RÉDACTION N° 126

COTE : NBR 033

TITRE : COMMENTAIRES CHEVALLEY SUR LA RÉDACTION WEIL DE LA DIVISIBILITÉ

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 19

NOMBRE DE FEUILLES : 19

COMMUNICABLE ULTÉRIEUREMENT

Archives Mars 1942

COMMENTAIRES CHEVALLEY SUR LA

REDACTION WEIL DE LA DIVISIBILITE .

I. Anneaux de spécialisation .

Weil définit l'anneau de spécialisation d'un idéal premier d'un domaine d'intégrité A . La notion suivante , un peu plus générale , est très fréquemment utile . Soit A un domaine d'intégrité , et soit E une partie de A , ne contenant pas 0 et stable pour la multiplication . Les éléments de la forme $e^{-1}x$, $e \in E$, $x \in A$, forment alors un sous-anneau A_E du corps des fractions de A (vérification triviale) qu'on peut appeler l'anneau des fractions de E (par rapport à A) . Cette notion intervient d'ailleurs plusieurs fois dans la rédaction Weil . On retrouve la notion d'anneau de spécialisation d'un idéal premier $\mathfrak{p}$ dans le cas où E est le complémentaire de $\mathfrak{p}$. Les propriétés dont on se sert sont les suivantes :

I . Si $y_1, \ldots, y_n$ sont dans A_E , il y a un $e \in E$ tel que $ey_i \in A$ $(1 \leq i \leq n)$.

II . Si $\mathfrak{a}$ est un idéal de A_E , $\mathfrak{a}$ est l'idéal engendré par $\mathfrak{a} \cap A$ dans A_E ; inversement , si $\mathfrak{p}$ est un idéal premier de A qui ne rencontre pas E , $\mathfrak{p}$ est l'intersection avec A de l'idéal $\mathfrak{P}$ engendré par $\mathfrak{p}$ dans A_E , lequel idéal est premier . De plus , $A_E/\mathfrak{P}$ est contenu dans le corps des fractionsde $A/\mathfrak{p}$.

III . Les notations étant celles de II , l'anneau de spécialisation de l'idéal $\mathfrak{P}$ de A_E est le même que celui de l'idéal $\mathfrak{p}$ de A , et $A_E/\mathfrak{P}$ est l'anneau des fractions de l'image de E par l'homomorphisme canonique de A sur $A/\mathfrak{p}$.

Les démonstrations de ces propriétés sont triviales .

Pratiquement , on utilise la notion décrite plus haut quand on veut étudier le comportement d'un idéal premier $\mathfrak{p}$ de A relativement à un sur-anneau B de A ; il est alors souvent commode de former l'anneau des fractions (par rapport à B) du complément de $\mathfrak{p}$ par rapport à A (c'est-à-dire aussi l'anneau engendré par B et par l'anneau de spécialisation de $\mathfrak{p}$ relativement à A) . L'une des raisons pour lesquelles les anneaux de fractions sont très commodes est la propriété suivante : si E est une partie multiplicativement stable d'un anneau A intégralement clos dans son corps des fractions , A_E est encore intégralement clos (vérification triviale - à faire quand on parle de la notion d'éléments entiers).

Remarque terminologique : Au lieu de dire anneau de spécialisation , on pourrait dire anneau local , moins lourd ; de plus , quand on dit anneau de spécialisation , on est toujours un peu gêné en se demandant s'il s'agit d'une spécialisation déjà considérée , ou si "de spécialisation" doit seulement être considéré comme un attribut de "anneau" . A vrai dire , on entend en général par anneau local un anneau qui est moins général que les anneaux de spécialisation en ce qu'on le suppose noethérien , mais plus général en ceci qu'on lui permet des diviseurs de O (et il est tout à fait essentiel qu'un anneau local puisse en avoir à cause des complétions). La condition supplémentaire de "noetherien" n'a pas grande importance ; dans les chapitres où elle interviendra , elle interviendra toujours , de sorte qu'elle pourra être couverte par une déclaration d'intention en tête du chapitre . Quant aux diviseurs de O , rien n'empêche de donner ici une définition générale les permettant et qui s'appliquera en particulier aux domaines d'intégrité locaux que l'on considère dans ce chapitre .

II . Notions relatives aux éléments entiers .

Un certain nombre de résultats très importants sur les éléments entiers se démontrent exactement avec les moyens qui sont introduits dans ce chapitre , et y devraient à mon avis figurer ; car on les utilise pratiquement toutes les fois qu'on considère des éléments entiers . Il s'agit des résultats suivants , ~~XXX~~ dans lesquels A représente un sous-anneau d'un corps K (avec $1 \in A$) , K étant le corps des fractions de A , et B un sous-anneau d'un surcorps L de K , contenant A et entier sur A .

I . Si E est une partie multiplicativement stable de A ne contenant pas O , l'anneau des fractions B_E de E par rapport à B est entier sur l'anneau A : trivial .

II . Si $\mathfrak{p}$ est un idéal premier de A , il existe un idéal premier $\mathfrak{P}$ de B tel que ~~XXXEXX~~ $\mathfrak{P} \cap A = \mathfrak{p}$. On prend une valuation v de L dont l'anneau contient A et dont l'idéal intersecte A suivant $\mathfrak{p}$; on prend pour $\mathfrak{P}$ l'intersection de l'idéal de v avec B .

Cela signifie que toute spécialisation de A se prolonge par une spécialisation de B .

III . Si $\mathfrak{P}$ et $\mathfrak{Q}$ sont des idéaux premiers différents de B tels que $\mathfrak{Q} \subset \mathfrak{P}$, on a $\mathfrak{Q} \cap A \neq \mathfrak{P} \cap A$. Posons $\mathfrak{Q} \cap A = \mathfrak{q}$; $B/\mathfrak{Q}$ contient $A/\mathfrak{q}$ et est entier sur lui . Tout revient donc à démontrer l'assertion dans le cas où $\mathfrak{Q} = \{0\}$. Soit $x \neq 0$ dan $\mathfrak{P}$; on a une relation de la forme $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, $a_i \in A$, et on peut supposer $a_n \neq 0$, puisqu'il n'y a pas de diviseurs de 0 dans B ; on a alors $a_n \in \mathfrak{P} \cap A$

Il résulte de là que si la contraction à A d'un idéal premier $\mathfrak{P}$ de B est maximale (resp. minimale) dans A , $\mathfrak{P}$ est maximal (resp. minimal) dans B .

IV . Soient $\mathfrak{p}$ et $\mathfrak{q}$ des idéaux premiers de A tels que $\mathfrak{q} \subset \mathfrak{p}$ et $\mathfrak{Q}$ un idéal premier de B tel que $\mathfrak{Q} \cap A = \mathfrak{q}$. Il y a alors un idéal premier $\mathfrak{P}$ de B tel que $\mathfrak{P} \supset \mathfrak{Q}$, $\mathfrak{P} \cap A = \mathfrak{p}$. Se déduit tout de suite de II en considérant $A/\mathfrak{q}$ et $B/\mathfrak{Q}$.

V . Supposons A intégralement clos dans K . Si $x \in B$, le polynome minimal $F(X)$ de x par rapport à K a ses coefficients dans A .

Il existe un polynome unitaire $G(X)$ à coefficients dans A tel que $G(x) = 0$,d'où $G = FH$, ~~XXXXXXX~~ $H \in K[X]$. Soit v une valuation de K dont l'anneau contient A ; soient V l'anneau de v et $\mathfrak{m}$ son idéal . Il existe a et b dans K tels que aF et bH aient leurs coefficients dans V et que chacun de ces polynomes ait au moins un coefficient non dans $\mathfrak{m}$; si F^* et H^* sont les polynomes déduits de aF et bH par réduction des coefficients modulo $\mathfrak{m}$, on a $F^* \neq 0$, $H^* \neq 0$,d'où $F^* H^* \neq 0$ ce qui montre que tous les coefficients de abG ne sont pas dans $\mathfrak{m}$,donc que $a \notin \mathfrak{m}$ et par suite que les coefficients de F sont dans V . Ceci étant vrai pour toute valuation dont l'anneau contient A , les coefficients de F sont dans A .

VI . Supposons A intégralement clos dans K , et soient $\mathfrak{p}$ et $\mathfrak{q}$ des idéaux premiers de A tels qu' $\mathfrak{q}\subset\mathfrak{p}$; soit $\mathfrak{P}$ premier dans B tel que $\mathfrak{P}\cap A=\mathfrak{p}$; il existe alors un idéal premier $\mathfrak{Q}\subset\mathfrak{P}$ de B tel que $\mathfrak{Q}\cap A=\mathfrak{q}$. Soit E l'ensemble des éléments de la forme ab de B , où $a\in A$, $a\notin\mathfrak{q}$, $b\in B$, $b\notin\mathfrak{P}$. On va montrer que l'idéal $\mathfrak{q}B$ engendré par $\mathfrak{q}$ dans B ne rencontre pas E . Soit $x\in\mathfrak{q}B$, et soit $F(X)=X^n+q_1X^{n-1}+\dots+q_n$ le polynome minimal de x par rapport à K ; les q_i sont dans A; on va montrer qu'ils sont dans $\mathfrak{q}$. Il y a une valuation v de K telle que l'intersection de son idéal $\mathfrak{m}$ avec A soit $\mathfrak{q}$. Ecrivons $x=\sum_i x_iy_i$, avec $x_i\in\mathfrak{q}$, $y_i\in B$; on a $v(x_i)>0$, et on peut supposer que $v(x_1)=\min(v(x_i))$. On a alors $x=x_1v$ où v est entier sur l'anneau de v . Ce dernier anneau étant intégralement clos , les coefficients du polynome minimal de y , qui est $X^n+x_1^{-1}q_1X^{n-1}+\dots+x_1^{-n}q_n$ sont dans l'anneau de v , d'où il résulte que les q_i sont dans $\mathfrak{m}\cap A=\mathfrak{q}$.
Montrons qu'on ne peut avoir $x=ab$, où a et b satisfont aux conditions énoncées plus haut . Le polynome minimal de b serait alors $X^n+a^{-1}q_1X^{n-1}+\dots+a^{-n}q_n$; ses coefficients seraient dans A , et par suite , puisque $a\notin\mathfrak{q}$, dans $\mathfrak{q}$. Il en résulterait que $b^n\in\mathfrak{q}B\subset\mathfrak{P}$, d'où $b\in\mathfrak{P}$ ce qui n'est pas . Ceci dit , soit A_E l'anneau des fractions de E ; l'idéal $\mathfrak{q}A_E$ ne contient pas 1 , et est par suite contenu dans un idéal premier $\mathfrak{Q}'$ de A_E . L'idéal $\mathfrak{Q}'\cap B=\mathfrak{Q}$ est premier (à propos , il faudrait dire quelque part cette trivialité que l'intersection avec un sous-anneau d'un idéal premier d'un anneau est un idéal premier du sous-anneau) ; il contient $\mathfrak{q}$, mais il ne rencontre pas E , d'où il résulte que $\mathfrak{Q}\cap A=\mathfrak{q}$; également parce qu'il ne rencontre pas E , il est contenu dans $\mathfrak{P}$.

Il convient naturellement de donner en exerc. un contre-exemple pour le cas où A n'est pas intégralement clos .

Géométriquement , VI signifie que , si on projette une variété V sur une variété <u>normale</u> de même dimension , et si un point P se projette en P' , alors toute variété passant par P' est projection d'une variété passant par P ; c'est l'une des propriétés importantes des variétés normales .

<u>3 . Valuation: et ordinations</u> :

J'ai des doutes très sérieux sur l'avantage qu'il y a à considérer les valuations comme des spécialisations maximales ; et ceci pour la raison suivante . Supposons qu'on ait une spécialisation f d'un anneau A dans un corps L . On peut bien prolonger f par une spécialisation maximale g du corps des fractions K de A : mais on n'a pratiquement aucun contrôle sur le corps M qui va être engendré par les éléments finis de g(K) . On peut , il est vrai , s'arranger pour que M soit algébrique sur L (encore que je n'aie jamais vu de cas où l'importance de cette condition soit évidente) ; mais , même alors , et même pour de "bons" anneaux A (anneaux de variétés algébriques) le corps M peut parfaitement être de degré infini sur L et n'a qu'un rapport à peu près inexistant avec la nature de la spécialisation dont on est parti . Mon expérience est que les valuations (qui ne sont apr`s tout que des outils techniques d'usage momentané au cours des démonstrations) fonctionnent toujours comme ordinations (au sens de Weil). Cette irpression s'est confirmée récemment dans l'étude que j'ai faite des travaux de Zariski sur les transformations birationnelles , étude qui m'a conduit d'ailleurs à une nouvelle définition des variétés (un peu dans l'esprit des Variétés de Weil , mais sans utiliser jamais de coordonnées et par suite sans avoir à passer d'abord par les variétés avec un "v" ; but this is another story.)

Je propose donc de continuer à utiliser valuation au sens de Zariski (et d'autres d'ailleurs) ; on pourrait à vrai dire au besoin les noter multiplicativement , pour accentuer l'analogie avec les "normes" dans les anneaux . En tout état de cause , je m'oppose avec énergie au mot "ordination" : tout le monde sait ce que c'est qu'un corps ordonné , et il n'y a vraiment pas lieu de brouiller les idées des gens~~é~~ sur ce point . Si on veut un mot , on pourrait utiliser "résiduation" pour les valuations de Weil , et appeler résidu de x pour v ce que Weil appelle v(x) .

Quoi qu'il en soit , on pourrait indiquer les notions suivantes . On peut dire qu'une valuation v' est plus fine qu'une valuation v si l'anneau de v' est contenu dans celui de v ; v' donne alors lieu à une valuation v* du corps des résidus de v (j'appelle ainsi ~~xxx~~ le quotient de l'anneau de v par son idéal) , et on a une correspondance biunivoque entre les valuations du corps des résidus de v et les valuations plus fines que v . Si on a une famille totalement ordonnée par inclusion d'anneaux de valuation d'un corps K , l'intersection de ces anneaux est encore un anneau de valuation de K . Ceci dit , soit A un anneau de spécialisation et $\mathfrak{p}$ son idéal premier . Il y a alors (par Zorn) une valuation v dont l'anneau contient A , dont l'idéal contient $\mathfrak{p}$ et telle qu'il n'y ait pas de valuation plus fine avec les mêmes propriétés . Le corps des résidus de cette valuation est alors algébrique~~xxxx~~ sur $A/\mathfrak{p}$, comme on le voit en observant que si un corps M est transcendant sur un corps L , il n'y a qu'une valuation non triviale de M qui est triviale sur L .

Incidemment , Zariski utilise une ou deux fois le fait que , si les x_i sont des éléments de M (surcorps de L) algébriquement indépendants sur L , toute valuation w de ~~xxxxxxx~~ L peut se prolonger par une valuation w de M telle que les résidus des x_i pour w soient algébriquement indépendants sur le corps des résidus de v ; cela n'est pas bien important , mais ne coûte pas cher .

<u>4 . Groupes ordonnés</u> . Tout ce qu'on tire des groupes ordonnés pour l'arithmétique est exactement ce qui ne fait pas intervenir la structure additive : c'est maigre . Mais , si on veut les garder , voici une proposition transactionnelle. En ce qui concerne les groupes multiplicatifs , on considérerait partout des groupes préordonnés et on y introduirait <u>directement</u> la terminologie arithmétique (divisibilité , p.g.c.d., p.p.c.m., éléments premiers). De cette manière ,on

NSR 053

n'aurait pas à répéter tous les énoncés dans un autre langage , ce que je trouve intolérablement agaçant . De plus , les résultats énoncés s'appliqueraient directement à l'arithmétique dans les groupes , que certains généralisateurs à tout prix aiment à considérer .

5 . Remarques diverses .

La prop.2, § 2,n°3 , doit venir avec la notion d'entier ; elle exprime qu'un anneau factoriel est intégralement clos .

P.27 : les 4 lignes du haut sont trop elliptiques .

P.27 . Ne serait-il pas approprié d'avoir la notion d'anneau muni d'un algorithme d'Euclide ; le problème de l'existence d'algorithmes d'Euclide dans les corps imaginaires quadratiques est après tout - à tort ou à raison - un problème célèbre . La prop.12,p.32 devrait se démontrer pour de tels anneaux : pourquoi se priver de la prop.correspondante pour les entiers , qui est utile à l'occasion?

P.34 . Lemme de Gauss . On peut probablement s'en passer . En tout état de cause , le lemme suivant est plus important . Soit $\mathfrak{p}$ idéal premier d'un anneau A absolument quelconque , et soient F et G polynomes à coefficients dans A tels que les coefficients de FG soient dans $\mathfrak{p}$; alors les coefficients de l'un des polynomes F ou G sont dans $\mathfrak{p}$ (trivial par passage aux quotients suivant $\mathfrak{p}$) . Le lemme de Gauss se déduit d'ailleurs de là sans difficulté .

P.51 . Mon expérience est qu'il est commode d'imposer qu'un idéal premier ne contienne pas 1 ; c'est d'ailleurs nécessaire pour avoir l'équivalence avec les spécialisations telles que les définit Weil .

Exercice de la p.77 : si A B , les éléments de B entiers sur A forment un anneau . Quand on a les anneaux noetheriens , on peut donner de cela une démonstration plus élégante . Si x et y sont entiers sur A , ils sont entiers sur un sous-anneau A_1 de A engendré par un nombre fini d'éléments , donc noetherien .On en déduit tout de suite que $A_1[x,y]$ est module fini sur A_1 , donc aussi $A_1[x+y]$

et $A_1[xy]$; d'où le résultat .

A propos des anneaux de Dedekind , Weil semble tout heureux d'avoir remplacé le "fourbi noetherien" (que je trouve quant à moi fort joli) par un "fourbi kroneckérien" (que je trouve absolument affreux). Par ailleurs , cela l'oblige à passer à une extension normale (ce qui est une des nombreuses inélégances de la démonstration) et à avoir à se livres en exercice à des contorsions nouvelles pour couvrir le cas où l'anneau de base est lui-même de Dedekind ; je veux bien que ce ne soit pas particulièrement important en pratique . Mais ce n'est pas joli ; et qui saurait garantir que des anneaux de Dedekind non obtenus par le th.2 ne se présentent pas un de ces jours ? D'ailleurs , conformément aux papiers que j'ai donnés à Bourbaki , j'estime que cela doit se faire au moyen des anneaux normaux .

Question des anneaux noetheriens .

Il me parait de plus en plus saugrenu de faire 8 pages de généralités sur les noetheriens sans en arriver aux théorèmes essentiels . Je comprendrais qu'on en agisse ainsi si les dits théorèmes demandaient une somme d'efforts considérables ; mais il n'en est rien . Pour le montrer , j'ai fait une rédaction , en 9 pages $\frac{1}{2}$, de tout ce qu'il sera jamais utile d'en connaître ; si on voulait se limiter aux théorèmes essentiels , les 5 premières pages de ma rédaction seraient suffisantes ; les n^os^ 5 et 6 sont des résultats plus fins , dont on a besoin de temps à autre , mais qu'on pourrait au besoin démontrer quand on aura à les utiliser . Du point de vue géométrique , à laisser les choses en l'état , nous serions dans la situation quelque peu ridicule de savoir décomposer une hypersurface en ses composantes irréductibles , mais pas une courbe de l'espace à 3 dimensions .

IDEAUX DANS LES ANNEAUX NOETHERIENS .

Dans ce qui suit , A désignera un anneau noetherien commutatif , que nous supposerons posséder un élément unité (bien que ce ne soit pas essentiel).

1 . Diviseurs premiers minimaux et composantes .

On appelle *diviseur premier minimal* d'un idéal $\mathfrak{a}$ un élément minimal de l'ensemble des idéaux premiers qui contiennent $\mathfrak{a}$ (ordonné par inclusion).

Lemme 1 .- Tout idéal premier $\mathfrak{p}$ *qui contient un idéal* $\mathfrak{a}$ *contient un diviseur premier minimal de* $\mathfrak{a}$.

Soit P_0 une partie totalement ordonnée maximale de l'ensemble des idéaux premiers contenus dans $\mathfrak{p}$ qui contiennent $\mathfrak{a}$; l'intersection $\mathfrak{p}_0$ des idéaux de P_0 est un idéal , et on a $\mathfrak{a} \subset \mathfrak{p}_0 \subset \mathfrak{p}$. Le complémentaire de $\mathfrak{p}_0$ est la réunion des complémentaires des ensembles de P_0 ; ces complémentaires forment une famille totalement ordonnée de parties multiplicativement stables de A ; leur réunion est donc multiplicativement stable , ce qui montre que $\mathfrak{p}_0$ est premier . Il est clair que $\mathfrak{p}_0$ est un diviseur premier minimal de $\mathfrak{a}$.

Il résulte de là que tout idéal qui ne contient pas 1 admet au moins un diviseur premier minimal .

Soient $\mathfrak{a}$ un idéal et $\mathfrak{p}$ un diviseur premier minimal de $\mathfrak{a}$. On appelle *$\mathfrak{p}$-composante* de $\mathfrak{a}$ l'ensemble $\mathfrak{q}$ des $x \in A$ pour lesquels il existe un $y \notin \mathfrak{p}$ tel que $xy \in \mathfrak{a}$; c'est un idéal , car si $x, x' \in \mathfrak{q}$ et si y, y' sont des éléments non contenus dans $\mathfrak{p}$ tels que $xy \in \mathfrak{a}$, $x'y' \in \mathfrak{a}$, on a $(x-x')yy' \in \mathfrak{a}$, $yy' \notin \mathfrak{p}$, d'où $x-x' \in \mathfrak{q}$; et il est clair que $ax \in \mathfrak{q}$ pour tout $a \in A$.

Lemme 2 .- Soient $\mathfrak{a}$ *un idéal de* A , $\mathfrak{p}$ *un diviseur premier minimal de* $\mathfrak{a}$ *et* $\mathfrak{q}$ *la* $\mathfrak{p}$*-composante de* $\mathfrak{a}$. *Alors* : a) *on a* $\mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}$; b) *il y a un* $y \notin \mathfrak{p}$ *tel que* $y\mathfrak{q} \subset \mathfrak{a}$; c) $\mathfrak{p}$ *est diviseur premier minimal de* $\mathfrak{q}$, *et* $\mathfrak{q}$ *est sa propre* $\mathfrak{p}$*-composante* ; d) *il y a un idéal* $\mathfrak{b}$ *qui ne contient pas* $\mathfrak{p}$, *tel que* $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{q}$.

a). Si $x \in \mathfrak{a}$, on a $x.1 \in \mathfrak{a}$, d'où $x \in \mathfrak{q}$; si $x \in \mathfrak{q}$, il y a un $y \notin \mathfrak{p}$ tel que

$xy \in \mathfrak{a} \subset \mathfrak{p}$, d'où $x \in \mathfrak{p}$. b). Soit $\{x_1, \ldots, x_m\}$ un ensemble fini de générateurs de $\mathfrak{q}$, et soit $y_i \notin \mathfrak{p}$ tel que $x_i v_i \in \mathfrak{a}$; soit $y = y_1 \ldots y_m$: on a ~~xy~~ $yx_i \in \mathfrak{a}$ $(1 \leq i \leq m)$,d'où $y\mathfrak{q} \subset \mathfrak{a}$, et $y \notin \mathfrak{p}$ parce que $\mathfrak{p}$ est premier . c). Il résulte de a) que $\mathfrak{p}$ est diviseur premier minimal de $\mathfrak{q}$. Soient u et v tels que $uv \in \mathfrak{q}$, $u \notin \mathfrak{p}$. Il y a un $w \notin \mathfrak{p}$ tel que $uvw \in \mathfrak{a}$; on a $vw \notin \mathfrak{p}$, d'où $u \in \mathfrak{q}$; ceci montre que $\mathfrak{q}$ est sa propre $\mathfrak{p}$-composante . d). Soit $\mathfrak{b} = \mathfrak{a} + Ay$, où $y \notin \mathfrak{p}$ est tel que $y\mathfrak{q} \subset \mathfrak{a}$; $\mathfrak{b}$ et $\mathfrak{q}$ contiennent $\mathfrak{a}$. Soit $q = a + uy$ un élément de $\mathfrak{b} \cap \mathfrak{q}$ $(q \in \mathfrak{q},\ a \in \mathfrak{a},\ u \in A)$; on a $uy = q - a \in \mathfrak{q}$ (par a)), d'où $u \in \mathfrak{q}$ (par c)) et $uy \in \mathfrak{a}$, $q \in \mathfrak{a}$; on a donc $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{q}$, et puisque $y \notin \mathfrak{p}$, $\mathfrak{b} \not\subset \mathfrak{p}$.

2 . Diviseurs premiers essentiels .

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A , on désigne par $\mathfrak{a}:\mathfrak{b}$ l'ensemble des $x \in A$ tels que $x\mathfrak{b} \subset \mathfrak{a}$. Les propriétés suivantes sont évidentes :

1. $\mathfrak{a}:\mathfrak{b}$ est un idéal qui contient $\mathfrak{a}$.
2. Si $\mathfrak{c}$ est un idéal contenu dans $\mathfrak{b}$, $\mathfrak{a}:\mathfrak{c}$ contient $\mathfrak{a}:\mathfrak{b}$.
3. Si $\mathfrak{c}$ est un idéal quelconque , $\mathfrak{a}:\mathfrak{b}\mathfrak{c} = (\mathfrak{a}:\mathfrak{b}):\mathfrak{c} = (\mathfrak{a}:\mathfrak{c}):\mathfrak{b}$.
4. On a $\mathfrak{b} \supset \mathfrak{a}:(\mathfrak{a}:\mathfrak{b})$.

On appelle <u>diviseur premier essentiel</u> de $\mathfrak{a}$ un idéal premier $\mathfrak{p}$ qui contient $\mathfrak{a}$ et qui est tel que $\mathfrak{a}:\mathfrak{p} \neq \mathfrak{a}$.

<u>Lemme 3 .- Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A , pour que $\mathfrak{a}:\mathfrak{b} \neq \mathfrak{a}$, il faut et il suffit que $\mathfrak{b}$ soit contenu dans un diviseur premier essentiel de $\mathfrak{a}$</u> .

Si $\mathfrak{b}$ est contenu dans un diviseur premier essentiel $\mathfrak{p}$ de $\mathfrak{a}$, $\mathfrak{a}:\mathfrak{b}$ contient $\mathfrak{a}:\mathfrak{p} \neq \mathfrak{a}$, d'où $\mathfrak{a}:\mathfrak{b} \neq \mathfrak{p}$. Supposons maintenant que $\mathfrak{a}:\mathfrak{b} \neq \mathfrak{a}$, et soit $\mathfrak{p}$ un élément maximal de l'ensemble des idéaux $\mathfrak{b}'$ contenant $\mathfrak{b}$ tels que $\mathfrak{a}:\mathfrak{b}' \neq \mathfrak{a}$. Soit $z \in \mathfrak{a}:\mathfrak{p}$, $z \notin \mathfrak{a}$; on a $\mathfrak{p} \subset \mathfrak{a}:Az$; de plus , $\mathfrak{a}:(\mathfrak{a}:Az)$ est $\neq \mathfrak{a}$ parce qu'il contient z ; $\mathfrak{p}$ étant maximal , on a $\mathfrak{p} = \mathfrak{a}:Az$, d'où en particulier $\mathfrak{a} \subset \mathfrak{p}$. Montrons que $\mathfrak{p}$ est premier . Soient x et y tels que $xy \in \mathfrak{p}$, $y \notin \mathfrak{p}$. On a $zy(\mathfrak{p} + Ax) \subset z\mathfrak{p} + Azxy \subset z\mathfrak{p} \subset \mathfrak{a}$, mais $zy \notin \mathfrak{a}$, puisque $\mathfrak{a}:Az = \mathfrak{p}$ et $y \notin \mathfrak{p}$. Donc $\mathfrak{a}:(\mathfrak{p} + Ax) \neq \mathfrak{a}$, d'où $\mathfrak{p} + Ax = \mathfrak{p}$ puisque $\mathfrak{p}$ est maximal , et par suite $x \in \mathfrak{p}$, ce qui montre que $\mathfrak{p}$ est premier , donc est un diviseur premier essentiel de $\mathfrak{a}$ contenant $\mathfrak{b}$.

Corollaire .- Tout idéal $\mathfrak{a} \neq A$ admet au moins un diviseur premier essentiel .

Il suffit de prendre $\mathfrak{b} = \mathfrak{a}$ dans le lemme 3 .

Lemme 4 .- Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux . Tout diviseur premier essentiel $\mathfrak{p}$ de $\mathfrak{a}:\mathfrak{b}$ l'est aussi de $\mathfrak{a}$.

On a $(\mathfrak{a}:\mathfrak{b}):\mathfrak{p} \neq \mathfrak{a}:\mathfrak{b}$, d'où $(\mathfrak{a}:\mathfrak{p}):\mathfrak{b} = (\mathfrak{a}:\mathfrak{b}):\mathfrak{p} \neq \mathfrak{a}:\mathfrak{b}$ et $\mathfrak{a}:\mathfrak{p} \neq \mathfrak{a}$; de plus $\mathfrak{p}$ contient $\mathfrak{a}$, puisqu'il contient $\mathfrak{a}:\mathfrak{b}$.

3 . Idéaux primaires .

Un idéal $\mathfrak{q}$ est dit primaire pour un idéal premier $\mathfrak{p}$ si $\mathfrak{p}$ est diviseur premier minimal de $\mathfrak{q}$ et si $\mathfrak{q}$ est sa propre $\mathfrak{p}$-composante . Si $\mathfrak{p}$ est un diviseur premier minimal d'un idéal $\mathfrak{a}$, la $\mathfrak{p}$-composante de $\mathfrak{a}$ est primaire pour $\mathfrak{p}$ en vertu du lemme 2 .

THÉORÈME 1 .- Soit $\mathfrak{q}$ un idéal primaire pour un idéal premier $\mathfrak{p}$. Il y a un $n > 0$ tel que $\mathfrak{p}^n \subset \mathfrak{q}$; pour qu'un $x \in A$ soit dans $\mathfrak{p}$, il faut et il suffit qu'une puissance de x soit dans $\mathfrak{q}$. L'idéal $\mathfrak{p}$ est à la fois le seul diviseur premier minimal et le seul diviseur premier essentiel de $\mathfrak{q}$.

Soit $\mathfrak{p}'$ un diviseur premier essentiel de $\mathfrak{q}$. Il y a donc un $x \notin \mathfrak{q}$ tel que $x\mathfrak{p}' \subset \mathfrak{q}$; si $y \in \mathfrak{p}'$, les conditions $x \notin \mathfrak{q}$, $xy \in \mathfrak{q}$ entraînent $y \in \mathfrak{p}$. On a donc $\mathfrak{p}' \subset \mathfrak{p}$, d'où $\mathfrak{p}' = \mathfrak{p}$ puisque $\mathfrak{p}$ est diviseur premier minimal de $\mathfrak{q}$. Soit $\mathfrak{q}_m = \mathfrak{q}:\mathfrak{p}^m$; les $\mathfrak{q}_m$ forment une suite croissante d'idéaux ; il y a donc un n tel que $\mathfrak{q}_n = \mathfrak{q}_{n+1}$. Montrons que $1 \in \mathfrak{q}_n$. S'il n'en était pas ainsi , $\mathfrak{q}_n$ aurait un diviseur premier essentiel (cor. au lemme 3) qui le serait aussi de $\mathfrak{q}$ (lemme 4) et serait par suite $\mathfrak{p}$; mais c'est impossible , car $\mathfrak{q}_n:\mathfrak{p} = \mathfrak{q}:\mathfrak{p}^n\mathfrak{p} = \mathfrak{q}:\mathfrak{p}^{n+1} = \mathfrak{q}_n$. On a donc $1 \in \mathfrak{q}_n$, d'où $\mathfrak{p}^n \subset \mathfrak{q}$. Si $x \in \mathfrak{p}$, on a $x^n \in \mathfrak{q}$; si x est tel que $x^m \in \mathfrak{q}$ pour un $m > 0$, on a $x^m \in \mathfrak{p}$, d'où $x \in \mathfrak{p}$. Si un idéal premier $\mathfrak{p}'$ contient $\mathfrak{q}$, on a $x^n \in \mathfrak{p}'$, d'où $x \in \mathfrak{p}'$ pour tout

$x \in \mathfrak{p}'$, d'où $\mathfrak{p}' \supset \mathfrak{p}$, ce qui montre que $\mathfrak{p}$ est le seul diviseur premier minimal de $\mathfrak{q}$.

Si un idéal $\mathfrak{q}$ est primaire pour au moins un idéal premier $\mathfrak{p}$, on dit que $\mathfrak{q}$ est primaire ; $\mathfrak{p}$ est alors uniquement déterminé, et s'appelle l'idéal premier de $\mathfrak{q}$. Le plus petit n tel que $\mathfrak{p}^n \subset \mathfrak{q}$ s'appelle l'<u>exposant</u> de $\mathfrak{q}$. L'idéal $\mathfrak{p}^n$ n'est en général pas lui-même primaire ; mais $\mathfrak{p}$ en est évidemment un diviseur premier minimal. La $\mathfrak{p}$-composante de $\mathfrak{p}^n$ s'appelle la <u>puissance symbolique n-ème de</u> $\mathfrak{p}$, et se désigne par $\mathfrak{p}^{(n)}$.

PROPOSITION 1 .- <u>Si</u> $\mathfrak{q}_1, \dots, \mathfrak{q}_h$ <u>sont des idéaux primaires pour le même idéal premier</u> $\mathfrak{p}$, $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$ <u>est primaire pour</u> $\mathfrak{p}$.

Si $\mathfrak{p}'$ est un idéal premier qui ne contient pas $\mathfrak{p}$, il y a, pour chaque i, un $x_i \in \mathfrak{q}_i$ qui n'est pas dans $\mathfrak{p}'$ (th.1) ; on a $x_1 \dots x_h \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$, et $x_1 \dots x_h \notin \mathfrak{p}'$, ce qui montre que $\mathfrak{p}$ est diviseur premier minimal de $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$. Soient x et y tels que $y \notin \mathfrak{p}$, $xy \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$; on a $xy \in \mathfrak{q}_i$ $(1 \leq i \leq h)$, d'où $x \in \mathfrak{q}_i$, et $x \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$, ce qui montre que $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$ est sa propre $\mathfrak{p}$-composante.

<u>4 . Décomposition en idéaux primaires</u> .

THEOREME 2 .- <u>Tout idéal</u> $\mathfrak{a} \neq A$ <u>de</u> A <u>peut se représenter comme intersection d'un nombre fini d'idéaux primaires</u> .

Posons $\mathfrak{a}_1 = \mathfrak{a}$. Si $\mathfrak{a}_i$ est déjà défini et est $\neq A$, soit $\mathfrak{p}_i$ un diviseur premier minimal de $\mathfrak{a}_i$, et $\mathfrak{q}_i$ la $\mathfrak{p}_i$-composante de $\mathfrak{a}_i$; il existe alors un idéal $\mathfrak{a}_{i+1} \not\subset \mathfrak{p}_i$ tel que $\mathfrak{a}_i = \mathfrak{a}_{i+1} \cap \mathfrak{q}_i$, d'où $\mathfrak{a}_{i+1} \neq \mathfrak{a}_i$. La suite d'idéaux $(\mathfrak{a}_i)$ étant strictement croissante, n'a qu'un nombre fini de termes ; si $\mathfrak{a}_{r+1} = A$, on a $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$: or les $\mathfrak{q}_i$ sont tous primaires .

Il y a en général plusieurs représentations de $\mathfrak{a}$ comme intersection d'idéaux primaires . Faisant usage de la prop.1 , on voit qu'on peut en trouver au moins une , soit $\mathfrak{a} = \bigcap_{i=1}^{k} \mathfrak{q}_i$ qui possède les propriétés suivantes : a) les idéaux premiers des $\mathfrak{q}_i$ sont tous différents ; b) aucun des $\mathfrak{q}_i$ n'est contenu dans l'intersection des autres . Une telle représentation est dite <u>réduite</u> ; il y a encore en général plusieurs représentations réduites de $\mathfrak{a}$.

PROPOSITION 2 .- <u>Soit $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ une représentation réduite de $\mathfrak{a}$ comme intersection d'idéaux primaires , et soit $\mathfrak{p}_i$ l'idéal premier de $\mathfrak{q}_i$. Chaque $\mathfrak{p}_i$ est alors un diviseur premier essentiel de $\mathfrak{a}$. Si $\mathfrak{p}$ est un diviseur premier minimal de $\mathfrak{a}$, $\mathfrak{p}$ est l'un des $\mathfrak{p}_i$, et si $\mathfrak{p} = \mathfrak{p}_i$, $\mathfrak{q}_i$ est la $\mathfrak{p}$-composante de $\mathfrak{a}$.</u>

Soit $\mathfrak{b}_i$ l'intersection des $\mathfrak{q}_j$ pour $j \neq i$. Si $x \in A$, pour que $x\mathfrak{b}_i$ soit dans $\mathfrak{a}$, il faut et il suffit qu'il soit dans $\mathfrak{q}_i$, d'où $\mathfrak{a} : \mathfrak{b}_i = \mathfrak{q}_i : \mathfrak{b}_i$. Puisque $\mathfrak{b}_i \not\subset \mathfrak{q}_i$, on a $1 \notin \mathfrak{q}_i : \mathfrak{b}_i$, et $\mathfrak{q}_i : \mathfrak{b}_i$ admet au moins un diviseur premier essentiel $\mathfrak{p}'$; $\mathfrak{p}'$ est aussi diviseur premier essentiel de $\mathfrak{q}_i$, d'où $\mathfrak{p}' = \mathfrak{p}_i$, et de $\mathfrak{a}$ (lemme 4) , ce qui montre que $\mathfrak{p}_i$ est diviseur premier essentiel de $\mathfrak{a}$. Soit $\mathfrak{p}$ un diviseur premier minimal de $\mathfrak{a}$, et soit $\mathfrak{q}$ la $\mathfrak{p}$-composante de $\mathfrak{a}$. Si $\mathfrak{p} \neq \mathfrak{p}_i$, $\mathfrak{p}$ ne contient pas $\mathfrak{p}_i$, et il y a un $y_i \in \mathfrak{p}_i$ tel que $y_i \notin \mathfrak{p}$. Soit n_i l'exposant de $\mathfrak{q}_i$, d'où $y_i^{n_i} \in \mathfrak{q}_i$; soit y le produit des $y_i^{n_i}$ pour ceux des indices i pour lesquels $\mathfrak{p}_i \neq \mathfrak{p}$. Si $\mathfrak{p}$ n'était égal à aucun des $\mathfrak{p}_i$, y serait dans $\mathfrak{a}$ mais non dans $\mathfrak{p}$, ce qui est impossible . Supposons que $\mathfrak{p} = \mathfrak{p}_i$; on a alors $y \in \mathfrak{b}_i$, $y\mathfrak{q}_i \subset \mathfrak{a}$, $y \notin \mathfrak{p}$, d'où $\mathfrak{q}_i \subset \mathfrak{q}$. De plus , si $x \in \mathfrak{q}$, il y a un $y' \notin \mathfrak{p}$ tel que $y'x \in \mathfrak{a} \subset \mathfrak{q}_i$, et puisque $y' \notin \mathfrak{p}$, $x \in \mathfrak{q}_i$, d'où $\mathfrak{q} \subset \mathfrak{q}_i$; on a donc $\mathfrak{q} = \mathfrak{q}_i$.

COROLLAIRE .- <u>Un idéal $\mathfrak{a}$ de A n'a qu'un nombre fini de diviseurs premiers minimaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$, et il existe des $m_j > 0$ $(1 \leq j \leq g)$ tels que l'intersection des $\mathfrak{p}_j^{m_j}$ soit contenue dans $\mathfrak{a}$.</u>

Utilisons les notations de la démonstration de la prop.2 , en supposant que $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ soient les éléments minimaux de l'ensemble $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$. Il suffit de prendre pour m_j le plus grand des n_i pour les i tels que $\mathfrak{p}_j \subset \mathfrak{p}_i$; si $\mathfrak{p}_j \subset \mathfrak{p}_i$, on a alors en effet $\mathfrak{p}_j^{m_j} \subset \mathfrak{p}_i^{n_i} \subset \mathfrak{q}_i$.

5 . Passage aux anneaux quotients et anneaux de fractions .

PROPOSITION 3 .- Soit $\mathfrak{m}$ un idéal de A et soit φ l'homomorphisme canonique de A sur $A'=A/\mathfrak{m}$. Si $\mathfrak{p}$ est un idéal qui contient $\mathfrak{m}$, pour que $\varphi(\mathfrak{p})$ soit premier , il faut et il suffit que $\mathfrak{p}$ soit premier . Supposons qu'il en soit ainsi , et soit $\mathfrak{b}$ un idéal de A qui admet $\mathfrak{p}$ comme diviseur premier minimal ; $\varphi(\mathfrak{p})$ est alors un diviseur premier minimal de $\varphi(\mathfrak{b})$. Si $\mathfrak{q}$ est la $\mathfrak{p}$-composante de $\mathfrak{b}+\mathfrak{m}$, $\varphi(\mathfrak{q})$ est la $\varphi(\mathfrak{p})$-composante de $\varphi(\mathfrak{b})$.

Pour qu'un idéal soit premier dans un anneau , il faut et il suffit que l'anneau quotient par cet idéal soit un anneau d'intégrité ; la première assertion résulte donc du fait que $A'/\varphi(\mathfrak{p})$ est isomorphe à $A/\mathfrak{p}$ si $\mathfrak{p} \supset \mathfrak{m}$. Si $\mathfrak{p}'$ est un idéal premier de A' tel que $\varphi(\mathfrak{b}) \subset \mathfrak{p}' \subset \varphi(\mathfrak{p})$, on a , puisque $\mathfrak{p} = \varphi^{-1}(\varphi(\mathfrak{p}))$ $\mathfrak{b} \subset \varphi^{-1}(\mathfrak{p}') \subset \mathfrak{p}$, et $\varphi^{-1}(\mathfrak{p}')$ est premier , d'où $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$, $\mathfrak{p}' = \varphi(\mathfrak{p})$. Il est clair que $\mathfrak{p}$ est encore diviseur premier minimal de $\mathfrak{b}+\mathfrak{m}$; soit $\mathfrak{q}$ la $\mathfrak{p}$-composante de $\mathfrak{b}+\mathfrak{m}$. Il y a donc un $y \notin \mathfrak{p}$ tel que $y\mathfrak{q} \subset \mathfrak{b}+\mathfrak{m}$, d'où $\varphi(y)\varphi(\mathfrak{q}) \subset \varphi(\mathfrak{b}+\mathfrak{m}) = \varphi(\mathfrak{b})$, ce qui montre , puisque $\varphi(y) \notin \varphi(\mathfrak{p})$, que $\varphi(\mathfrak{q})$ est contenu dans la $\varphi(\mathfrak{p})$-composante de $\varphi(\mathfrak{b})$. Soit inversement x' un élément de cette composante; il y a alors un $y' \in A'$ tel que $y' \notin \varphi(\mathfrak{p})$, $x'y' \in \varphi(\mathfrak{b})$. Si x et y sont des représentants des classes x' et y' modulo $\mathfrak{m}$, on a $xy \in \varphi^{-1}(\varphi(\mathfrak{b})) = \mathfrak{b}+\mathfrak{m}$, et $y \notin \mathfrak{p}$ d'où $x \in \mathfrak{q}$, et par suite $x' \in \varphi(\mathfrak{q})$; $\varphi(\mathfrak{q})$ est donc la $\varphi(\mathfrak{p})$-composante de $\varphi(\mathfrak{b})$.

COROLLAIRE .- Les notations étant celles de la prop.3 , si $\mathfrak{q}'$ est un idéal de A' primaire pour $\varphi(\mathfrak{p})$, il existe un idéal $\mathfrak{q}$ de A primaire pour $\mathfrak{p}$ et contenant $\mathfrak{m}$, tel que $\varphi(\mathfrak{q}) = \mathfrak{q}'$.

Il suffit de prendre pour $\mathfrak{q}$ la $\mathfrak{p}$-composante de $\varphi^{-1}(\mathfrak{q}')$.

PROPOSITION 4 .- Supposons que A soit un anneau d'intégrité et soit E une partie multiplicativement stable de A qui ne contient pas 0 . Soit $\mathfrak{p}$ un idéal premier de A et soit $\mathfrak{p}'$ l'idéal engendré par $\mathfrak{p}$ dans l'anneau des fractions A_E de E . Pour que $\mathfrak{p}'$ soit premier , il faut et il suffit que $\mathfrak{p}\cap E=\emptyset$. Supposons qu'il en soit ainsi , et soit $\mathfrak{a}$ un idéal de A qui admet $\mathfrak{p}$ comme diviseur premier minimal ; l'idéal $\mathfrak{a}'$ engendré par $\mathfrak{a}$ dans A_E admet alors $\mathfrak{p}'$ comme diviseur premier minimal ; si $\mathfrak{q}$ est la $\mathfrak{p}$-composante de $\mathfrak{a}$, la $\mathfrak{p}'$-composante de $\mathfrak{a}'$ est l'idéal $\mathfrak{q}'$ engendré par $\mathfrak{q}$ dans A_E , et on a $\mathfrak{q}=A\cap\mathfrak{q}'$. Soit $\mathfrak{a}=\mathfrak{q}_1\cap\dots\cap\mathfrak{q}_h$ une représentation d'un idéal $\mathfrak{a}$ quelconque de A comme intersection d'idéaux primaires. Si $\mathfrak{a}'$ est l'idéal engendré par $\mathfrak{a}$ dans A_E , $\mathfrak{a}'\cap A$ est l'intersection de ceux des $\mathfrak{q}_i$ qui ne rencontrent pas E .

Si $\mathfrak{p}\cap E\neq\emptyset$, il est clair que $1\in\mathfrak{p}'$, donc que $\mathfrak{p}'$ n'est pas premier . Supposons que $\mathfrak{p}\cap E=\emptyset$; soient x', y' des éléments de A_E tels que $x'y'\in\mathfrak{p}'$; on sait que $\mathfrak{p}'$ se compose des éléments de la forme $e^{-1}z$, où $z\in\mathfrak{p}$, $e\in E$. Il existe donc des éléments e,f,g de E ~~XXXX~~ tels que ex', fy' soient dans A et $gx'y'$ dans $\mathfrak{p}$; $efgx'y'$ est donc dans $\mathfrak{p}$; puisque $g\notin\mathfrak{p}$, l'un des éléments ex' , fy' est dans $\mathfrak{p}$, et l'un des éléments x', y' est dans $\mathfrak{p}'$; puisque $1\notin\mathfrak{p}'$, $\mathfrak{p}'$ est premier . Supposons que $\mathfrak{p}$ soit diviseur minimal de $\mathfrak{a}$, et soit $\mathfrak{p}''$ un idéal premier de A_E tel que $\mathfrak{a}'\subset\mathfrak{p}''\subset\mathfrak{p}'$; $\mathfrak{p}''\cap A$ est alors un idéal premier de A contenant $\mathfrak{a}$ et contenu dans $\mathfrak{p}$ (car $\mathfrak{p}'\cap A=\mathfrak{p}$) , d'où $\mathfrak{p}''\cap A=\mathfrak{p}$ et $\mathfrak{p}''=\mathfrak{p}'$, ce qui montre que $\mathfrak{p}'$ est diviseur premier minimal de $\mathfrak{a}'$. Soit $\mathfrak{q}$ la $\mathfrak{p}$-composante de $\mathfrak{a}$, et soit $y\notin\mathfrak{p}$ tel que $y\mathfrak{q}\subset\mathfrak{a}$; on a alors $y\mathfrak{q}'\subset\mathfrak{a}'$, $y\notin\mathfrak{p}'$, de sorte que $\mathfrak{q}'$ est contenu dans la $\mathfrak{p}'$-composante de $\mathfrak{a}'$. Soit inversement x' un élément de cette composante , et soit y' un élément de A' non contenu dans $\mathfrak{p}'$ tel que $x'y'\in\mathfrak{a}'$. Il existe des éléments e,f,g de E tels que ex' et fy' soient dans A et $gx'y'$ dans $\mathfrak{a}$. On a $efgx'y'\in\mathfrak{a}$, mais gfy' n'est pas dans $\mathfrak{p}$, d'où $ex'\in\mathfrak{p}$ $x'\in\mathfrak{p}'$, ce qui montre que $\mathfrak{q}'$ est la $\mathfrak{p}'$-composante de $\mathfrak{a}'$. Soit maintenant $\mathfrak{a}=\mathfrak{q}_1\cap\dots\cap\mathfrak{q}_h$ une représentation d'un idéal $\mathfrak{a}$ comme intersection d'idéaux primaires . Supposons que $\mathfrak{q}_i \cap E = \emptyset$ pour $1 \leq i \leq g$, $\mathfrak{q}_i \cap E \neq \emptyset$ si $i > g$. Soit $\mathfrak{q}'_i$ l'idéal engendré par $\mathfrak{q}_i$ dans A_E ; soient $\mathfrak{p}_i$ l'idéal premier de $\mathfrak{q}_i$ et $\mathfrak{p}'_i$ l'idéal engendré par $\mathfrak{p}_i$ dans A_E . Si $i \leq g$, $\mathfrak{p}_i$ ne rencontre par E , comme il résulte tout de suite du fait qu'une puissance d'un élément quelconque de $\mathfrak{p}_i$ appartient à $\mathfrak{q}_i$ et que toute puissance d'un élément de E est dans E . Soit x un élément de $A \cap \mathfrak{q}'_i$; il y a un $e \in E$ tel que $ex \in \mathfrak{q}_i$ et , puisque $e \notin \mathfrak{p}_i$, on a $x \in \mathfrak{q}_i$, ce qui montre que $\mathfrak{q}'_i \cap A = \mathfrak{q}_i$ si $i \leq g$. L'idéal $\mathfrak{a}'$ engendré par $\mathfrak{a}$ dans A_E est évidemment contenu dans $\mathfrak{q}'_i$, d'où $\mathfrak{a}' \cap A \subset \bigcap_{i=1}^{g} \mathfrak{q}_i$. Si $j > g$, choisissons un $e_j \in \mathfrak{q}_j \cap E$, et soit $e = e_{g+1} \cdots e_h$. Si u est un élément de $\bigcap_{i=1}^{g} \mathfrak{q}_i$, on a $eu \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h = \mathfrak{a}$, d'où $u \in \mathfrak{a}' \cap A$; on a donc $\mathfrak{a}' \cap A = \bigcap_{i=1}^{g} \mathfrak{q}_i$.

COROLLAIRE .- <u>Supposons que A ne contienne pas de diviseurs de 0 ; soient $\mathfrak{a}$ un idéal de A et $\mathfrak{p}$ un diviseur premier minimal de $\mathfrak{a}$. Si A' est l'anneau local de $\mathfrak{p}$, et $\mathfrak{a}'$ l'idéal engendré par $\mathfrak{a}$ dans A' , $\mathfrak{a}' \cap A$ est la $\mathfrak{p}$-composante de $\mathfrak{a}$</u> .

Il existe en effet une représentation de $\mathfrak{a}$ comme intersection d'idéaux primaires dont l'un est la $\mathfrak{p}$-composante $\mathfrak{q}$ de $\mathfrak{a}$, les autres $\mathfrak{q}_1, \dots, \mathfrak{q}_h$ ayant leurs idéaux premiers tous $\neq \mathfrak{p}$. Si $\mathfrak{p}_i$ est l'idéal premier de $\mathfrak{q}_i$, $\mathfrak{p}_i$ n'est pas contenu dans $\mathfrak{p}$ (parce que $\mathfrak{p}$ est un diviseur premier minimal de $\mathfrak{a}$) et contient un $e_i \notin \mathfrak{p}$; il y a une puissance de e_i dans $\mathfrak{q}_i$, ce qui montre que $\mathfrak{q}_i$ rencontre le complémentaire de $\mathfrak{p}$; le corollaire résulte alors tout de suite de la dernière assertion de la prop.4 .

6 . L'intersection des puissances d'un idéal .

PROPOSITION 5 .- <u>Supposons que l'idéal $\{0\}$ de A soit primaire . Si $\mathfrak{a}$ est un idéal de A qui ne contient pas 1 , on a $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = \{0\}$</u> .

Nous procéderons par l'absurde . Supposons la proposition fausse . L'ensemble des idéaux primaires $\mathfrak{q}$ de A tels que $\bigcap_{n=1}^{\infty} (\mathfrak{a}^n + \mathfrak{q}) \not\subset \mathfrak{q}$ et que $1 \notin \mathfrak{a} + \mathfrak{q}$ n'est pas vide puisqu'il contient $\{0\}$; soit $\mathfrak{q}_0$ un idéal maximal de cet ensemble ,et soit $\mathfrak{p}_0$ l'idéal premier de $\mathfrak{q}_0$. Posons $A'=A/\mathfrak{q}_0$, $\mathfrak{p}'_0=\mathfrak{p}_0/\mathfrak{q}_0$; il résulte alors de la prop.3 que $\mathfrak{p}'_0$ est un diviseur premier minimal de l'idéal nul de A' et que ce dernier est sa propre $\mathfrak{p}'_0$-composante , donc qu'il est primaire .Soit $\mathfrak{q}'$ un idéal primaire de A' différent de $\{0\}$; on a alors $\mathfrak{q}'=\mathfrak{q}/\mathfrak{q}_0$, où $\mathfrak{q}$ est un idéal primaire de A contenant $\mathfrak{q}_0$ et $\neq\mathfrak{q}_0$ (cor. à la prop.3). Soit $\mathfrak{a}'=(\mathfrak{a}+\mathfrak{q}_0)/\mathfrak{q}_0$; on a $\mathfrak{a}'^n=(\mathfrak{a}^n+\mathfrak{q}_0)/\mathfrak{q}_0$ et $\mathfrak{a}'^n+\mathfrak{q}'=(\mathfrak{a}^n+\mathfrak{q})/\mathfrak{q}_0$; on en conclut que $\bigcap_{n=1}^{\infty}\mathfrak{a}'^n\neq\{0\}$ et que , ou bien $1\in\mathfrak{a}'+\mathfrak{q}'$, ou bien $\bigcap_{n=1}^{\infty}\mathfrak{a}'^n\subset\mathfrak{q}'$. Nous sommes donc ramenés à prouver la prop.5 sous l'hypothèse supplémentaire suivante :pour tout idéal primaire $\mathfrak{q}$, ou bien $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\subset\mathfrak{q}$, ou bien $1\in\mathfrak{a}+\mathfrak{q}$. Soit $\mathfrak{p}_0$ l'idéal premier de l'idéal primaire $\{0\}$; si $\mathfrak{a}\subset\mathfrak{p}_0$, il y a un n tel que $\mathfrak{a}^n=\{0\}$ et $\bigcap_{n=1}^{\infty}\mathfrak{a}^n=\{0\}$. Supposons que $\mathfrak{a}\not\subset\mathfrak{p}_0$, et soit y un élément de $\mathfrak{a}$ non contenu dans $\mathfrak{p}_0$. Soit x un élément $\neq0$ de $\bigcap_{n=1}^{\infty}\mathfrak{a}^n$; puisque $y\notin\mathfrak{p}_0$, on a $xy\neq0$. Soit $Axy=\bigcap_{i=1}\mathfrak{q}_i$ une représentation de Axy comme intersection d'idéaux primaires . Si $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\subset\mathfrak{q}_i$, on a $x\in\mathfrak{q}_i$; pour chacun des indices i pour lesquels cela ne se produit pas , il y a un $q_i\in\mathfrak{q}_i$ tel que $q_i\equiv1\ (\mathrm{mod.}\ \mathfrak{a})$; soit q le produit des q_i pour les indices i tels que $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\not\subset\mathfrak{q}_i$. On a donc $xq\in\mathfrak{q}_i$ pour $1\leq i\leq h$, d'où $xq\in Axy$; écrivons $xq=bxy$, $b\in A$, d'où $x(q-by)=0$. On a $q-by\equiv1\ (\mathrm{mod.}\ \mathfrak{a})$; soit $q-by=1+a$, $a\in\mathfrak{a}$. Puisque $x\neq0$, $x(1+a)=0$, on a $1+a\in\mathfrak{p}_0$, donc il existe un n >0 tel que $(1+a)^n=0$; mais $(1+a)^n$ est congru à 1 modulo $\mathfrak{a}$; puisque $(1+a)^n=0$, on a $1\in\mathfrak{a}$, ce qui implique contradiction .

THÉORÈME 3 .- <u>Si $\mathfrak{a}$ est un idéal de</u> A , <u>pour que</u> $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\neq0$, <u>il faut et il suffit qu'il y ait dans A un diviseur de</u> 0 <u>congru à</u> 1 <u>modulo</u> $\mathfrak{a}$.

Supposons que $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\neq\{0\}$. Soit $\{0\}=\mathfrak{q}_1\cap\ldots\cap\mathfrak{q}_h$ une représentation réduite de $\{0\}$ comme intersection d'idéaux primaires ; il y a au moins un i tel que $\bigcap_{n=1}^{\infty}\mathfrak{a}^n\not\subset\mathfrak{q}_i$; supposons qu'il en soit ainsi pour i=1. Si $\mathfrak{a}'=(\mathfrak{a}+\mathfrak{q}_1)/\mathfrak{q}_1$,l'intersection des puissances de $\mathfrak{a}'$ dans $A'=A/\mathfrak{q}_1$ est $\neq\{0\}$; de plus , l'idéal nul de $A/\mathfrak{q}_1$ est primaire . Il en résulte en vertu de la prop.5 que $1 \in \mathfrak{a}'$, d'où $1 \in \mathfrak{a} + \mathfrak{q}_1$. Soit q un élément de $\mathfrak{q}_1$ qui est $\equiv 1 \pmod{\mathfrak{a}}$; notre représentation de $\{0\}$ étant réduite , il y a un $x \neq 0$ dans $\bigcap_{i=2}^{h} \mathfrak{q}_i$; on a alors $qx \in \bigcap_{i=1}^{h} \mathfrak{q}_i = \{0\}$, d'où $qx=0$, et q est un diviseur de 0 . Supposons réciproquement qu'il y ait un $a \in \mathfrak{a}$ et un $x \neq 0$ dans A tels que $(1-a)x=0$; on a alors $x=ax$, d'où par récurrence $x=a^n x$ pour tout n , et $x \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n$.
