout $i \in I$, x_i est étale sur k, i.e. la sous-algèbre $k[x_i]$ de A engendrée par x_i est étale, ou encore (cor. de la prop. 9) les racines du polynôme minimal de x_i sur k sont simples.

Notons que dire que A est entière sur k revient à dire que la famille filtrante croissante des sous-algèbres B_j de A de degré fini sur k a pour réunion A, qui s'identifie par suite à leur limite inductive (§3, n°1 !). Donc pour toute extension K de k, $A \otimes_k K$ est la réunion de la famille filtrante croissante de sous-algèbres $B_j \otimes_k K$, d'où on conclut que $A \otimes_k K$ est réduit si et seulement si il en est de même des $B_j \otimes_k K$. Cela montre que pour que A satisfasse la condition (i) (resp. (i bis)), il faut et il suffit que chacun des B_j la satisfasse. En vertu de la déf. 3 (resp. de la prop. 6), cela signifie que les B_j sont étales, ce qui prouve que chacune des conditions (i), (i bis) est équivalente à (ii). Dans ce raisonnement, il est d'ailleurs loisible de remplacer la famille des B_j par n'importe quelle famille cofinale de sous-algèbres de degré fini de A. Désignant, pour toute partie finie J de I, par A_J la sous-algèbre de A engendrée par les x_i pour $i \in J$, et appliquant la remarque précédente, on voit que les conditions envisagées équivalent aussi à dire que les A_J sont des algèbres étales sur k. En vertu de prop. 8 (iv) appliqué à chacun des A_J, cela signifie aussi que les x_i sont étales sur k, i.e. équivaut à (iii).

Corollaire 1. — *Soient k un corps, A une algèbre commutative entière sur k. Si A est séparable, il en est de même de toute sous-algèbre et de toute algèbre quotient de A.*

Le cas d'une sous-algèbre n'a été mis que pour mémoire, étant déjà donné dans prop. 12 (i). Soit donc B une algèbre quotient de A. On sait déjà que, puisque A est entière, il en est de même de B (§3, n°1). Supposons de plus A séparable, donc (prop. 14) réunion filtrante croissante de sous-algèbres étales A_i. Alors l'algèbre B est réunion filtrante croissante des sous-algèbres B_i images des A_i, qui sont étales en vertu de prop. 8 (i), donc B est séparable en vertu de prop. 14 (ou de prop. 12 (i), au choix).

Corollaire 2. — *Soient k un corps, A une k-algèbre commutative entière, $(A_i)_{i\in I}$ une famille de sous-algèbres de A engendrant A. Pour que A soit séparable, il faut et il suffit que les A_i le soient.*

Appliquant prop. 14 en prenant comme famille génératrice de A celle définie par la réunion des A_i, la conclusion résulte aussitôt du critère (iii) de la prop. 14.

Corollaire 3. — *Soient k un corps, E une extension de k, K et L deux sous-extensions de E. Si K est algébrique séparable sur k, alors $L(K)$ est algébrique séparable sur L ; la réciproque est vraie si K et L sont linéairement disjointes sur k.*

Comme K est algébrique sur k, il s'ensuit que $L(K)$ est la sous-L-algèbre de E engendrée par K, (§3, n°2, prop. 7). Donc $L(K)$ est isomorphe à une algèbre quotient de la L-algèbre $K \otimes_k L$, donc est séparable sur L en vertu de prop. 12 (iv) et du corollaire précédent. La réciproque résulte de même de prop. 12 (iv).

Corollaire 4. — *Soient k un corps, E une extension de k, $(K_i)_{i\in I}$ une famille de sous-extensions algébriques de E, K l'extension engendrée par cette famille. Pour que K soit séparable sur k, il faut et il suffit que les K_i le soient.*

C'est un cas particulier du corollaire 2, compte tenu que K est aussi la *k-algèbre* engendrée par les K_i, puisque ces dernières sont algébriques sur k.

Corollaire 5. — *Soit A une algèbre entière sur un corps k. Alors il existe une plus grande sous-algèbre A_0 de A séparable sur k, et A_0 est formée des éléments de A qui sont séparables sur k.*

Nous appellerons A_0 la fermeture séparable de k dans A.

Corollaire 6. — *Soient A une algèbre entière séparable sur un corps k, Ω une extension algébriquement close de k, $P(A)$ l'ensemble des homomorphismes de k-algèbres de A dans Ω. Alors on a*

$$[A : k] = \mathit{card}\, P(A),$$

en particulier, pour que A soit de degré fini sur k, il faut et suffit que $P(A)$ soit fini.

Compte tenu de la prop. 7, on est ramené à prouver la dernière assertion, et plus précisément le fait suivant : si A est de degré infini sur k, alors $P(A)$ est infini. Or A est réunion filtrante croissante de ses sous-algèbres de degré fini A_i, qui sont étales sur k, donc on a une bijection canonique

$$P(A) \longrightarrow \varprojlim P(A_i),$$

où dans le système projectif formé des $P(A_i)$, les applications de transition sont surjectives, et les $P(A_i)$ sont finis. Il s'ensuit que les applications canoniques $P(A) \longrightarrow P(A_i)$ sont surjectives (Top. Gén.!!), donc que card $P(A) \geq$ card $P(A_i)$, or comme A est de degré infini sur k, on aura évidemment card $P(A_i) \longrightarrow +\infty$, d'où card $P(A) = \infty$. (N. B. - Le rédacteur s'aperçoit qu'il vient d'utiliser la notation card dans un sens peu orthodoxe savoir en lui attribuant une valeur unique ∞ pour un ensemble infini, et qu'il utilise Top. Gén. qui vient après. Next Redactor !).

Proposition 15. — *Soient k un corps, A une algèbre entière sur k, et K une sous-algèbre de A qui soit un corps. Pour que A soit séparable sur k, il faut et il suffit que K soit séparable sur k, et que A soit séparable sur K.*

Si A est séparable sur k, il en est de même de la sous-algèbre K (prop. 12, (i)), d'autre part, pour tout élément x de A, x est étale sur k (prop. 14 appliqué à la k-algèbre A), i.e. la sous-k-algèbre $k[x]$ de A engendrée par x est étale ; or la sous-K-algèbre $K[x]$ de A engendrée par x est isomorphe à une K-algèbre quotient de $k[x] \otimes_k K$, donc est étale (prop. 8, (v) et (i)), ce qui en vertu de prop. 14 prouve que A est étale sur K. La réciproque est un cas particulier de prop. 12 (v).

Remarque. — Nous prouverons au §11 que prop. 15 reste vraie lorsqu'on suppose seulement que K (mais pas nécessairement A) est entière sur k. Sans cette dernière restriction, nous verrons cependant que la réciproque devient inexacte (réf. exerc. au §11...).

5. — Extensions radicielles

Proposition 16. — *Soient k un corps, d'exposant caractéristique p, K une extension de k, x un élément de K, $f \in k[X]$ son polynôme minimal, e le plus grand des entiers h tels que $f \in k[X^{p^h}]$.*

(i) On a $f(X) = g(X^{p^e})$, où $g \in k[X]$ est un polynôme uniquement déterminé, et où $g \notin k[X^p]$, g est irréductible, et identique au polynôme minimal de $y = x^{p^e}$.

(ii) L'élément $y = x^{p^e}$ est étale sur k, et e est le plus petit des entiers h tels que x^{p^h} soit étale sur k.

(iii) L'application $z \rightsquigarrow z^{p^e}$ induit une bijection de l'ensemble des conjugués de x (dans une extension algébriquement close fixée Ω de k) sur l'ensemble des conjugués de y.

Démonstration. — Les assertions de (i) sont triviales, le fait que g est le polynôme minimal de y provenant (en vertu du § 3, th. 1) du fait qu'il est unitaire (comme on vérifie aussitôt), irréductible, et satisfait $g(y) = 0$. Plus généralement, pour tout entier $h \leq e$, on aura $f(X) = g_h(X^{p^h})$, où $g_h \in k[X]$, g_h est irréductible, et de façon précise est le polynôme minimal de x^{p^h}. En vertu de prop. 9 et son corollaire 1, il s'ensuit que x^{p^h} est étale sur k si et seulement si $g_h \notin k[X^p]$, ce qui équivaut manifestement à $h = e$. Cela prouve (ii). Enfin (iii) résulte aussitôt de la définition et du fait que l'application $z \rightsquigarrow z^{p^e}$ est une application bijective de Ω dans elle-même, commutant à tous les k-automorphismes de Ω.

Définition 6. — *Soit K une extension d'un corps k d'exposant caractéristique p. Un élément x de K est dit radiciel sur k s'il existe un entier $n \geq 0$ tel que $x^{p^n} \in k$. On dit que K est une extension radicielle de k, si tous ses éléments sont radiciels sur k.*

Corollaire 1. — *Sous les conditions de la définition 6, si K est algébriquement clos, un élément x de K est radiciel si et seulement si il est invariant par tous les k-automorphismes de K. En tous cas, si x est un élément de K radiciel sur k, et si e est le plus petit des entiers h tels que $x^{p^h} \in k$, alors le polynôme minimal de x sur k est $X^{p^e} - a$, où $a = x^{p^e} \in k$.*

En effet, dire que x est invariant par tous les k-automorphismes de l'extension algébriquement close K de k, revient à dire que x est algébrique sur k et que le nombre de ses conjugués est égal à 1, ou encore que son polynôme minimal n'a qu'une seule racine (§6, n° 2, prop. 3 et cor. à prop. 3). Avec les notations de la prop. 16, cela signifie donc que y n'a qu'un seul conjugué (prop. 16, (iii)), i.e. que son polynôme minimal g n'a qu'une seule racine. Comme ces racines sont simples, cela signifie que g est de degré 1, i.e. de la forme $X - a$, ce qui prouve que f est de la forme $X^{p^e} - a$, donc on a $x^{p^e} = a \in k$. Inversement, s'il existe un entier $n \geq 0$ tel que $x^{p^n} \in k$, alors pour tout k-automorphisme u de K, on a $u(x^{p^n}) = x^{p^n}$ i.e. $u(x)^{p^n} = x^{p^n}$, ce qui implique $u(x) = x$ (§1, prop. 1, cor. 1) donc x est invariant par tout k-automorphisme de K. Cela prouve la première assertion du corollaire. Pour prouver la seconde, on peut supposer que K est algébriquement clos (quitte à le remplacer par une clôture algébrique),

et il reste à prouver, avec les notations de la démonstration qui précède, que $x^{p^n} \in k$ implique $n \geq e$. Or cela résulte évidemment de la partie (ii) de la prop. 16.

Corollaire 2. — *Une extension K d'un corps k qui est radicielle et séparable est triviale.*

En effet, il revient au même de dire que tout élément d'une extension K de k, qui est radiciel et étale sur k, est dans k. Or avec les notations du corollaire 1, cela signifie que $e = 0$, et résulte en effet du fait que dans une clôture algébrique Ω de k, le polynôme $X^{p^e} - a$ doit avoir des racines simples, et qu'il s'écrit d'autre part sous la forme $(X-b)^{p^e}$, où $b \in \Omega$ est tel que $b^{p^e} = a$.

Corollaire 3. — *Soient k un corps, K une extension de k, K' une sous-extension de K telle que K soit radicielle sur K', enfin L une sous-extension de K algébrique et séparable sur k. Alors L est contenue dans K'.*

En effet, il est immédiat par définition que K étant radiciel sur K', L est radiciel sur $L \cap K'$, d'autre part il est séparable sur $L \cap K'$ (prop. 15) donc identique à $L \cap K'$ en vertu du cor. 2, ce qui prouve que $L \subset K'$.

Corollaire 4. — *Soient k un corps, K une extension algébrique de k, K_0 la fermeture séparable de k dans K (prop. 14, cor. 5). Alors K est une extension radicielle de K_0, de façon plus précise, K_0 est la plus petite sous-extension de K sur laquelle K soit radicielle, et la seule sous-extension séparable de K sur laquelle K soit radicielle.*

Si p est l'exposant caractéristique de k, dire que K est radiciel sur K_0 signifie en effet que pour tout $x \in K$, existe un entier $n \geq 0$ tel que $x^{p^n} \in K_0$ i.e. tel que x^{p^n} soit étale sur k, ce qui résulte de prop. 16 (ii). Soit L une sous-extension de K telle que K soit radiciel sur L, alors en vertu du cor. 3 on a $K_0 \subset L$. Si de plus L est séparable sur k, i.e. $L \subset K_0$, on aura donc $L = K_0$. Cela prouve le corollaire.

Corollaire 5. — *Soit K une extension radicielle de degré fini d'un corps k, d'exposant caractéristique p. Alors le degré de K sur k est une puissance de p.*

Par récurrence sur le degré de K sur k et utilisant la formule de transitivité des degrés, on est ramené au cas où K est une extension monogène $k(z)$ de k, donc son degré est égal au degré du polynôme minimal de x sur k. Comme ce polynôme est de la forme $X^{p^e} - a$

en vertu du cor. 1, donc de degré p^e, cela prouve le corollaire.

Remarque 11. — Au §11, nous généraliserons la notion d'extension radicielle en la notion d'algèbre radicielle sur un anneau, et donnerons diverses autres caractérisations des extensions radicielles d'un corps, ainsi qu'une généralisation du cor. 4 ci-dessus au cas où K est une algèbre entière sur un corps k.

6. — Corps parfaits. Clôture parfaite d'un corps

Proposition 17. — *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) Toute extension de degré fini de k est étale.

(ii) Toute algèbre réduite de degré fini sur k est étale.

(iii) Toute extension algébrique de k est séparable.

(iv) Toute algèbre entière réduite sur k est séparable.

(v) La clôture algébrique Ω de k est séparable sur k.

En effet, on a d'abord trivialement les implications

$$\begin{array}{ccccc} \text{(iv)} & \Longrightarrow & \text{(iii)} & \Longrightarrow & \text{(v)} \\ \Downarrow & & \Downarrow & & \\ \text{(ii)} & \Longrightarrow & \text{(i)}, & & \end{array}$$

d'autre part (i) implique (ii) puisque toute algèbre réduite de degré fini sur k est isomorphe à un produit fini d'extensions de degré fini de k, de sorte qu'on peut appliquer la prop. 8 (ii). D'autre part (ii) implique (iv) par le critère de la prop. 14 (ii). Enfin (v) $\Rightarrow$ (iii) puisque toute extension algébrique de k est isomorphe à une sous-extension de Ω.

Définition 7. — *On dit qu'un corps k est parfait s'il satisfait aux conditions équivalentes de la prop. 17.*

Remarque. — Nous verrons au §12 que si k est un corps parfait, alors toute algèbre réduite sur k (pas nécessairement entière), en particulier toute extension de k (pas nécessairement algébrique), est séparable.

Signalons tout de suite qu'un corps algébriquement clos est évidemment parfait. Pour d'autres exemples, cf. cor. 1 du th. 1 ci-dessous.

Proposition 18. — *Toute extension algébrique K d'un corps parfait k est un corps parfait.*

En effet, si K' est une extension algébrique de K, c'est une extension algébrique de k, donc séparable sur k puisque k est parfait, donc séparable sur K en vertu de prop. 15.

On notera que la proposition précédente ne s'étend pas au cas où K n'est pas une extension algébrique de k, cf. cor. 2 au th. 1 ci-dessous.

Théorème 1. — *Soient k un corps, p son exposant caractéristique, Ω une extension algébriquement close de k. Les conditions suivantes sont équivalentes :*

(i) Le corps k est parfait.

(ii) On a $k = k^p$.

(iii) Le corps k est identique au corps des invariants du groupe des k-automorphismes de Ω.

La condition (ii) signifie que pour $x \in \Omega$, la relation $x^p \in k$ implique $x \in k$; par suite, pour tout entier $n \geq 0$, la relation $x^{p^n} \in k$ implique $x \in k$, comme on voit par récurrence sur n. Ainsi (ii) signifie que tout élément de Ω radiciel sur k est dans k, ce qui équivaut à (iii) en vertu de prop. 16, cor. 1.

D'ailleurs comme la sous-extension $k^{p^{-\infty}}$ de Ω formée des éléments radiciels sur k est radicielle sur k, elle ne peut être séparable sur k que si elle est triviale (prop. 16, cor. 2), ce qui prouve que (i) $\Rightarrow$ (iii). Reste à prouver que (ii) $\Rightarrow$ (i).

Or supposons $k = k^p$, et soit E une extension de degré fini de k, prouvons que E est étale, ou encore que pour tout $x \in E$, le polynôme minimal f de x sur k admet x comme racine simple (prop. 9, cor. 2). En vertu de §3, n° 1, prop. 1, il suffit pour cela de vérifier que f n'appartient pas à $k[X^p]$, i.e. ne s'écrit pas sous la forme $\sum_i a_i X^{ip}$. Or un polynôme g de cette forme ne peut être irréductible, car par l'hypothèse $k = k^p$, chaque a_i s'écrit sous la forme b_i^p, avec $b_i \in k$, donc on a $\sum a_i X^{ip} = (\sum b_i X^i)^p$. Comme f est irréductible, cela achève la démonstration.

Corollaire 1. — *Tout corps de caractéristique nulle est parfait. Tout corps fini est parfait. Tout corps premier est parfait.*

La première assertion résulte trivialement du critère (ii) ci-dessus. Pour la deuxième, on note que l'application $x \mapsto x^p$ de k dans lui-même est injective ; elle est bijective si k est fini, ce qui prouve l'assertion. La dernière assertion en résulte, compte tenu du théorème 1 et du fait qu'un corps premier est fini ou de caractéristique nulle (§1, n° 1).

Corollaire 2. — *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) Le corps k est de caractéristique nulle.

(ii) Toute extension de k est parfaite.

(iii) L'extension transcendante pure $k(X)$ de k est parfaite.

On a (i) $\Rightarrow$ (ii) en vertu du théorème 1, puisque toute extension de k est de caractéristique nulle si k l'est. L'implication (ii) $\Rightarrow$ (iii) est triviale, il reste à prouver que (iii) $\Rightarrow$ (i), donc que si k est de caractéristique $p > 0$, alors $k(X)$ n'est pas parfait. En effet notez que X n'est pas dans $k(X)^p$, i.e. ne peut s'écrire sous la forme $(f/g)^p$ avec $f, g \in k[X]$, $g \neq 0$, car autrement on aurait une identité

$$f(X)^p = Xg(X)^p,$$

ce qui est impossible, car le premier (resp. le deuxième) membre ne fait intervenir que des puissances de X d'exposant congru à 0 (resp. à 1) $\pmod p$, donc l'égalité ne peut avoir lieu que si les deux membres sont nuls, ce qui contredit l'hypothèse $g \neq 0$.

Remarque. — On verra au §13, que les conditions du corollaire 2 équivalent encore à l'existence d'*une* extension *de type fini non algébrique* qui soit parfaite, en d'autres termes : si k est de caractéristique non nulle, alors toute extension de type fini non algébrique est non parfaite. Cela montre que sur un corps de base k de caractéristique non nulle (même si k est parfait, ou même algébriquement clos), les "corps de fonctions" qui s'introduisent le plus fréquemment en Géométrie Algébrique sont non parfaits.

Corollaire 3. — *Soient K un corps, $(K_i)_{i\in I}$ une famille de sous-corps, k son intersection. Si les K_i sont parfaits, il en est de même de k.*

En effet, Ω étant une clôture algébrique de K, il suffit de noter que si les K_i sont stables par l'application $x \mapsto x^{p^{-1}}$ de Ω dans lui-même, il en est de même de leur intersection.

Définition 8. — *Soit k un corps. Une extension k' de k est appelée une clôture parfaite de k si c'est une extension parfaite de k, et si tout sous-extension parfait de k' est identique à k'.*

Proposition 19. — *Soit k un corps. Il existe une clôture parfaite de k, et étant donné deux clôtures parfaites de k, il existe un unique k-isomorphisme de l'une sur l'autre. Si Ω est une extension parfaite de k, alors la sous-extension $k^{p^{-\infty}}$ formée des $x \in \Omega$ radiciels sur k est une clôture parfaite de k.*

Si K est une sous-extension parfaite de Ω, on a $K = K^p$, donc par récurrence sur n, on a $K = K^{p^n}$ pour $n \geq 0$, d'où évidemment $k^{p^{-\infty}} \subset K$. D'autre part, on a évidemment $k'^p = k'$ (posant $k' = k^{p^{-\infty}}$), donc k' est une extension parfaite de k. C'est donc la plus petite sous-extension parfaite de Ω, donc c'est une clôture parfaite de k. Soient maintenant k', k'' deux clôtures parfaites de k, prouvons qu'il existe un unique k-isomorphisme de k' sur k''. En vertu de §4, n° 2, prop. 2 on peut supposer que k' et k'' sont des sous-extensions d'une même extension Ω de k, qu'on peut d'ailleurs supposer algébriquement close, donc parfaite. Mais alors k' et k'' sont identiques d'après ce qui précède. Il reste à prouver seulement que tout k-automorphisme u de k' est l'identité. Or pour tout $x \in k'$, il existe un entier $n \geq 0$ tel que $a = x^{p^n} \in k$, donc on aura $u(x)^{p^n} = a$, i.e. $u(x)^{p^n} = x^{p^n}$, ce qui implique $u(x) = x$, donc u est bien l'identité. Cela achève la démonstration.

Compte tenu de la prop. 19, il n'y a pas d'inconvénient à identifier canoniquement les diverses clôtures parfaites du corps k, et nous désignerons généralement cette clôture parfaite par le symbole $k^{p^{-\infty}}$, où p désigne l'exposant caractéristique de k. Bien entendu, si $p = 1$ i.e. k est de caractéristique nulle, on a $k^{p^{-\infty}} = k$. Notons aussi la caractérisation suivante des clôtures parfaites :

Proposition 20. — *Soient k un corps, K une extension de k. Pour que K soit une clôture parfaite de k, il faut et il suffit qu'elle soit radicielle, et que pour toute extension radicielle k' de k, il existe un k-homomorphisme de k' dans K.*

Soit en effet Ω une extension algébriquement close de K ; alors la première condition exprime que K est contenue dans la sous-k-extension $k^{p^{-\infty}}$ de Ω, la seconde que toute sous-k-extension radicielle de Ω, ou encore, la plus grande sous-k-extension radicielle $k^{p^{-\infty}}$ de Ω, est contenue dans K (compte tenu qu'une extension radicielle k' de k, étant algébrique sur k, est isomorphe à une sous-extension de Ω). La conjonction des deux conditions signifie donc que $K = k^{p^{-\infty}}$ i.e. que K est une clôture parfaite de k.

7. — Clôture séparable d'un corps

Proposition 21. — *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) Toute extension étale de k est triviale.

(ii) Toute extension algébrique séparable de k est triviale.

(iii) Toute algèbre étale sur k est diagonalisable.

(iv) La clôture algébrique de k est radicielle sur k.

(v) La clôture parfaite de k est algébriquement close.

On a évidemment $(ii) \Rightarrow (i)$ et $(iii) \Rightarrow (i)$, d'autre part $(i) \Rightarrow (ii)$ puisque toute extension algébrique séparable de k est réunion de ses sous-extensions étales, et $(i) \Rightarrow (iii)$ puisque toute algèbre étale sur k est isomorphe au produit d'une famille finie d'extensions étales. L'équivalence des conditions (iv) et (v) résulte aussitôt de la construction de la clôture parfaite $k^{p^{-\infty}}$ de k en termes d'une clôture algébrique Ω, (prop. 17). D'autre part $(ii) \Rightarrow (iv)$ en vertu du corollaire 4 à prop. 16, et $(iv) \Rightarrow (ii)$ en vertu du cor. 2 à prop. 16.

Définition 9. — *Un corps est dit séparablement clos s'il satisfait aux conditions équivalentes de la prop. 21.*

Par exemple, un corps algébriquement clos est évidemment séparablement close.

Corollaire. — *Soient k un corps, Ω une extension séparablement close de k, K une extension algébrique séparable de k. Alors K est isomorphe à une sous-extension de Ω.*

En effet, si Ω' est une clôture algébrique de Ω, on sait que Ω' est radicielle sur Ω, et que K est isomorphe à une sous-extension K' de Ω'. En vertu de prop. 16, cor. 3 on a $K' \subset \Omega$; ce qui prouve notre assertion.

Proposition 22. — *Soient k un corps, K une extension de k, Ω une extension séparablement close de k. Les conditions suivantes sont équivalentes :*

(i) *K est une extension algébrique séparable et un corps séparablement clos.*

(ii) *K est une extension algébrique séparable, et toute extension algébrique séparable k' de k est isomorphe à une sous-extension de K.*

(iii) *K est k-isomorphe à la fermeture algébrique séparable k_s (prop. 14, cor. 5) de k dans Ω.*

Les implications $(i) \Rightarrow (ii)$ et $(iii) \Rightarrow (ii)$ résultent aussitôt du corollaire précédent. Il suffit donc de prouver que deux extensions K, K' de k satisfaisant à (ii) sont isomorphes. Or soient $u : K \longrightarrow K'$ et $u' : K' \longrightarrow K$ des k-homomorphismes, alors uu' et $u'u$ sont des k-endomorphismes de K' resp. K, donc des automorphismes de ces extensions (§6, prop. 4), donc u et u' sont des isomorphismes, ce qui prouve notre assertion. (N. B. — Il y aurait lieu, après §6, prop. 6, de signaler en corollaire que deux extensions algébriques dont chacune est isomorphe à une sous-extension de l'autre sont isomorphes).

Définition 10. — *Une extension K de k, satisfaisant aux conditions équivalentes de la prop. 22, est appelée une clôture séparable de k.*

On conclut aussitôt de cette définition :

Définition 10. — *Soit k un corps. Il existe une clôture séparable de k, et deux clôtures séparables sont isomorphes. Si Ω est une extension séparablement close de k, la sous-extension k_s, fermeture séparable de k dans Ω, est une clôture séparable de k.*

Par abus de langage, on désigne souvent par k_s une clôture séparable quelconque de k. On fera attention cependant qu'en général, étant données deux clôtures séparables du corps k, il peut exister plusieurs k-isomorphismes distincts de l'une sur l'autre, en d'autres termes, le groupe des k-automorphismes de k_s n'est pas en général réduit à l'élément

neutre. De façon précise, comme k_s est une extension quasi-galoisienne de k, on conclut de prop. 16, cor. 1 et cor. 2, que le groupe des k-automorphismes de k_s n'est réduit au groupe unité que si k_s est radiciel sur k, donc égal à k, i.e. si et seulement si k est déjà séparablement clos.

Proposition 23. — *Soit k un corps. Pour que k soit algébriquement clos, il faut et il suffit qu'il soit parfait et séparablement clos.*

Il est trivial qu'un corps algébriquement clos est parfait et séparablement clos. Inversement, si k est séparablement clos (i.e. sa clôture algébrique Ω est radicielle sur k) et parfait (donc Ω est séparable sur k), il s'ensuit par la prop. 16, cor. 2 que $k = \Omega$ donc que k est algébriquement clos.

Corollaire. — *Soit k un corps. Pour que k soit parfait, il faut et il suffit que sa clôture séparable k_s soit algébriquement close.*

Si k est parfait, il en est de même de k_s en vertu de prop. 18, donc k_s est algébriquement clos en vertu de prop. 23. Réciproquement, si k_s est algébriquement clos i.e. la clôture algébrique de k est une extension algébriquement close de k, k est parfait.

§ 8. — EXTENSIONS GALOISIENNES ET THÉORIE DE GALOIS

1. — Extensions galoisiennes

Proposition 1. — *Soient K un corps, E une extension algébrique de K, G le groupe des K-automorphismes de E. Les conditions suivantes sont équivalentes :*

(i) Le corps des invariants de G dans E est identique à K.

(ii) E est quasi-galoisienne et séparable.

(iii) Pour tout $x \in E$, le polynôme minimal de x sur K a toutes ses racines (dans une clôture algébrique donnée Ω de E) simples et contenues dans E.

La condition (ii) équivaut à (iii) en vertu du critère §6, n° 3, prop. 5 (iv) (cf. commentaires à la rédaction), suivant lequel E est quasi-galoisienne si et seulement si les polynômes minimaux de ses éléments ont toutes leurs racines dans E, et du critère §7, n° 3, prop. 11 (iii), suivant lequel E est séparable sur K si et seulement si ces racines sont toutes simples. Montrons que (i) implique (iii).

En effet, soit $x \in E$ et soient x_i $(1 \leq i \leq n)$ les éléments distincts de l'ensemble des conjugués de x contenus dans E. Tout K-automorphisme u de E permute entre eux les x_i, donc le polynôme $g(X) = \prod_{1 \leq i \leq n}(x - x_i) \in E[X]$ est invariant par G, i.e. ses coefficients sont invariants par G, donc en vertu de l'hypothèse (i) appartiennent à K. Comme $g(x) = 0$, g est un multiple du polynôme minimal f de x sur K (§3, th. 1), ce qui montre que f a toutes ses racines simples et contenues dans E. Prouvons enfin que (iii) implique (i). Soit en effet x un élément de E non dans K ; comme le polynôme

minimal f de x sur K a toutes ses racines simples et contenues dans E, et qu'il est de degré > 1, il s'ensuit qu'il existe au moins un élément y de E conjugué de x et distinct de x. Comme nous savons déjà que E est une extension quasi-galoisienne de K, donc que tout K-automorphisme de Ω induit un K-automorphisme de E, il s'ensuit qu'il existe un $u \in G$ tel que $u(x) = y$, ce qui prouve que le corps des invariants de G dans E est réduit à K, et achève la démonstration de la proposition.

Corollaire. — *Supposons que E soit de degré fini n sur K, et soit G le groupe des K-automorphismes de E. Alors les conditions précédentes équivalent aussi à la condition :*

(iv) On a card$(G) = n$ (ou seulement : card$(G) \geq n$).

En effet, en vertu de §7, prop. 7, dire que E est séparable (i.e. ici étale) sur K revient à dire qu'il y a exactement n K-homomorphismes de E dans Ω, et dire que E est quasi-galoisienne revient à dire que ces K-homomorphismes sont en fait des K-automorphismes de E, d'où l'équivalence de (ii) et (iv).

Définition 1. — *Soient K un corps, E une extension de K. On dit que E est galoisienne si elle est quasi-galoisienne et séparable, c'est-à-dire si elle satisfait les conditions équivalentes de la prop. 1. Le groupe des K-automorphismes de E s'appelle alors le groupe de Galois de E (ou le groupe de Galois de E sur K, si une ambiguïté est à craindre sur le corps de base). Il sera noté* Gal(E/K).

Proposition 2. — *Soit E une extension d'un corps K, K' une sous-extension de E. Si E est galoisienne sur K, elle est galoisienne sur K', et* Gal(E/K') *est un sous-groupe de* Gal(E/K).

La première assertion résulte de la définition et des assertions analogues relatives aux extensions quasi-galoisiennes resp. séparables (§6, n° 3, prop. 10 — cf. "commentaires" — et §7, n° 3, prop. 14). Le fait que Gal(E/K') soit alors un sous-groupe de Gal(E/K) est trivial sur les définitions.

Corollaire 1. — *Sous les conditions de la prop. 2, soit $u \in$ Gal(E/K), alors le groupe de Galois de E sur $u(K')$ est le conjugué par u du groupe de Galois de E sur K' :*

$$\text{Gal}(E/u(K')) = u\,\text{Gal}(E/K')u^{-1}.$$

C'est évident par transport de structure.

Corollaire 2. — *Sous les conditions de la prop. 2, pour que K' soit une extension galoisienne de K, il faut et il suffit que le sous-groupe* $\mathrm{Gal}(E/K')$ *de* $\mathrm{Gal}(E/K)$ *soit un sous-groupe distingué de ce dernier. Dans ce cas, l'homomorphisme $u \rightsquigarrow u|K'$ de* $\mathrm{Gal}(E/K)$ *dans* $\mathrm{Gal}(K'/K)$ *est surjectif de noyau Gal(E/K'), donc fournit un isomorphisme canonique*

$$\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/K').$$

La première assertion résulte aussitôt du corollaire 1. Lorsque K' est galoisienne, tout K-automorphisme de E induit bien un K-automorphisme de K', et d'autre part tout K-automorphisme de K' peut se prolonger en un K-automorphisme de E (§6, n° 3), ce qui prouve la deuxième assertion.

N. B. — Le rédacteur s'aperçoit qu'il serait commode de disposer de la terminologie "groupe de Galois" également dans le cas quasi-galoisien, et qu'il serait commode de donner également dans ce cas la proposition 2 et les deux corollaires précédents, de nature purement soritale. Il laisse au rédacteur définitif le petit réajustage à faire au §6, $n^\circ 3$.

On dit qu'une extension E d'un corps K est *abélienne* si elle est galoisienne et si son groupe de Galois est abélien. On déduit donc de la proposition 2 de son corollaire 2 :

Corollaire 3. — *Soit E une extension d'un corps K, K' une sous-extension de E. Si E est abélienne, il en est de même de K', et E est abélienne sur K'.*

Proposition 3. — *Soient K un corps, Ω une extension de K, $(E_i)_{i\in I}$ une famille de sous-extensions de Ω. Si les E_i sont galoisiennes, il en est de même de leur intersection, et de l'extension engendrée par les E_i.*

Cela résulte des énoncés analogues concernant les extensions quasi-galoisiennes resp. les extensions entières séparables, (§6, n° 3, prop. 7 — cf. commentaires — et §7, prop. 13 (i) et (iii)).

Corollaire 1. — *Soient K un corps, Ω une extension algébriquement close de K, S une partie de Ω, et E la sous-extension quasi-galoisienne de Ω engendrée par S (§3, n° 3). Alors E est galoisienne si et seulement si les éléments de S sont séparables sur K.*

En effet, si G est le groupe des K-automorphismes de Ω, E est l'extension engendrée

par la réunion T des $u(S)$, pour $u \in G$. Comme cette extension est quasi-galoisienne, il reste à prouver qu'elle est séparable, ce qui revient à dire que les éléments de T sont séparables sur K (§7, n° 3, prop. 11). Comme un élément y conjugué d'un élément x algébrique sur K est évidemment séparable sur K si et seulement si x l'est, la condition obtenue équivaut aussi à dire que les éléments de S sont séparables sur K, ce qui prouve notre affirmation.

Corollaire 2. — *Soit $(f_i)_{i\in I}$ une famille de polynômes séparables de $K[X]$ (§7, n° 2, déf. 4). À l'ensemble de leurs racines dans l'extension algébriquement close Ω de K, alors $K(A)$ est une extension galoisienne de K.*

N. B. — On peut, si on le juge bon, recopier ici le laïus de l'édition actuelle fin de §10, n° 3, page 149. Le rédacteur n'y tient pas particulièrement. Il propose aussi de laisser tomber le corollaire qu'une extension composée d'extensions abéliennes est abélienne (qu'on peut néanmoins, si on y tient, rajouter en un corollaire 3 ici même).

Théorème 1. — *Soient K un corps, Ω une extension de K, E et K' deux sous-extensions de Ω, $E' = K'(E)$ l'extension composée et $L = E \cap K'$. Supposons E galoisienne sur K. Alors E' est galoisienne sur K', et K' et E sont linéairement disjointes sur L. De plus, tout K'-automorphisme de E' induit un L-automorphisme de E, et l'homomorphisme de restriction $u \rightsquigarrow u|E$ ainsi obtenu est un isomorphisme :*

$$\mathrm{Gal}(E'/K') \xrightarrow{\sim} \mathrm{Gal}(E/L).$$

Corollaire 1. — *Pour toute sous-extension F' de la K'-extension E', posant $F = F' \cap E$, on a $F' = K'(F)$.*

En effet, en vertu de prop. 2 E' est galoisienne sur F', et son groupe de Galois sur F' est un sous-groupe H' du groupe de Galois $\mathrm{Gal}(E'/K')$. Soit H l'image de H' par l'isomorphisme $\mathrm{Gal}(E'/K') \longrightarrow \mathrm{Gal}(E/L)$ du th. 1, alors le corps des invariants de H n'est autre que $F = E \cap F'$, compte tenu que F' est le corps des invariants de H'. Identifiant alors, grâce au th. 1, $K'(E)$ à $E \otimes_K K'$ et les opérations de H' aux opérations $u \otimes_K \mathrm{id}_{K'}$, $(u \in H)$, on constate aussitôt que l'ensemble des invariants de H' n'est autre que $F \otimes_K K'$, ce qui signifie aussi que $F' = K'(F)$.

Le Corollaire ne se généralise pas au cas où E et K' sont deux extensions

linéairement disjointes de K, mais où on ne suppose pas E galoisienne (exerc....).

Corollaire 2. — *Soient E_1 et E_2 deux extensions galoisiennes d'un corps K, telles que $E_1 \cap E_2 = K$. Alors E_1 et E_2 sont linéairement disjointes, $E = K(E_1 \cup E_2)$ est une extension galoisienne de K, et l'homomorphisme $u \rightsquigarrow (u|E_1, u|E_2)$ induit un isomorphisme de groupe*

$$\mathrm{Gal}(E/K) \xrightarrow{\sim} \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K).$$

On sait par le th. 1 que E_1 et E_2 sont linéairement disjointes, par la prop. 3 que E est galoisienne, et il est immédiat que l'homomorphisme envisagé dans le cor. 2 est injectif. Pour prouver qu'il est surjectif, il suffit de noter que, puisque E_1 et E_2 sont linéairement disjointes, E s'identifie à l'algèbre $E_1 \otimes_K E_2$, et si u_1 (resp. u_2) est un K-automorphisme de E_1 (resp. E_2) alors $u = u_1 \otimes u_2$ est un K-automorphisme de $E_1 \otimes_K E_2$ induisant u_1 et u_2 sur les deux sous-algèbres E_1 et E_2.

2. — Applications aux extensions quasi-galoisiennes

N. B. — Ce n° pourrait être mis en petits caractères ; il ne resservira pas dans la suite du livre.

Proposition 4. — *Soient K un corps, E une extension quasi-galoisienne de K, E_0 la fermeture séparable de X dans E (§7, prop. 14, cor. 5), E_1 le corps des invariants du groupe* $\mathrm{Gal}(E/K)$ *des K-automorphismes de E. Alors :*

(i) *E_1 est la plus grande sous-extension radicielle de E.*

(ii) *E_0 est une extension galoisienne de K, linéairement disjointe de E_1, et $E = K(E_0 \cup E_1)$, donc l'homomorphisme canonique $E_0 \otimes_K E_1 \longrightarrow E$ est un isomorphisme.*

(iii) *E est une extension galoisienne de E_1, et l'application de restriction* $\mathrm{Gal}(E/E_1) = \mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(E_0/K)$ *est un isomorphisme.*

Soit Ω une clôture algébrique de E. Comme tout K-automorphisme de E se prolonge en un K-automorphisme de Ω, et que par l'hypothèse quasi-galoisienne sur E, E est stable par les K-automorphismes de Ω, E_0 n'est autre que l'intersection de E avec le corps des

invariants du groupe des K-automorphismes de Ω, et l'assertion (i) résulte donc de §7, prop. 16, cor. 1. D'autre part, on a $E_0 \cap E_1 = K$, car $E_0 \cap E_1$ est une extension séparable et radicielle de K, donc triviale en vertu de §7, prop. 16, cor. 2. D'autre part, comme E est stable par les K-automorphismes de Ω, il en est évidemment de même de E_0, qui est donc une extension quasi-galoisienne de K, et comme elle est séparable, elle est galoisienne. Il résulte alors du th. 1 que E_0 et E_1 sont linéairement disjoints sur K. D'autre part, en vertu de §7, prop. 16, cor. 3, E est radicial sur E_0, donc ses éléments sont invariants par les E_0-automorphismes de E (§7, prop. 16, cor. 1), d'où on conclut aussitôt que tout K-automorphisme de E_0 se prolonge de façon unique en un K-automorphisme de E ; il est trivial d'ailleurs par définition que E est une extension galoisienne de E_1, ce qui établit (iii). Soit enfin $E' = E_1(E_0)$, alors en vertu de th. 1 E' est une extension galoisienne de E_1 et l'application de restriction $\mathrm{Gal}(E'/E_1) \longrightarrow \mathrm{Gal}(E_0/K)$ est un isomorphisme. Comme il en est de même, par (iii), de l'application composée des applications de restriction $\mathrm{Gal}(E/E_1) \longrightarrow \mathrm{Gal}(E'/E_1) \longrightarrow \mathrm{Gal}(E_0/K)$, on voit que l'application de restriction $\mathrm{Gal}(E/E_1) \longrightarrow \mathrm{Gal}(E'/E_1)$ est un isomorphisme, ce qui signifie en vertu de prop. 2 cor. 2 que $\mathrm{Gal}(E/E')$ est le groupe unité, de sorte que E est une extension galoisienne de E' dont le groupe de Galois est le groupe unité, donc E est une extension radicielle et séparable et par suite triviale de E (§7, prop. 16, cor. 1 et cor. 2). Donc $E = E'_0$, ce qui prouve (ii) et achève de prouver la proposition.

On conclut de la partie (i) de la proposition qui précède une généralisation partielle du th. 1 au cas des extensions quasi-galoisiennes :

Corollaire 1. — *Soient K un corps, Ω une extension de K, E et K' deux sous-extensions de Ω, $E' = K'(E)$ l'extension composée et $L = E \cap K'$. Si E est une extension quasi-galoisienne de K, E' est une extension quasi-galoisienne de K', et l'homomorphisme de restriction $u \rightsquigarrow u|E$ de $\mathrm{Gal}(E'/K')$ dans $\mathrm{Gal}(E/L)$ est un isomorphisme.*

On sait déjà que E' est une extension quasi-galoisienne de K' et que E est une extension quasi-galoisienne de L (§6, n° 3) ; donc c'est une extension galoisienne d'une extension radicielle E_1 de L. Soit $E'_1 = K'(E_1)$, alors E'_1 est une extension radicielle de K', car engendrée par les éléments de E_1, qui sont radicielles sur L, donc sur K' qui contient L. D'ailleurs $E \cap E_1$ est une sous-extension radicielle de E, donc par construction de E_1 est contenue dans E_1, donc égale à E_1. Appliquons maintenant le th. 1 aux extensions E et E'_1 de E_1. On trouve que E' est une extension galoisienne de E'_1, et que

l'homomorphisme de restriction $\mathrm{Gal}(E'/E'_1) \longrightarrow \mathrm{Gal}(E/E_1)$ est un isomorphisme. Or comme E_1 (resp. E'_1) est une extension radicielle de L (resp. K'), les groupes précédents ne sont autres que les groupes $\mathrm{Gal}(E/L)$ et $\mathrm{Gal}(E'/K')$ et l'homomorphisme envisagé l'homomorphisme de restriction envisagé dans le corollaire 1. Cela prouve le corollaire 1. De plus :

Corollaire 2. — *Sous les conditions du corollaire 1, soit E_0 (resp. E_1) la plus grande sous-L-extension séparable (resp. radicielle) de E, et soient de même E'_0 (E'_1) la plus grande sous-extension séparable (resp. radicielle) de E' sur K'. Alors on a $E'_0 = K'(E_0)$, $E'_1 = K'(E'_1)$, E_0 et K' sont linéairement disjoints sur L et E et E'_1 sont linéairement disjoints sur E_1. Pour que E et K' soient linéairement disjoints sur L, i.e. pour que l'homomorphisme canonique $E \otimes_L K' \longrightarrow E'$ soit un isomorphisme, il faut et il suffit que E_1 et K' soient linéairement disjoints sur L.*

La relation $E'_1 = K'(E_1)$ a déjà été prouvée dans la démonstration du corollaire 1, pour prouver la relation $E'_0 = K'(E_0)$, on note que $K'(E_0)$ est une sous-extension de E' séparable sur K' (§7, prop. 14, cor. 3) et que E' est radicielle sur $K'(E_0)$, car engendrée par E dont les éléments sont radicielles sur E_0 donc sur $K'(E_0)$. En vertu de §7, prop. 16, cor. 3, cela montre que $K'(E_0) = E'_0$. Comme on a évidemment $E_0 \cap K' = L$ puisque $E \cap K' = L$, on conclut par le th. 1 que E_0 et K' sont linéairement disjoints sur L. D'ailleurs le même th. 1 appliqué aux extensions E et E'_1 de E prouve que E et E'_1 sont linéairement disjoints sur E_1. On en conclut que l'homomorphisme canonique $E \otimes K' \longrightarrow E'$ s'identifie à l'homomorphisme déduit, par changement du corps de base $E_1 \longrightarrow E$, de l'homomorphisme canonique $E_1 \otimes_L K' \longrightarrow E'_1$. Donc le premier est un isomorphisme si et seulement si le deuxième l'est, ce qui achève la démonstration du corollaire 2.

Remarque. — Nous verrons au §12, avec le critère de Mac-Lane, qu'une extension séparable d'un corps est linéairement disjointe de toute extension radicielle de ce corps. Comme, avec les notations du cor. 2, E_1 est une extension radicielle de L, il s'ensuit que ni K' est une extension séparable de L. E_1 et K' sont linéairement disjoints sur L et par suite E et K' sont linéairement disjoints sur L.

3. — La théorie de Galois : classification des sous-extensions d'une extension galoisienne finie

Théorème 2. — *Soient E un corps, G un sous-groupe du groupe des automorphismes de E, K le corps des invariants de G. Pour que E soit de degré fini sur K, il faut et il suffit que G soit fini. Dans ce cas, E est une extension galoisienne de K, G est son groupe de Galois, et le degré de E sur K est égal à l'ordre de G.*

Si E est une extension de degré fini n de K, c'est une extension algébrique, et il résulte immédiatement de la définition qu'elle est galoisienne. De plus, en vertu de App. 5.5 le groupe de *tous* les K-automorphismes de E a au plus n éléments, a fortiori l'ordre de G est au plus n. Il reste à démontrer que si G est d'ordre fini m, alors E est de degré fini sur K et $[E : K] \leq m$. Or c'est un cas particulier du théorème d'Artin (§6, n° 4, th. 1).

Théorème 3. — *Soient E une extension galoisienne de degré fini d'un corps K, G son groupe de Galois, $\mathcal{K}$ l'ensemble des sous-extensions de E, $\mathcal{G}$ l'ensemble des sous-groupes de G. Pour tout sous-groupe H de G, soit $\underline{k}(H)$ le corps des invariants de H, et pour toute sous-extension F de E, soit $\underline{g}(F)$ son groupe de Galois, qui est donc un sous-groupe de G (prop. 2). On obtient ainsi deux applications :*

$$\underline{k} : \mathcal{G} \longrightarrow \mathcal{K} \quad \textit{et} \quad \underline{g} : \mathcal{K} \longrightarrow \mathcal{G}$$

Ces applications sont bijectives, et inverses l'une de l'autre. Pour tout couple (H, F), avec $H \in \mathcal{G}$ et $F = \underline{k}(H)$, on a :

$$[H : e] = [E : F] \quad , \quad [G : H] = [F : K].$$

En effet, le fait que $\underline{k} \circ \underline{g}$ soit l'application identique n'est autre que la prop. 2, et le fait que $\underline{g} \circ \underline{k}$ soit l'application identique est un cas particulier du th. 2. La formule $[H : e] = [E : F]$ est un cas particulier de th. 2, en particulier $[G : e] = [E : K]$; la deuxième formule en résulte compte tenu des relations

$$[E : F][F : K] = [E : K] \quad \text{et} \quad [G : H][H : e] = [G : e]$$

Corollaire 1. — *Ordonnons $\mathcal{G}$ et $\mathcal{K}$ par inclusion. Alors les applications $\underline{k}$ et $\underline{g}$ sont strictement décroissantes. Si $(F_i)_{i \in I}$ est une famille de sous-extensions de E, F leur inter-*

section, alors $\mathrm{Gal}(E/F) = \underline{g}(F)$ *est le sous-groupe de* G *engendré par les* $\mathrm{Gal}(E/F_i) = \underline{g}(F_i)$.

Il est trivial que $\underline{k}$ et $\underline{g}$ sont décroissantes, d'où il résulte aussitôt qu'elles sont strictement décroissantes, compte tenu qu'elles sont inverses l'une de l'autre. Par suite, chacune de ces applications induit un isomorphisme de l'ensemble ordonné source avec l'ensemble but, muni de la structure d'ordre opposée de sa structure d'ordre envisagée dans le corollaire 1. Cela implique que chacune de ces applications échange entre elles les opérations Inf et Sup, d'où en particulier la dernière assertion du corollaire.

Corollaire 2. — *Soit* H *un sous-groupe de* G. *Pour que le corps des invariants* F *de* H *soit une extension galoisienne de* K, *il faut et il suffit que* H *soit distingué.*

Cela résulte aussitôt du th. 1 et de prop. 2, cor. 2.

Corollaire 3. — *Soient* F_1 *et* F_2 *deux sous-extensions de* E, H_1 *et* H_2 *leurs groupes de Galois. Pour que* F_1 *et* F_2 *soient linéairement disjointes, il faut et il suffit qu'on ait*

$$[G : H_1 \cap H_2] = [G : H_1][G : H_2]$$

En effet, $F = K(F_1 \cup F_2)$, cette relation équivaut à

$$[F : K] = [F_1 : K][F_2 : K]$$

qui est un critère de disjonction linéaire (§2, prop. 4).

Corollaire 4. — *Soit* E *une extension galoisienne de degré fini d'un corps* K, G *son groupe de Galois,* G_1 *et* G_2 *deux sous-groupes de* G, E_1 *(resp.* E_2*) le corps des invariants de* G_1 *(resp.* G_2*). Les conditions suivantes sont équivalentes :*

(i) On a $G_1 \cap G_2 = (e)$ *et* $G_1 \cdot G_2 = G$.

(i bis) Tout élément de G *peut s'écrire, de façon unique, sous la forme* $g_1 g_2$, *avec* $g_1 \in G_1, g_2 \in G_2$.

(1 ter) On a $G_1 \cap G_2 = (e)$ *et* $[G : G_1 \cap G_2] = [G : G_1][G : G_2]$.

(ii) Les extensions E_1 *et* E_2 *sont linéairement disjointes et engendrent* E, *i.e. l'homomorphisme naturel*

$$E_1 \otimes_K E_2 \longrightarrow E$$

est un isomorphisme.

L'équivalence des conditions (i) (i bis) (i ter) est une question de pure théorie des groupes, et a été vue (?) au Chap. I. En vertu du th. 3, $G_1 \cap G_2 = (e)$ équivaut à $K(E_1 \cup E_2) = E$, donc l'équivalence de (i ter) et de (ii) résulte du corollaire 3.

Notons qu'il résulte du cor. 4 et du cor. 2 que, pour que G_2 soit invariant dans G et que G soit le produit semi-direct de G_1 et G_2, il faut et il suffit que la condition (ii) soit satisfaite et que de plus E_2 soit une extension galoisienne de K. Plus particulièrement, on obtient :

Corollaire 5. — *Avec les notations du corollaire 4, pour que G soit le produit direct des sous-groupes G_1 et G_2, il faut et il suffit que E_1 et E_2 soient deux sous-extensions galoisiennes de E engendrant E, et que leur intersection soit K (ce qui implique déjà qu'elles sont linéairement disjointes, donc que l'homomorphisme canonique $E_1 \otimes_K E_2 \longrightarrow E$ est un isomorphisme).*

Proposition 5. — *Soient K un corps, E une extension étale de K, n son degré. Alors il y a au plus 2^n sous-extensions de E.*

En effet, soit E' l'extension quasi-galoisienne engendrée par E dans une clôture algébrique Ω de E, alors E' est galoisienne (prop. 3, cor. 1) ; soit G son groupe de Galois, et H le groupe de Galois de E' sur E. En vertu du th. 3 et de son cor. 1, il y a une correspondance biunivoque entre l'ensemble des sous-extensions de E, et l'ensemble des sous-groupes de G contenant H. Ce dernier ensemble est en correspondance biunivoque avec un sous-ensemble de l'ensemble des parties de G/H. Comme card $G/H = n$ (th. 1), la prop. 5 en résulte.

N. B. — La prop. 5 me semble bonne pour être mise en exercice. Il serait camularesque en tous cas de la donner sans la précision du 2^n, car pour ce qui concerne la seule assertion de finitude, elle est pratiquement triviale sans théorie de Galois, et vraie pour l'ensemble des sous-algèbres d'une algèbre étale : on est en effet ramené au cas d'une algèbre diagonalisable par extension de la base, et dans ce cas on regarde (les sous-algèbres correspondent alors biunivoquement aux relations d'équivalence sur un ensemble à n éléments).

4. — Algèbres galoisiennes sur un corps

Le présent n° et le suivant sont indépendants de la théorie de Galois (n° 3).

Soit k un corps, et G un groupe. Dans le présent numéro, nous étudions certaines structures A de l'espèce suivante : A est une k-algèbre commutative de degré fini, sur laquelle G opère par automorphismes de k-algèbre. Nous savons (App. 3) qu'il y a une correspondance biunivoque canonique entre l'ensemble des idéaux maximaux de A et l'ensemble des facteurs indécomposables (ou encore, locaux) de A. En vertu de App. 5, A s'identifie canoniquement à un produit fini d'algèbres B_i à groupe d'opérateurs G, tel que pour chaque B_i, G opère transitivement sur l'ensemble des idéaux maximaux de B_i. De plus, si $A \neq 0$, pour que ce produit soit réduit à un seul facteur, i.e. pour que G opère transitivement sur l'ensemble des idéaux maximaux de A, il faut et il suffit que A soit isomorphe, comme algèbre à opérateurs, à une algèbre de la forme $\mathrm{Hom}_H(G, A_0)$, où A_0 est une k-algèbre de degré fini *locale* sur laquelle opère un sous-groupe H de G ; de façon précise, on peut alors prendre pour A_0 un quelconque des facteurs locaux de A, qui est un quotient de A, et pour H son stabilisateur, ou ce qui revient au même, le stabilisateur de l'idéal maximal correspondant. Bien entendu, sous ces conditions A est réduit si et seulement si A_0 l'est, i.e. si et seulement si A_0 est un corps. Notons également que, si Ω désigne une extension algébriquement close de k, alors l'application $u \rightsquigarrow \mathrm{Ker}\, u$ de l'ensemble $P(A) = \mathrm{Hom}_{k\text{-alg}}(A, \Omega)$ des homomorphismes de k-algèbres de A dans Ω, dans l'ensemble des idéaux premiers (c'est-à-dire maximaux) de A, est surjective, et commute aux opérations de G définies par transport de structure. Par suite si G opère transitivement sur $P(A)$, il opère transitivement sur l'ensemble des idéaux maximaux de A, et on peut par suite appliquer les remarques qui précèdent.

Proposition 6. — *Soient k un corps, G un groupe fini, A une k-algèbre à groupe d'opérateurs. Les conditions suivantes sont équivalentes :*

(i) *A est diagonalisable, et G opère de façon simplement transitive sur l'ensemble* $\mathrm{Hom}_{k\text{-}alg}(A, k)$.

(ii) *A est isomorphe, comme algèbre à groupe d'opérateurs, à l'algèbre $k(G)$ du groupe G, à coefficients dans k, sur laquelle G opère par translations à gauche, i.e. l'algèbre*

des fonctions $\varphi : G \longrightarrow k$, sur laquelle G opère par

$$(g\varphi)(x) = \varphi(g^{-1}x).$$

En effet, on sait que l'ensemble des homomorphismes dans k de l'algèbre k^I des applications de l'ensemble fini I dans k est en correspondance biunivoque avec I par l'application qui, à tout $i \in I$, associe l'application $\varphi \rightsquigarrow \varphi(i)$ de k^I dans k (App. 5.4). Cette bijection est évidemment compatible avec toute bijection de I sur lui-même, induisant un automorphisme de k^I par transport de structure. Ceci montre aussitôt que (i) équivaut (ii).

Définition 2. — *Une k-algèbre A à groupe d'opérateurs fini G est dite galoisienne triviale si elle satisfait aux conditions équivalentes de prop. 6. Elle est dite galoisienne si l'algèbre à groupe d'opérateurs G, déduite par extension des scalaires de k à une clôture algébrique Ω de k, est galoisienne triviale.*

Évidemment, cette condition ne dépend pas de la clôture algébrique choisie, en vertu du théorème de Steinitz. On peut même, dans cette définition, remplacer la clôture algébrique par n'importe quelle extension algébriquement close Ω' de k : en effet, on peut supposer $\Omega \subset \Omega'$, et il suffit de prendre la forme (i) de la définition des algèbres galoisiennes triviales.

Corollaire. — *Soient A, A' deux k-algèbres à groupe d'opérateurs G galoisiennes. Tout homomorphisme u d'algèbres de A dans A' commutant aux opérations de G est un isomorphisme. Si $\sigma : A \longrightarrow \Omega$ est un k-homomorphisme de A dans une extension Ω de k, u est uniquement déterminé par la connaissance de $\sigma \circ u^{-1} : A' \longrightarrow \Omega$.*

On peut supposer évidemment que Ω est algébriquement close, puis (quitte à faire le changement de corps de base k) que $k = \Omega$. Alors le corollaire devient évident.

Proposition 7. — *Soit k un corps, G un groupe fini, A une k-algèbre à groupe d'opérateurs G.*

(i) Soient k' une extension de k, $A' = A \otimes_k k'$ la k'-algèbre à groupe d'opérateurs G déduite de A par changement de corps de base. Si A est galoisienne (resp. galoisienne triviale), il en est de même de A'. Si A' est galoisienne, A est galoisienne.

(ii) Soit $u : G \longrightarrow G'$ un homomorphisme de G dans un groupe fini G'. Si A est galoisienne, l'algèbre A' à groupe d'opérateurs G' induite, $A' = \mathrm{Hom}_G(G', A)$, est galoisienne. Réciproquement, si u est injectif et si A' est galoisienne, A est galoisienne.

(iii) Soit H un groupe fini, B une k-algèbre à groupe d'opérateurs H. Si A et B sont des algèbres à opérateurs galoisiennes (resp. gal. triviales), il en est de même de l'algèbre $A \otimes_k B$ à groupe d'opérateurs $G \times H$. Le foncteur $(A, B) \rightsquigarrow A \otimes_k B$ de la catégorie produit des catégories des k-algèbres galoisiennes à groupe d'opérateurs G (resp. H), dans la catégorie des k-algèbres galoisiennes à groupe d'opérateurs $G \times H$, est une équivalence de catégories.

La première assertion de (i), les assertions (ii), et la première assertion de (iii), se ramènent aussitôt, compte tenu des définitions, au cas des algèbres galoisiennes triviales, où la vérification est triviale et laissée au lecteur. La deuxième assertion dans (ii), résulte aussitôt de la remarque faite après la déf. 2. Reste à prouver la dernière assertion dans (iii). Pour ceci, nous allons exhiber un foncteur quasi-inverse $\mathfrak{h}$ du foncteur envisagé φ : c'est celui qui associe à l'algèbre C à groupe d'opérateurs $G \times H$, le couple A, B avec

$$A = \mathrm{Hom}_{G \times H}(G, C) \quad , \quad B = \mathrm{Hom}_{G \times H}(H, C).$$

On définit de façon évidente des homomorphismes :

$$\mathfrak{h}\varphi \longrightarrow \mathrm{id} \quad , \quad \mathrm{id} \longrightarrow \varphi\mathfrak{h}$$

et il reste à vérifier que ce sont des isomorphismes. C'est trivial pour le premier (transitivité de l'opération d'induction), pour le second on est ramené au cas où le corps de base est algébriquement clos, donc au cas des algèbres galoisiennes triviales, où c'est également trivial.

N. B. — Il faut certainement garder la partie (ii) de prop. 7, qui donne la loi fonctorielle de $\mathrm{H}^1(k, G)$ par rapport à G. Quant à la partie (iii), qui servira à montrer que le foncteur $G \rightsquigarrow \mathrm{H}^1(k, G)$ commute aux produits, on peut éventuellement la rejeter en exercice ; de toutes façons, on retrouverait ce résultat au n° 6, grâce à l'interprétation de $\mathrm{H}^1(k, G)$ en termes du groupe fondamental de k. Mais cela obligerait à rejeter à ce n°

(et subordonner à des considérations topologiques) la structure de groupe sur $\mathrm{H}^1(k, G)$ lorsque G est abélien, ce qui semble peu naturel.

Bien entendu, il faut avoir fait au Chap. I les opérations induites dans le cas d'un homomorphisme quelconque $G \longrightarrow G'$ de groupes, pas seulement l'inclusion d'un sous-groupe comme dans App. n° 5, où on avait en vue des phénomènes spéciaux au cas d'une telle inclusion.

Remarques. —

a) La partie (i) de prop. 7 implique en particulier qu'une algèbre à opérateurs galoisienne triviale est bien galoisienne, ce qui justifie la terminologie. Il est évident d'autre part que deux algèbres à opérateurs galoisiennes triviales, relatives au même groupe G, sont G-isomorphes.

b) On voit aussitôt, par réduction au cas galoisien trivial, que si A est une k-algèbre à groupe d'opérateurs G qui est quasi-galoisienne, alors G opère *fidèlement* sur A et on a :

$$[A : k] = [G : e].$$

Proposition 8. — *Soient k un corps, Ω une extension algébriquement close de k, G un groupe fini, A une k-algèbre commutative à groupe d'opérateurs G. Les conditions suivantes sont équivalentes :*

(i) *A est une algèbre à opérateurs galoisienne.*

(ii) *A est une k-algèbre étale, et G opère de façon simplement transitive sur l'ensemble $P(A) = \mathrm{Hom}_{k\text{-}alg}(A, \Omega)$.*

(iii) *Il existe une extension galoisienne finie K de k, un sous-groupe H de G, et un isomorphisme de H sur le groupe $\mathrm{Gal}(K/k)$, tels que A soit isomorphe, comme algèbre à groupe d'opérateurs G, à l'algèbre induite $\mathrm{Hom}_H(G, K)$.*

Ces conditions impliquent $A \neq 0$, donc l'existence d'un corps résiduel de A. Lorsqu'on s'est donné un corps résiduel $K = A/\mathfrak{m}$ de A, et qu'on désigne par H le sous-groupe de G stabilisateur de K, les conditions précédentes équivalent aussi à la condition suivante :

(iv) *A est réduit, G opère transitivement sur l'ensemble des idéaux maximaux de A, K est une extension galoisienne de k et l'application canonique $H \longrightarrow \mathrm{Gal}(K/k)$ est un isomorphisme.*

Dire que A est une algèbre étale signifie que $A \otimes_k \Omega$ est une Ω-algèbre diagonalisable, donc (ii) signifie que $A \otimes_k \Omega$ est galoisienne triviale, ce qui équivaut à (i) comme on a observé après la définition 2. Ces conditions impliquent manifestement que A est non nulle. L'équivalence de (iii) et (iv) résulte aussitôt des remarques préliminaires à la prop. 6. D'autre part (iii) $\Rightarrow$ (ii), car en vertu de prop. 7 (ii) on est ramené à prouver qu'une extension galoisienne K de k, de degré fini, de groupe de Galois G, est une algèbre à opérateurs galoisienne, pour les opérations naturelles de G sur K, ce qui se voit en effet trivialement sur la condition (ii). Enfin, prouvons (ii) $\Rightarrow$ (iv). On sait déjà, moyennant (i), que A est réduit, et que G opère transitivement sur l'ensemble des idéaux maximaux de A. Cela implique déjà que A est isomorphe, comme algèbre à groupe d'opérateurs G, à l'algèbre induite $\mathrm{Hom}_H(G, K)$, et compte tenu de prop. 7 (ii), on sait que K est une algèbre à groupe d'opérateurs H galoisienne. Cela implique que H opère fidèlement sur K, et que son ordre est égal au degré n de K sur k, en vertu de la remarque ci-dessous, donc que K est une extension galoisienne de k et que $G \longrightarrow \mathrm{Gal}(K/k)$ est un isomorphisme, grâce au cor. à la prop. 1.

On conclut de ce qui précède :

Corollaire. — *Soient k un corps, K une extension de degré fini de k. Les conditions suivantes sont équivalentes :*

(i) *K est une extension galoisienne de k (déf. 1).*

(ii) *Il existe un groupe fini G et une structure d'algèbre à groupe d'opérateurs G sur K, compatible avec la structure d'algèbre déjà donnée sur K, tels que K soit une algèbre à opérateurs galoisienne (déf. 2).*

(iii) *Désignant par Γ le groupe des k-automorphismes de K, et munissant K de sa structure naturelle d'algèbre à groupe d'opérateurs Γ, K devient une algèbre à opérateurs galoisienne (déf. 2).*

De plus, si ces conditions sont vérifiées, alors avec les notations de (ii) et (iii), l'homomorphisme $G \longrightarrow \Gamma$, définissant les opérations de G sur K, est un isomorphisme.

En d'autres termes, la terminologie de la définition 2 est en accord avec celle introduite dans la définition 1, et de plus, si K est une extension de degré fini galoisienne de k, alors il existe sur K essentiellement une seule structure d'algèbre à groupe d'opérateurs, compatible avec la structure d'algèbre déjà donnée de K, et en faisant une algèbre à opérateurs galoisienne. De plus, la proposition 8 ramène l'étude des k-algèbres à opérateurs galoisiennes à celle des extensions galoisiennes de degré fini de k.

5. — Les ensembles ponctués $\mathrm{H}^1(k, G)$ et $\mathrm{H}^1(k, \Omega; G)$

Définition. — *Soient k un corps, G un groupe fini, Ω une extension algébriquement close de k. On appelle k-algèbre à groupe G d'opérateurs Ω-ponctuée un couple $X = (A, \xi)$, où A est une k-algèbre à groupe d'opérateurs G, et où ξ est un k-homomorphisme de k-algèbres de A dans Ω. On dit que X est galoisienne (resp. galoisienne triviale) si l'algèbre à opérateurs A est galoisienne (resp. galoisienne triviale).*

La notion d'isomorphisme pour cette espèce de structure (pour k, Ω, G fixés) est claire. L'intérêt technique de la notion de ponctuation tient du fait qu'elle a pour effet de *rigidifier* la structure envisagée ; en d'autres termes, tout automorphisme d'une algèbre à groupe d'opérateurs G galoisienne ponctuée est l'identité. C'est ce que dit le cor. à prop. 6, qui prouve même que la catégorie de ces algèbres à opérateurs est *discrète*. On notera que si A est une k-algèbre à groupe d'opérateurs G qui est galoisienne, elle provient toujours d'une algèbre à opérateurs Ω-ponctuée $X = (A, \xi)$, puisque l'ensemble $\mathrm{Hom}_{k\text{-alg}}(A, \Omega)$ est non vide ; de façon plus précise, comme G opère de façon simplement transitive sur ce dernier ensemble, il opère de façon simplement transitive sur l'ensemble des structures de k-algèbres à opérateurs ponctuées dont A est l'algèbre à opérateurs sous-jacente. Mais on notera que si $X = (A, \xi)$ et $Y = (B, \eta)$ sont deux k-algèbres à groupes d'opérateurs G ponctuées, galoisiennes, un isomorphisme de A avec B n'est pas nécessairement un isomorphisme de X sur Y, et A et B peuvent fort bien être isomorphes (et même égaux) sans que X et Y le soient (cf. prop. 10 plus bas). Cependant, on voit aussitôt que si X et Y sont triviales, elles sont isomorphes.

Proposition 9. — *Soient k un corps, G un groupe fini.*

(i) Soit $R(X)$ la relation : "X est une k-algèbre à groupe d'opérateurs G galoisienne", et soit $S(X)$ la relation "$R(X)$ et $X = \tau(R(X))$". Alors la relation S est collec-

tivisante.

(ii) Soit Ω une extension algébriquement close de k. Soit $R'(X)$ la relation : "X est une k-algèbre à groupe d'opérateurs G, Ω-ponctuée galoisienne", et soit $S'(X)$ la relation "$R'(X)$ et $X = \tau(R'(X))$". Alors la relation S' est collectivisante.

La démonstration est laissée à Bourbaki, d'autant plus que le style définitif de l'énoncé et de sa démonstration dépend de décisions pendantes sur le livre des Ensembles.

Définition 4. — *Les notations étant celles de la prop. 9, on désigne par $\mathrm{H}^1(k, G)$ (resp. par $\mathrm{H}^1(k, \Omega; G)$) l'ensemble des X satisfaisant la relation $S(X)$ (resp. $S'(X)$) de la prop. 9.*

Comme d'habitude, si X est une k-algèbre à groupe d'opérateurs G galoisienne, on appelle l'élément

$$cl(X) = \tau_Y(R(Y) \text{ et } Y \text{ est isomorphe à } X) \in \mathrm{H}^1(k, G)$$

(qui est l'unique élément de $\mathrm{H}^1(k, G)$ qui soit isomorphe à X) la classe (ou si on veut préciser, la classe à isomorphisme près) de X, et on adopte une notation et une terminologie analogues pour le cas des algèbres à groupes d'opérateurs ponctuées.

Nous allons considérer les deux ensembles de la déf. 4 comme *ponctués* par la classe des algèbres à opérateurs galoisiennes (resp. ponctuées) triviales.

La prop. 7 (ii) nous montre que l'expression $\mathrm{H}^1(k, G)$ resp. $\mathrm{H}^1(k, \Omega; G)$, pour k (resp. k et Ω) fixé(s), peuvent être considérés comme la valeur, en G, d'un foncteur (covariant)

$$G \rightsquigarrow \mathrm{H}^1(k, G) \quad \text{resp.} \quad G \rightsquigarrow \mathrm{H}^1(k, \Omega; G),$$

allant de la catégorie des groupes finis dans celle des ensembles ponctués. La prop. 7 (iii) implique que ces deux foncteurs "commutent aux produits de deux facteurs", d'ailleurs ils transforment évidemment objets finaux (les groupes réduits à l'élément unité) en objets finaux (ensembles réduits à un élément), donc "commutent aux produits finis". (N.B. — Le deuxième foncteur est même exact à gauche, ce qui équivaut au fait qu'il est proreprésentable; mais il n'y a pas lieu de le démontrer ici, car ce fait résultera trivialement du n°7).

On a une application canonique, fonctorielle en G, déduite du foncteur associant à toute algèbre à opérateurs ponctuée l'algèbre à opérateurs déduite par oubli de la ponctuation :

$$\mathrm{H}^1(k, \Omega; G) \longrightarrow \mathrm{H}^1(k, G).$$

Proposition 10. — *L'application précédente est surjective. Faisons opérer G sur lui-même par automorphismes intérieurs, donc sur les deux ensembles $\mathrm{H}^1(k, \Omega; G)$ et $\mathrm{H}^1(k, G)$ par la loi fonctorielle de ces expressions. Alors l'application précédente est compatible avec les opérations de G, et pour que deux éléments de $\mathrm{H}^1(k, \Omega; G)$ aient même image dans $\mathrm{H}^1(k, G)$, il faut et il suffit qu'ils soient transformés l'un de l'autre par une opération de G.*

En d'autres termes, l'application envisagée induit une bijection canonique (évidemment fonctorielle en G) :

$$\mathrm{H}^1(k, \Omega; G)/G \xrightarrow{\sim} \mathrm{H}^1(k, G)$$

permettant de reconstituer l'ensemble $\mathrm{H}^1(k, G)$ à partir de la connaissance de l'ensemble de $\mathrm{H}^1(k, \Omega; G)$ et des opérations de G sur ce dernier.

Démontrons la proposition. L'assertion de surjectivité provient de la remarque, déjà faite après la déf. 3, que toute algèbre à opérateurs galoisienne provient d'une algèbre à opérateurs galoisienne ponctuée. Le fait que l'application envisagée commute aux opérations de G provient du fait que cette application est fonctorielle. Enfin, soient $X = (A, \xi)$ et $Y = (B, \eta)$ deux algèbres à groupe G d'opérateurs ponctuées galoisiennes; pour que les algèbres à opérateurs A et B soient isomorphes, il faut et il suffit évidemment que Y soit isomorphe à une $Y' = (A, \xi')$, définie par une ponctuation ξ' de A. Comme G opère transitivement sur l'ensemble des ponctuations de A par Ω, cela signifie aussi que Y est isomorphe à une Y' de la forme $(A, g \cdot \xi)$, où $g \in G$ et où $g \cdot \xi$ désigne la ponctuation $\xi \circ g_A^{-1}$ déduite de ξ par transport de structure au moyen de g_A. La proposition sera donc démontrée si nous démontrons que pour Y' défini en termes de X et de g de cette façon, on a

$$\mathrm{cl}(Y') = g \cdot \mathrm{cl}(X),$$

en d'autres termes que Y' est isomorphe à l'algèbre à opérateurs ponctuée induite à partir de $X = (A, \xi)$ par $v = \mathrm{int}(g) : G \longrightarrow G$. Il revient au même de dire qu'il existe un

isomorphisme $u : A \longrightarrow A$, satisfaisant aux relations :

$$\begin{cases} u(v(h) \cdot x) = h \cdot u(x), \quad h \in G, x \in A, \\ g \cdot \xi = \xi \circ u. \end{cases}$$

On prendra alors $u = g_A^{-1}$, de sorte que la seconde relation est vérifiée par définition, et la première s'écrit

$$g^{-1}(ghg^{-1} \cdot x) = h(g^{-1} \cdot x),$$

qui est également vérifiée. Cela achève la démonstration.

Corollaire 1. — *Pour tout $g \in G$, la permutation de $\mathrm{H}^1(k, G)$ induite par l'automorphisme int(g) de G est l'identité.*

Corollaire 2. — *Supposons G abélien. Alors l'application canonique $\mathrm{H}^1(k, \Omega; G) \longrightarrow \mathrm{H}^1(k, G)$ est bijective.*

En effet, G opère trivialement sur lui-même par automorphismes intérieurs, donc opère trivialement sur $\mathrm{H}^1(k, \Omega; G)$.

Notons maintenant que si G est abélien, alors l'application $(g, h) \rightsquigarrow gh$ de $G \times G$ dans G est un homomorphisme de groupes, et induit donc une application

$$\mathrm{H}^1(k, G) \times \mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k, G),$$

compte tenu que le foncteur $\mathrm{H}^1(k, -)$ commute aux produits finis.

Proposition 11. — *Soient k un corps, G un groupe fini abélien. La loi de composition qu'on vient de définir sur $\mathrm{H}^1(k, G)$ en fait un groupe abélien, admettant le point marqué comme élément unité. Si $u : G \longrightarrow H$ est un homomorphisme de groupes finis abéliens, l'application correspondante $\mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k, H)$ est un homomorphisme de groupes.*

La deuxième assertion s'exprime encore en disant que $\mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k, H)$ est compatible avec les lois de composition internes mises sur ces deux ensembles, et provient aisément par application du foncteur H^1 de la commutativité du diagramme

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow & & \downarrow \\ H \times H & \longrightarrow & H, \end{array}$$

où les flèches verticales sont $u \times u$ et u, et les flèches horizontales sont les applications somme. Le fait que $\mathrm{H}^1(k, G)$ soit un groupe commutatif pour sa loi de composition se vérifie de façon analogue. (N.B. — La vérification n'est autre que celle du fait général qu'un foncteur commutant aux produits finis transforme monoïdes, resp. groupes, resp. groupes commutatifs...de la première catégorie en animaux de même nature de la seconde. Bien entendu, c'est là un résultat constamment utilisé dans toutes sortes de contextes, à tel point qu'on omet généralement d'en donner la justification, ou même de signaler qu'il y aurait lieu d'en donner une. Les seules références existantes sont quelques nobles et vagues affirmations, dans le style de celle-ci. Bourbaki juge-t-il que c'est son rôle de donner un sorite utilisable sur les structures algébriques dans les catégories, ou préfère-t-il se taper deux ou trois pages d'explications et diagrammes dans chaque situation particulière qu'il rencontrera ? Quant au rédacteur, il se détourne avec horreur et effroi d'une telle alternative). Cela achève la démonstration.

Soit maintenant k' une extension de k. Utilisant prop. 7, (i), on trouve une application d'ensembles ponctués

$$\mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k', G),$$

fonctorielle en le groupe fini G. Lorsque G est abélien, cette application est compatible avec les structures de groupes envisagées sur les deux membres. Si d'autre part Ω est une extension de k, Ω' une extension de k', et si on se donne un homomorphisme de k-extensions $\Omega \longrightarrow \Omega'$, de sorte qu'on a donc un carré commutatif :

$$\begin{array}{ccc} k & \longrightarrow & \Omega \\ \downarrow & & \downarrow \\ k' & \longrightarrow & \Omega', \end{array}$$

alors on définit de même une application d'ensembles ponctués

$$\mathrm{H}^1(k, \Omega; G) \longrightarrow \mathrm{H}^1(k', \Omega'; G).$$

Cette application est encore fonctorielle en G, en particulier commute aux opérations de G envisagées dans la prop. 10, d'autre part le carré d'applications

$$\begin{array}{ccc} \mathrm{H}^1(k, \Omega; G) & \longrightarrow & \mathrm{H}^1(k, G) \\ \downarrow & & \downarrow \\ \mathrm{H}^1(k', \Omega'; G) & \longrightarrow & \mathrm{H}^1(k', G) \end{array}$$

est commutatif.

Lorsqu'on se donne également une extension k'' de k', alors l'application $\mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k'', G)$ correspondante est la composée des applications de changement de corps de base $\mathrm{H}^1(k, G) \longrightarrow \mathrm{H}^1(k', G) \longrightarrow \mathrm{H}^1(k'', G)$. On peut présenter la variance de $\mathrm{H}^1(k, G)$ par rapport aux deux arguments en disant que $\mathrm{H}^1(k, G)$ est un *bifoncteur* en le couple (k, G), contravariant en le premier argument et covariant en le second, où k varie dans la catégorie des corps, G dans la catégorie des groupes finis, et $\mathrm{H}^1(k, G)$ est à valeurs dans la catégorie des ensembles pointés. Lorsque G est astreint à être abélien, on peut considérer ce bifoncteur comme étant à valeurs dans la catégorie des groupes abéliens.

6. — Groupe de Galois topologique et théorie de Galois des extensions galoisiennes infinies

Le présent n° et le suivant utilisent certaines notions de Topologie Générale, qui ne seront développées que dans le livre suivant. Comme les résultats donnés ici ne seront utilisés, dans la suite de ce traité, qu'après le livre de Topologie Générale, un cercle vicieux n'est pas à craindre.

Propostion 12. — *Soit G un groupe topologique. Les conditions suivantes sont équivalentes :*

(i) *G est compact et totalement discontinu.*

(ii) *G est compact, et il existe un système fondamental de voisinages de l'élément neutre qui sont des sous-groupes ouverts.*

(iii) *Comme (ii), mais en exigeant que les sous-groupes envisagés soient distingués.*

(iv) *On peut trouver un système projectif $(G_i)_{i\in I}$ de groupes finis, indexé par un ensemble ordonné filtrant I, tel que G soit isomorphe au groupe topologique limite projective de ce système (les G_i étant considérés comme groupes topologiques à l'aide de leur topologie discrète).*

Par définition de la topologie de $\varprojlim G_i$, il est évident que (iv) implique (iii), d'autre part (iii) implique (iv), comme on voit en prenant le système projectif formé des groupes quo-

tients G/U, où U est un sous-groupe ouvert distingué de G. En effet, les groupes G/U sont finis (car compacts et discrets), et l'homomorphisme naturel de G dans $\varprojlim G/U$ est injective grâce à (iii), et a une image dense, donc est un isomorphisme puisque G est compact et $\varprojlim G/U$ est séparé. Ainsi (iv) équivaut à (iii), qui implique trivialement (ii). D'autre part (ii) implique (iii) en vertu du :

Lemme 1. — *Soit G un groupe, H un sous-groupe d'indice fini de G, alors l'ensemble des sous-groupes de G conjugués de H est fini, et leur intersection H' est un sous-groupe distingué d'indice fini de G.*

En effet, soit $E = G/H$ l'espace homogène défini par le sous-groupe H, et soit G' le groupe des permutations de E, qui est un groupe fini. On a donc un homomorphisme naturel $G \longrightarrow G'$. On sait (Chap. I) que les conjugués de H sont les stabilisateurs des éléments de E, et sont donc en nombre fini, et que leur intersection est le noyau de $G \longrightarrow G'$, qui est donc d'indice fini.

Corollaire. — *Si G est un groupe topologique, et H un sous-groupe ouvert de G, d'indice fini, alors H' est un sous-groupe ouvert d'indice fini et distingué contenu dans H.*

En effet, une intersection finie d'ouverts est ouverte.

On a donc prouvé l'équivalence des conditions (ii) à (iv). D'autre part (ii) implique évidemment que la composante connexe l'élément unité e de G est réduite à $\{e\}$, donc par translation que pour tout $g \in G$ la composante connexe de g est réduite à $\{g\}$. Donc (ii) implique (i), et il reste à prouver que (i) implique (ii). Nous utiliserons le lemme suivant :

Lemme 2. — *Soient G un groupe topologique, X un espace compact sur lequel G opère continûment à gauche (de sorte que, par définition, l'application $(g, x) \mapsto g.x$ de $G \times X$ dans X est continue), R une relation d'équivalence dans X telle que les classes d'équivalence mod R soient des parties ouvertes de X. Alors le sous-groupe H de G, formé des $g \in G$ qui laissent R invariante, est un sous-groupe ouvert, et si de plus X est compact, il existe une relation d'équivalence R', plus fine que R, satisfaisant à la même condition que R, et stable par les opérations de G.*

Comme toute classe d'équivalence est le complémentaire de la réunion des autres classes d'équivalence, il s'ensuit qu'elle est fermée. D'ailleurs, X étant compact,

l'ensemble de ces classes est nécessairement fini, donc la donnée de R équivaut à celle d'une partition $(X_i)_{i\in I}$ de X en un ensemble fini de parties à la fois ouvertes et fermées. Pour tout $i \in I$, soit U_i l'ensemble des $g \in G$ tels que $g(X_i) \subset X_i$. Je dis que U_i est ouvert : en effet, soit V_i l'image inverse de X_i par l'application $(g, x) \mapsto g.x$ de $G \times X_i$ dans X. C'est une partie ouverte de $G \times X_i$, et si $p_i : G \times X_i \longrightarrow G$ désigne la projection canonique, U_i n'est autre que $G - p_i(G \times X_i - V_i)$. Comme p_i est *propre*, X_i étant compact (réf.), il transforme parties fermées en parties fermées, ce qui prouve que U_i est ouvert. Il en est donc de même de l'intersection des U_i, I étant fini, or cette intersection n'est autre que le groupe H stabilisateur de R. Donc H est un sous-groupe ouvert.

Lorsque G est compact, cela implique que H est d'indice fini, donc que l'ensemble des relations d'équivalence $g.R$ transformées de R par des éléments de G est fini (cet ensemble étant en effet en correspondance biunivoque avec les éléments de G/H). Si R' est la relation d'équivalence borne supérieure des $g.R$, on voit alors que ces classes d'équivalence sont ouvertes comme intersection finies de parties ouvertes, et de plus R' est évidemment stable par G et plus fine que R. Cela achève la démonstration du lemme 2.

Soit maintenant G un groupe topologique compact totalement discontinu, prouvons que tout voisinage ouvert U de l'élément neutre contient un sous-groupe ouvert de G. On peut supposer déjà U ouvert et fermé. Il suffit alors d'appliquer le lemme 2 au groupe G et à $X = G_s$, et à la relation d'équivalence définie par la partition de G_s en les ensembles U et $G - U$ (en supposant $G - U \neq \varnothing$, ce qui est loisible, car sinon il suffit de prendre le sous-groupe G lui-même) : si H est le stabilisateur de cette relation d'équivalence, H est un sous-groupe ouvert en vertu du lemme 2, et on a $H \subset U$, puisque $H.U \subset U$ et $e \in U$, ce qui achève la démonstration.

N. B. — J'ai inclus le lemme 2 pour fournir une référence commode pour la démonstration du fait suivant, qui pourrait être indiqué en exercice : si G est un groupe compact opérant continûment sur un espace compact totalement discontinu, alors il existe un système projectif $(X_i)_{i\in I}$ d'espaces quotients finis discrets de X, stables par G, indexé par un ensemble d'indices ordonné filtrant croissant, tel que l'application canonique $X \longrightarrow \varprojlim X_i$ soit un isomorphisme d'espaces topologiques à groupe topologique G d'opérateurs. Cela implique alors ceci : soient k un corps, G son groupe fondamental relativement à une extension sép. close Ω de k, alors le foncteur $A \mapsto \mathrm{Hom}_{k\text{-alg}}(A, \Omega)$

établit une antiéquivalence entre la catégorie des k-algèbres entières séparables, et la catégorie des espaces topologiques compacts totalement discontinus à groupe topologique G d'opérateurs.

Définition 5. — *Un groupe topologique G satisfaisant les conditions équivalentes de la prop. 12 est appelé un groupe profini.*

Proposition 13. — Soit G un groupe topologique, H un sous-groupe. Si H est fermé et d'indice fini dans G, alors H est ouvert, et la réciproque est vraie si G est compact.

Si H est ouvert, G compact, alors G/H est compact et discret, donc fini, d'autre part on sait qu'un sous-groupe ouvert est fermé. Si H est fermé i.e. G/H séparé, et si H est d'indice fini i.e. G/H fini, donc discret, H est ouvert puisqu'il est l'image inverse d'un point de G/H, lequel est ouvert.

Proposition 14. — Soient G un groupe profini, H un sous-groupe fermé. Muni de la topologie induite, H est un groupe profini. De plus, H est intersection des sous-groupes ouverts de G qui le contiennent. L'espace homogène G/H est un espace compact totalement discontinu, et si H est invariant, le groupe topologique quotient G/H est profini.

La première assertion provient du fait que G étant compact et totalement discontinu, il en est de même de toute partie fermée. D'autre part, on sait que toute partie fermée est intersection de ses voisinages à la fois ouverts et fermés. Pour prouver que H est l'intersection des sous-groupes ouverts de G qui le contiennent, il suffit de prouver que tout voisinage U de H dans G qui est ouvert et fermé contient un voisinage qui est un sous-groupe ouvert de G. Considérons une relation d'équivalence R dans G dont les classes sont ouvertes, l'une d'elles contenant H et contenue dans U (par exemple la relation ayant comme seules classes U, et $G - U$ si ce dernier est non vide). Appliquant le lemme 2 à H opérant sur X par translations à gauche, on voit que l'ensemble des transformées de R par les opérations de H est fini, donc quitte à remplacer R par la borne supérieure de ses transformées par H, on peut supposer R invariante par les opérations de H. Appliquons maintenant le lemme 2 à G opérant sur lui-même par translations à gauche, et soit H' le sous-groupe de G stabilisateur de R. C'est un sous-groupe ouvert de G, contenant H par hypothèse, et contenu dans la classe d'équivalence V contenant H (puisque $H.V \subset V$ et $e \in V$), et a fortiori contenu dans U. Ceci prouvé, on en conclut que l'image de l'élément neutre de G dans G/H admet

un système fondamental de voisinages à la fois ouverts et fermés, donc par translation on voit qu'il en est de même de tout point de G/H, qui est donc totalement discontinu. Comme il est manifestement compact, cela achève la démonstration de prop. 14.

Proposition 15. — Soit $(G_i)_{i\in I}$ un système projectif de groupes topologiques, et soit G le groupe topologique limite projective de ce système. Si les G_i sont profinis, il en est de même de G.

En effet, on sait qu'une limite projective d'espaces compacts est un espace compact, et d'autre part la condition (iii) de prop. 12 est vérifiée, comme on voit aussitôt en utilisant la même condition sur les G_i et la description des voisinages de l'élément neutre dans G.

Définition 6. — Soient K un corps, E une extension quasi-galoisienne de K, G son groupe de Galois. On appelle groupe de Galois topologique de E (ou, s'il y a lieu de préciser, de E sur K) le groupe G, muni de la topologie de la convergence simple, E étant considéré comme muni de la topologie discrète.

Nous verrons un peu plus bas que cette topologie fait bien de G un groupe topologique (réf.), ce qui justifiera la terminologie. Par la suite, on dira souvent "groupe de Galois" au lieu de "groupe de Galois topologique", étant entendu que, lorsqu'un groupe de Galois sera considéré comme groupe topologique, c'est toujours de la topologie qu'on vient de définir qu'il s'agira. Signalons tout de suite que le groupe de Galois topologique de E sur K est égal par définition au groupe de Galois topologique de E sur le corps des invariants K^G de G; c'est ce qui permettrait, dans l'étude des groupes de Galois topologiques, de se ramener au cas des extensions galoisiennes. Signalons aussi que si E est une extension quasi-galoisienne de degré fini de K, son groupe de Galois, qui est alors fini, est discret, car si S est un ensemble générateur fini de l'extension E, pour tout $g \in G$, l'ensemble des $g' \in G$ tels que $g'(x) = g(x)$ pour tout $x \in S$ est un voisinage de g réduit à $\{g\}$.

Proposition 16. — *Soit E une extension quasi-galoisienne de K, réunion filtrante d'une famille d'extensions quasi-galoisiennes E_i. Alors l'homomorphisme naturel*

$$\mathrm{Gal}(E/K) \longrightarrow \varprojlim_i \mathrm{Gal}(E_i/K)$$

est un isomorphisme de groupes topologiques.

Cela résulte trivialement des définitions.

Corollaire 1. — *Le groupe de Galois topologique d'une extension quasi-galoisienne est un groupe topologique pro-fini.*

En effet, E est réunion filtrante croissante de ses sous-extensions quasi-galoisiennes E_i de degré fini sur K, donc prop. 16 implique que G est isomorphe à une limite projective de groupes finis discrets, ce qui montre à la fois que c'est un groupe topologique, et que ce dernier est profini.

Corollaire 2. — *Soit E une extension galoisienne du corps K, G son groupe de Galois topologique. Les conditions suivantes sont équivalentes :*

(i) Le groupe G est fini.

(ii) Le groupe topologique G est discret.

(iii) L'extension E est de degré fini.

L'équivalence de (i) et (ii) provient du fait que G est compact (cf. prop. 13), celle de (i) et (iii) provient du théorème 2.

Rappelons que si $u : G \longrightarrow H$ est un homomorphisme de groupes topologiques, G étant compact et H séparé (condition vérifiée si G et H sont tous deux profinis), $u(G)$ et $\ker u$ sont fermés dans H et G et u induit un isomorphisme de groupes topologiques de $G/\ker u$ sur $u(G)$, muni de la topologie induite par H ; en particulier, si u est injectif (resp. bijectif), u induit un isomorphisme de groupes topologiques de G avec $u(G)$ (resp. de G avec H). De ceci, on conclut immédiatement les résultats suivants :

Proposition 17. — *Soit E une extension galoisienne du corps K, F une sous-extension de E. Alors* $\mathrm{Gal}(E/F)$ *est un sous-groupe fermé de* $\mathrm{Gal}(F/K)$. *Si F est galoisien, alors l'isomorphisme de groupes* $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$ *de prop. 2. cor. 2 est un isomorphisme de groupes topologiques.*

Corollaire. — Sous les conditions du théorème 1, l'isomorphisme

$$\mathrm{Gal}(E'/K') \simeq \mathrm{Gal}(E/K)$$

est un isomorphisme de groupes topologiques.

Proposition 18. — *Soient E une extension galoisienne du corps K, G son groupe de Galois topologique, H un sous-groupe de G. Pour que le corps des invariants de H soit égal à K, il faut et il suffit que H soit dense dans G.*

La condition est suffisante, car si H est dense dans G, pour tout $x \in E$, l'orbite de x sous G est égale à son orbite sous H, ce qui montre que le corps des invariants de H est égal à celui de G, c'est-à-dire à K. Inversement, supposons que le corps des invariants de H soit réduit à K. Pour toute sous-extension galoisienne F de degré fini de E, l'ensemble des restrictions à F des $g \in H$ est alors un sous-groupe H_F du groupe G_F des K-automorphismes de F ; comme le corps des invariants est réduit à K, en vertu du théorème 3, cela implique que $H_F = G_F$; donc que H est dense dans G.

Nous pouvons maintenant généraliser aux extensions galoisiennes éventuellement infinies le théorème fondamental de la théorie de Galois :

Théorème 4. — *Soient E une extension galoisienne d'un corps K, G son groupe de Galois, $\mathcal{K}$ l'ensemble des sous-extensions de E, $\mathcal{G}$ l'ensemble des sous-groupes fermés de G. Pour tout sous-groupe H de G, soit $k(H)$ le corps des invariants de H, qui est un élément de $\mathcal{K}$, et pour toute sous-extension F de E, soit $g(F)$ son groupe de Galois, qui est un élément de $\mathcal{G}$. On obtient ainsi deux applications : $\underline{k} : \mathcal{G} \longrightarrow \mathcal{K}$ et $\underline{g} : \mathcal{K} \longrightarrow \mathcal{G}$ Ces applications sont bijectives et inverses l'une de l'autre. Si $H \in \mathcal{G}$ et $F \in \mathcal{K}$ se correspondent, alors F est de degré fini sur K si et seulement si H est d'indice fini dans G, ou encore si et seulement si H est un sous-groupe ouvert de G, on a alors :*

$$[G : H] = [F : K]. \quad (*)$$

En effet, le fait que $\underline{k} \circ \underline{g}$ soit l'application identique n'est autre que la prop. 2, et le fait que $\underline{g} \circ \underline{k}$ soit l'application identique résulte aussitôt de la prop. 18. Comme G/H est en correspondance biunivoque avec l'ensemble des K-monomorphismes de F dans E (ou ce qui revient au même, dans une clôture algébrique donnée de E), cela montre l'égalité (*) en tous cas, compte tenu de §7, prop. 14, cor. 6, ce qui implique que H est d'indice fini dans G si et seulement si H est ouvert dans G. Cela achève la démonstration du théorème.

7. — Groupe fondamental d'un corps, et structure de la catégorie des algèbres étales sur un corps

Définition 6. — *Soient k un corps, Ω une extension séparablement close de k. On appelle groupe fondamental de k relativement à Ω, et on notera $\pi_1(k, \Omega)$, le groupe de Galois topologique de la fermeture algébrique séparable k_s de k dans Ω.*

Dans cette définition, Ω n'intervient que via la fermeture algébrique séparable k_s de k dans Ω. Compte tenu de §7, prop. 22, cor., cette dernière ne dépend pas, à isomorphisme près, du choix de Ω. On obtient donc :

Proposition 19. — *Les groupes fondamentaux d'un corps k, relatifs à deux extensions séparablement closes quelconques de k, sont isomorphes.*

Remarques. — 1) On notera que l'isomorphisme $\theta : \pi \longrightarrow \pi'$ construit dans la démonstration de la prop. 19 dépend du choix d'un isomorphisme u entre deux clôtures séparables k_s et k'_s de k. Ce dernier est évidemment déterminé modulo composition par un automorphisme v de l'extension k'_s. Or $v \in \pi'$, et désignant par $\mathrm{int}(v)$ l'automorphisme intérieur de π' défini par u :

$$\mathrm{int}(v)(w) = vwv^{-1},$$

on voit aussitôt que l'isomorphisme $\theta' : \pi \longrightarrow \pi'$ associé à l'isomorphisme $w : k_s \longrightarrow k'_s$ est donné par

$$\theta' = \mathrm{int}(v) \circ \theta.$$

On peut donc dire qu'on a défini une *classe* d'isomorphismes $\theta : \pi \longrightarrow \pi'$, modulo composition par des automorphismes intérieurs de π'. Lorsque en particulier le groupe fondamental π de k est abélien, on voit qu'on a défini un isomorphisme *canonique* entre les groupes fondamentaux π et π', relatifs à deux extensions séparablement closes quelconques de k.

2) En vertu de la prop. 19, on se permet parfois, par abus de langage, de parler du groupe fondamental de k, qu'on note simplement $\pi_1(k)$, sans préciser le choix d'une extension séparablement close. Ce langage ne présente pas d'inconvénients tant qu'il n'est question que de propriétés de ce groupe qui sont invariantes par isomorphisme, mais

doit être évité en tous cas dans les questions où interviennent les propriétés fonctorielles du groupe fondamental.

Rappelons nous que, si k_s est une clôture séparable de k, les extensions algébriques séparables de k sont isomorphes à des sous-extensions de k_s, et deux telles sous-extensions sont isomorphes si et seulement si elles sont conjuguées par un élément du groupe de Galois de k_s. On obtient alors, compte tenu du théorème 4 :

Proposition 20. — *Soient k un corps, Ω une extension séparablement close de k, et $G = \pi_1(k, \Omega)$ le groupe fondamental de k relatif à Ω. Alors il y a une correspondance biunivoque canonique entre les classes, à isomorphisme près, d'extensions algébriques séparables de k, et les classes à conjugaison près, de sous-groupes fermés de G. Aux classes des extensions finies correspondent les classes des sous-groupes ouverts i.e. d'indice fini.*

Il convient de préciser ce dernier énoncé, en donnant un théorème de structure sur la *catégorie* des algèbres étales sur k. L'importance de la notion de groupe fondamental d'un corps k tient en premier lieu au fait qu'elle permet de formuler un tel théorème de structure. Pour ceci, introduisons la

Définition 7. — *Soit G un groupe topologique. Un ensemble E à groupe d'opérateurs G est dit admissible si l'application $(g, x) \mapsto g.x$ de $G \times E$ dans E est continue, lorsque E est muni de la topologie discrète et $G \times E$ de la topologie produit.*

Comme $G \times E$ est l'ensemble somme des $G \times \{x\}$, pour $x \in E$, on voit que cette condition signifie aussi que pour tout $x \in E$, l'application $g \rightsquigarrow g.x$ de G dans E muni de la topologie discrète est continue, ou encore que le stabilisateur G_x de x dans G est un sous-groupe ouvert. Ainsi, les ensembles à groupe d'opérateurs G admissibles sont ceux qui sont isomorphes à un ensemble de opérateurs *somme* d'espaces homogènes G/H_i, où (H_i) est une famille de sous-groupes ouverts de G. Notons que lorsque E est fini, cela signifie aussi (comme on voit grâce au lemme 1 du n° 6) que l'on peut trouver un sous-groupe ouvert distingué H, tel que Π opère trivialement sur E, i.e. tel que la structure externe de E provienne d'une structure à groupe d'opérateurs G/H.

Si G est un groupe topologique, nous désignons par

$$\mathrm{Ensf}(G)$$

la sous-catégorie pleine de la catégorie des ensembles à groupe d'opérateurs G, qui sont

finis et *admissibles*. D'autre part, si k est un corps, nous désignons par

$$\mathrm{Et}(k)$$

la catégorie des algèbres étales sur k. Supposons maintenant choisi une extension séparablement close Ω de k, et que l'on ait

$$G = \pi_1(k, \Omega).$$

Nous allons, sous ces conditions, définir une anti-équivalence entre les deux catégories qu'on vient de définir, et de façon plus précise, nous allons définir deux foncteurs

$$\varphi : \mathrm{Et}(k)^\circ \longrightarrow \mathrm{Ens}(G),$$

$$\mathfrak{h} : \mathrm{Ens}(G) \longrightarrow \mathrm{Et}(k)^\circ,$$

quasi-inverses l'un de l'autre.

1) Définition du foncteur φ. On posera pour toute k-algèbre étale :

$$\varphi(A) = \mathrm{Hom}_{k\text{-alg}}(A, k_s) \simeq \mathrm{Hom}_{k\text{-alg}}(A, \Omega),$$

où k_s est la fermeture algébrique séparable de k dans Ω, et où le deuxième membre est considéré comme ensemble à groupe d'opérateurs G, en faisant agir ce dernier par

$$g.u = g \circ u \qquad (g \in G,\ u \in \varphi(A)).$$

Cet ensemble à opérateurs est manifestement fini (de cardinal égal à $[A : k]$) et admissible. Si $u : A \longrightarrow B$ est un homomorphisme de k-algèbres étales, on définit

$$\varphi(u) : \varphi(B) \longrightarrow \varphi(A)$$

par la formule

$$\varphi(u)(v) = v \circ u.$$

Il est immédiat qu'on définit bien ainsi un foncteur φ de $\mathrm{Et}(k)^\circ$ dans $\mathrm{Ensf}(G)$.

2) Définition du foncteur $\mathfrak{h}$. On posera, pour tout ensemble à groupe d'opérateurs G fini et admissible :

$$\mathfrak{h}(E) = \mathrm{Hom}_G(E, k_s),$$

où le deuxième membre est considéré comme k-algèbre par la structure de k-algèbre induite par k_s :

$$(\lambda\, u)(x) = \lambda(u(x)) \qquad (\lambda \in k,\ x \in E,\ u \in \mathrm{Hom}_G(E, k_s)).$$

Si $u : E \longrightarrow F$ est un homomorphisme d'ensembles à groupe d'opérateurs G, finis et admissibles, on définit

$$\mathfrak{h}(u) : \mathfrak{h}(F) \longrightarrow \mathfrak{h}(E)$$

par la formule

$$\mathfrak{h}(u)(v) = v \circ u.$$

Il est immédiat qu'on définit ainsi un foncteur contravariant de la catégorie Ensf(G) dans la catégorie des k-algèbres. Prouvons que ce foncteur prend ses valeurs en fait dans la catégorie Et(k), plus précisément, que $\mathfrak{h}(E)$ est une algèbre étale de degré égal à card(E). Pour ceci, observons que $\mathfrak{h}$ transforme sommes en produits, comme on constate aussitôt ; compte tenu qu'un produit fini d'algèbres étales est une algèbre étale, on est ramené à prouver que notre assertion dans le cas où E est de la forme G/H, où H est un sous-groupe ouvert de G. Mais alors $\mathfrak{h}(E)$ est isomorphe au corps des invariants de H dans k_s, qui est une extension de degré fini de k_s de degré $G : H$, (théorème 4), donc une extension étale. Cela prouve en particulier que $\mathfrak{h}$ définit bien un foncteur de Ensf(G) dans Et$(k)^\circ$.

3) Définition d'un isomorphisme fonctoriel :

$$\alpha_A : A \longrightarrow \mathfrak{h}\varphi(A).$$

Pour toute k-algèbre étale A, on désigne par α_A l'homomorphisme défini par

$$\alpha_A(x)(u) = u(x) \qquad \text{pour } x \in A,\ u \in \varphi(A) = \mathrm{Hom}_{k\text{-alg}}(A, k_s).$$

Il est immédiat que c'est un homomorphisme de k-algèbres, fonctoriel en A. Prouvons que c'est un isomorphisme. Pour cela, observons que le foncteur φ transforme manifestement produits finis en sommes, et comme $\mathfrak{h}$ transforme sommes en produits, il s'ensuit que $\mathfrak{h}\varphi$ est un foncteur qui commute aux produits finis. Cela nous ramène au cas où A est une extension. Donc α_A est nécessairement injectif. Mais en vertu de ce qui a été dit dans 1) et 2), A et $\mathfrak{h}\mathfrak{f}(A)$ ont même degré fini sur k, donc α_A est un isomorphisme.

4) Définition d'un isomorphisme fonctoriel

$$\beta_E : E \longrightarrow \varphi\mathfrak{h}(E).$$

Pour tout ensemble E à groupe d'opérateurs G, fini et admissible, on désigne par β_E l'homomorphisme défini par

$$\beta_E(x)(u) = u(x) \qquad \text{pour } x \in E,\ u \in \mathfrak{h}(E) = \mathrm{Hom}_G(E, k_s).$$

Il est immédiat que c'est un homomorphisme d'ensembles à groupe d'opérateurs G, fonctoriel en E. Prouvons que c'est un isomorphisme. Utilisant le fait que $\varphi\mathfrak{h}$ transforme sommes en sommes, on est ramené au cas où E est de la forme G/H, où H est un sous-groupe ouvert de G. Mais alors $\mathfrak{h}(E)$ est isomorphe au corps des invariants de H dans k_s, qui est une extension étale de k, d'où résulte que G opère transitivement sur $\varphi(\mathfrak{h}(E))$, donc, comme E est non vide, que $E \longrightarrow \varphi\mathfrak{h}(E)$ est surjectif. Or il résulte de ce qu'on a dit dans 1) et 2) que E et $\varphi\mathfrak{h}(E)$ ont même cardinal fini, donc l'application considérée est bijective.

Remarque. — On vérifie aussitôt que les isomorphismes de foncteurs α_E et β_E satisfont la condition de compatibilité habituelle pour deux foncteurs adjoints, cf. Ens. Chap. ...§...n° ....

On conclut de ceci :

Théorème 5. — *Soient k un corps, Ω une extension séparablement close de k, G le groupe fondamental de k relativement à Ω. Alors les foncteurs φ et $\mathfrak{h}$ précédents définissent des équivalences, quasi-inverses l'une de l'autre, entre la catégorie des algèbres étales sur k, et la catégorie opposée de la catégorie des ensembles à groupe d'opérateurs G qui sont finis et admissibles. De plus, si l'algèbre étale A sur k et l'ensemble à opérateurs E se correspondent, on a*

$$[A : k] = \mathrm{card}(E).$$

Théorème 5. — *Supposons que A et E se correspondent. Pour que A soit une extension de k, il faut et il suffit que $E \neq \varnothing$ et que G opère transitivement sur E. Pour que A soit de plus une extension galoisienne de k, il faut et il suffit que le stabilisateur d'un (ou encore, de tout) point de E dans G soit un sous-groupe distingué.*

Corollaire 2. — *Supposons que A et E se correspondent. Pour qu'on ait $A = 0$ (resp. $A \simeq k$) il faut et il suffit que $E = \varnothing$ (resp. que E soit réduit à un point).*

En effet, les objets finaux (resp. initiaux) de $\mathrm{Et}(k)$ correspondent aux objets initiaux (resp. finaux) de $\mathrm{Ensf}(G)$. On peut aussi prouver ce corollaire directement sans utiliser le th. 5 !

Corollaire 3. — *Les produits tensoriels finis dans* $\mathrm{Et}(k)$ *correspondent par les équivalences φ et $\mathfrak{h}$ aux produits finis dans* $\mathrm{Ensf}(G)$.

En effet, les produits tensoriels d'algèbres étales sont les sommes, au sens de la catégorie $\mathrm{Et}(k)$. (N. B. — Bien entendu, le fait que φ transforme produits tensoriels d'algèbres en produits ordinaires d'ensembles à opérateurs est trivial directement ; ce qui l'est moins, c'est que $\mathfrak{h}$ transforme produits ordinaires en produits tensoriels).

Corollaire 4. — *Soient A une k-algèbre étale à groupe Γ d'opérateurs (à gauche), de sorte que $\varphi(A)$ est un ensemble à groupe d'opérateurs G, fini et admissible, sur lequel Γ opère par fonctorialité à droite (en commutant donc aux opérations de G). Pour que A soit une algèbre à groupe d'opérateurs Γ galoisienne, il faut et il suffit que Γ opère de façon simplement transitive sur $\varphi(A)$. On obtient ainsi une équivalence de la catégorie des k-algèbres à groupe d'opérateurs Γ qui sont galoisiennes, avec la catégorie des espaces principaux homogènes (brrr) à droite sous Γ, munis du groupe d'opérateurs à gauche G, opérant de façon admissible.*

La première assertion est une conséquence triviale de la définition 2 et du critère (i) de prop. 6. Les autres assertions s'ensuivent aussitôt, grâce au théorème 5.

Proposons nous maintenant d'interpréter de même la structure de k-algèbre à groupe d'opérateurs Γ galoisienne munie d'une ponctuation relativement à Ω (déf. 3).

Par définition, en termes de l'ensemble E à opérateurs G et Γ correspondant, une ponctuation correspond simplement au choix d'un point x de E. Or un tel choix permet d'identifier l'espace principal homogène à droite E à Γ_a, à l'aide de l'application $\gamma \mapsto x.\gamma$. Cette identification faite, l'ensemble des automorphismes d'ensemble à groupe Γ d'opérateurs de E peut être identifié à Γ, opérant sur Γ_a par translation à gauche, ce qu'on peut expliciter aussi en disant que pour tout $\gamma \in \Gamma$, il y a un unique Γ-automorphisme $g = \rho(\gamma)$ de E tel que $g.x = x.\gamma$, et qu'on obtient ainsi un isomor-

phisme ρ de Γ sur $\mathrm{Aut}_\Gamma(E)$. Par suite, la donnée, sur le Γ-ensemble E, d'une structure d'objet à groupe d'opérateurs G équivaut à celle d'un homomorphisme $G \longrightarrow \Gamma$, et cette structure est admissible si et seulement si cet homomorphisme est continu. On a ainsi, a toute k-algèbre étale à groupe d'opérateurs G galoisienne et ponctuée, associé canoniquement un homomorphisme continu

$$G \longrightarrow \Gamma,$$

et de ce qui précède il résulte immédiatement que : a) deux structures de l'espace précédent sont isomorphes si et seulement si elles définissent le même homomorphisme $G \longrightarrow \Gamma$, et b) tout homomorphisme continu $G \longrightarrow \Gamma$ provient d'une structure de l'espace envisagée. Notons enfin qu'il résulte immédiatement des définitions que si A est une algèbre à groupe d'opérateurs Γ galoisienne ponctuée, et si $\Gamma \longrightarrow \Gamma'$ est un homomorphisme de Γ dans un groupe fini Γ', alors l'homomorphisme $G \longrightarrow \Gamma'$ associé à A', l'algèbre à groupe d'opérateurs Γ' galoisienne ponctuée déduite de A par extension contravariant du groupe structural, n'est autre que le composé $G \longrightarrow \Gamma \longrightarrow \Gamma'$. On obtient donc :

Corollaire 5. — *Le procédé qui précède définit un isomorphisme, fonctoriel en le groupe fini* Γ *:*

$$\mathrm{H}^1(k, \Omega; \Gamma) \xrightarrow{\sim} \mathrm{Hom\ cont}(G, \Gamma),$$

où le deuxième membre désigne l'ensemble des homomorphismes continus de G *dans* Γ.

Utilisant maintenant la prop. 10, on trouve par suite :

Corollaire 6. — *Pour tout groupe fini* Γ*, désignons par* $\mathrm{H}^1(G, \Gamma)$ *l'ensemble quotient de l'ensemble* $\mathrm{Hom\ cont}(G, \Gamma)$ *par les opérations du groupe* Γ*, en faisant opérer* $\gamma \in \Gamma$ *sur cet ensemble par composition avec l'automorphisme intérieur* $\mathrm{int}(\gamma)$*. Alors on a un isomorphisme fonctoriel en* Γ *:*

$$\mathrm{H}^1(k, \Gamma) \xrightarrow{\sim} \mathrm{H}^1(G, \Gamma).$$

De plus, nous rappelant que lorsque Γ est un groupe abélien, on a défini sur $\mathrm{H}^1(k, \Gamma)$ une loi de groupe abélien, en termes de la propriété de commutation du foncteur $\Gamma \rightsquigarrow \mathrm{H}^1(k, \Gamma)$ aux produits finis, et que la loi de groupe naturelle sur $\mathrm{H}^1(G, \Gamma) \xrightarrow{\sim}$

Hom cont(G, Γ) peut manifestement être décrite par le même procédé, (N. B. — un foncteur d'une catégorie abélienne dans (Ens) qui commute aux produits finis se factorise par (Ab) *d'une seule manière*). On en conclut :

Corollaire 7. — *Lorsque* Γ *est un groupe fini abélien, l'isomorphisme du corollaire 6 est compatible avec les structures de groupe naturelles sur les deux membres.*

Remarque. — Le corollaire 5 permettrait de donner une description du groupe profini $G = \pi_1(k, \Omega)$, indépendamment de la théorie de Galois, à isomorphisme unique près, comme *proreprésentant* le foncteur $\mathrm{H}^1(k, \Omega; \Gamma)$ en le groupe fini Γ, cf. exerc. ...

(N. B. — On peut donner en exercice le sortie de la proreprésentation en général, le lieu au groupe fondamental et à l'exercice suggéré dans le N. B. avant le déf. 5. On peut également mettre en exercice la théorie de Galois axiomatique dans les catégories (cf. SGA V et SGAD X 7.5).)

Considérons maintenant un carré commutatif de corps

$$(0) \qquad \begin{array}{ccc} k' & \longrightarrow & \Omega' \\ \uparrow & & \uparrow \\ k & \longrightarrow & \Omega \end{array}$$

où Ω (resp. Ω') est une extension séparablement close de k (resp. k'). Soit k_s (resp. k'_s) la fermeture algébrique séparable de k (resp. k') dans Ω (resp. Ω'), d'où un carré commutatif de corps correspondant

$$(1) \qquad \begin{array}{ccc} k' & \longrightarrow & k'_s \\ \uparrow & & \uparrow \\ k & \longrightarrow & k_s \end{array}$$

compte tenu que $k'(k_s)$ dans Ω' est une extension algébrique séparable de k' (§7 ...), donc contenue dans k'_s. Considérons alors le diagramme de corps

$$(2) \qquad \begin{array}{ccccc} & & k' & \longrightarrow & k'(k_s) & \longrightarrow & k'_s \\ & & \uparrow & & \uparrow & & \\ k & \longrightarrow & k' \cap k_s & \longrightarrow & k_s & & \end{array}$$

Le diagramme (1), compte tenu que k'_s est une extension galoisienne de k, définit un homomorphisme canonique

$$(3) \qquad \mathrm{Gal}(k'_s/k') \longrightarrow \mathrm{Gal}(k_s/k),$$

qui, grâce à (2), peut aussi se factoriser en

$$(4) \qquad \mathrm{Gal}(k'_s/k') \longrightarrow \mathrm{Gal}(k'(k_s)/k') \longrightarrow \mathrm{Gal}(k_s/k'k_S) \longrightarrow \mathrm{Gal}(k_s/k),$$

où le premier homomorphisme est surjectif (cor. 2 à prop. 2), le deuxième bijectif (théorème 1), le troisième injectif (prop. 2) ; en d'autres termes, (4) donne une interprétation en termes de théorie des corps de la factorisation de l'homomorphisme canonique (3) associé au carré (0). Cet homomorphisme, par définition, peut aussi s'écrire :

$$(5) \qquad \pi_1(k', \Omega') \longrightarrow \pi_1(k, \Omega),$$

et il s'appelle *l'homomorphisme sur les groupes fondamentaux induit par le carré (0)*.

Le plus souvent, on se borne à prendre une extension Ω' de k', et on désigne par Ω l'extension correspondante de k ; il est évident que le choix d'une autre sous-extension séparablement close Ω de Ω' sur k ne modifie pas, à isomorphisme canonique près, le carré (1), donc ne modifie pas, à isomorphisme canonique près, l'homomorphisme (5).

En vertu de prop. 17, l'homomorphisme (5) est continu, en particulier son image est fermée. De plus, la factorisation canonique (4) donne :

Proposition 21. — *Le noyau de l'homomorphisme (5) est canoniquement isomorphe au groupe de Galois topologique de k'_s sur $k'(k_s)$, et l'espace homogène quotient du groupe but par l'image est en correspondance biunivoque canonique avec l'ensemble des k-homomorphismes de k'_1 dans k_s, où $k'_1 = k' \cap k_s$ est la clôture algébrique séparable de k dans k'. Pour que l'image de l'homomorphisme (5) soit d'indice fini dans $\pi_1(k, \Omega)$ il faut et il suffit que k'_1 soit une extension de degré fini de k.*

N. B. — On aimerait pouvoir dire : c'est le cas particulier si k' est une extension de type fini de k. Or il aurait fallu pour cela avoir dit qu'une sous-extension d'une extension de type fini est de type fini. C'est là un résultat utile, que je propose d'inclure dans un nouveau n° au §5, intitulé : *extensions de type fini*.

Il manque un résultat de transitivité sur les homomorphismes des groupes fondamentaux de corps, permettant de dire que $\pi_1(k, \Omega)$ est un foncteur contravariant en (k, Ω), à valeurs dans la catégorie des groupes profinis, et de dire que, pour un carré (0) donné, le foncteur "extension du corps de base" de $\mathrm{Et}(k)$ dans $\mathrm{Ensf}(k')$, s'interprète, compte tenu des équivalences $\mathrm{Et}(k') \approx \mathrm{Ensf}(\pi)$ et $\mathrm{Et}(k') \approx \mathrm{Ensf}(\pi')$ du théorème 5,

comme le foncteur restriction du groupe d'opérateurs ; comme corollaire, on obtient que les bijections du th. 5, cor. 5 et 6, sont fonctorielles également en (k, Ω), non seulement en le groupe Γ. Le rédacteur suppose que Bourbaki peut se faire une idée suffisamment nette de l'allure qu'aurait un n° sur le groupe fondamental d'un corps, sans qu'il soit nécessaire d'aller jusqu'au bout du sorite.

Autocritique du rédacteur. Il est manifeste qu'on comprend moins bien que si on pouvait renverser les flèches et parler de schémas étales sur k, de sorte que l'anti-équivalence du théorème 5 devient une équivalence, et les algèbres à opérateurs galoisiennes deviennent les fibrés principaux homogènes. On pourrait essayer, dans un n° heuristique, d'expliquer ce point de vue, et la relation entre la théorie de Galois et la théorie des revêtements ; on pourrait y dire aussi que les petits bouts de H^1 introduits ici s'insèrent dans la théorie générale de la cohomologie, permettant d'utiliser des suites exactes diverses etc, ce qui fait l'intérêt du formalisme. Évidemment, on peut proposer également de vider purement et simplement le groupe fondamental et le théorème 5, en disant qu'il est toujours temps de faire cette théorie avec la généralité qui lui appartient (sic) plus tard, quand on dispose d'un langage géométrique. Je pense cependant que le cas des corps est assez important pour mériter un traitement séparé, utilisant les simplifications techniques spéciales à ce cas pour obtenir le théorème de structure pratiquement sans travail. — Le seul travail étant d'aligner dans un ordre agréable les sorties fonctoriels utiles de la théorie.

PROJECT DE RÉÉDITION D'ALGÈGRE, CHAP. V (CORPS COMMUTATIFS)
(suite et fin)
COMMENTAIRES

Contrairement à son intention première, le rédacteur s'est abstenu de faire figurer dans la rédaction un paragraphe sur les algèbres radicicielles. Après une rédaction au brouillon sur ce sujet, il a jugé en effet que ce sorte peu substentiel est plus à sa place en Géométrie Algébrique, où il devient plus intuitif, que dans un Chapitre de théorie des corps (ou d'Algèbre Commutative). Compte tenu de la décision louable de Bourbaki de faire figurer la sortie des normes et traces dans un Chapitre antérieur (et les énoncés spéciaux au cas d'algèbres ou extensions étales, dans les par. 7 et 8 du présent Chap. V), le plan prévu pour la rédaction du Chap. V se présente donc maintenant ainsi (avec par. 1 à 6 ne variature) :

7. Algèbres entières séparables.

8. Théorie de Galois.

9. Racines de l'unité, corps finis, extensions kummériens.

10. Algèbres séparables transcendantes. Produits tensoriels d'extensions.

11. Dérivations et différentielles dans les corps.

On trouvera ici une rédaction à peu près en forme du par. 10. Le rédacteur s'est dispensé de reprendre la rédaction du présent par. 9 ; il suffira de faire par rapport au texte imprimé quelques modifications, énumérées dans les commentaires à la rédaction n° 457 (page 3). Je me suis également dispensé de faire une rédaction du par. 11, bien qu'il convienne ici de faire des modifications subtantielles par rapport au texte imprimé, et me suis contenté de proposer au Maître un plan possible pour ce paragraphe, inspiré par EGA IV, par. 18 à 21 (qui pourront fournir, pour le moins, une quantité respectable d'exercices pour l'édition nouvelle du chap. V).

§ 10. — ALGÈBRES ENTIÈRES SÉPARABLES SUR UN CORPS. CLÔTURE SÉPARABLE ET CLÔTURE PARFAITE D'UN CORPS

---

1. — Critères de séparabilité de Mr N. bourbaki et de Mac-lane

Lemme 1. — *Soient k un corps, Ω une extension de k, V un vectoriel sur k, $(u_i)_{i\in I}$ une famille d'homomorphismes de V dans le k-espace vectoriel sous-jacent à Ω. Les deux conditions suivantes sont équivalentes :*

(i) L'homomorphisme $V \otimes_k \Omega \longrightarrow \Omega^I$ déduit de la famille (u_i) est injectif.

(ii) Pour tout sous-espace vectoriel W de V, de rang fini n, le rang sur Ω de la famille des restrictions $u_i|W : W \longrightarrow \Omega$ est égal à n.

On est réduit aussitôt à prouver le lemme dans le cas où V est lui-même de rang fini sur k, utilisant le fait que V est limite inductive de ses sous-espaces vectoriels de rang fini W, et que $V \otimes_k \Omega$ est alors la limite des $W \otimes_k \Omega$. De plus, quitte à remplacer V par $V \otimes_k \Omega$, et les u_i par les homomorphismes $V \otimes_k \Omega \longrightarrow \Omega$ correspondants, on peut supposer que $k = \Omega$. Mais dire que (ii) est vérifiée, signifie aussi que les u_i engendrent le dual V' de V (qui, on le sait, est en effet de rang égal au rang n de V), ou encore que l'orthogonal dans V de la famille des u_i est réduit à zéro ; or cet orthogonal n'est autre que le noyau de l'homomorphisme envisagé dans (i), d'où notre assertion.

Corollaire. — *Soient k un corps, A une k-algèbre, Ω une extension de k. Les conditions suivantes sont équivalentes :*

(i) La Ω-algèbre $A \otimes_k \Omega$ est isomorphe à une sous-algèbre d'une algèbre de la forme Ω^I, où I est un ensemble d'indices convenable.

(ii) Pour tout sous-k-espace vectoriel V de A, de rang fini n sur k, le rang sur Ω de l'ensemble des restrictions à V des k-homomorphismes de A dans Ω est égal à n.

De plus, ces deux conditions équivalentes impliquent que A est une extension séparable sur k.

L'équivalence des conditions (i) et (ii) est un cas particulier du lemme, obtenu en prenant $V = A$, $(u_i)_{i\in I}$ = famille de tous les homomorphismes de k-algèbres de A dans Ω. D'autre part, le fait que (i) implique que A est séparable sur k, résulte aussitôt de (Par. 7, n° 3, prop. 12, (iv), (i) et (ii)).

Lemme 2. — *Soient k un corps d'exposant caractéristique p, A une k-algèbre. Les conditions suivantes sont équivalentes :*

(i) $A \otimes_k k^{p^{-\infty}}$ est réduit.

(i bis) $A \otimes_k k^{p^{-1}}$ est réduit.

(ii) Pour toute extension radicielle k' de k, $A \otimes_k k'$ est réduit.

(ii bis) Pour toute sous-extension finie k' de $k^{p^{-1}}$, $A \otimes_k k'$ est réduit.

(iii) Pour toute famille $(x_i)_{i\in I}$ d'éléments de A linéairement libre sur k, la famille $(x_i^p)_{i\in I}$ est linéairement libre sur k.

(iii bis) Il existe une base $(x_i)_{i\in I}$ de A sur k telle que la famille (x_i^p) soit linéairement libre sur k.

Comme pour toute sous-extension k'' d'une extension k' de k, $A \otimes_k k''$ s'identifie à un sous-anneau de $A \otimes_k k'$, et que lorsque k' est réunion d'une famille filtrante croissante de sous-extensions k_α, alors $A \otimes_k k'$ est réunion filtrante croissante des sous-anneaux $A \otimes_k k_\alpha$, donc réduit si et seulement si ces derniers le sont, on voit aussitôt que l'on a les implications $(i) \iff (ii)$, (i bis) $\iff$ (ii bis). De plus, (i) équivaut aussi (pour la même raison) à la condition (i_r) : $A \otimes_k k^{p^{-r}}$ est réduit pour tout entier naturel

$r \geq 1$. Or pour un r donné, montrons que $A \otimes_k k^{p^{-r}}$ réduit équivaut à chacune des conditions (iii) et $(iii$ bis$)$; comme ces dernières sont indépendantes de r, le lemme 2 en résultera évidemment. Notons d'abord qu'on voit aussitôt, par récurrence sur r, que chacune des conditions (iii) et $(iii$ bis$)$ reste inchangée, à équivalence près, quand on y remplace x_i^p par $x_i^{p^r}$. Ceci dit, montrons que (i_r) implique (iii) : si $B = A \otimes_k k^{p^{-r}}$ est réduit, l'homomorphisme $x \mapsto x^{p^r}$ de B dans lui-même induit un *isomorphisme* de B sur $B^{p^r} = k(A^{p^r}) \subset A$, d'ailleurs semi-linéaire relativement aux structures naturelles d'algèbres de B et B^{p^r} sur $k^{p^{-r}}$ et k respectivement, et à l'homomorphisme $\lambda \mapsto \lambda^{p^r}$ de $k^{p^{-r}}$ dans k. Si alors $(x_i)_{i\in I}$ est une famille d'éléments de A linéairement libre sur k, alors $(x_i \otimes 1)_{i\in I}$ est une famille linéairement libre de $B = A \otimes_k k^{p^{-r}}$ sur $k^{p^{-r}}$, donc par transport de structure la famille des $(x_i \otimes 1)^{p^r} = x_i^{p^r}$ est linéairement libre sur k, d'où (iii). Évidemment (iii) implique $(iii$ bis$)$, enfin $(iii$ bis$)$ implique (i_r), comme on voit en reprenant en sens inverse le raisonnement précédent : $(iii$ bis$)$ implique que l'homomorphisme $x \mapsto x^{p^r}$ de A dans lui-même est injectif, puisque les images des x_i, étant linéairement indépendantes sur k, le sont a fortiori sur k^{p^r}. Cela implique déjà que A est réduit, et l'hypothèse que $(x_i^{p^r})$ est linéairement libre sur k s'interprète en disant que l'homomorphisme canonique $A^{p^r} \otimes_{k^{p^r}} k \longrightarrow A$ est un isomorphisme. Donc le premier membre est réduit. Par transport de structure à l'aide de $x \mapsto x^{p^{-r}}$, on en conclut que $A \otimes_k k^{p^{-r}}$ est également réduit. Cela achève la démonstration du lemme 2.

Nous verrons un peu plus bas que les conditions envisagées équivalent à celle que A soit *séparable* sur k. Bornons-nous pour l'instant à la précision suivante :

Corollaire. — *Supposons que A soit une extension de k, et supposons A et $k^{p^{-\infty}}$ plongés dans une même sur-extension Ω. Alors les conditions équivalentes du lemme 2 équivalent aussi aux suivantes :*

(iv) A et $k^{p^{-\infty}}$ sont linéairement disjoints sur k.

(iv bis) A et $k^{p^{-1}}$ sont linéairement disjoints sur k.

On sait en effet que (iii bis) et (iv bis) sont équivalents ; plus généralement, pour tout entier $r \geq 1$, la condition (iii bis) (où on peut, on l'a déjà signalé, remplacer x_i par $x_i^{p^r}$) équivaut à la disjonction linéaire de A et $k^{p^{-r}}$ sur k. Ces dernières conditions, pour r variable, sont donc équivalentes entre elles, et comme leur conjonction équivaut à (iv), on voit que (iv) équivaut à (iv bis), ce qui achève la démonstration du corollaire.

Théorème 1. — *Soient k un corps d'exposant caractéristique p, K une extension de k, Ω une extension algébriquement close de K, $k^{p^{-\infty}}$ la clôture parfaite de k dans Ω, et $k^{p^{-1}}$ la sous-extension de celle-ci formée des éléments dont la puissance p-ème est dans k. Les conditions suivantes sont équivalentes :*

(i) *K est une extension séparable de k (par. 7, n° 3, déf. 5).*

(ii) *K est linéairement disjoint sur k avec $k^{p^{-\infty}}$.*

(ii bis) *K est linéairement disjoint sur k avec $k^{p^{-1}}$.*

(iii) *La Ω-algèbre $K \otimes_k \Omega$ est isomorphe à une sous-algèbre d'une algèbre de la forme Ω^I, pour un ensemble d'indices convenable I.*

(iv) *Pour tout sous-k-espace vectoriel V de rang fini n de K, l'ensemble des restrictions à V de la famille des k-automorphismes de Ω a un rang sur Ω égal à n.*

Les implications $(iv) \Rightarrow (iii) \Rightarrow (i)$ sont un cas particulier du corollaire au lemme 1. L'équivalence de (iv) et (ii) est un cas particulier du théorème d'Artin (Par. 6, n° 4, th. 1) où on fait $K = k$, $G =$ ensemble des k-automorphismes de Ω ; on tient compte de plus du fait que $k^{p^{-\infty}}$ est le corps des invariants du groupe G des k-automorphismes de Ω (Par. 7, n° 5, prop. 16, cor. 1), et que la disjonction linéaire de K sur k avec une extension k' (ici $k' = k^{p^{-\infty}}$) signifie que tout sous-k-espace vectoriel V de K, de rang fini n, est de rang n également sur k'. Enfin on a $(i) \Rightarrow (ii) \iff (ii$ bis) en vertu du corollaire au lemme 2, compte tenu que par définition, si K est séparable sur k, $K \otimes_k k^{p^{-\infty}}$ est réduit.

Cela achève la démonstration du théorème 1.

Corollaire 1. — *Soit k un corps parfait. Alors toute extension de k est séparable. Plus généralement, pour toute algèbre A sur k, A est séparable si et seulement si elle est réduite.*

La première assertion résulte aussitôt de l'implication $(ii) \Rightarrow (i)$ du théorème, et de l'égalité $k = k^{p^{-\infty}}$ exprimant que k est parfait. Il reste à en déduire que toute k-algèbre réduite A est séparable. Or en vertu de App. 2.12, dire que A est réduite signifie que A se plonge dans un produit de corps, qui sont donc des extensions séparables de k d'après ce qui précède ; on en conclut que A est séparable sur k grâce à (Par. 7, n° 3, prop. 12, (i) et (ii)).

Corollaire 2. — *Soient k un corps, A une k-algèbre, k' une extension parfaite de k. Pour que A soit séparable sur k, il faut et il suffit que $A \otimes_k k'$ soit un anneau réduit.*

En effet (Par. 7, n° 3, prop. 12, (iv)) A est séparable sur k si et seulement si $A' = A \otimes_k k'$ l'est sur k', et on applique le corollaire 1.

Corollaire 3. — *Soient k un corps parfait, A et B deux k-algèbres réduites, alors $A \otimes_k B$ est une k-algèbre réduite.*

C'est une conséquence du corollaire 1 et de (Par. 7, n° 3, prop. 11).

Remarques. — 1) Soit k un corps. Pour que k soit parfait, il faut et il suffit que toute extension de k soit séparable, ou encore que toute algèbre réduite sur k soit séparable, ou ce qui revient encore au même, que le produit tensoriel de deux extensions de k (resp. de deux algèbres réduites sur k) soit un anneau réduit. La nécessité a été vue dans les corollaires 1 et 3 précédents, la suffisance résulte trivialement de la définition des corps parfaits (Par. 7, n° 6, déf. 7).

2) Comme tout corps de caractéristique nulle est parfait, (Par. 7, n° 6, th. 1, cor. 1), on conclut que le produit tensoriel de deux algèbres réduites sur un tel corps est un anneau réduit.

Proposition 1. — *Soient k un corps d'exposant caractéristique p, A une k-algèbre. Les conditions suivantes sont équivalentes :*

(i) *A est une k-algèbre séparable.*

(ii) *$A \otimes_k k^{p^{-\infty}}$ est un anneau réduit.*

(ii bis) *$A \otimes_k k^{p^{-1}}$ est un anneau réduit.*

(ii ter) *Pour toute sous-extension finie k' de $k^{p^{-1}}$, $A \otimes_k k'$ est réduit.*

(iii) *Il existe une extension Ω de k, telle que $A \otimes_k \Omega$ soit Ω-isomorphe à une sous-algèbre d'une algèbre de la forme Ω^I, I un ensemble d'indices convenable.*

(iv) *Il existe une extension Ω de k, telle que pour tout sous-k-espace vectoriel V de K, de rang fini n sur k, l'ensemble des restrictions à V de la famille des homomorphismes de k-algèbres de A dans Ω soit de rang sur Ω égal à n.*

(v) A *est réduit, et pour tout entier premier minimal* $\mathfrak{p}$ *de* A*, le corps des fractions de* $A/\mathfrak{p}$ *est une extension séparable de* k*.*

En effet, l'équivalence des conditions (iii) et (iv), et le fait que celles-ci impliquent la condition (i), résulte encore du lemme 1 et de son corollaire. D'autre part il est trivial que l'on a les implications $(i) \Rightarrow (ii) \Rightarrow (ii \text{ bis}) \iff (ii \text{ ter})$. Il reste à prouver les implications $(ii \text{ bis}) \Rightarrow (v)$ et $(v) \Rightarrow (iii)$. Or, utilisant (Par. 7, n° 3, lemmes 2 et 3), on trouve que l'hypothèse $(ii \text{ bis})$ est stable par passage de A à tout anneau de fractions $S^{-1}A$, relativement à une partie multiplicativement stable S de A. Prenant pour S un ensemble de la forme $A - \mathfrak{p}$, $\mathfrak{p}$ un idéal premier *minimal* de A, on trouve que $S^{-1}A$ est isomorphe au corps des fractions $k(\mathfrak{p})$ et $A/\mathfrak{p}$ (compte tenu que A est réduit, ce qui résulte du fait que A est isomorphe à un sous-anneau de $A \otimes_k k^{p^{-1}}$, qui est réduit par hypothèse). Donc $k(\mathfrak{p}) \otimes_k k^{p^{-1}}$ est réduit, ce qui signifie aussi que $k(\mathfrak{p})$ est linéairement disjoint de $k^{p^{-1}}$ sur k (cor. au lemme 2), et implique en vertu du théorème 1 (implication $(ii \text{ bis}) \Rightarrow (i)$) que $k(\mathfrak{p})$ est séparable sur k. Cela montre que $(ii \text{ bis}) \Rightarrow (v)$.

Enfin, (v) implique que A est isomorphe à une sous-k-algèbre de l'algèbre produit des $k(\mathfrak{p})$, où $\mathfrak{p}$ parcourt les idéaux premiers minimaux de A. Appliquant le théorème 1 (implication $(i) \Rightarrow (iii)$) à chaque $k(\mathfrak{p})$, et prenant une extension Ω de k contenant pour chaque $\mathfrak{p}$ une sous-extension k-isomorphe à une clôture algébrique de $k(\mathfrak{p})$, on trouve que pour tout $\mathfrak{p}$, $k(\mathfrak{p}) \otimes_k \Omega$ est Ω-isomorphe à une sous-algèbre d'une algèbre produit $\Omega^{I(\mathfrak{p})}$, où $I(\mathfrak{p})$ est un ensemble convenable. Prenant pour I un ensemble somme des $I(\mathfrak{p})$, on voit que le produit des $k(\mathfrak{p}) \otimes_k \Omega$ se plonge dans Ω^I, d'autre part en vertu de (Par. 7, n° 3, lemme 1) $A \otimes_k \Omega$ se plonge dans le produit des $k(\mathfrak{p}) \otimes_k \Omega$, donc aussi dans Ω^I, ce qui montre la validité de la condition (iii), et établit que (v) implique (iii). C.Q.F.D..

N.B. — Autocritique. On a utilisé le fait que si A est un anneau réduit, et $\mathfrak{p}$ un idéal premier minimal de A, alors le localisé $A_{\mathfrak{p}}$ est canoniquement isomorphe au corps des fractions de $A/\mathfrak{p}$. Si Bourbaki tient à la proposition 1, il faudrait donc, soit donner ici la propriété énoncée sous forme de lemme ad hoc, soit l'inclure antérieurement dans le sorite sur les anneaux réduits, idéaux premiers etc. préconisé dans l'Appendice. (On pourrait éventuellement faire un petit paragraphe à part, dans le Chapitre V de théorie des corps, contenant les résultats d'algèbre plus ou moins commutative dont on aimerait pouvoir disposer et qui n'auraient pas trouvé leur place dans un Chapitre antérieur.) Si

la prop. 1 est adoptée, il semblerait d'ailleurs plus raisonnable de la baptiser th. 1, le th. 1 actuel devenant corollaire (m. pour la disjonction linéaire !).

Corollaire 1. — *Soient k un corps, K une extension algébrique de k, A une K-algèbre. Pour que A soit séparable sur k, il faut et il suffit que K soit séparable sur k, et A soit séparable sur K.*

Le "il suffit" a été mis pour mémoire, étant établi sous des conditions plus générales dans (Par. 7, n° 3, prop. 12, (v)). Pour le "il faut", on note d'abord que si A est séparable sur k, il en est de même du sous-anneau K, en vertu de (Par. 7, n° 3, prop. 12, (i)). Reste à prouver que A est séparable sur K, ou ce qui revient au même en vertu de la proposition 1, que $A \otimes_K K^{p^{-\infty}}$ est réduit. Or comme K/k est séparable, donc linéairement disjoint de $k^{p^{-\infty}}$, qui est algébrique sur k, on en conclut que $K \otimes_k k^{p^{-\infty}}$ est un corps, isomorphe au composé $K(k^{p^{-\infty}})$ dans $k^{p^{-\infty}}$. Ce composé, étant algébrique sur $k^{p^{-\infty}}$ (puisque K est algébrique sur k), est un corps parfait, comme il contient K et est contenu dans $K^{p^{-\infty}}$, il est isomorphe à $K^{p^{-\infty}}$. Par suite

$$A \otimes_K K^{p^{-\infty}} \simeq A \otimes_K (K \otimes_k k^{p^{-\infty}}) \simeq A \otimes_k k^{p^{-\infty}},$$

et comme le dernier terme est réduit, A étant séparable sur k, il en est de même du premier terme, ce qui prouve le corollaire.

Corollaire 2. — *Soient k un corps d'exposant caractéristique p, A est une k-algèbre, S une famille d'éléments de A entiers sur k. Pour que $k[S]$ soit séparable sur k, il faut que l'on ait $k[S] = k[S^p]$, et cette condition est également suffisante lorsqu'on suppose S de rang fini sur k.*

Posons $K = k[S]$, la relation $k[S] = k[S^p]$ s'écrit aussi $K = k[K^p]$. On peut évidemment dans la première assertion se borner au cas où S est fini, donc on est ramené au cas où K est fini sur k. On peut alors remplacer K par une base linéaire S de K sur k, $S = (x_i)_{i \in I}$. Pour que K soit séparable sur k, il faut et il suffit que $S^p = (x_i^p)$ soit libre sur k (en vertu de prop. 1) ou encore que ce soit une base (puisque K est de degré fini sur k), ce qui signifie $K = k[S^p]$.

N.B. — Le rédacteur ne serait pas opposé à un vidage de ce corollaire, qui s'est borné à copier sur l'état actuel de Bourbaki.

2. — Fermature entière et extension du corps de base

Théorème 2. — *Soient k un corps, A une k-algèbre, B une sous-algèbre de A, C l'ensemble des éléments de A entiers sur B, k' une extension de k, A', B', C' les k'-algèbres déduites respectivement des k-algèbres A, B, C par extension du corps de base. On identifie B' et C' à des sous-algèbres de A', avec $B' \subset C'$.*

Alors :

a) Si l'extension k' de k est séparable, alors C' est la fermeture intégrale de B' dans A'.

b) En tous cas, si D' désigne la fermeture entière de B' dans A', on a $C' \subset D'$, et pour tout $x' \in D'$, il existe un entier $r \geq 0$ tel que $x'^{p^r} \in C'$, où p est l'exposant caractéristique de k.

Il est trivial que l'on a $C' \subset D'$. Montrons l'implication inverse lorsque k' est une extension séparable de k. Supposons d'abord k parfait. On voit aussitôt que si l'assertion voulue est prouvée en remplaçant k' par une sur-extension k'', elle est également vraie pour k'. Cela nous permet de supposer k' algébriquement clos, l'hypothèse k parfait nous assurant que toute extension de k est séparable, donc que l'hypothèse de séparabilité n'est pas perdue. Nous savons alors (Par. 7, n° 6, th. 1) que k est identique au corps des invariants du groupe des k-automorphismes de k'. Pour tout tel automorphisme g, considérons l'automorphisme correspondant $\bar{g} = \mathrm{id}_A \otimes_k g$ de A'; on a évidemment $\bar{g}(B') = B'$, d'où résulte par transport de structure que $\bar{g}(D') = D'$. Comme ceci a lieu pour tous les g, on conclut de (Chap. III...) que l'on a $D' = D \otimes_k k'$, où $D = D' \cap A$. Comme on a $D \supset C$ et que D est évidemment entier sur C, on en conclut par définition de C que $D = C$, ce qui achève la démonstration dans ce cas. Lorsque k est quelconque, considérons la clôture parfaite k_1 de k (réf.), et posons $k'_1 = k_1 \otimes_k k'$. Comme k' est une extension séparable de k, k'_1 est un corps, extension séparable de k (Par. 7, prop. 12, (iv)). Définissons A_1, B_1, C_1 resp. A'_1, B'_1, C'_1 à partir de A, B, C par le changement de corps de base $k \longrightarrow k_1$ resp. $k \longrightarrow k'_1$. Utilisant l'énoncé déjà démontré dans le cas du changement de base $k_1 \longrightarrow k'_1$, pour la fermeture entière D_1 de B_1 dans A_1, on trouve que la fermeture entière de B'_1 dans A'_1 n'est autre que $D'_1 = D_1 \otimes_{k_1} k'_1$. Par suite la fermeture entière D' de B' dans A' est contenue dans $D'_1 \cap A'$, évidemment égal à $(D_1 \cap A) \otimes_k k'$. Or $D_1 \cap A$ est égal à la fermeture entière C de B dans A (réf. Par.

3), donc D' est contenu dans $C' = C \otimes_k k'$, ce qui prouve l'assertion a) du théorème 2. (N.B. – On a utilisé le fait suivant, qui devrait donc figurer au Par. 7 dans le sorite des algèbres entières : si A est une algèbre sur un corps k, B une sous-algèbre, k_1 une extension de k, A_1 et B_1 déduits de A, B par changement de corps de base, et si enfin $x \in A$, alors x est entier sur B si et seulement si il est entier sur B_1.)

Il reste à prouver, lorsque k' n'est plus supposé séparable sur k, que pour tout $x' \in D'$, il existe $r \geq 0$ tel que $x'^{p^r} \in C'$. Quitte à remplacer k' par une sur-extension, on peut supposer k' parfait, donc que k' contient une clôture parfaite k_1 de k. Désignant par D_1 la fermeture entière de $B_1 = B \otimes_k k_1$ dans $A_1 = A \otimes_k k_1$, on sait d'après ce qui précède, appliqué à l'extension séparable k' de k_1 et à la sous-algèbre B_1 de A_1, que $D' = D_1 \otimes_{k_1} k'$, ce qui nous ramène aussitôt au cas où $k' = k_1$ est la clôture parfaite de k. Alors k' est limite inductive de ses sous-extensions finies k'_i, qui sont des extensions finies radicielles de k, et A' et B' sont respectivement limites inductives des $A'_i = A \otimes_k k'_i$ et $B'_i = B \otimes_k k'_i$. Ainsi pour i assez grand, x' provient d'un A'_i, et de même les coefficients d'une équation de dépendance intégrale de x' sur B' proviennent, pour i assez grands, d'un B'_i. Ceci nous ramène au cas où k' est une extension radicielle finie de k. Mais alors il existe un entier $r \geq 0$ tel que pour tout $\lambda' \in k'$, on ait $\lambda'^{p^r} \in k$. Il en résulte que pour tout $x' \in A'$, on a $x'^{p^r} \in A$. Si donc $x' \in A'$ est entier sur B', alors x'^{p^r} est entier sur B'^{p^r}, qui est contenu dans B, donc il est dans C, et a fortiori dans C'. Cela achève la démonstration du théorème 2.

Corollaire 1. — *Avec les notations du théorème 2 pour k, A, k', si k est algébriquement fermé dans A, et si k' est une extension séparable de k, alors k' est algébriquement fermé dans $A' = A \otimes_k k'$.*

Cela résulte en effet du fait que tout élément de A' qui est régulier dans A' est régulier dans A''.

Corollaire 2. — *Avec les notations précédentes, supposons que A soit un corps, et qu'on ait $k' = k((x_i)_{i\in I})$, où $(x_i)_{i\in I}$ est une base de transcendance de k'' sur k. Alors l'anneau total des fractions de $A \otimes_k k'' = A''$ s'identifie à $A((x_i)_{i\in I}) \otimes_{k'} k''$.*

En effet, avec les notations du corollaire 1, on a évidemment un isomorphisme canonique $A'_1 \simeq A((x_i)_{i\in I})$, et tout revient à prouver que $A'_1 \otimes_{k'} k''$ est égal à son propre anneau total des fractions, de sorte que notre corollaire se réduit au résultat suiv-

ant :

Lemme 4. — *Soient k un corps, K une extension de k, k' une extension algébrique de k, alors $K \otimes_k k'$ est égal à son propre anneau total des fractions, i.e. tout élément régulier de cet anneau est inversible.*

En effet (par. 3), $K' = K \otimes_k k'$ est entier sur K puisque k' est entier sur k, d'où aussitôt le résultat en écrivant K' comme limite inductive de ses sous-algèbres finies sur K. (N.B. — Bien entendu, le lemme 4 est un remords du par. 3, qui de toutes façons devait être réécrit.)

Proposition 2. — *Soient k un corps, L une extension de k, K une sous-extension de L, k' une extension de k, K' (resp. L') l'anneau total des fractions de $K \otimes_k k'$ (resp. $L \otimes_k k'$). Sous ces conditions :*

1) *Si K est algébriquement fermé dans L, et si l'extension k' de k est séparable, alors K' est intégralement fermé dans L'.*

2) *Si tout élément de L algébrique sur K est radiciel sur K, alors pour tout élément x' de L' entier sur K', il existe une puissance $p^r (r \geq 0)$ de l'exposant caractéristique p de k, telle que $x'^{p^r} \in K'$.*

On notera que cet énoncé a un sens grâce au corollaire 2 du lemme 3, qui permet d'identifier K' à un sous-anneau de L'. Démontrons la proposition 2 d'abord dans le cas où $k' = k((x_i)_{i \in I})$ est une extension pure de k, de sorte que l'on a alors $L' = L((x_i)_{i \in I}), K' = K((x_i)_{i \in I})$. Dans ce cas, la proposition est essentiellement équivalente au

Corollaire. — *Soient K un corps, L une extension de $K, (x_i)_{i \in I}$ une famille d'indéterminées alors la fermeture algébrique de $K((x_i)_{i \in I})$ dans $L((x_i)_{i \in I})$ est égale à $M((x_i)_{i \in I})$, où M est la fermeture algébrique de K dans L.*

Comme $M((x_i)_{i \in I})$ est évidemment algébrique sur $K((x_i)_{i \in I})$, on est réduit à prouver que tout élément $f \in L((x_i)_{i \in I})$ algébrique sur $K' = K((x_i)_{i \in I})$ appartient à $M' = M((x_i)_{i \in I})$. On est ramené aussitôt au cas où I est fini, puis de proche en proche au cas où I est réduit à un seul élément, de sorte que f est une fonction rationnelle en

une variable x. Ecrivons f sous la forme P/Q, où P et Q sont deux polynômes étrangers de $L[x]$ (réf. Chap. IV ?? Cf. commentaires dans App. 4). Ecrivant une équation de dépendance intégrale pour f sur $K(x)$, et chassant les dénominateurs, il vient une relation

$$(*) \qquad g_0 P^n + g_1 P^{n-1} Q + \cdots + g_n Q^n = 0,$$

les $g_i \in K[x]$, et $g_0 \neq 0$. On conclut de cette relation que Q divise $g_0 P^n$, donc étant étranger à P, il divise g_0 (réf....), de sorte que, quitte à multiplier P et Q par un même facteur, on peut supposer $Q = g_0$, donc $Q \in K[x]$. Par suite $P = fQ$ est algébrique sur $K(x)$, et on est ramené à prouver que $P \in M[x]$, i.e. on est ramené au cas où f est un *polynôme*. Ecrivons donc

$$f = a_0 x^n + \cdots + a_n, \qquad a_i \in L,$$

et prouvons que les a_i sont algébriques sur K. Nous procédons par récurrence sur le degré de f, l'assertion étant triviale si ce dernier est < 0. Ceci nous ramène à prouver que le terme constant a_n est algébrique sur K (en appliquant alors l'hypothèse de récurrence à $(f - a_n)/x$). Or considérons l'équation de dépendance intégrale $(*)$ (où maintenant $P = f, Q = 1$), on y peut supposer que les g_i ne s'annulent pas tous simultanément à l'origine (quitte à diviser par une puissance convenable de x). Faisant la substitution $x = 0$ dans cette équation, on trouve une équation de dépendance algébrique pour $a_n = f(0)$ sur K, ce qui achève de prouver le corollaire.

Pour prouver la proposition 2, 2° dans le cas général, on écrit k' comme une extension algébrique d'une extension pure de k, ce qui, compte tenu du corollaire, nous ramène au cas où k' est une extension algébrique de k. Mais alors, en vertu du lemme 4, K' et L' s'identifient respectivement aux produits tensoriels $K \otimes_k k'$ et $L \otimes_k k'$, et l'assertion à prouver est un cas particulier du théorème 2, b). Un argument analogue, invoquant cette fois-ci le théorème 2 a), prouve la validité de la conclusion de la partie 1°) de la proposition 2, dans le cas particulier où k' est une extension algébrique *séparable* d'une extension pure de k. Or nous verrons au paragraphe suivant qu'il en est ainsi, chaque fois que k' est une extension séparable *de type fini* de k. D'autre part, on se ramène aussitôt au cas où l'extension envisagée k' de k est de type fini, en écrivant k' comme limite inductive de ses sous-extensions de type fini. Cela achève la démonstration de la proposition 2, sous

réserve (pour la partie 1°) de la démonstration du résultat du paragraphe suivant qu'on vient d'invoquer ; le lecteur notera d'autre part que ledit paragraphe est logiquement indépendant du paragraphe présent.

N.B. — Au concours : éliminer le résultat en question de la démonstration du 1° de la prop. 2. Signalons que la démonstration (par Cartier) dans le vieux séminaire Cartan-Chevalley du corollaire à la proposition 2 se faisait également par voie différentielle (en utilisant le critère différentiel d'étalité d'une extension de type fini). Le rédacteur s'est fatigué à trouver une démonstration plus directe, dans le but de rendre le présent paragraphe (à l'exception de prop. 2, 1°, qu'on peut rejeter dans le par. suivant) indépendant du tapis différentiel.

3. — Algèbres géométriquement irréductibles et algèbres géométriquement intègres

Théorème 3. — *Soient k un corps, A une k-algèbre, B l'anneau réduit quotient de A par son nilradical (réf.). Les conditions suivantes sont équivalentes :*

(i) Pour toute extension k' de k, $A \otimes_k k'$ est un anneau irréductible, i.e. son quotient par son nilradical est intègre.

(i bis) Il existe une extension séparablement close (réf.) k' de k, telle que $A \otimes_k k'$ soit un anneau irréductible.

(i ter) Pour toute extension étale k' de k, $A \otimes_k k'$ est un anneau irréductible.

(ii) Pour toute extension séparable k' de k, $B \otimes_k k'$ est intègre.

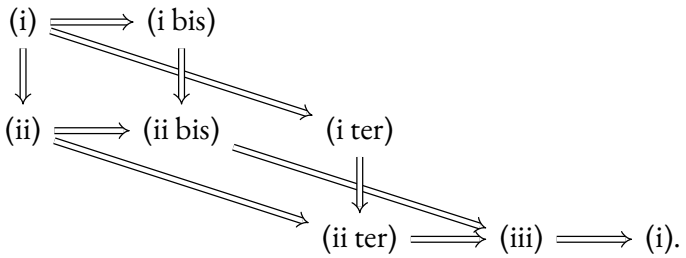
(ii bis) Il existe une extension séparablement close k' de k telle que $B \otimes_k k'$ soit intègre.

(ii ter) Pour toute extension étale k' de k, $B \otimes_k k'$ est intègre.

(iii) B est intègre, et si K désigne son corps des fractions, K_0 la fermeture algébrique de k dans K (réf.), K_0 est une extension radicielle (réf.) de k.

Notons que si C est un anneau, et J un nilidéal de C, alors C est irréductible si et seulement si C/J l'est ; cela implique déjà que chacune des conditions envisagées est invariante quand on y remplace A par B, de sorte qu'on est ramené au cas où A est *réduit*.

Nous prouverons le théorème 3 suivant le diagramme d'implications :



Les implications $(i) \Rightarrow (i\text{ bis})$, $(i) \Rightarrow (i\text{ ter})$, $(ii) \Rightarrow (ii\text{ bis})$, $(ii) \Rightarrow (ii\text{ ter})$ sont triviales. Comme pour toute extension séparable k' de k, $A \otimes_k k'$ est réduit, donc intègre si et seulement si il est irréductible, nous concluons aussitôt les implications verticales $(i) \Rightarrow (ii)$, $(i\text{ bis}) \Rightarrow (ii\text{ bis})$, $(i\text{ ter}) \Rightarrow (ii\text{ ter})$. Comme un sous-anneau d'un anneau intègre est intègre, on voit que les conditions $(ii$ bis$)$ et $(ii$ ter$)$ impliquent chacune que A est intègre. Soient alors K, K_0 comme dans l'énoncé de (iii), et prouvons que K_0 (sous l'une ou l'autre des conditions précédentes) est une extension radicielle de k. Notons d'abord qu'en vertu de (Par. 7, n° 3, lemme 2), et compte tenu qu'un anneau localisé d'un anneau intègre est intègre, on trouve que l'une et l'autre hypothèse $(ii$ bis$)$, $(ii$ ter$)$ est stable par passage de A à K. Les conditions envisagées étant également stables par passage à un sous-anneau, on voit que K_0 satisfait à la même hypothèse que A. L'implication $(ii$ bis$) \Rightarrow (iii)$ et $(ii$ ter$) \Rightarrow (iii)$ résulte alors de la partie "il suffit" du corollaire suivant :

Corollaire 1. — *Soient k un corps, K une extension algébrique de k. Pour que K soit une extension radicielle, il faut et il suffit que pour une extension k' séparable et séparablement close de k, ou encore pour toute extension étale k' de k, l'anneau $K \otimes_k k'$ soit intègre (donc un corps, étant entière sur k').*

Il nous suffira ici de démontrer le "il suffit", pour notre preuve du théorème 3, qui à son tour implique trivialement le corollaire. Or si K n'est pas radicielle, alors en vertu de (Par. 7, n° 5, prop. 16, cor. 4) il existe une sous-extension étale L de K de degré ≥ 2. Si k' est, soit une extension séparablement close de k, soit une extension étale "assez grande" de k, il résulte de (Par. 7, n° 2, prop. 5) que $L \otimes_k k'$ est diagonalisable, et étant de degré ≥ 2, c'est donc un anneau non intègre, ce qui contredit l'hypothèse $(ii$ bis$)$ resp. $(ii$ ter$)$.

Pour prouver le théorème 3, il nous reste donc à établir l'implication $(iii) \Rightarrow (i)$, qui est la partie non triviale de la preuve. Il suffit évidemment de prouver que les conditions

(iii) sont stables par toute extension k'/k du corps de base, et pour ceci on est ramené à le prouver séparément dans les deux cas suivants : $1°$) k' est une extension pure de k, et $2°$) k' est une extension algébrique de k. D'ailleurs, pour k' quelconque, quitte à remplacer A par B, ce qui ne change pas la conclusion qu'on veut établir, on peut supposer déjà A intègre. Comme alors $A \otimes_k k'$ est isomorphe à un sous-anneau de $K \otimes_k k'$, on peut de plus supposer que $A = K$. Il faut prouver alors que $K \otimes_k k'$ est irréductible, et que le corps des fractions K' de son quotient par son nilradical est tel que tout élément de K' algébrique sur k' est radiciel sur k'. Or dans le cas $1°$) c'est ce qu'affirme le corollaire à la proposition 2. Dans le cas $2°$), un passage à la limite immédiat nous ramène au cas où k' est une extension *finie* de k, de sorte que $K \otimes_k k'$ est une algèbre finie sur le corps K. En vertu du théorème 2, b), pour tout élément e de $K \otimes_k k'$ qui est entier sur K, il existe une puissance p^r de l'exposant caractéristique p, telle que $e^{p^r} \in k'$. Appliquant ceci au cas où e est un idempotent de $K \otimes_k k'$, on trouve que $e \in k'$ donc $e = 1$, ce qui prouve que $K \otimes_k k'$ est irréductible. Si K' est son quotient par son nilradical, K' est donc un corps (extension finie de K). Soit alors $x' \in K'$ algébrique sur K, et soit $y' \in K \otimes_k k'$ relevant x', alors y' est entier sur k' (N.B. — sorite oublié dans par. 3), et en vertu du théorème 2, b), il existe un $r \geq 0$ tel que $y'^{p^r} \in k'$, d'où a fortiori $x'^{p^r} \in k'$. Cela achève la démonstration du théorème 3.

Définition 1. — *Soient k un corps, A une k-algèbre. On dit que A est géométriquement irréductible (ou, si une confusion est à craindre, géométriquement irréductible sur k) si elle satisfait les conditions équivalentes du théorème 3. Une extension K de k est dite primarie si elle est une algèbre géométriquement irréductible.*

N.B. — Le rédacteur a gardé la terminologie spéciale "primaire", dans le cas particulier d'une extension, par piété. Il ne serait pas opposé au vidage de ce terme. Noter que l'expression "algèbre primaire" au lieu de "algèbre géom. irr." est manifestement impossible (à cause des confusions possibles avec les autres significations de "primaire").

Corollaire 2. — *Soient k un corps, A une k-algèbre. Les conditions suivantes sont équivalentes :*

(i) A est séparable et géométriquement irréductible.

(ii) Pour toute extension k' de k, $A \otimes_k k'$ est intègre.

(ii bis) *Pour toute k-algèbre intègre A', $A \otimes_k A'$ est intègre.*

(iii) *Il existe une extension algébriquement close k' de k, telle que $A \otimes_k k'$ soit intègre.*

(iii bis) *Pour toute extension finie k' de k, $A \otimes_k k'$ est intègre.*

(iv) *A est intègre, et le corps des fractions K de A est une extension séparable et primaire (déf. 1) de k.*

C'est clair, grâce au théorème 3 et prop. 1.

Définition 2. — *Soient k un corps, A une k-algèbre. On dit que A est géométriquement intègre si elle satisfait aux conditions équivalentes du corollaire 2.*

Corollaire 3. — *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) *Le corps k est séparablement clos.*

(ii) *Si A et B sont deux k-algèbres irréductibles, alors $A \otimes_k B$ est une k-algèbre irréductible.*

(ii bis) *Si A et B sont deux k-algèbres intègres, $A \otimes_k B$ est irréductible.*

(ii ter) *Si K et L sont deux extensions de k, alors $K \otimes_k L$ est irréductible.*

(iii) *Toute extension de k est primaire.*

C'est clair, grâce au théorème 2. (N.B. — Si Bourbaki désire vider la variante (ii bis) et (ii ter) du corollaire, le rédacteur n'objecte pas.)

Corollaire 4. — *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) *Le corps k est algébriquement clos.*

(ii) *Si A et B sont deux k-algèbres intègres, $A \otimes_k B$ est intègre.*

(ii bis) *Itou, avec A et B deux extensions finies de k.*

(iii) *Toute extension de k est géométriquement intègre (déf. 2), i.e. primaire et séparable.*

Comme k algébriquement clos signifie : k séparablement clos et k parfait (Par. 7, n° 7, prop. 23), le corollaire 4 résulte de la conjonction du corollaire 3 et de la remarque du n° 1.

A l'usage des membres fondateurs, s'il en reste :

Corollaire 5. — *Soient K une extension d'un corps k, Ω une surextension algébriquement close. Pour que K soit une extension primaire de k, il faut et il suffit que K soit linéairement disjointe de la fermeture séparable k_s de k dans Ω (Par. 7, n° 4, prop. 14, cor. 5), ou encore que K soit linéairement disjointe de toute sous-extension étale k' de Ω.*

Comme les k' envisagées sont précisément les sous-extensions finies de k_s (Par. 7, n° 7, prop. 22, cor.), les deux conditions énoncées de disjonction linéaire sont bien équivalentes (réf.). D'autre part, comme k_s est une extension algébrique de k, la disjonction linéaire de K et k_s sur k signifie simplement que $K \otimes_k k_s$ est intègre, ce qui en vertu du critère (ii bis) du théorème 2 équivaut au fait que K est une extension primaire de k. On prouve de même, à l'aide du cor. 2 :

Corollaire 6. — *Soient K, k, Ω comme dans le cor. 5. Pour que K soit une extension primaire séparable de k (i.e. soit une k-algèbre géométriquement intègre), il faut et il suffit que K soit linéairement disjointe de la fermeture algébrique $\bar{k}$ de k dans Ω, ou encore que K soit linéairement disjointe de toute sous-extension finie k' de Ω.*

N.B. — La notion "extension primaire et séparable" est appelée chez Weil "extension régulière". On ne peut adopter cette terminologie, qui conflicte avec celle d'anneau régulier, qu'on ne peut plus guère songer à changer. Il ne semble pas que la notion soit assez importante pour qu'il faille absolument trouver un nom lapidaire, plus court que "géométriquement intègre" utilisé par le rédacteur de ses lignes (qui se trouve fort bien de cet usage, comme de bien entendu).

Pour terminer, n'en déplaise aux canons esthétiques du Maître, voici le sorite des notions introduites dans le présent numéro, résumé en une proposition à six points :

Proposition 3. — *Soit k un corps.*

(i) Soit A une k-algèbre. Si A est géométriquement irréductible (resp. géométriquement intègre) il en est de même de toute sous-algèbre de A, et de toute algèbre de fractions de A.

(ii) Toute limite inductive filtrante de k-algèbres géométriquement irréductibles (resp. géométriquement intègres) est itou.

(iii) Soit $(A_i)_{i\in I}$ une famille de k-algèbres, A l'algèbre produit. Pour que A soit géométriquement irréductible (resp. géométriquement intègre) il faut et il suffit que pour tout $i \in I$, A_i le soit.

(iv) Soient A et B deux k-algèbres. Si A et B sont géométriquement irréductibles (resp. géométriquement intègres) il en est de même de $A \otimes_k B$, et la réciproque est vraie si A et B sont non nulles.

(v) Soient A une k-algèbre, k' une extension de k. Pour que A soit géométriquement irréductible (resp. géométriquement intègre) il faut et il suffit que la k'-algèbre $A \otimes_k k'$ le soit.

(vi) Soit K une extension de k, et A une K-algèbre. Si K est géométriquement irréductible (resp. géométriquement intègre) sur k, et A est géom. irr. (resp. géom. intègre) sur K, alors A est géom. irréd. (resp. géom. intègre) sur k.

Le lecteur admirera (déplorera) la symétrie avec la prop. 12 du par. 7, n° 3, déparée seulement par l'oubli dans ladite de la limite inductive filtrante. La démonstration se fait par le même âne qui trotte. Le (i) résulte de la définition et du fait qu'un sous-anneau ou un localisé d'un anneau irréductible (resp. intègre) est itou. Argument analogue pour (ii). Dans (iii), même argument, en utilisant le par. 7, n° 3, lemme 1, et pour la réciproque le (i) déjà établi. Pour (v), voir la démonstration de son homologue dans loc. cit. Cela nous ramène dans (iv) au cas où k est algébriquement clos, et à prouver alors que le produit tensoriel de deux k-algèbres irréductibles (resp. intègres) est irréductible (resp. intègre). On est ramené aussitôt, pour cela, à l'énoncé respé, qui est contenu dans le cor. 4 précédent. La réciproque dans (iv) est conséquence immédiate de (i). Pour (vi), compte tenu de l'assertion analogue dans loc. cit., on est ramené à prouver l'assertion non respée, et pour ceci, que pour toute extension étale k' de k, $A \otimes_k k'$ est irréductible. Or $A \otimes_k k' = A \otimes_K (K \otimes_k k')$, et l'hypothèse de primarité sur K/k implique que $K \otimes_k k'$ est un *corps*, extension étale de K, donc $A \otimes_K k'$ est irréductible d'après l'hypothèse faite pour A/K, C.Q.F.D.

Corollaire 1. — *Soient k un corps, A une k-algèbre (resp. une extension de k). Pour que A soit géométriquement irréductible (resp. géométriquement intègre) il faut et il suffit que toute sous-algèbre (resp. toute sous-extension) de type fini de A le soit.*

Cela résulte aussitôt de la conjonction de (i) et (ii).

Corollaire 2. — *Soient k un corps, K une extension algébrique de k, A une K-algèbre non nulle. Pour que A soit géométriquement irréductible (resp. séparable, resp. géom. intègre) sur k, il faut et il suffit que K soit géom. irréd. (resp. séparable, resp. géom. intè.) sur k, et que A soit géom. irréd. (resp. séparable, resp. géom. intègre) sur K.*

Le il suffit a déjà été vu dans (vi) et par. 7, prop. 12 (v), prouvons la réciproque. La conclusion sur K/k est contenue dans (i), reste à voir que si A est géom. irréd. (resp. séparable, resp. géom. intègre) sur k, il l'est sur K. Dans le cas non respé, désignant par k_s une clôture séparable de k, le fait que K soit algébrique et géom. irréd. sur k (donc radicielle sur k) implique que $K \otimes_k k_s$ est un corps, extension algébrique de k_s, donc séparablement clos comme k_s, et comme $A \otimes_k k_s = A \otimes_K (K \otimes_k k_s)$ est irréductible, il résulte du critère (i bis) du th. 3 que A est géométriquement irréductible sur K. Dans le premier cas respé, désignant par k_p la clôture parfaite de k, le fait que K est algébrique séparable sur k implique que $K \otimes_k k_p$ est un corps, extension algébrique de corps parfait k_p, donc un corps parfait (par. 7, n° 6, prop. 18). Ceci dit, $A \otimes_k k_p = A \otimes_K (K \otimes_k k_p)$ est réduit d'après l'hypothèse de séparabilité pour A/k, ce qui implique que A/K est également séparable en vertu du critère de prop. 1 (ii). Enfin, le deuxième cas respé résulte aussitôt de la conjonction des deux cas déjà traités.

§ 11. — DÉRIVATIONS ET DIFFÉRENTIELLES DANS LES CORPS (PLAN)

---

1. — Algèbres formellement lisses, non ramifiées, resp. étales

Tous les anneaux et algèbres sont commutatifs.

Définition 1.2. — *Une algèbre B sur l'anneau A est dite formellement lisse (resp. formellement non ramifiée, resp. formellement étale) si pour toute algèbre C sur A, toute extension E de C par un idéal nilpotent J, et tout homomorphisme de A-algèbres $u_0 : B \longrightarrow C$, il existe au moins un (resp. au plus un, resp. exactement un) homomorphisme de A-algèbres $u : B \longrightarrow E$ qui relève u_0.*

Proposition 1.2. — *Dans cette définition, on peut se borner au cas $C = B$, $u_0 = \mathrm{id}_B$, et J de carré nul, donc à demander l'existence (resp. l'unicité, resp. l'existence et l'unicité) d'une trivialisation pour une extension de A-algèbres de B par un idéal de carré nul.*

C'est immédiat.

Remarque 1.3. — Formellement étale = formellement lisse + formellement non ramifiée.

Exemple 1.4. — Soit (X_i) une famille d'indéterminées, alors l'algèbre de polynômes $A[(X_i)_{i\in I}]$ est formellement lisse sur A.

Sorite 1.5. —

(i) Stabilité par changement de base $A \longrightarrow A'$.

(ii) Transitivité : si C est formellement lisse (resp....) sur B et B formellement lisse (resp....) sur A, alors C est formellement lisse (resp....) sur A.

(iii) Stabilité par localisation en haut (passage de B à $S^{-1}B$).

C'est tout immédiat.

Corollaire 1.6. — *Si k est un corps, toute extension pure de k est formellement lisse sur k. (Elle est formellement étale sss l'extension est triviale.)*

Résulte de 1.4 et 1.5 (iii).

2. — Propriétés différentielles des algèbres formellement lisses

Proposition 2.1. — *Soit B formellement lisse sur A, A une algèbre sur k. Alors la suite d'homomorphismes canoniques*

$$0 \longrightarrow \Omega^1_{A/k} \otimes_A B \longrightarrow \Omega^1_{B/k} \longrightarrow \Omega^1_{B/A} \longrightarrow 0$$

est exacte et splitte.

Cf. EGA 0_{IV} 20.5.7.

N.B. — Un complément intéressant, mais qu'on ne peut donner dans Bourbaki faute de disposer de la notion voulue, est que $\Omega^1_{B/A}$ est un B-module *projectif*.

Proposition 2.2. — *Soient B une algèbre sur A, J un idéal de B, $C = B/J$, et supposons C formellement lisse sur A. Alors la suite d'homomorphismes canoniques*

$$0 \longrightarrow J/J^2 \longrightarrow \Omega^1_{B/A} \otimes_B C \longrightarrow \Omega^1_{C/A} \longrightarrow 0$$

est exacte et splitte.

Cf. EGA 0_{IV} 20.5.12.

Proposition 2.3. — *Soit B une A-algèbre. Pour que B soit formellement non ramifiée sur A, il faut et il suffit que l'on ait $\Omega^1_{B/A} = 0$, i.e. que toute A-dérivation de B dans un B-module M soit nulle.*

Cela provient du fait que, sous les conditions de 1.2, les splittages de l'extension envisagée forment un ensemble vide ou principal homogène sous le groupe des A-dérivations de B dans J.

Corollaire 2.4. — *Soit B une A-algèbre formellement étale, A étant une k-algèbre. Alors l'homomorphisme canonique $\Omega^1_{A/k} \otimes_A B \longrightarrow \Omega^1_{B/k}$ est un isomorphisme.*

On conjugue 2.1 et 2.3.

3. — Caractérisation différentielle des algèbres étales sur un corps

Théorème 3.1. — *Soient k un corps, A une k-algèbre de type fini. Conditions équivalentes :*

(i) *A est étale.*

(ii) *A est formellement étale.*

(iii) *A est formellement non ramifiée, i.e. $\Omega^1_{A/k} = 0$.*

Démonstration. — (i) $\Rightarrow$ (ii). On peut supposer A une extension étale de k, donc de la forme $k[X]/Fk[X]$, où $F \in k[X]$ est un polynôme séparable. Soit $x \in A$ défini par X, et soit E une extension de A par un idéal J de carré nul, à montrer que x se relève en un élément y satisfaisant $F(y) = 0$. On choisit "au hasard" un élément a relevant x, et on cherche $z \in J$ tel que $F(a + z) = 0$, i.e. $F(a) + F'(a)z = 0$, ce qui se résout par $z = -F(a)/F'(a)$, compte tenu que F étant séparable, on a $F'(a) = F'(x) \neq 0$.

L'implication (ii) $\Rightarrow$ (iii) étant triviale, il reste à prouver (iii) $\Rightarrow$ (i). Faisons d'abord la démonstration lorsque A est déjà supposé finie sur k. Quitte à faire une extension sur le corps de base k, on peut supposer k algébriquement clos, puis on peut supposer A local, donc extension de k par un idéal nilpotent $\mathfrak{m}$. Mais $\mathfrak{m}/\mathfrak{m}^2$, étant isomorphe à $\Omega^1_{A/k} \otimes_A k$, est nul, donc $\mathfrak{m} = 0$, donc $A = k$, on gagne. Reste à prouver que la condition (iii) implique que A est fini sur k. Quand on dispose d'un peu d'Algèbre commutative, on peut encore procéder comme dessus, en se ramenant au cas k alg. clos et notant que pour tout idéal maximal $\mathfrak{m}$ de A, l'anneau local noethérien $A_\mathfrak{m}$ est tel que $\mathfrak{m}/\mathfrak{m}^2 = 0$, donc est réduit à son corps résiduel, donc tout point fermé de Spec(A) est isolé, et on gagne. Dans le cadre du chap. V, on peut donner une démonstration par récurrence sur le nombre n de générateurs de A sur k, le cas $n \leq 1$ étant immédiat. Si $n \geq 2$,

soit x_1 le premier générateur, et soit $B = k[x_1] \subset A$, à prouver qu'il n'est pas possible que x_1 soit transcendant sur k. Sinon, soit en effet $B' = k(x_1)$ le corps des fractions de B, et $A' = A \otimes_B B' \subset B'$. Alors la relation $\Omega^1_{A/k} = 0$ implique $\Omega^1_{A/B} = 0$, donc par changement de base $\Omega^1_{B'/A'} = 0$, donc par hypothèse de récurrence B' est étale sur A', d'où on conclut que $\Omega^1_{A'/k} \simeq \Omega^1_{B'/k} \otimes_{B'} A'$ en vertu de 2.4. Comme $\Omega^1_{B'/k} \simeq \Omega^1_{B/k} \otimes_B B'$ est libre de rang 1 donc non nul, et que $A' \supset B'$ est non nul, on conclut que $\Omega^1_{A'/k} \neq 0$, or le premier membre est localisé de $\Omega^1_{A/k}$ qui est nul par hypothèse, d'où une contradiction.

Corollaire 3.2. — *Soit k_0 un sous-corps parfait de k (par exemple le corps premier), alors les conditions de 3.1 équivalentes encore à la suivante :*

(iv) $\Omega^1_{k/k_0} \otimes_k A \longrightarrow \Omega^1_{A/k_0}$ *est un isomorphisme, i.e. pour tout A-module M, toute k_0-dérivation $k \longrightarrow M$ se prolonge de façon unique en une k_0-dérivation $A \longrightarrow M$.*

En effet, (ii) implique (iv) en vertu de 2.4, et (iv) $\Rightarrow$ (iii) puisque $\Omega^1_{A/k}$ est isomorphe au conoyau de l'homomorphisme envisagé dans (iv).

Corollaire 3.3. — *Extension de 3.1 au cas où A, au lieu d'être une algèbre de type fini sur k, est localisée $S^{-1}B$ d'une telle algèbre B (par exemple lorsque A est une extension de type fini de k).*

Cela résulte facilement de 3.1 sous la forme envisagée, compte tenu qu'on aura $\Omega^1_{A/k} = \Omega^1_{B/k} \otimes_B A = S^{-1}\Omega^1_{B/k}$, et comme $\Omega^1_{A/k}$ est un module de type fini, s'il devient nul par localisation par rapport à S, il existe $f \in S$ qui l'annule, de sorte que l'on peut appliquer 3.1 à l'algèbre de type fini A_f.

Proposition 3.4. — *Soient k un corps, A une algèbre entière sur k, J le nilradical de A, $A_0 = A/J$, A' (resp. A'_0) la clôture séparable de k dans A (resp. dans A_0). Alors le morphisme canonique $A \longrightarrow A_0$ induit un isomorphisme $\Phi : A' \longrightarrow A'_0$. Pour tout $x \in A'_0$, $\Phi^{-1}(x)$ est l'unique élément de A relevant x et séparable sur k, a fortiori Φ^{-1} est l'unique homomorphisme de k-algèbres de A'_0 dans A qui relève l'inclusion de A'_0 dans A_0.*

Démonstration. — Comme Φ est évidemment injectif (A' étant réduit), pour prouver que c'est un isomorphisme il suffit de prouver que tout élément x de A'_0 provient

d'un élément de A' (manifestement unique), ce qui prouvera 3.4. Or il suffit pour ceci d'appliquer à l'algèbre $k[x]$ l'implication (i) $\Rightarrow$ (ii) de 3.1. On conclut aussitôt de 3.4 :

Proposition 3.5. — *Toute algèbre entière séparable sur un corps k est formellement étale sur k.*

4. — Caractérisation différentielle des extensions séparables : cas des extensions de type fini

Théorème 4.1. — *Soient k un corps, K une extension de type fini de k. Alors $\Omega^1_{K/k}$ est un vectoriel de dimension finie sur K, et on a*

$$(*) \qquad \textit{deg tr } K/k \leq \textit{rang}_K \Omega^1_{K/k}.$$

De plus les conditions suivantes sont équivalentes :

(i) *K est une extension séparable de k.*

(ii) *L'inégalité (*) est une égalité.*

(iii) *K est une extension étale d'une sous-extension pure.*

On prouve d'abord le

Corollaire 4.2. — *Soient $x_1, \ldots, x_m \in K$, alors les $d_{K/k}x_i$ engendrent $\Omega^1_{K/k}$ si et seulement si K est une extension étale de $k(x_1, \ldots, x_m) = K'$.*

En effet, on utilise le critère différentiel d'étalité 3.3, en notant que $\Omega^1_{K/K'}$ est isomorphe à $\Omega^1_{K/k}$ divisé par le sous-espace vectoriel engendré par les $d_{K/k}x_i$.

Le corollaire 4.2 implique aussitôt l'inégalité (*) et l'implication $(ii) \Rightarrow (iii)$. D'autre part (iii) implique trivialement (i), et il reste à prouver que (i) implique (ii). Pour ceci, voir le texte Bourbaki imprimé, p. 142.

On pourra, si on veut, introduire (comme dans l'ancienne rédaction) la terminologie : base de transcendance séparante ; cela ne semble pas indispensable. Notons aussi :

Corollaire 4.3. — *Les conditions précédentes impliquent la suivante :*

(iv) *K est formellement lisse sur k.*

Cela résulte en effet de la transitivité 1.5 (ii), de 1.6 et de 3.1.

Corollaire 4.4. — *Soit k_0 un sous-corps de k. Alors les conditions de 3.1 impliquent la suivante :*

(v) L'homomorphisme $\Omega^1_{k/k_0} \otimes_{k_0} K \longrightarrow \Omega^1_{K/k_0}$ est injectif, i.e. toute k_0-dérivation de k dans K se prolonge en une k_0-dérivation de K dans K.

On utilise 4.3 et 2.1.

Remarque 4.5. — Nous verrons au n° 7 que les conditions (iv) et (v) sont même équivalentes à la condition (i), pourvu que dans (v) on suppose que k_0 est parfait (et sans supposer nécessairement K de type fini sur k).

5. — p-bases

Dans le présent n° et le suivant, p désigne un nombre premier, et sauf dans 6.9 tous les anneaux envisagés sont de caractéristique p.

Définition 5.1. — *Soient A un anneau, B une A-algèbre, $(x_i)_{i\in I}$ une famille d'éléments de B. On dit que cette famille est une famille p-génératrice sur A (resp. est p-libre sur A, resp. est une p-base sur A) si la famille des monômes*

$$\prod_{i\in I} x_i^{n_i} \text{ (où } (n_i) \in \mathbf{Z}^{(I)}, 0 \leq n_i < p \text{ pour tout } i)$$

est une famille génératrice (resp. libre, resp. une base) du A-module sous-jacent à B. Si $A = \mathbf{F}_p$, on omet la référence à A, et on dit aussi famille p-génératrice (resp....) absolue.

Remarque 5.2. — Pour que (x_i) soit une famille p-génératrice, il f. et s. qu'elle engendre B comme algèbre sur $A[B^p]$.

Proposition 5.2. — *Soient $A \longrightarrow B \longrightarrow C$ des homomorphismes d'anneaux, tels que $Im(B \longrightarrow C) \supset C^p$, M une partie de B, N une partie de C.*

a) Si M est p-génératrice dans B sur A, et N est p-génératrice dans C sur B, alors $M \cup N$ est p-génératrice dans C sur A.

b) Si M est une p-base de B sur A, alors N est p-libre sur B si et seulement si $M \cup N$ est p-libre sur A.

C'est immédiat, cf. EGA 0_{IV} 21.1.10.

Théorème 5.3. — *Soient k un corps, K une extension de k, S une partie p-génératrice de K sur k, $L \subset S$ une partie p-libre de K sur k. Il existe alors une p-base B de K sur k telle que $L \subset B \subset S$. En particulier, toute extension de k admet une p-base sur k.*

Démonstration par application facile de Zorn (cf. EGA 0_{IV} 21.4.2), en utilisant le

Lemme 5.4. — *Pour qu'un élément x de K soit p-libre sur k, il f. et suffit que $x \notin k(K^p)$.*

Corollaire 5.5. — *Pour qu'une famille $(x_i)_{i\in I}$ d'éléments de K soit p-libre sur k, il f. et s. que pour tout i, x_i n'appartienne pas au corps K_i engendré par $k(K^p)$ et les x_j avec $j \neq i$.*

6. — Dérivations et différentielles en caractéristique p

Proposition 6.1. — *Soient A un anneau, B une A-algèbre. Alors :*

a) Pour tout B-module, toute A-dérivation D de B dans M s'annule sur B^p, donc est une $A[B^p]$-dérivation. Si A et B sont des corps, D est même une $A(B^p)$-dérivation.

b) L'homomorphisme canonique

$$\Omega^1_{B/A} \longrightarrow \Omega^1_{B/A[B^p]}$$

est un isomorphisme. De même, si A et B sont des corps, l'homomorphisme

$$\Omega^1_{B/A} \longrightarrow \Omega^1_{B/A(B^p)} \quad .$$

Par suite, en car. $p > 0$, pour l'étude des propriétés des dérivations resp. différentielles d'une A-algèbre B, on se ramène généralement au cas où A est un sous-anneau de B contenant B^p.

Proposition 6.2. — *Soient B un anneau, A un sous-anneau contenant B^p, $(x_i)_{i\in I}$ une p-base de B sur A, L un A-module. Alors :*

a) Pour qu'une dérivation D de A dans L se prolonge en une dérivation de B dans L, il faut et suffit que D s'annule dans B^p.

b) Lorsqu'il en est ainsi, pour toute famille $(y_i)_{i\in I}$ d'éléments de L, il existe une dérivation D' et une seule de B dans L, prolongeant D, et telle que $D'(x_i) = y_i$ pour tout i.

Cf. EGA 0_{IV} 21.2.3., où cette proposition est présentée comme cas particulier d'une autre plus générale, concernant le prolongement d'un relèvement partiel $A \longrightarrow E$, où E est une extension de B par un idéal nilpotent. — Le dictionnaire habituel en termes de différentielles donne :

Corollaire 6.3. — *La suite*

$$0 \longrightarrow \Omega^1_{A/B^p} \otimes_A B \longrightarrow \Omega^1_{B/B^p} \longrightarrow \Omega^1_{B/A} \longrightarrow 0$$

est exacte et scindée, et la famille $(\mathrm{d}_{B/A}x_i)_{i\in I}$ forme une base du B-module $\Omega^1_{B/A}$.

Corollaire 6.4. — *Soient A un anneau, B une A-algèbre admettant une p-base $(x_i)_{i\in I}$, alors la famille $(\mathrm{d}_{B/A}x_i)_{i\in I}$ est une base de $\Omega^1_{B/A}$ sur B.*

En effet, grâce à 6.1 on est ramené au cas où $B^p \subset A \subset B$, et on est alors sous les conditions de 6.3.

Théorème 6.5. — *Soient k un corps, K une extension de k, $(x_i)_{i\in I}$ une famille d'éléments de K. Pour que celle-ci soit p-libre (resp. p-génératrice, resp. une p-base) sur k, il faut et il suffit que la famille $(\mathrm{d}_{K/k}x_i)_{i\in I}$ soit une famille libre (resp. génératrice, resp. une base) du K-module $\Omega^1_{K/k}$.*

Cf. EGA 0_{IV} 21.4.5.

Corollaire 6.6. — *Pour que $\Omega^1_{K/k} = 0$, il faut et il suffit que $K = k(K^p)$. En particulier, si k est parfait (par exemple est le corps premier) cela signifie que $\Omega^1_K = 0$ (module des différentielles absolues), ou encore que K est parfait.*

Corollaire 6.7. — *Soient K une extension de k, et $x \in K$. Conditions équivalentes :*

(i) $x \notin k(K^p)$.

(ii) $\mathrm{d}_{K/k}x \neq 0$.

(iii) L'élément x est p-libre sur k.

Corollaire 6.8. — *Soient B un anneau réduit, A un sous-anneau contenant B^p. Supposons que B admette une p-base sur A, et que A admette une p-base sur B^p (conditions vérifiées si A et B sont des corps, en vertu de 5.3). Alors, on a un isomorphisme canonique*

$$(\Omega^1_{B/A})^{(p)} \simeq \mathrm{Ker}(\Omega^1_A \otimes_A B \longrightarrow \Omega^1_B)\,,$$

envoyant l'élément $(d_{B/A}x)^{(p)}$ du premier membre en l'élément $d_A x \otimes 1$ du second.

Cf. EGA 0_{IV} 21.3.5. Pour un B-module M, on a posé $M^{(p)} = M \otimes_B (B, \Phi)$ où (B, Φ) désigne B considéré comme B-algèbre à l'aide de l'homomorphisme $\Phi : x \rightsquigarrow x^p$.

Théorème 6.9. — (Egalité de Cartier). *Soient k un corps de caractéristique quelconque (N.B. la caractéristique nulle n'est pas exclue), K une extension de type fini. Alors $\Omega^1_{L/K}$ et $\gamma_{L/K} = Ker(\Omega^1_K \otimes_K L \longrightarrow \Omega^1_L)$ sont des vectoriels de dimension finie sur K, et on a :*

$$\mathrm{rang}_L\, \Omega^1_{L/K} - \mathrm{rang}_L\, \gamma_{L/K} = deg\ tr\ L/K\,.$$

Cf. EGA 0_{IV} 21.7.1.

Corollaire 6.10. — *On a $rang_L \Omega^1_{L/K} \geq deg\ tr\ L/K$, avec égalité si et seulement si l'homomorphisme canonique $\Omega^1_K \otimes_K L \longrightarrow \Omega^1_L$ est injectif, i.e. sss toute dérivation de K dans L se prolonge en une dérivation de L dans L.*

N. B. — Ceci établit l'équivalence des conditions (ii) et (v) du n° 4, annoncée dans 4.5.

7. — Caractérisation différentielle des extensions séparables : cas général

Théorème 7.1. — *Soient K une extension d'un corps k, k_0 un sous-corps parfait de k (par ex. le corps premier). Conditions équivalentes :*

(i) K est une extension séparable de k.

(ii) K est une algèbre formellement lisse sur k.

(iii) L'homomorphisme canonique $\Omega^1_{k/k_0} \otimes_k K \longrightarrow \Omega^1_{K/k_0}$ *est injectif, i.e. toute* k_0*-dérivation de* k *dans* K *se prolonge en une* k_0*-dérivation de* K *dans lui-même.*

Démonstration. — $(i) \Rightarrow (ii)$. Le cas où K est une extension de type fini de k est déjà connu (4.1) et on peut passer de là au cas général par un passage à la limite (EGA 0_{IV} 19.6.1), indépendant de toute considération différentielle, mais qui a l'inconvénient de se rédiger assez mal avec les moyens dont Bourbaki dispose ici, puisqu'il y est question de l'homologie d'un certain complexe à la Hochschild. Il sera donc sans doute plus simple de distinguer deux cas :

1°) k de caractéristique nulle, alors K est une extension algébrique séparable d'une extension pure de k, et on conclut comme dans 4.3, en utilisant ici 3.4 au lieu de 3.1 ;

2°) k de car. $p > 0$.

On a alors un énoncé plus précis :

Corollaire 7.2. — *Soient* k *un corps de car.* $p > 0$*,* K *une extension séparable de* k*,* $(x_i)_{i\in I}$ *une* p*-base de* K *sur* k*,* E *une* k*-algèbre extension d'une algèbre* C *par un idéal nilpotent* J*,* $u : K \longrightarrow C$ *un homomorphisme de* k*-algèbres, et pour tout* $i \in I$*, soit* $y_i \in E$ *relevant* $u(x_i)$*. Alors il existe un unique* k*-homomorphisme* $v : K \longrightarrow E$ *tel que* $v(x_i) = y_i$ *pour tout* i*.*

Pour la démonstration, cf. EGA 0_{IV} 21.2.7 (qui donne un énoncé plus général, sans corps).

L'implication $(ii) \Rightarrow (iii)$ étant évidente (2.1), il reste à prouver $(iii) \Rightarrow (i)$. Or si k est de caractéristique nulle, il n'y a rien à prouver. Si la caractéristique est $p > 0$, soit $(x_i)_{i\in I}$ une p-base absolue de k. Il résulte alors du critère de séparabilité de Mac-Lane que K/k est séparable si et seulement si (x_i) est p-libre dans K. Or cela signifie que les $d_K(x_i)$ forment un système libre sur K dans Ω^1_K. Comme ce sont les images des éléments $d_k x_i$ de $\Omega^1_k \otimes_k K$, qui forment une base de cet espace, on voit bien que (iii) implique (i). Cela achève la démonstration de 7.1.

Remarque 7.3. — Compte tenu de l'égalité de Cartier, le théorème 7.1 redonne l'équivalence des conditions (i) et (ii) de 4.1 (qui était la partie non triviale de (4.1), pour

laquelle on a renvoyé au texte imprimé de Bourbaki). On pourrait donc (avec avantage semble-t-il) reporter 4.1 en corollaire à 7.1. La raison pour laquelle j'ai gardé une démonstration directe de 4.1, est que la démonstration en question est indépendante des phénomènes spéciaux à la caractéristique $p > 0$.

APPENDICE

---

1. — Décomposition d'un anneau en produit fini d'anneaux

Proposition 1.1. — *Soient A un anneau, I un ensemble fini. Désignons par $E(A;I)$ l'ensemble des familles $(e_i)_{i\in I}$ d'éléments centraux de A, indexées par I, telles qu'on ait*

$$\begin{cases} e_i^2 = e_i & \text{pour tout } i \in I, \\ e_i e_j = 0 & \text{pour } i, j \in I, i \neq j, \\ \sum_I e_i = 1. \end{cases}$$

Désignons par $D(A,I)$ l'ensemble des familles $(A_i)_{i\in I}$, indexées par I, d'anneaux quotients A_i de A, telles que l'homomorphisme canonique $A \longrightarrow \prod_i A_i$, déduit des homomorphismes canoniques $A \longrightarrow A_i$, soit un isomorphisme. Soit

$$\varphi : D(A,I) \longrightarrow E(A,I)$$

l'application définie de la manière suivante : si $d = (A_i)_{i\in I} \in D(A,I)$, et si u désigne l'isomorphisme canonique $A \longrightarrow \prod_i A_i$, désignons par e'_i l'élément de $\prod_i A_i$ dont la composante d'indice j est égale à 0 si $j \neq i$, égale à l'élément unité de A_i si $j = i$, et posons $e_i = u^{-1}(e'_i)$. On pose alors $\varphi(d) = (e_i)_{i\in I}$.

Ceci posé, l'application précédente φ est bijective. Si $e = (e_i)_{i\in I} \in E(A,I)$, l'unique élément $d = (A_i)_{i\in I}$ tel que $\varphi(d) = e$ est défini par la condition :

$$A_i = A/\sum_{j\neq i} e_j A ;$$

de plus, l'application

$$v_i : e_i A \longrightarrow A_i$$

induite par l'application canonique $A \longrightarrow A_i$ *est bijective et applique* e_i *sur l'élément unité de* A_i*.*

Remarque 1.2. — On peut donc dire que l'application précédente $e_i A \longrightarrow A_i$ induit un isomorphisme d'anneaux, lorsque l'idéal $e_i A$ est muni des lois d'addition et de multiplication induites par celles de A, qui font de $e_i A$ un anneau admettant e_i comme élément unité. On fera attention cependant que pour cette structure d'anneau, $e_i A$ *n'est pas* en général un sous-anneau de A ; c'est pourquoi nous nous garderons toujours d'identifier l'*anneau* quotient A_i de A avec l'*idéal* $e_i A$ de A.

Remarque 1.3. — Soit $(B_i)_{i \in I}$ une famille d'anneaux (pas nécessairement des anneaux quotients de A) et $u : A \longrightarrow \prod_i B_i$ un isomorphisme. Alors chacun des homomorphismes composants $u_i : A \longrightarrow B_i$ est évidemment surjectif, donc se factorise de façon unique en un composé $A \longrightarrow A_i \longrightarrow B_i$, où $A \longrightarrow A_i$ est un homomorphisme canonique sur un anneau quotient, et $A_i \longrightarrow B_i$ un isomorphisme. Par suite, u se factorise en un composé

$$A \longrightarrow \prod_i A_i \longrightarrow \prod_i B_i,$$

où la première flèche correspond à un élément bien déterminé de $D(A, I)$, et la deuxième est déduite de la famille des isomorphismes $A_i \longrightarrow B_i$. On peut donc dire *à un isomorphisme près*, tout isomorphisme tel que $u : A \longrightarrow \prod_i B_i$ peut être défini par une famille $e = (e_i)_{i \in I} \in E(A, I)$, déterminée de façon unique.

Remarque 1.4. — On appelle *idempotent* d'un anneau A tout élément e de A tel que $e^2 = e$. On dit parfois que deux idempotents e et f de A sont "*orthogonaux*" si on a $ef = fe = 0$. On peut donc dire que les éléments de $E(A; I)$ sont les familles d'idempotents centraux, mutuellement orthogonaux, de somme 1, indexées par I.

Corollaire 1.5. — *Il y a une correspondance biunivoque entre l'ensemble des couples* (A', A'') *d'anneaux quotients de* A *tels que l'homomorphisme canonique* $A \longrightarrow A' \times A''$ *soit un isomorphisme, et l'ensemble des idempotents centraux de* A*.*

En effet, il suffit d'établir une bijection entre ce dernier ensemble et l'ensemble

$E(A; I)$, où $I = \{1, 2\}$, et pour ceci il suffit de faire correspondre à l'idempotent central e le couple $(e, 1 - e)$.

Proposition 1.6. — *Soit A un anneau. On dit que A est indécomposable si A n'est pas nul, et si A n'est pas isomorphe à un produit de deux anneaux non nuls.*

Par exemple, un corps, un anneau commutatif intègre, sont indécomposables.

Compte tenu de 1.5 et de 1.3 on obtient :

Proposition 1.7. — *Pour que l'anneau A soit indécomposable, il faut et il suffit que $A \neq 0$ et que 0 et 1 soient les seuls idempotents centraux de A, ou encore, que A ait exactement deux idempotents centraux.*

Remarque 1.8. — Ainsi, pour que A soit indécomposable, il faut et il suffit que son centre le soit, ce qui nous ramène au cas d'un anneau commutatif. * D'autre part, pour qu'un anneau commutatif soit indécomposable, il faut et il suffit que son *spectre premier* soit connexe. *

Proposition 1.9. — *Soient A un anneau. Les conditions suivantes sont équivalentes :*

(i) *A est isomorphe au produit d'une famille finie d'anneaux indécomposables.*

(ii) *Il existe une famille finie d'idempotents centraux e_i dans A, mutuellement orthogonaux (1.4), de somme 1, dont chacun est un "idempotent indécomposable" i.e. n'est pas la somme de deux idempotents centraux non nuls.*

(iii) *L'ensemble des idempotents centraux de A est fini.*

Sous ces conditions, si $u : A \longrightarrow \prod_{i \in I} A_i$ et $u' : A \longrightarrow \prod_{j \in J} A'_j$ sont deux isomorphismes de A avec des produits finis d'anneaux indécomposables A_i ($i \in I$) resp. A'_j ($j \in J$), il existe une bijection $w : I \longrightarrow J$, et des isomorphismes $v_i : A_i \longrightarrow A'_{w(i)}$, tels que u' soit égal à $v \circ u$, où $v : \prod A_i \longrightarrow \prod A'_j$ est l'isomorphisme défini par w et le système des v_i. D'ailleurs, w et les v_i sont uniquement déterminés par les données précédentes.

N. B. — On pourrait vouloir donner un nom à un anneau satisfaisant aux conditions de 1.9, par exemple l'appeler "complètement décomposable" ; mais cette terminologie conduit au résultat qu'un anneau indécomposable est complètement décomposable ! — La dernière partie de 1.9 a un énoncé assez lourd, il serait sans doute plus pigeable de le

remplacer par l'énoncé suivant : "Sous ces conditions, soit $(A_i)_{i\in I}$ la famille des anneaux quotients de A qui sont indécomposables. Alors I est fini et l'homomorphisme canonique $u : A \longrightarrow \prod A_i$ est un isomorphisme." On pourrait aussi en faire une quatrième condition équivalente."

Remarque 1.10. — On voit facilement que si toute suite croissante d'idéaux bilatères de A est stationnaire, alors A satisfait aux conditions de la proposition 1.9. * Il en est en particulier ainsi si A est noethérien à gauche ou à droite. *

Remarque 1.11. — Si A satisfait aux conditions de 1.9, le cardinal de l'ensemble d'indices I, pour un isomorphisme donné de A avec le produit d'une famille finie $(A_i)_{i\in I}$ d'anneaux indécomposables, ne dépend que de A. C'est un entier $n \geq 0$, nul si et seulement si A est nul, égal à 1 si et seulement si A est indécomposable. On peut aussi le caractériser par la condition que le cardinal de l'ensemble des idempotents centraux de A est égal à 2^n. Noter que cet entier est le même pour A et pour le centre de A. * D'autre part, si A est commutatif, alors A satisfait aux conditions de 1.9 si et seulement si les composantes connexes de son spectre premier sont ouvertes, ou encore si leur ensemble est fini, et l'entier précédent n n'est alors autre que le cardinal de l'ensemble des composantes connexes de ce spectre. *

La proposition qui suit pourrait passer n'importe où après la définition des idéaux (mais de préférence dans le n° consacré aux anneaux produits) :

Proposition 1.12. — *Soit $(A_i)_{i\in I}$ une famille finie d'anneaux, A leur produit. Soit, pour tout anneau B, $J(B)$ l'ensemble des idéaux à gauche (resp....) de B.*

Définissons une application

$$\chi : \prod J(A_i) \longrightarrow J(A),$$

en associant à la famille $(J_i)_{i\in I}$ d'idéaux à gauche (resp. ..) des A_i, le produit $\prod J_i$, qui est bien un idéal à gauche (resp. ...) de A (que I soit fini ou non). Alors χ est bijective.

Corollaire 1.13. — *Les idéaux à gauche (resp....) maximaux de A sont les idéaux de la forme $pr_i^{-1}(J_i)$, où $i \in I$ et où J_i est un idéal à gauche (resp....) maximal de A_i, i et J_i étant d'ailleurs uniquement déterminés par l'idéal envisagé de A.*

Corollaire 1.14. — *Supposons que les A_i soient des corps. Alors tout idéal à gauche (resp. à droite) de A est bilatère. L'ensemble des idéaux de A est en correspondance biu-*

nivoque avec l'ensemble des parties de I, en associant à toute partie I' de I le noyau $J_{I'}$ de la projection canonique de $A = \prod_{i\in I} A_i$ sur le produit partiel $A_{I'} = \prod_{i\in I'} A_i$. Cette correspondance renverse les relations d'ordre, en particulier les idéaux maximaux de A correspondent aux éléments de I, comme noyaux des projections canoniques $pr_i : A \longrightarrow A_i$.

Plus généralement, il résulte de 1.13 que si chaque A_i admet exactement un idéal à gauche (resp....) maximal, alors l'ensemble des idéaux à gauche (resp....) maximaux de A est en correspondance biunivoque avec I.

Lemme 1.15. — *Soient A un groupe abélien, $(J_i)_{i\in I}$ une famille finie de sous-groupes de A, et pour tout $i \in I$, soit $A_i = A/J_i$. Pour que l'homomorphisme canonique*

$$u : A \longrightarrow \prod_{i\in I} A_i$$

soit surjectif, il faut et il suffit que pour tout $i \in I$, on ait :

$$J_i + \bigcap_{j\in I-\{i\}} J_j = A.$$

Démonstration. — L'assertion est triviale pour card I égal à 0 ou 1, et pour card $I = 2$ se vérifie en notant que de façon générale, si on a un homomorphisme de groupes abéliens $A \longrightarrow B$, et si B' est un sous-groupe de B, $B'' = B/B'$, alors $A \longrightarrow B$ est surjectif si et seulement si son composé avec $B \longrightarrow B''$ l'est, et si de plus l'homomorphisme induit $J'' \longrightarrow B'$ est surjectif, où J'' est le noyau de $A \longrightarrow B''$. On applique ceci au cas où $B = A/J' \times A/J''$ et où B' est le premier facteur A/J', donc $B'' \simeq A/J''$, on trouve que $A \longrightarrow A/J' \times A/J''$ est surjectif si et seulement si $J'' \longrightarrow A/J'$ l'est, i.e. si et seulement si $J' + J'' = A$. Dans le cas où card $I \geq 3$, on procède par récurrence sur ce cardinal. Choisissons un $i \in I$, et soit $K_i = \bigcap_{j\in I-\{i\}} J_j$, par hypothèse on a $J_i + K_i = A$ i.e. l'homomorphisme $A \longrightarrow A/J_i \times A/K_i$ est surjectif. Or K_i est précisément le noyau de l'homomorphisme $A \longrightarrow \prod_{j\in I-\{i\}} A_j$, qui se factorise donc par $A/K_i \longrightarrow \prod_{j\in I-\{i\}} A_j$, et on est ramené à prouver que ce dernier est surjectif. Or pour prouver que $A \longrightarrow \prod_{j\in I-\{i\}} A_j$ est surjectif, on utilise l'hypothèse de récurrence et les relations $J_j + K_j = A$ pour $j \in I - \{i\}$, qui donnent ce qu'on veut.

Définition 1.16. — *Soit A un anneau. Un idéal bilatère J de A est dit premier si pour deux idéaux bilatères quelconques I, I' de A, la relation $J \supset I \cdot I'$ implique $J \supset I$ ou $J \supset I'$.*

Alors, pour toute suite finie d'idéaux bilatères $I_1, \ldots, I_n$ de A, la relation $J \supset I_1 \cdot I_2 \cdot \cdots \cdot I_n$ implique l'existence d'un i, $1 \leq i \leq n$, tel que $J \supset I_i$. Cela se voit en effet aussitôt par récurrence sur n.

Proposition 1.17. — *Soit J un idéal bilatère de A. Pour que J soit premier, il suffit que A/J soit "sans diviseur de zéro" i.e. que le produit de deux éléments non nuls de A/J soit non nul. La condition est également nécessaire si A est commutatif.*

Pour la première assertion, notons que si J ne contient ni I ni I', il existe $x \in I$ et $x' \in I'$ qui ne soient pas dans J, donc si A/J est sans diviseur de zéro, on a $xx' \notin J$, donc $II' \not\subset J$. Pour la seconde assertion, il suffit de remarquer que si $x, x' \in A - J$ étaient tels que $xx' \in J$, alors les idéaux $I = Ax$ et $I' = Ax'$ seraient tels que I et I' soient non contenus dans J, et II' contenu dans J.

Proposition 1.18. ("Lemme Chinois" ?) — *Soient A un anneau commutatif, $(J_i)_{i\in I}$ une famille finie d'idéaux de A. Supposons que pour tout $i \in I$, il existe un seul idéal maximal J_i' de A contenant J_i, et supposons que les J_i' ($i \in I$) soient deux à deux distincts. Alors l'homomorphisme canonique $A \longrightarrow \prod_{i\in I} A_i$, où $A_i = A/J_i$, est surjectif, donc induit un isomorphisme $A/\bigcap_{i\in I} J_i \longrightarrow \prod_{i\in I} A_i$.*

En vertu de 1.15 il suffit de vérifier les relations

$$J_i + \bigcap_{j\in I-\{i\}} J_j = A.$$

En vertu du théorème de Krull (...), il suffit de prouver pour ceci qu'aucun idéal maximal $\mathfrak{m}$ de A ne peut contenir le premier membre, i.e. ne peut contenir à la fois J_i et $\bigcap_{j\in I-\{i\}} J_j$. Or s'il contient J_i, il est égal à J_i' par hypothèse, et s'il contient $\bigcap_{j\in I-\{i\}} J_j$, il résulte de 1.17 qu'il contient un des J_j, $j \in I - \{i\}$ donc par hypothèse est égal à J_j', ce qui contredit l'hypothèse $J_i' \neq J_j'$ pour $i \neq j$, C.Q.F.D.

Corollaire 1.19. — *Soit $(\mathfrak{m}_i)_{i\in I}$ une famille d'idéaux maximaux distincts de l'anneau commutatif A. Alors l'homomorphisme canonique*

$$A \longrightarrow \prod_{i\in I} k_i, \quad \text{où } k_i = A/\mathfrak{m}_i,$$

est surjectif.

Définition 1.20. — *Soit A un anneau commutatif. On dit que A est local s'il admet un unique idéal maximal (ce qui implique que $A \neq 0$). On dit que A est semi-local si l'ensemble de ses idéaux maximaux est fini (c'est le cas par exemple si A est nul).*

Par exemple, un corps commutatif est local.

Proposition 1.21. — *Soit A un anneau commutatif. Si A est local, A est indécomposable.*

Proposition 1.22. — *Soit A un produit fini d'anneaux commutatifs. Alors A est semi-local si et seulement si les A_i le sont. Il est local si et seulement si il existe $i \in I$ tel que A_i soit local et que $A_j = 0$ pour $j \in I - \{i\}$.*

Ces propositions résultent aussitôt des définitions et de 1.13.

Corollaire 1.23. — *Un produit fini de corps commutatifs est un anneau semi-local.*

Alors que tout ce qui précède semble le mieux à sa place dans le Chap. I, voici un résultat qui serait plutôt un remords au Chap. II, puisqu'il s'exprime le plus aisément dans le langage des modules. Il doit figurer sans doute (du moins sous une forme voisine) au Chap. VIII. Il va être utilisé dans le Chap. V, § 7 à propos des familles diagonalisables d'endomorphismes d'un vectoriel ; à la rigueur on pourrait l'y donner sous forme d'un lemme.

Proposition 1.24. — *Soient $(A_i)_{i\in I}$ une famille finie d'anneaux, A leur produit. Pour toute famille $(M_i)_{i\in I}$, où pour tout $i \in I$, M_i est un A_i-module, considérons sur $M = \prod_{i\in I} M_i$ la loi d'opération externe de A définie par*

$$(a_i)_{i\in I} \cdot (x_i)_{i\in I} = (a_i x_i)_{i\in I}.$$

Cette loi fait de M un A-module, c'est d'ailleurs la seule structure de A-module sur M pour laquelle, pour tout $i \in I$, la projection canonique $M \longrightarrow M_i$ soit semi-linéaire relativement à l'homomorphisme canonique $A \longrightarrow A_i$. Ceci posé, $(M_i)_{i\in I} \rightsquigarrow M = \prod_{i\in I} M_i$ peut être considéré comme un foncteur (murmure d'horreur) de la catégorie produit $\prod_{i\in I} \mathrm{Mod}(A_i)$ dans la catégorie $\mathrm{Mod}(A)$, — où pour tout anneau B, $\mathrm{Mod}(B)$ désigne la catégorie des B-modules. Eh bien, ce foncteur, c'est une équivalence de catégories.

Le rédacteur n'explicite pas, et pour cause, la définition du foncteur, ne sachant pas

plus que Bourbaki ce que Bourbaki entendra par ce terme. Il laisse au prochain rédacteur hypothétique une rédaction de cette proposition sans utiliser le mot de catégorie ni de foncteur.

J'ai oublié d'expliciter le foncteur quasi-inverse naturel : M_i se déduit de M par le changement de base $A \longrightarrow A_i$:

$$M_i \simeq M \otimes_A A_i.$$

Corollaire 1.25. — *Soit $(A_i)_{i\in I}$ une famille finie d'anneaux commutatifs, A leur produit. Pour toute famille $(M_i)_{i\in I}$, où pour tout $i \in I$, M_i est une A_i-algèbre, considérons chaque M_i comme une A algèbre à l'aide de la projection canonique $A \longrightarrow A_i$, et formons la A-algèbre produit $M = \prod_i M_i$. On obtient de cette façon un foncteur $(M_i)_{i\in I} \rightsquigarrow \prod_i M_i$ de la catégorie produit $\prod_i \mathrm{Alg}(A_i)$ dans la catégorie $\mathrm{Alg}(A)$, où pour tout anneau commutatif B, $\mathrm{Alg}(B)$ désigne la catégorie des algèbres sur B. Le foncteur précédent est une équivalence. De plus, avec les notations précédentes, pour que M soit associatif (resp. commutatif, resp. unitaire) il faut et il suffit que chacun des M_i le soit ; en particulier le foncteur précédent induit des équivalences entre les sous-catégories obtenues en se restreignant partout aux algèbres associatives (resp. commutatives, resp. unitaires, resp. associatives unitaires, resp. associatives unitaires commutatives, resp. transjordaniennes).*

2. — Éléments nilpotents, nilradical, anneaux réduits

Définition 2.1. — *Soit A un anneau. Un élément x de A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. Un idéal à gauche (resp. à droite, resp. bilatère) de A est dit un nilidéal à gauche (resp. à droite, resp. bilatère) si ses éléments sont tous nilpotents ; on dit que I est un idéal nilpotent s'il existe un entier $n \geq 1$ tel que $I^n = 0$, i.e. tel que pour toute suite $(x_1, \ldots, x_n)$ de n éléments de I, on ait $x_1 x_2 \ldots x_n = 0$. Si A est commutatif, on dit que A est réduit si tout élément nilpotent de A est nul.*

Bien entendu, si A est commutatif, on parlera simplement d'idéal nilpotent ou de nilidéal, sans spécifier par une mention comme "à gauche" etc. On notera qu'un idéal nilpotent est un nilidéal, l'inverse n'étant pas vrai en général. * C'est vrai cependant dans le cas particulier important où A est un anneau commutatif noethérien. *

Remarque 2.2. — Supposons A commutatif, et soit $x \in A$. Alors les conditions suivantes sont équivalentes :

(i) x est nilpotent,

(ii) Ax est nilpotent,

(iii) Ax est un nilidéal.

En effet, les implications (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) sont évidentes en tous cas, et (i) $\Rightarrow$ (ii) également pour A commutatif, puisqu'alors on a, pour tout entier $n \geq 1$, $(Ax)^n = Ax^n$, donc $x^n = 0$ implique $(Ax)^n = 0$.

Proposition 2.3. — *Soit A un anneau commutatif. L'ensemble J des éléments nilpotents de A est un idéal de A, distinct de A si $A \neq 0$. C'est le plus grand nilidéal de A, et aussi le plus petit idéal K de A tel que A/K soit réduit.*

Si $x \in J$, alors pour tout $a \in A$ on a $ax \in J$, car $x^n = 0$ implique $(ax)^n = a^n x^n = 0$. D'autre part, si $x \in J$, $y \in J$, alors $x + y \in J$, car si on a $x^n = y^n = 0$, alors la formule du binôme montre que $(x + y)^{2n} = 0$. Cela prouve que J est un idéal de A. Si $A \neq 0$, alors l'élément unité de A n'est pas nilpotent, donc $J \neq A$. Il est trivial que J est le plus grand nilidéal de A. Prouvons que A/J est réduit : en effet, si K est un idéal de A, on voit aussitôt que A/K est réduit si et seulement si pour tout $x \in A$ tel que $x^n \in K$ pour un entier $n \geq 1$ convenable, on a $x \in K$. Or cette condition est remplie pour $K = J$, car si $x^n \in J$, il existe un entier $m \geq 1$ tel que $(x^n)^m = 0$ i.e. $x^{nm} = 0$, donc $x \in J$. D'ailleurs, si K satisfait la condition envisagée plus haut, alors K contient évidemment tout élément nilpotent de A, i.e. $K \supset J$, ce qui achève la démonstration.

Définition 2.4. — *Soit A un anneau commutatif. L'idéal des éléments nilpotents de A (cf. 2.3) est appelé le nilradical de A.*

On notera que A est donc réduit si et seulement si son nilradical est nul.

Proposition 2.5. — *Soient A un anneau commutatif, J un nilidéal de A, $A_0 = A/J$, $u : A \longrightarrow A_0$ l'homomorphisme canonique. Alors u induit une bijection de l'ensemble des idempotents de A avec l'ensemble des idempotents de A_0.*

Compte tenu du n° 1, on en conclut aussitôt le

Corollaire 2.6. — *Pour que A soit indécomposable (resp. isomorphe à un produit fini d'anneaux indécomposables) il faut et il suffit qu'il en soit de même de A_0. Dans le cas respé, le nombre de facteurs indécomposables envisagé dans 1.11 est le même pour A et pour A_0.*

Corollaire 2.7. — *Soit I un ensemble fini, alors pour toute famille $(A_{0,i})_{i\in I}$ d'anneaux quotients de A_0 appartenant à $D(A_0, I)$ (1.1), il existe une famille unique d'anneaux quotients $(A_i)_{i\in I}$ de A qui soit élément de $D(A, I)$ et telle que pour tout $i \in I$, l'homomorphisme composé $A \longrightarrow A_0 \longrightarrow A_{0,i}$ se factorise par A_i. De plus, si $A_i = A/J_i$, on a $A_{0,i} = A_0/u(J_i) \simeq A/(J + J_i)$.*

N. B. — La démonstration de 2.6 est triviale quand on dispose du langage des schémas affines, impliquant que les idempotents de A correspondent aux parties à la fois ouvertes et fermées de Spec(A). Ici, nous donnons une démonstration directe, à l'aide du lemme 2.8 ci-dessous. Elle peut certainement se rédiger sans utiliser la notion de polynôme ni la formule de Taylor pour les polynômes, si on y tient (et pourrait donc passer au Chap. I).

Lemme 2.8. — *Soient A un anneau commutatif, J un nilidéal de A, $\varphi \in A[T]$ un polynôme, $\varphi(T) = a_0 + a_1T + \cdots + a_rT^r$. On suppose que $a_0 \in J$ et que a_1 est inversible. Alors il existe un unique élément x de J tel que $\varphi(x) = 0$.*

Par hypothèse, il existe un entier $n \geq 1$ tel que $a_0^n = 0$. Nous procédons par récurrence sur n, en notant que l'énoncé est trivial si $n = 1$, i.e. $a_0 = 0$, auquel cas on prend $x = 0$, solution qui est unique comme on voit en écrivant $\varphi(x) = 0$ sous la forme $x(a_1 + a_2x + \dots) = 0$ et en notant que si $x \in J$, alors le deuxième facteur $a_1 + a_2x + \cdots = a_1 + ux$ est inversible, car a_1 est inversible et ux nilpotent. Supposons donc $n \geq 2$, et le lemme prouvé pour des entiers $n' < n$. On met x sous la forme

$$x = -a_1^{-1}a_0 + z,$$

ce qui donne sur z les conditions $z \in I$ (équivalente à $x \in I$, puisque $a_0 \in I$), et $\varphi(-a_1^{-1}a_0 + z) = 0$. Développant par la formule de Taylor le premier membre, on trouve une équation de la forme $\psi(z) = 0$, où $\psi(T) \in A[T]$, $\psi(T) = b_0 + b_1T + \cdots + b_rT^r$, où $b_0 = \varphi(-a_1^{-1}a_0) \in a_0^2A$, et où $b_1 = \varphi'(-a_1^{-1}a_0)$ est de la forme $a_1 + ua_0$, donc est inversible puisque a_1 est inversible et a_0 donc ua_0 nilpotent. D'ailleurs, la forme

donnée de b_0 montre que $b_0^{n-1} = 0$, ce qui permet d'appliquer l'hypothèse de récurrence à ψ ; donc il existe un unique z satisfaisant aux conditions voulues, C.Q.F.D..

Nous pouvons maintenant prouver 2.5. Soit e_0 un idempotent de A_0, e un élément de A qui le relève. Alors, $e^2 - e \in J$. Tout revient à montrer qu'il existe un unique $x \in J$ tel que $e + x$ soit idempotent, i.e. tel que $(e + x)^2 - (e + x) = 0$, ce qui s'écrit aussi

$$x^2 + (2e - 1)x + (e^2 - e) = 0.$$

Compte tenu de 2.8, il suffit donc de prouver que $2e - 1$ est inversible, ou ce qui revient au même (cf. 2.10, ci-dessous) que $2e_0 - 1$ est inversible, ce qui résulte du

Lemme 2.9. — *Soit e un idempotent d'un anneau A. Alors $2e - 1$ est inversible, de façon précise, son carré est 1.*

En effet, on a $(2e - 1)^2 = 4e^2 - 4e + 1 = 1$ puisque $e^2 = e$.

Nous avons utilisé plusieurs fois, (pour démontrer 2.8 et 2.5) le résultat suivant, qui devrait donc passer avant 2.5 :

Proposition 2.10. — *Soient A un anneau, J un nilidéal bilatère de A, $A_0 = A/J$ l'anneau quotient. Alors pour tout élément x de A, x est inversible si et seulement si son image canonique dans A_0 l'est. En particulier, si x est inversible, il en est de même de $x + h$ pour tout $h \in J$.*

Supposons en effet x_0 inversible, d'inverse y_0, image canonique de y. On a donc $xy = 1 + a$, avec $a \in J$, et tout revient à prouver que $1 + a$ est inversible, car alors $y(1+a)^{-1}$ sera un inverse à droite de x, et on prouvera de même l'existence d'un inverse à gauche. Or pour trouver un inverse de $1 + a$, a étant nilpotent, on utilise la formule de Newton, qui donne l'inverse $\sum_{n\geq 0}(-1)^n a^n$.

Proposition 2.11. — *Soit $(A_i)_{i\in I}$ une famille finie d'anneaux commutatifs, A leur produit. Alors le nilradical de A est le produit des nilradicaux des A_i. L'anneau A est réduit si et seulement si les A_i le sont.*

Beweis klar. Remords : donner la dernière assertion de 2.11 pour le produit d'une famille pas nécessairement finie d'anneaux.

La proposition qui suit, pour venir sans larmes, suppose soit que l'anneau de frac-

tions soit défini au Chap. I sans se borner au passage aux fractions par rapport à une partie d'un anneau formée d'éléments réguliers ; soit qu'on dispose de la notion d'anneau de polynômes (ce qui la rejetterait après le Chap. IV) :

Proposition 2.12. — *Soit A un anneau commutatif. Alors le nilradical de A est l'intersection des idéaux premiers de A.*

En vertu de 2.3, il est contenu dans cette intersection, car si $\mathfrak{p}$ est un idéal premier de A, $A/\mathfrak{p}$ est intègre donc réduit, donc $\mathfrak{p}$ contient le nilradical. Pour l'inclusion en sens inverse, il faut prouver que si $f \in A$ n'est pas nilpotent, il existe un idéal premier $\mathfrak{p}$ de A ne contenant pas f. Pour ceci, on introduit l'anneau de fractions $B = A_f$ de A, qu'on peut définir aussi comme l'anneau quotient $B = A[T]/(1 - fT)$, T étant une indéterminée. On voit aisément que, pour un élément donné f de B, A_f est nul si et seulement si f est nilpotent (pourrait être dégagé en lemme). En l'occurrence, f étant supposé non nilpotent, donc A_f non nul, il existe par Krull un idéal maximal de A_f. Son image inverse dans A est un idéal premier ne contenant pas f. C.Q.F.D..

Proposition 2.13. — *Soient A un anneau commutatif, J un nilidéal de A, $A_0 = A/I$ l'anneau quotient, $\varphi : A \longrightarrow A_0$ l'application canonique. Alors l'application $\mathfrak{p} \rightsquigarrow \varphi^{-1}(\mathfrak{p})$ établit une correspondance biunivoque entre l'ensemble des idéaux premiers (resp. maximaux) de A_0, et l'ensemble des idéaux premiers (resp. maximaux) de A.*

C'est une conséquence immédiate de 2.3 qui implique qu'un idéal premier de A contient J. Pourrait être bloqué en corollaire à 2.3.

Proposition 2.14. — *Sous les conditions de 2.13, A est local (resp. semi-local) si et seulement si A_0 l'est.*

3. — Structures des anneaux artiniens commutatifs

Définition 3.1. — *Un anneau A est dit artinien à gauche (resp. à droite) lorsque toute suite décroissante d'idéaux à gauche (resp. à droite) de A est stationnaire.*

Lorsque A est commutatif, on dit simplement que A est artinien s'il est artinien à gauche (ou ce qui revient au même, à droite).

Proposition 3.2. — *Soit A un anneau commutatif artinien. Alors tout idéal premier*

de A est maximal, et l'ensemble de ces idéaux est fini (en d'autres termes, A est semi-local).

Soit $\mathfrak{p}$ un idéal premier de A, il faut prouver que $A/\mathfrak{p}$ est un corps. Comme $A/\mathfrak{p}$ est évidemment artinien, il suffit de prouver pour ce point le

Corollaire 3.3. — *Un anneau artinien à gauche non nul dont tout élément non nul est régulier à gauche (par exemple un anneau commutatif intègre artinien) est un corps.*

Il suffit de prouver que tout élément non nul f de A est inversible à droite, donc que l'application $g \rightsquigarrow fg$ de A dans lui-même est surjective. Or par hypothèse elle est injective, et si elle n'était pas surjective, les images des homomorphismes itérés, i.e. les idéaux à gauche $f^n A$, formeraient une suite strictement décroissante d'idéaux à gauche de A, contrairement à l'hypothèse artinienne sur A.

Pour prouver 3.2, il reste à prouver que l'ensemble des idéaux maximaux de A est fini. Mais si on pouvait trouver une suite infinie $(\mathfrak{m}_i)_{i\in\mathbb{N}}$ de tels idéaux, alors la suite des idéaux $N_i = \bigcap_{j\leq i} \mathfrak{m}_j$ serait strictement décroissante, comme il résulte aussitôt de 1.19, ce qui contredirait encore l'hypothèse artinienne sur A.

Corollaire 3.4. — *Soit A comme dans 3.2. Alors l'intersection de l'ensemble (fini) des idéaux maximaux de A est identique au nilradical de A, et ce dernier est nilpotent.*

Cela résulte de 3.2 et de 2.12 ; le caractère artinien de A impliquant qu'un nilidéal de A est nécessairement nilpotent.

Proposition 3.5. — *Soit A un anneau commutatif artinien.*

(i) Pour que A soit local, il faut et il suffit qu'il soit indécomposable, ou encore qu'il admette un idéal maximal nilpotent.

(ii) A est isomorphe au produit d'une famille finie d'anneaux artiniens locaux, et ceci de façon essentiellement unique.

Si N est le nilradical de A, alors il résulte de 3.4 et 1.19 que A/N est isomorphe à un produit fini de corps $k_i, i \in I$. Cette décomposition se remonte en une décomposition de A en vertu de 2.7, chaque facteur A_i de A dans cette décomposition ayant un idéal $\mathfrak{n}_i$ nilpotent tel que $A/\mathfrak{n}_i$ soit isomorphe au corps k_i. En vertu de 2.14, chaque A_i est local,

et a fortiori indécomposable. La propriété d'unicité d'une décomposition de A en produit fini d'anneaux indécomposables a été explicitée dans 1.9, ce qui prouve (ii). On voit de plus, sur cette décomposition, que A est indécomposable si et seulement si l'ensemble d'indices I est réduit à un élément, i.e. A est local, et ceci implique que A admet un idéal maximal nilpotent ; l'inverse a déjà été observé plus haut comme conséquence de 2.14. Cela achève la démonstration de 3.5.

Corollaire 3.6. — *Soit A un anneau commutatif artinien. Pour que A soit réduit, il faut et il suffit qu'il soit isomorphe à un produit fini de corps (et ces derniers sont déterminés alors de façon essentiellement unique).*

Résulte de 3.5 et de 2.11.

Corollaire 3.7. — *Soit A un anneau commutatif artinien. Pour que A soit un corps, il faut et il suffit que A soit local et réduit.*

N. B. — On aurait dû après 3.1 noter qu'un quotient d'un artinien, ou un produit d'une famille finie d'artiniens, est artinien, ce qui montre en particulier, grâce à 3.5 (ii), que la classification des anneaux commutatifs artiniens se ramène entièrement à celle des anneaux commutatifs artiniens *locaux*.

4. — Existence et unicité de la décomposition d'un polynôme à une indéterminée sur un corps en produit de puissances de polynômes irréductibles

Peut se traiter en une proposition, à la place de la proposition 8 du Chap. IV, n° 5. Inutile d'attendre le Chapitre des anneaux principaux pour donner cette propriété, qu'il serait absurde de se refuser à utiliser dans le Chapitre des corps commutatifs, en cas de besoin. Nous l'appliquerons dans 5.8 à la structure des algèbres commutatives de degré fini sur un corps, qui pourrait être donnée dans un n° à part, faisant suite au précédent, dans le Chap. IV, ou bien former le §7, du Chap. V, après le §6 de l'état publié actuel.

5. — Algèbres de degré fini sur un corps k

Définition 5.1. — *Soient k un corps, A une k-algèbre. On appelle* ***degré de*** *A* ***sur*** *k, ou simplement degré de A, et on note $[A : k]$, la dimension du k-espace vectoriel sous-jacent à A.*

Remarque 5.2. — On s'abstiendra par contre, pour une k-algèbre, d'utiliser le terme "dimension de A" pour désigner son degré sur k, à cause des confusions possibles avec la notion de dimension d'un anneau, qui sera étudiée en Alg. Comm.. Cet inconvénient ne se présente pas quand on utilise le synonyme "rang d'un espace vectoriel" pour désigner sa dimension, et on pourra alors utiliser le terme "rang de la k-algèbre A" comme synonyme de "degré de la k-algèbre A".

On dira donc que A est de degré fini sur k (ou de rang fini sur k, — mais non "de dimension finie sur k" ! —) si son degré sur k est fini. Dans le cas contraire, ce degré est égal à $+\infty$ (N. B. — à vérifier si cela ne contredit pas la notion de dimension d'un vectoriel, qui serait un cardinal — le rédacteur ne dispose pas, au moment de rédiger, des textes canoniques. En tous cas, la convention utile ici est bien de prendre $+\infty$ et non le cardinal d'une base).

Proposition 5.3. — *Soit A une algèbre sur un corps k. Si A est de degré fini sur k, A est artinienne à gauche et même à droite.*

On pourrait même se borner à supposer k artinien au lieu d'un corps.

Grâce à 5.3, nous pouvons donc appliquer tous les résultats du n°3 à la structure des algèbres commutatives de degré fini sur un corps k ! Noter que si $\mathfrak{m}_i$ ($i \in I$) sont les idéaux maximaux de A (en nombre fini, rappelons le), et $k_i = A/\mathfrak{m}_i$ les corps correspondants (appelés aussi *corps résiduels* en les $\mathfrak{m}_i$, terminologie qui aurait pu être introduite dès la notion d'idéal maximal), alors les k_i sont des corps qui sont des k-algèbres, i.e. sont des *extensions* de k, qu'on appellera aussi les *extensions résiduelles* de A. Noter qu'on aura évidemment $\sum [k_i : k] \leq [A : k] = n$ (égalité si et seulement si A est réduite) et a fortiori card $I \leq n$ (égalité si et seulement si A est isomorphe à k^n).

Proposition 5.4. — *Soient k un corps, A une algèbre commutative sur k, de degré fini n, K une extension de k, k_i ($i \in I$) les extensions résiduelles de A, $\varphi_i : A \longrightarrow k_i$ les homomorphismes canoniques. Alors tout k-homomorphisme u de A dans K peut s'écrire, de*

façon unique, sous la forme $v \circ \varphi_i$, où $i \in I$ et où $v : k_i \longrightarrow K$ est un k-homomorphisme.

Il suffit de noter que le noyau de u est un idéal premier de A, donc maximal (3.2), d'où aussitôt l'assertion.

Corollaire 5.5. — *Les k-homomorphismes de A dans K sont linéairement indépendants dans le K-espace vectoriel des homomorphismes des k-espaces vectoriels sous-jacents à A et à K. En particulier, il y a au plus n k-homomorphismes de A dans K.*

En effet, quitte à faire l'extension de la base $k \longrightarrow K$, on se ramène au cas où $K = k$, et où l'assertion est immédiate, compte tenu que A s'envoie sur le produit des k_i.

N. B. 5.6. — On retrouve ici par la bande, dans un cas particulier, le théorème de Dedekind de l'indépendance des homomorphismes, qui pourrait s'énoncer ainsi : si S est un monoïde, K un corps, l'ensemble des représentations de S dans K^* est libre dans l'espace vectoriel sur K des applications de S dans K. On peut prouver cet énoncé assez naturellement dans l'esprit des présentes notes, en introduisant l'algèbre A de S sur K, ce qui nous ramène à prouver que, pour une K-algèbre A, l'ensemble des homomorphismes de A dans K est libre dans le dual de l'espace vectoriel sous-jacent à A. On se ramène aussitôt au cas K commutatif (diviser par l'idéal des commutateurs), et alors le lemme chinois 1.19 donne aisément le résultat.

Proposition 5.7. — *Soient A une algèbre commutative de degré fini n sur un corps k, Ω une extension algébriquement close de k, $P(A)$ l'ensemble des k-homomorphismes de A dans Ω. Alors l'application $u \mapsto \mathrm{Ker}(u)$ induit une bijection de $P(A)$ avec l'ensemble des idéaux maximaux $\mathfrak{m}$ de A tels que l'extension résiduelle correspondante $A/\mathfrak{m}$ de k soit triviale. De plus, les conditions suivantes sont équivalentes :*

(i) *A est isomorphe à l'algèbre k^n.*

(ii) *A est réduit, et pour tout k-homomorphisme $u : A \longrightarrow \Omega$, on a $u(A) = k$.*

(ii bis) *A est réduit et ses extensions résiduelles sont triviales.*

(iii) *On a $\mathrm{card}(P(A)) = n$.*

(iv) *A a n idéaux maximaux.*

La première assertion est triviale (et indépendante de l'hypothèse $[A : k] < +\infty$), ainsi que l'équivalence de (ii) et (ii bis), compte tenu de 5.4. L'équivalence de (i) et (ii bis) est immédiate, compte tenu que A réduit implique que A est isomorphe au produit de ses extensions résiduelles. D'ailleurs, (i) $\Rightarrow$ (iii) est trivial par 5.4, et on a (iii) $\implies$ (i), car on a un homomorphisme *surjectif* canonique $A \longrightarrow k^{P(A)}$, et (iii) assure que les deux côtés de la flèche ont même degré sur k, donc l'homomorphisme est un isomorphisme. L'équivalence de (i) et (iv) a déjà été observée plus haut.

Proposition 5.8. — *Soient k un corps, $f \in k[X]$ un polynôme en une indéterminée X, on suppose f non constant et on considère sa décomposition en facteurs premiers*

$$f = cf_1^{r_1} \dots f_s^{r_s},$$

où les f_i ($1 \leq i \leq s$) sont des polynômes unitaires irréductibles, et les r_i sont des entiers > 0. Alors la k-algèbre

$$A = k[X]/fk[X]$$

est finie sur k, de rang égal à $n = \deg f$, et elle est isomorphe au produit des algèbres $A_i = k[X]/f_i^{r_i}k[X]$, ces dernières étant des algèbres locales, dont les extensions résiduelles sont isomorphes aux extensions $k[X]/f_ik[X]$.

Preuve par AQT.

Corollaire 5.9. — *Pour que A soit locale, il faut et il suffit que $s = 1$. Pour que A soit réduite, il faut et suffit que f soit sans facteurs multiples, i.e. que $r_i = 1$ pour $1 \leq i \leq s$. Pour que A soit un corps, il faut et il suffit que f soit irréductible.*

6. — Ensembles à groupes d'opérateurs induits

Soient G un groupe, H un sous-groupe, M un ensemble sur lequel H opère (à gauche). Désignant, pour deux ensembles E, F sur lesquels H opère, par $\mathrm{Hom}_H(E, F)$ l'ensemble des applications de E dans F compatibles avec l'action de H, et munissant G de la structure d'ensemble à groupe d'opérateurs H, grâce aux translations à gauche par les éléments de H, on définit l'ensemble $\mathrm{Hom}_H(G, M)$. Utilisant le fait que la translation à droite par un élément $g \in G$ commute aux opérations de H sur G, on met sur $\mathrm{Hom}_H(G, M)$ une structure naturelle d'ensemble à groupe d'opérateurs G, en posant

donc

$$(g.\varphi)(x) = \varphi(xg), \quad g, x \in G, \varphi \in \mathrm{Hom}_H(G, M);$$

on appelle parfois $\mathrm{Hom}_H(G, M)$ l'ensemble à opérateurs déduit de l'ensemble M à groupe d'opérateurs H par extension contravariante du groupe d'opérateurs H à G. Pour tout ensemble P à groupe d'opérateurs G, on a une bijection canonique, fonctorielle en tous les arguments :

$$(*) \qquad \mathrm{Hom}_G(P, \mathrm{Hom}_H(G, M)) \longrightarrow \mathrm{Hom}_H(P, M),$$

où dans le deuxième membre, on considère P comme muni du groupe d'opérateurs H, par restriction des scalaires : ainsi, le foncteur extension du groupe d'opérateurs apparaît comme l'adjoint à droite du foncteur restriction du groupe d'opérateurs — particularité que Bourbaki sera le seul à lui reprocher. Lorsque M est un groupe (resp. un groupe abélien, resp. un anneau, resp. un n'importe quoi), on voit aussitôt qu'il en est de même de $\mathrm{Hom}_H(E, M)$, quel que soit l'ensemble E à groupe d'opérateurs H, et cette structure est stable par les automorphismes induits par les H-automorphismes de E ; en particulier, G opère par automorphismes sur $\mathrm{Hom}_H(G, M)$.

Partons maintenant d'un ensemble P à groupe d'opérateurs G, et soit M un ensemble quotient de P. Soit H le sous-groupe de G formé des $g \in G$ qui laissent ce quotient invariant (i.e. qui laissent invariante la relation d'équivalence correspondante). L'application canonique $P \longrightarrow M$ est donc un H-homomorphisme, et l'isomorphisme (*) lui associe un homomorphisme

$$(**) \qquad P \longrightarrow \mathrm{Hom}_H(G, M).$$

Lorsque ce dernier est un isomorphisme, on dira que l'ensemble P à groupe d'opérateurs G est *induit* par son quotient M. Lorsque P est un groupe (resp. anneau) à groupe d'opérateurs, et que M est un groupe (resp. anneau) quotient $M = P/R$, alors H est aussi le sous-groupe de G des éléments qui laissent invariants R, et l'homomorphisme ou isomorphisme précédent respecte les structures de groupe (resp. anneau).

Supposons qu'on ait un ensemble $(M_i)_{i \in I}$ de quotients de P, et que l'homomorphisme canonique $P \longrightarrow \prod M_i$ soit un isomorphisme. Supposons de plus que l'ensemble de quotients envisagé soit stable par G, de sorte que G opère sur I. Choisissons un $i_0 \in I$, alors le stabilisateur H de $M = M_{i_0}$ est par définition le

stabilisateur H de i_0 dans G. L'application (**) ci-dessus s'identifie alors à la projection canonique du produit $\prod M_i$ sur le produit partiel $\prod_{i \in Gi_0} M_i$. Par suite, pour que P soit induit par son quotient $M = M_{i_0}$, il suffit que G opère transitivement sur I, et cette condition est d'ailleurs également nécessaire comme on voit facilement (en traitant séparément les cas où M aurait 0, ou 1, éléments). Dans le cas général, il y a lieu d'introduire l'ensemble J des orbites I_j de G dans I, et de regarder la décomposition de P en produit partiel $P \simeq \prod_{j \in J} P_j$, où pour tout $j \in J$, on pose $P_j = \prod_{i \in I_j} M_i$. Alors G opère sur P via ses opérations sur les facteurs P_j ; et chacun des ensembles (resp. groupes...) P_j à groupe d'opérateurs G est justiciable du cas favorable, i.e. se représente comme induit par n'importe lequel de ses quotients $M_i (i \in I_j)$. En résumé, pour un groupe donné G et un ensemble (resp. groupe...) P donné comme produit d'un ensemble de quotients $(M_i)_{i \in I}$, on peut expliciter complètement les manières de faire opérer G sur P, laissant stable l'ensemble I envisagé, en termes des opérations des sous-groupes H de G sur des facteurs M_i.

Prenons par exemple le cas où P est un anneau A satisfaisant aux conditions 1.19, donc qui s'écrit comme produit fini de quotients indécomposables $A = \prod_i A_i$. L'ensemble de ces quotients est manifestement stable par tout automorphisme de A, donc les réflexions précédentes sont applicables. En particulier, si un groupe G opère sur A de façon à opérer transitivement sur A_i, on reconstitue l'anneau A à groupe d'opérateurs G à partir de l'anneau A_{i_0} à groupe d'opérateurs H (stabilisateur de i_0 dans G) comme l'anneau induit $\mathrm{Hom}_H(G, A_{i_0})$.