Séminaire de mathématiques

Première année 1933-1934

Théorie des Groupes et des Algèbres

J.- L'arithmétique dans une algèbre simple

Exposé fait par M. Claude Chevalley, le lundi 30 Avril 1934

Notations. On désignera par k un corps qui sera ou un corps de nombres algébriques on un corps de nombres $\mathfrak{p}$-adiques ; par $\mathcal{A}$ une algèbre simple de centre k, qui sera algèbre complète de matrices sur un corps gauche $\widetilde{k}$. On désignera par $\mathcal{N}$ l'anneau des entiers de k.

I. Ordres maxima.

On oherche à définir dans $\mathcal{A}$ une notion d'entier. La première idée consiste à appeler *entiers*, les éléments de $\mathcal{A}$ qui satisfont dans k à une équation à coefficients entiers, dont le premier coefficient soit 1. Mais on trouve qu'en général ces éléments ne forment pas un anneau. On est alors conduit à utiliser la notion d'ordre maximum, introduite par Weil dans le précédent exposé.

D'une manière générale, on appelle *ordre* de $\mathcal{A}$ un anneau $\mathcal{V}$ contenu dens $\mathcal{A}$, contenant $\mathcal{N}$, qui est $\mathcal{N}$-module fini, et qui satisfait à la condition $k\mathcal{V} = \mathcal{A}$. La troisiène condition peut se traduire de la manière suivante : soit $(u_1, u_2, \ldots, u_N)$ une k-base minima de $\mathcal{A}$; les éléments de $\mathcal{V}$ étant mis sous la forme $\sum_1^N \alpha_i u_i$ $(\alpha_i \in k)$, i1 doit exister un entier δ de k tel que, pour tous les éléments de $\mathcal{V}$, les produits $\delta\alpha_i$ soient entiers. La dernière condition signifie que tout élément de $\mathcal{A}$ peut être amené dans $\mathcal{V}$ en le multipliant par un élément convenable de $\mathcal{N}$.

On appelle *ordre maximum* (o.m.) un ordre qui n'est contenu dans aucun autre ordre.

Il est clair que si v est un ordre maximum, et φ un élément régulier de $\mathcal{A}$, $\varphi^{-1}v\varphi$ est encore un ordre maximum. Dans le cas où k est un corps p-adique et où $\mathcal{A} = \widetilde{k}$, il n'y a, comme on l'a vu, qu'un o.m. Dans tous les autres cas, il y en a une infinité.

On appelle (Artin) *idéal à gauche* (ou à droite) par rapport à un o.m. $\mathcal{V}$ un $\mathcal{V}$-module à gauche (ou à droite) fini contenu dans $\mathcal{A}$ et contenant des éléments de $\mathcal{N}$.

Nous démontrerons les propriétés suivantes des idéaux :

Si $\mathfrak{I}$ est un $\mathcal{V}$-idéal à gauche, l'ensemble des éléments α de $\mathcal{A}$ tels que $\alpha\mathfrak{I} \subset \mathfrak{I}$ est $\mathcal{V}$; l'ensemble des éléments α' tels que $\mathfrak{I}\alpha' \subset \mathfrak{I}$ est un ordre maximum $\mathcal{V}'$ en général $\neq \mathcal{V}$.

$\mathcal{V}$ et $\mathcal{V}'$ s'appellent ordre à gauche et à droite de $\mathfrak{I}$.

Un idéal $\mathfrak{I}$ possède un inverse, c'est à dire qu'il existe un idéal $\mathfrak{I}^{-1}$ tel que $\mathfrak{I}\mathfrak{I}^{-1} = \mathcal{V}, \mathfrak{I}^{-1}\mathfrak{I} = \mathcal{V}'$. $\mathfrak{I}^{-1}$ est l'ensemble des éléments s de $\mathcal{A}$ tels que $\mathfrak{I}s \subset \mathcal{V}, s\mathfrak{I} \subset \mathcal{V}'$.

On remarquera que si un ordre $\mathcal{V}$ est tel que tout $\mathcal{V}$-idéal à gauche $\mathfrak{I}$ possède un inverse $\mathfrak{I}^{-1}$ tel que $\mathfrak{I}\mathfrak{I}^{-1} = \mathcal{V}$, $\mathcal{V}$ est maximum. En effet, si $\mathcal{V}'$ est un ordre contenant $\mathcal{V}$, $\mathcal{V}'$ est $\mathcal{V}$-idéal à gauche, et $\mathcal{V}' = \mathcal{V}'^2$. En multipliant par $\mathcal{V}'^{-1}$, il vient : $\mathcal{V}' = \mathcal{V}$.

Un idéal $\mathfrak{I}$ est entier quand son inverse contient 1, c'est-à-dire encore quand il est contenu dans ses ordres à droite et à gauche. Un o.m. $\mathcal{V}$ étant $\mathcal{N}$-module fini, satisfait au Teilerkettensatz pour les idéaux entiers à ganche (ou à droite). Il en résulte que tout idéal entier $\mathfrak{I} \neq \mathcal{V}$ est divisible par un idéal entier maximum $\mathcal{R}_1$, (c'est à dire qui n'est divisible par aucun autre idéal $\neq \mathcal{V}$) ou *irréductible.* Si $\mathfrak{I}\mathcal{R}_1^{-1} \neq \mathcal{V}$, cet idéal qui est entier, est encore divisible per un idéal irréductible $\mathcal{R}_2$, etc... On en déduit, en vertu du Teilerkettensatz, que :

Tout $\mathcal{V}$-idéal à gauche entier se décompose en produit de facteurs irréductibles.

Cette décomposition n'est d'ailleurs pas unique.

II. Cas des corps $\mathfrak{p}$-adiques.

Pour établir les propositions précédentes, nous prendrons d'abord le cas où k est un corps de nombres $\mathfrak{p}$-adiques.

Nous introduirons un module de représentation $\mathcal{M}_{\widetilde{k}}$ de $\mathcal{A}$ dans $\widetilde{k}$; ce sera le module des formes linéaires à n variables $u_1, u_2, \ldots, u_n$, à coefficients dans $\widetilde{k}$; $\mathcal{M}_{\widetilde{k}}$ est $\mathcal{A}$-module droit, et toute base $(v_1, v_2, \ldots, v_n)$ de $\mathcal{M}_{\widetilde{k}}$ conduit à une représentation, qui associe à l'élément φ de $\mathcal{A}$ la matrice $(\alpha_{i,j})$ définie par :

$$v_i\varphi = \sum_{j=1}^{n} \alpha_{ij} v_j \quad (i = 1, 2, \ldots, n)$$

Réciproquement, étant donnés n éléments $w_1, w_2, \ldots, w_n$ de $\mathcal{M}_{\widetilde{k}}$, il y a un élément φ de $\mathcal{A}$ et un seul tel que $v_i\varphi = w_i \quad (i = 1, 2, \ldots, n)$.

Nous désignerons par v l'ordre maximum de $\widetilde{k}$, et nous considérerons les divers v-modules finis $\mathfrak{N}$ de rang n contenus dans $\mathcal{M}_{\widetilde{k}}$. Pour chacun d'eux, nous introduirons l'anneau $\widehat{\mathcal{V}}$ des éléments φ tels que $\mathfrak{N}_\varphi \subset \mathfrak{N}.\widehat{\mathcal{V}}$ est un anneau qui contient $\mathcal{N}$ et qui satisfait $k\widehat{\mathcal{V}} = \mathcal{A}$. D'autre part, v étant un anneau à idéaux tous principaux, $\mathfrak{N}$ possède par rapport à v une base minima $(v_1, v_2, \ldots, v_n)$ et s'écrit :

$$\mathfrak{N} = vv_1 \oplus vv_2 \oplus \ldots \oplus vv_n.$$

On voit alors que les éléments de $\widehat{\mathcal{V}}$ sont ceux qui, dans la représentation définie par la base $(v_1, v_2, \ldots, v_n)$ se représentent par des matrices à coefficients entiers. Il en résulte que $\widehat{\mathcal{V}}$ est v-module fini, donc aussi $\mathcal{N}$-module fini, et est un ordre.

Soit $\mathfrak{I}$ un $\widehat{\mathcal{V}}$-idéal à gauche. On constate tout de suite que $\mathfrak{N}\mathfrak{I}$ est un module $\mathfrak{N}'$ qui satisfait aux mêmes conditions que $\mathfrak{N}$. Donc $\mathfrak{N}'$ se met sous la forme

$$\mathfrak{N}' = vv_1' \oplus vv_2' \oplus \ldots \oplus vv_n'.$$

Soit φ l'élément de $\mathcal{A}$ défini par les formules $v_i\varphi = v_i'$ $(i = 1, 2......n)$. Il est clair que : $\mathfrak{I}\varphi = \mathfrak{I}'$. Je dis que : $\varphi \subset \mathfrak{I}$.

1) On a $v_i\widehat{\mathcal{V}} = \mathfrak{N}$ $(i = 1, 2, \ldots, n)$. En effet, soit u un élément quelconque de $\mathfrak{N}$. L'élément ψ de $\mathcal{A}$ défini par $v_i\psi = u, v_j\psi = 0$ (si $j \neq i$) est dans $\widehat{\mathcal{V}}$: donc $v_i\widehat{\mathcal{V}} \supset \mathfrak{N}$. Comme d'autre part, $\mathfrak{N}\widehat{\mathcal{V}} \subset \mathfrak{N}$, la formule est démontrée.

2) on en déduit $v_i\mathfrak{I} = \mathfrak{N}'$. Donc, pour chaque i, $\mathfrak{I}$ contient un élément ψ_i tel que $v_i\psi_i = v_i'$. Soit θ_i l'élément de $\widehat{\mathcal{V}}$ défini par $v_i\theta_i = v_j, v_j = 0$ $(j \neq i)$. L'élément $\sum \theta_i\psi_i$ est dans $\mathfrak{I}$, et on a : $v_i\left(\sum \theta_i\psi_i\right) = v_i'$ $(i = 1, 2, \ldots, n)$. Cet élément est donc égal à φ.

Donc $\mathfrak{I}\varphi^{-1} \supset \widehat{\mathcal{V}}$. Mais $\mathfrak{N}\mathfrak{I}\varphi^{-1} = \mathfrak{N}'\varphi^{-1} = \mathfrak{N}$, donc $\mathfrak{I}\varphi^{-1} \subset \widehat{\mathcal{V}}$. On en déduit que $\mathfrak{I} = \widehat{\mathcal{V}}\varphi$: $\mathfrak{I}$ est un idéal principal.

L'ensemble des éléments ψ tels que $\mathfrak{I}\psi \subset \widehat{\mathcal{V}}$ est évidemment $\varphi^{-1}\widehat{\mathcal{V}}$, et on a $\mathfrak{I}.\varphi^{-1}\widehat{\mathcal{V}} = \widehat{\mathcal{V}}$. Donc $\mathfrak{I}$ possède un inverse : il en résulte, comme nous l'avons vu, que $\widehat{\mathcal{V}}$ est un o.m. L'ordre à droite de $\mathfrak{I} = \widehat{\mathcal{V}}\varphi$ est évidemment $\varphi^{-1}\widehat{\mathcal{V}}\varphi$, qui est un o.m., car la transformation par φ produit un isomorphisme intérieur de $\mathcal{A}$. Nous avons démontré dans le cas considéré les propositions annoncées. Nous avons vu de plus que tout idéal est principal, et qu'un o.m. est l'ensemble des éléments de $\mathcal{A}$ qui, dans une certaine représentation de $\mathcal{A}$ dans $\widetilde{k}$ se représentent par des matrices à coefficients entiers.

Cherchons maintenant les idéaux bilatères. Reprenant les notations définies plus haut, il est clair que l'ordre à droite de $\mathfrak{I}$ est l'ensemble des éléments θ de $\mathcal{A}$ tels que $\mathfrak{N}'\theta \subset \mathfrak{N}'$. Si $\mathfrak{I}$ est bilatère, cet ensemble est $\mathcal{V}$. On a alors $v_1\mathcal{V} = \mathfrak{N}, v_1'\mathcal{V} = \mathfrak{N}'$. Dans ceci, v_1' n'est assujetti qu'à être un des éléments d'une base minima de $\mathfrak{N}'$. Or, soit i 1'ensemble des éléments α de v tels que $\alpha v_1 \subset \mathfrak{N}'$, i est idéal par rapport à v et se met per suite sous la forme $v\alpha_1$. On a vu dans l'exposé sur les modules, que $v\alpha v_1$ est un sous-module primitif de $\mathfrak{N}'$, et que par suite, αv_1 peut être pris pour premier élément d'une base minima de $\mathfrak{N}'$. Donc $\alpha v_1\mathcal{V} = \mathfrak{N}' = \alpha\mathfrak{N}$. On peut écrire aussi, $\mathfrak{N}' = \mathfrak{N}\alpha$, ce qui montre que $\mathfrak{I} = \mathcal{V}\alpha$. Donc :

Les idéaux bilatères par rapport à $\widehat{\mathcal{V}}$ sont les $\mathfrak{p}^m\widehat{\mathcal{V}}$ où $\mathfrak{p}$ est l'idéal premier de $\widetilde{k}$.

III. Cas du corps des nombres algébriques

Dans ce cas, la méthode introduite par Hasse qui s'est montrée excessivement féconde, consiste à considérer successivement ce qui se passe dans tous les corps $\mathfrak{p}$-adiques $k_\mathfrak{p}$ relatifs aux divers idéaux premiers $\mathfrak{p}$ de k.

Pour chaque $\mathfrak{p}$, nous introduirons $k_\mathfrak{p}\mathcal{A}$ qui est une algèbre simple $\mathcal{A}_\mathfrak{p}$ de centre $k_\mathfrak{p}$. Les éléments de $\mathcal{A}_\mathfrak{p}$ peuvent être considérés comme limites de suites d'éléments de $\mathcal{A}$, dans le sens suivant : soit $(u_1, u_2, \ldots, u_N)$ une k-base de $\mathcal{A}$. Une suite $\sum \alpha_i^{(m)} u_i$ d'éléments de $\mathcal{A}$ convergera pour $\mathfrak{p}$ si, pour chaque i, les $\alpha_i^{(m)}$ forment une suite convergente, dont la limite est α_i. La limite de la suite sera alors par définition l'élément $\sum \alpha_i u_i$ de $\mathcal{A}_\mathfrak{p}$. (On vérifie tout de suite que cette notion de limite est indépendante de la base choisie). $\bullet$ étant un ensemble d'éléments de $\mathcal{A}$, on désignera par $\bullet_\mathfrak{p}$ l'ensemble des limites des suites d'éléments de E.

Théorème fondamental de passage.

Soit $\mathfrak{M}$ un $\mathcal{N}$-module fini tel que $k\mathfrak{M} = \mathcal{A}.\mathfrak{M}$ est la partie commune à $\mathcal{A}$ et à tous les $\mathfrak{M}_\mathfrak{p}$. Si $\mathfrak{F}$ est un autre module du même type que $\mathfrak{M}$, on a pour presque tous les $\mathfrak{p}$, $\mathfrak{M}_\mathfrak{p} = \mathfrak{F}_\mathfrak{p}$. Enfin, si on se donne pour chaque $\mathfrak{p}$ un $\mathcal{N}_\mathfrak{p}$-module fini, $\widehat{\mathfrak{N}}_\mathfrak{p}$ tel que $k_\mathfrak{p}\widehat{\mathfrak{N}}_\mathfrak{p} = \mathcal{A}_\mathfrak{p}$ de manière à ce que pour presque tous les $\mathfrak{p}$, on ait $\widehat{\mathfrak{N}}_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$, l'intersection avec $\mathcal{A}$ de tous les $\widehat{\mathfrak{N}}_\mathfrak{p}$ est un module $\mathfrak{N}$ tel que, pour tous les $\mathfrak{p}$, on ait $\mathfrak{N}_\mathfrak{p} = \widehat{\mathfrak{N}}_\mathfrak{p}$.

1) Pour la première partie, il suffit de montrer que si φ est un élément de $\mathcal{A}$ contenu dans tous les $\mathfrak{M}_\mathfrak{p}$, φ est dans $\mathfrak{M}$. Soit $(u_1, u_2, \ldots, u_N)$ une k-base minima de $\mathcal{A}$, et $\varphi = \sum \alpha_i u_i \quad (\alpha_i \subset k)$. Si nous mettons les éléments de $\mathfrak{M}$ sous la forme $\sum \beta_i u_i$, β_N décrit un idéal $\mathfrak{I}_N$ de $\mathcal{N}$. L'hypothèse $\varphi \subset \mathfrak{M}_\mathfrak{p}$ entraîne $\alpha_N \subset (\mathfrak{I}_N)_\mathfrak{p}$ quel que soit $\mathfrak{p}$. On a donc $\alpha_N \subset \mathfrak{I}_N$ et par suite il y a un élément φ_N de $\mathfrak{M}$ dans lequel le dernier coefficient est α_N. On a $\varphi = \varphi_N = \sum_1^{N-1} \alpha'_i u_i$ et $\varphi - \varphi_N \subset \mathfrak{M}_\mathfrak{p}$ quel que soit $\mathfrak{p}$. On en conclut comme plus haut qu'il y a un élément φ_{N-1} de $\mathfrak{M}$ de la forme $\beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_{N-2} u_{N-2} + \alpha'_{N-1} u_{N-1}$. On forme $\varphi - \varphi_{N-1} - \varphi_{N-2}$, et on continue de la même manière. Finalement, φ se met sous la forme d'une somme $\varphi_1 + \varphi_2 + \ldots + \varphi_N$ d'éléments de $\mathfrak{M}$, ce qui démontre la proposition.

2) Prenons des bases $(v_1, v_2, \ldots, v_R)$ de $\mathfrak{M}$ et $(w_1, w_2, \ldots, w_s)$ de $\mathfrak{N}$. Il existe deux éléments α, β de $\mathcal{N}$ tels que :

1) $\alpha v_1, \alpha v_2, \ldots, \alpha v_R$ soient dans $\mathfrak{N}$,

2) $\beta w_1, \beta w_2, \ldots, \beta w_S$ soient dans $\mathfrak{M}$.

Supposons $\mathfrak{p}$ premier à $\alpha\beta$. Alors $\mathfrak{M}_\mathfrak{p} \subset \alpha^{-1}\mathfrak{N}_\mathfrak{p}, \mathfrak{N}_\mathfrak{p} \subset \beta^{-1}\mathfrak{M}_\mathfrak{p}$. Mais α^{-1}, β^{-1} sont dans $\mathcal{N}_\mathfrak{p}$. On a donc $\mathfrak{M}_\mathfrak{p} = \mathfrak{N}_\mathfrak{p}$.

3) Prenons un élément $\sum \alpha_i u_i$ de $\widehat{\mathfrak{N}}_{\mathfrak{p}}$. Pour chaque m, on a des décompositions $\alpha_i = \overline{\alpha}_i^{(m)} + \pi^m \beta_i$, $\overline{\alpha}_i^{(m)} \subset k, \beta_i \subset e_{\mathfrak{p}}$ (π représente un élément de $\mathcal{N}$ divisible par $\mathfrak{p}$. Il existe un entier m_0 tel que si $m > m_0$, les $\pi^m u_i$ soient dans $\widehat{\mathfrak{N}}_{\mathfrak{p}}$. On a alors $\varphi = \lim \overline{\varphi} m$ où $\overline{\varphi} m = \sum \alpha_i^{(m)} u_i$ est un élément de $\mathcal{A}$ qui est dans $\mathfrak{N}_{\mathfrak{p}}$ si $m > m_0$. Il existe d'autre part pour chaque m un entier δ_m de $\mathcal{N}$ tel que $\delta_m \varphi_m$ soit dans $\mathfrak{M}$. Mettons δ_m sous la fome $\mathfrak{p}^{-1}\mathfrak{i}$, $(\mathfrak{i}.\mathfrak{p}) = 1$. Alors si $\mathfrak{j}$ est un idéal premier $\neq \mathfrak{i}$, il y a un entier δ'_m divisible par $\mathfrak{i}$ et premier à $\mathfrak{p}$. $\delta'_m \varphi_m$ est dans $\widehat{\mathfrak{N}}_{\mathfrak{q}}$ et dans $\mathfrak{M}_{\mathfrak{q}}$, si $\mathfrak{q} \neq \mathfrak{p}$, donc aussi dans presque tous les $\widehat{\mathfrak{N}}_{\mathfrak{q}}$: prenons un entier $x_{\mathfrak{q}}$ premier à $\mathfrak{p}$ tel que $x_{\mathfrak{q}} \delta'_m \varphi_m$ soit dans $\mathfrak{N}_{\mathfrak{q}}$. Alors $\prod_{\mathfrak{q}} x_{\mathfrak{q}}.\delta'_m \varphi_m = \delta''_m \varphi_m$ est dans $\mathfrak{N}$, et δ''_m est premier à $\mathfrak{q}$. Donc φ_m est dans $\mathfrak{N}_q$. Comme $\varphi = \lim \varphi_m$, φ est aussi dans $\mathfrak{N}_{\mathfrak{p}}$.

Conséquences

Admettons l'existence dans $\mathcal{A}$ d'un o.m. $\mathcal{V}$. Alors pour chaque $\mathfrak{p}$, $\mathcal{V}_{\mathfrak{p}}$ est o.m. de $\mathcal{A}_{\mathfrak{p}}$. En effet, si pour un $\mathfrak{p}$, $\mathcal{V}_{\mathfrak{p}}$ était contenu dans un autre $\mathcal{V}'_{\mathfrak{p}}$, l'intersection de $\mathcal{A}$ avec tous les $\mathcal{V}_{\mathfrak{q}}$ ($\mathfrak{q} \neq \mathfrak{p}$) et avec $\mathcal{V}'_{\mathfrak{q}}$ serait un ordre $\mathcal{V}'$ contenant $\mathcal{V}$ et $\neq \mathcal{V}'$, ce qui est impossible.

Soit $\mathfrak{I}$ un idéal à gauche par rapport à $\mathcal{V}$. Les ensembles des éléments α, α' tels que $\alpha\mathfrak{I} \subset \mathfrak{I}, \mathfrak{I}\alpha' \subset \mathfrak{I}$ sont respectivement les intersections de $\mathcal{A}$ avec tous les $\mathcal{V}_{\mathfrak{p}}$ et avec tous les ordres à droite $\mathcal{V}'_{\mathfrak{p}}$ des idéaux $\mathfrak{I}_{\mathfrak{p}}$. Le premier ensemble est $\mathcal{V}$; le second est un $\mathcal{N}$-module fini de même rang que $\mathcal{V}$: c'est un ordre $\mathcal{V}'$ qui est maximum puisque chaque $\mathcal{V}'_{\mathfrak{p}}$ est maximum. De même, l'ensemble des éléments β de $\mathcal{A}$ tels que $\mathfrak{I}_\beta \subset \mathcal{V}$ est l'intersection de $\mathcal{A}$ avec tous les $\mathfrak{I}_{\mathfrak{p}}^{-1}$. C'est évidemment un $\mathcal{V}$-idéal à droite $\mathfrak{I}^{-1}$; des formules $\mathfrak{I}_{\mathfrak{p}}\mathfrak{I}_{\mathfrak{p}}^{-1} = \mathcal{V}_{\mathfrak{p}}$, $\mathfrak{I}_{\mathfrak{p}}^{-1}\mathfrak{I}_{\mathfrak{p}} = \mathcal{V}'_{\mathfrak{p}}$, on déduit $\mathfrak{I}\mathfrak{I}^{-1} = \mathcal{V}, \mathfrak{I}^{-1}\mathfrak{I} = \mathcal{V}'$. Les théorèmes fondamentaux sur les idéaux sont donc établis.

Étant donnés un idéal $\mathfrak{I}$ dont l'ordre à gauche est $\mathcal{V}$ et un idéal premier $\mathfrak{P}$ de k. On désigne encore par $\mathfrak{I}_{\mathfrak{P}}$ l'idéal de $\mathcal{A}$ formé de l'intersection de $\mathcal{A}$ avec tous les $\mathcal{V}_{\mathfrak{q}}$ ($\mathfrak{q} \neq \mathfrak{p}$) et avec $\mathfrak{I}_{\mathfrak{p}}$. C'est un idéal qui a même ordre à gauche $\mathcal{V}$ que $\mathfrak{I}$ et qui n'est différent de $\mathcal{V}$ que pour un nombre fini de $\mathfrak{p}$. $\mathfrak{I}_{\mathfrak{p}}$ s'appelle composante de $\mathfrak{I}$ suivant $\mathfrak{p}$. On a, si $\mathfrak{q} \neq \mathfrak{p}$, $(\mathfrak{I}_{\mathfrak{p}})_{\mathfrak{q}} = \mathcal{V}_{\mathfrak{q}}$.

Supposons maintenant $\mathfrak{I}$ bilatère, et formons le produit $\mathfrak{I}' = \prod \mathfrak{I}_{\mathfrak{p}}$, le produit étant étendu à tous les idéaux $\mathfrak{P}$ rangés dans un ordre quelconque. Alors, on a, pour chaque $\mathfrak{p}$, $\mathfrak{I}'_{\mathfrak{p}} = \mathfrak{I}_{\mathfrak{p}}$, d'où $\mathfrak{I} = \mathfrak{I}'$: *un idéal bilatère est le produit de toutes ses composantes.*

D'autre part, $\mathfrak{I}$ étant toujours bilatère, on a vu que $\mathfrak{I}_{\mathfrak{p}}$ est de la forme $\mathfrak{p}^{*m_{\mathfrak{p}}}\mathcal{V}_{\mathfrak{p}}$ où $\mathfrak{p}$ est l'idéal premier du corps gauche $\widetilde{k}^*_{\mathfrak{p}}$ sur lequel $\mathcal{A}_{\mathfrak{p}}$ est algèbre de matrices. Ce corps gauche est contenu dans $\widetilde{k}_{\mathfrak{p}}$ et par suite, on peut écrire $\mathfrak{I}_{\mathfrak{p}} = \overline{\mathfrak{p}}^{m_{\mathfrak{p}}}\mathcal{V}_{\mathfrak{p}}$ où $\overline{\mathfrak{p}}$ est l'idéal bilatère maximum (ou premier) de $\widetilde{k}_{\mathfrak{p}}$. On désigne encore par $\overline{\mathcal{R}}$ l'intersection de $\mathcal{A}$ avec l'idéal $\overline{\mathfrak{p}}\mathcal{V}_{\mathfrak{p}}$ de $\mathcal{A}_{\mathfrak{p}}$ et avec tous les $\mathcal{V}_{\mathfrak{q}}$ ($\mathfrak{q} \neq \mathfrak{p}$). C'est l'idéal bilatère premier de $\widetilde{k}$. On a $\mathfrak{I}_{\mathfrak{p}} = \mathcal{R}^{m_{\mathfrak{p}}}$. Il résulte de là que : *tout idéal bilatère s décompose en produit d'idéaux bilatères premiers ; le produit de deux idéaux bilatères relatifs à un même o.m. est commutatif et par suite la décomposition en idéaux premiers est unique à l'ordre près des facteurs. Tout idéal bilatère relatif à l'o.m. $\mathcal{V}$ de $\mathcal{A}$ est de la forme $i\mathcal{V}$, où i est un idéal de $\widetilde{k}$. Pour chaque idéal premier $\mathfrak{p}$ de k, il y a un idéal premier bilatère $\mathcal{R}$ de $\mathcal{A}$ et on a $\mathfrak{p} = \mathcal{R}^{\bullet_{\mathfrak{p}}}$ où $\bullet_{\mathfrak{p}}$ est le degré du corps gauche semblable à $\mathcal{A}_{\mathfrak{p}}$.*