Claude Chevalley

L'arithmétique dans une algèbre simple

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. nº 10, p. 1-11
<http://www.numdam.org/item?id=SMJ_1933-1934__1__A10_0>

SEMINAIRE DE MATHEMATIQUES

Première année 1933-1934

Théorie des Groupes et des Algèbres

J.- L'ARITHMETIQUE DANS UNE ALGEBRE SIMPLE

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

L'ARITHMETIQUE DANS UNE ALGEBRE SIMPLE (suite)

<u>Notations</u> .- On désignera par k un corps qui sera ou un corps de nombres algébriques ou un corps de nombres $\mathfrak{p}$-adiques; par $\mathfrak{A}$ une algèbre simple de centre k, qui sera algèbre complète de matrices sur un corps gauche $\mathfrak{K}$. On désignera par $\mathfrak{o}$ l'anneau des entiers de k .

I.- <u>ORDRES MAXIMA</u> .

On cherche à définir dans $\mathfrak{A}$ une notion d'entier. La première idée consiste à appeler <u>entiers</u>, les éléments de 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'odre maximum , introduite par Weil dans le précédent exposé .

D'une manière générale, on appelle <u>ordre</u> de $\mathfrak{A}$ un anneau $\mathfrak{O}$, contenu dans $\mathfrak{A}$, contenant $\mathfrak{o}$, qui est $\mathfrak{o}$-module fini, et qui satisfait à la condition k $\mathfrak{O}$ = $\mathfrak{A}$. La troisième condition peut se traduire de la manière suivante : soit ($u_1, u_2, \ldots\ldots u_N$) une k-base minima de $\mathfrak{A}$; Les éléments de $\mathfrak{O}$ étant mis sous la forme $\sum_1^N \alpha_i u_i$ ($\alpha_i \subset$ k) ,il doit exister un entier δ de k tel que, pour tous les éléments de $\mathfrak{o}$, les produits $S\alpha_i$ soient entiers. La dernière condition signifie que tout élément de $\mathfrak{S}$ peut être amené dans $\mathfrak{o}$ en le multipliant par un élément convenable de $\mathfrak{R}$.

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

Il est clair que si $\mathfrak{o}$ est un ordre maximum, et φ un élément régulier de $\mathfrak{S}$, $\varphi^{-1}\mathfrak{o}\varphi$ est encore un ordre maximum . Dans le cas où k est un corps $\mathfrak{p}$ -adique et où $\mathfrak{S} = k$, 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. $\mathfrak{o}$ un $\mathfrak{o}$ -module à gauche (ou à droite) fini contenu dans $\mathfrak{S}$, et contenant des éléments de $\mathfrak{R}$.

Nous démontrerons les propriétés suivantes des idéaux :

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

$\mathfrak{o}$ et $\mathfrak{o}'$ s'appellent ordre à gauche et à droite de $\mathfrak{a}$.

Un idéal $\mathfrak{a}$ possède un inverse, c'est à dire qu'il existe un idéal $\mathfrak{a}^{-1}$ tel que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$, $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}'$ $\mathfrak{a}^{-1}$ est l'ensemble des éléments β de $\mathfrak{S}$ tels que $\mathfrak{a}\beta \subset \mathfrak{o}$, $\beta\mathfrak{a} \subset \mathfrak{o}'$.

On remarquera que si un ordre $\mathfrak{o}$ est tel que tout $\mathfrak{o}$-

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

Un idéal $\mathfrak{a}$ 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. $\mathfrak{o}$ étant $\mathfrak{H}$-module fini, satisfait au Teilerkettensatz pour les idéaux entiers à gauche (ou à droite) . Il en résulte que tout idéal entier $\mathfrak{a} \neq \mathfrak{o}$ est divisible par un idéal entier maximum $\mathfrak{P}_1$, (c'est à dire qui n'est divisible par aucun autre idéal $\neq \mathfrak{o}$) <u>ou irréductible</u> . Si $\mathfrak{a}\mathfrak{P}_1^{-1} \neq \mathfrak{o}$, cet idéal qui est entier, est encore divisible par un idéal irréductible $\mathfrak{P}_2$, etc .... On en déduit, en vertu du Teilerkettensatz, que :

<u>Tout $\mathfrak{o}$-idéal à gauche entier se décompose en produit de facteurs irréductibles</u> .

Cette décomposition n'est d'ailleurs pas unique .

II.- <u>CAS DES CORPS $\mathfrak{p}$-ADIQUES</u>.

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 $\mathfrak{M}_{\bar{k}}$ de $\gamma\mathfrak{f}$ dans $\bar{k}$; ce sera le module des formes linéaires à n variables $u_1, u_2, \ldots u_n$, à coefficients dans $\bar{k}$; $\mathfrak{M}_{\bar{k}}$ est $\overset{\gamma}{\mathfrak{f}}$module droit , et toute base ($v_1, v_2, \ldots\ldots v_n$)

de $\mathfrak{M}_k$ conduit à une représentation, qui associe à l'élément φ de $\mathcal{S}$ la matrice $(\alpha_{i,j})$ définie par :

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

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

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

$$\mathfrak{N} = \mathfrak{o}\, v_1 \oplus \mathfrak{o}\, v_2 \oplus \ldots\ldots \oplus \mathfrak{o}\, v_n$$

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

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

$$\mathfrak{N}' = \mathfrak{o}\, v'_1 \oplus \mathfrak{o}\, v'_2 \oplus \ldots\ldots \oplus \mathfrak{o}\, v'_n$$

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

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

2) On en déduit $v_i \mathfrak{v} = \mathcal{H}'$. Donc , pour chaque i, $\mathfrak{v}$ contient un élément ψ_i tel que $v_i \psi_i = v'_i$. Soit θ_i l'élément de $\tilde{\mathfrak{v}}$ défini par $v_i \theta_i = v_i$, $v_j = 0$, ($j \neq i$) . L'élément $\Sigma\theta_i\psi_i$ est dans $\mathfrak{v}$, et on a : $v_i (\Sigma \theta_i \psi_i) = v'_i$ (i = 1,2 ..... n) . Cet élément est donc égal à φ .

Donc $\mathfrak{v}\varphi^{-1} \supset \tilde{\mathfrak{v}}$. Mais $\mathcal{H}\mathfrak{v}\varphi^{-1} = \mathcal{H}'\varphi^{-1} = \mathcal{H}$, donc $\mathfrak{v}\varphi^{-1} \subset \tilde{\mathfrak{v}}$. On en déduit $\mathfrak{v} = \tilde{\mathfrak{v}}\varphi$: $\mathfrak{v}$ est un idéal principal .

L'ensemble des éléments ψ tels que $\mathfrak{v}\psi \subset \tilde{\mathfrak{v}}$ est évidemment $\varphi^{-1}\tilde{\mathfrak{v}}$, et on a $\mathfrak{v} . \varphi^{-1}\tilde{\mathfrak{v}} = \tilde{\mathfrak{v}}$ .Donc $\mathfrak{v}$ possède un inverse : il en résulte comme nous l'avons vu, que $\tilde{\mathfrak{v}}$ est un o.m. L'ordre à droite de $\mathfrak{v} = \tilde{\mathfrak{v}}\varphi$ est évidemment $\varphi^{-1}\tilde{\mathfrak{v}}\varphi$, qui est un o.m., car la transformation par φ produit un isomorphisme intérieur de $\mathcal{S}\gamma$. 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 $\mathcal{S}\gamma$

qui, dans une certaine représentation de $\mathfrak{S}$ dans $\mathfrak{K}$ se représentent par des matrices à coefficients entiers .

Cherchons maintenant les idéaux bilatères . Reprenant les notations de plus haut, il est clair que l'ordre à droite de $\mathfrak{M}$ est l'ensemble des éléments θ de $\mathfrak{S}$ tels que $\mathfrak{M}'\theta \subset \mathfrak{M}'$. Si $\mathfrak{M}$ est bilatère, cet ensemble est $\mathfrak{V}$. On a alors $v_1 \mathfrak{V} = \mathfrak{M}$, $v'_1 \mathfrak{V} = \mathfrak{M}'$. Dans ceci, v'_1 n'est assujetti qu'à être un des éléments d'une base minima de $\mathfrak{M}'$. Or, soit $\mathfrak{m}$ l'ensemble des éléments α de $\mathfrak{v}$ tels que $\alpha v_1 \subset \mathfrak{M}'$, $\mathfrak{m}$ est idéal par rapport à $\mathfrak{v}$, et se met par suite sous la forme $\mathfrak{v}\alpha_1$. On a vu, dans l'exposé sur les modules, que $\mathfrak{v}\alpha v_1$ est un sous-module primitif de $\mathfrak{M}'$, et que par suite, αv_1 peut être pris pour premier élément d'une base minima de $\mathfrak{M}'$. Donc $\alpha v_1 \mathfrak{V} = \mathfrak{M}' = \alpha \mathfrak{M}$. On peut écrire aussi, $\mathfrak{M}' = \mathfrak{M}\alpha$ ce qui montre que $\mathfrak{M} = \mathfrak{V}\alpha$. Donc :

<u>Les idéaux bilatères par rapport à $\mathfrak{V}$ sont les $\mathfrak{p}^m\mathfrak{V}$ où $\mathfrak{p}$ est l'idéal premier de $\mathfrak{K}$</u> .

III.- <u>CAS DU CORPS DE NOMBRES ALGEBRIQUES</u>

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 $k_{\mathfrak{p}}\mathfrak{J}$ qui est une algèbre simple $\mathfrak{S}_\mathfrak{p}$ de centre $k_\mathfrak{p}$. Les éléments de $\mathfrak{S}_\mathfrak{p}$ peuvent être considérés comme limites de suites d'éléments de $\mathfrak{S}$, dans le sens suivant : soit (u_1, u_2, ... u_N) une k-base de $\mathfrak{S}$. Une suite $\sum \alpha_i^{(m)} u_i$ d'éléments de $\mathfrak{S}$ 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 $\mathfrak{S}_\mathfrak{p}$. (On vérifie tout de suite que cette notion de limite est indépendante de la base choisie) . E étant un ~~ensem~~ semble d'éléments de $\mathfrak{S}$, on désignera par $E_\mathfrak{p}$ l'ensemble des limites des suites d'éléments de E .

<u>Théorème fondamental de passage</u>.

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

1) Pour la première partie, il suffit de montrer que si φ est un élément de $\mathfrak{S}$ contenu dans tous les $\mathfrak{M}_\mathfrak{p}$, φ est dans $\mathfrak{M}$. Soit (u_1, u_2.... u_N) une k-base minima de $\mathfrak{S}$, et $\varphi = \sum \alpha_i u_i$ ($\alpha_i \subset k$) . Si nous

mettons les éléments de $\mathfrak{M}$ sous la forme $\sum \beta_i u_i$, β_N décrit un idéal $\mathfrak{n}_N$ de $\mathfrak{A}$. L'hypothèse $\varphi \subset \mathfrak{M}_{\mathfrak{q}}$ entraine $\alpha_N \subset (\mathfrak{n}_N)_{\mathfrak{q}}$ quel que soit $\mathfrak{q}$. On a donc $\alpha_N \subset \mathfrak{n}_N$ 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 $\varphi - \varphi_N \subset \mathfrak{M}_{\mathfrak{q}}$; quel que soit $\mathfrak{q}$. On en conclut comme plus haut qu'il y a un élément φ_{N-1} de $\mathfrak{M}$ de la forme $\beta_1 u_1 + \beta_2 u_2 + \dots + \beta_{N-2} u_{N-2} + \alpha'_{N-1} u_{N-1}$.
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 $\varphi_1 + \varphi_2 + \dots + \varphi_N$ d'éléments de $\mathfrak{M}$, ce qui démontre la proposition.

2) Prenons des bases ($v_1, v_2, \dots v_R$) de $\mathfrak{M}$ et ($w_1, w_2, \dots w_S$) de $\mathfrak{N}$. Il existe deux éléments α, β de $\mathfrak{A}$ tels que :
1) $\alpha v_1, \alpha v_2 \dots \alpha v_R$ soient dans $\mathfrak{N}$
2) $\beta w_1, \beta w_2 \dots \beta w_S$ soient dans $\mathfrak{M}$.
Supposons $\mathfrak{q}$ premier à $\alpha\beta$. Alors $\mathfrak{M}_{\mathfrak{q}} \subset \alpha^{-1}\mathfrak{N}_{\mathfrak{q}}$, $\mathfrak{N}_{\mathfrak{q}} \subset \beta^{-1}\mathfrak{M}_{\mathfrak{q}}$
Mais α^{-1}, β^{-1} sont dans $\mathfrak{A}_{\mathfrak{q}}$. On a donc $\mathfrak{M}_{\mathfrak{q}} = \mathfrak{N}_{\mathfrak{q}}$.

3) Prenons un élément $\sum \alpha_i u_i$ de $\mathfrak{N}_{\mathfrak{q}}$. Pour chaque m on a des décompositions $\alpha_i = \bar{\alpha}_i^{(m)} + \Pi^m \beta_i$, $\bar{\alpha}_i^{(m)} \subset k$, $\beta_i \subset \mathfrak{o}_{\mathfrak{q}}$. (Π représente un élément de $\mathfrak{A}$ divisible par $\mathfrak{q}$). Il existe un entier m_0 tel que si $m > m_0$, les $\Pi^m u_i$ soient dans $\bar{\mathfrak{N}}_{\mathfrak{q}}$. On a alors $\varphi = \lim. \bar{\varphi}_m$ où $\bar{\varphi}_m = \sum \bar{\alpha}_i^{(m)} u_i$ est un élément de $\mathfrak{f}$ qui est dans $\mathfrak{N}_{\mathfrak{q}}$

si $m > m_0$. Il existe d'autre part pour chaque m un entier δ_m de $\mathfrak{H}$ tel que $\delta_m \varphi_m$ soit dans $\mathfrak{M}$. Mettons δ_m sous la forme $\mathfrak{q}^{-1}\mathfrak{r}$. $(\mathfrak{r}, \mathfrak{q}) = 1$. Alors si $\mathfrak{y}$ est un idéal premier $\neq \mathfrak{q}$, il y a un entier δ'_m divisible par $\mathfrak{r}$ et premier à $\mathfrak{q}$, $\delta'_m \varphi_m$ est dans $\tilde{\mathfrak{N}}_{\mathfrak{q}}$ et dans $\mathfrak{M}_{\mathfrak{y}}$, si $\mathfrak{y} \neq \mathfrak{q}$, donc aussi dans presque tous les $\tilde{\mathfrak{N}}_{\mathfrak{y}}$; prenons un entier $\chi_{\mathfrak{y}}$ premier à $\mathfrak{q}$ tel que $\chi_{\mathfrak{y}} \delta'_m \varphi_m$ soit dans $\mathfrak{N}_{\mathfrak{y}}$. Alors $\prod_{\mathfrak{y}} \cdot \chi_{\mathfrak{y}} \cdot \delta'_m \varphi_m = \delta''_m \varphi_m$ est dans $\mathfrak{N}$, et δ''_m est premier à $\mathfrak{q}$. Donc φ_m est dans $\mathfrak{N}_{\mathfrak{q}}$. Comme $\varphi = \lim. \varphi_m$, φ est aussi dans $\mathfrak{N}_{\mathfrak{q}}$.

<u>Conséquences</u>

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

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

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

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

D'autre part, $\mathfrak{a}$ étant toujours bilatère, on a vu que $\mathfrak{a}_\mathfrak{p}$ est de la forme $\mathfrak{p}^{*m_\mathfrak{p}}\mathfrak{o}_\mathfrak{p}$, où $\mathfrak{p}$ est l'idéal premier du corps gauche $\mathfrak{K}_\mathfrak{p}^*$ sur lequel $\mathfrak{S}_\mathfrak{p}$ est algèbre de matrices . Ce corps gauche est contenu dans $\mathfrak{K}_\mathfrak{p}$, et par suite , on peut écrire $\mathfrak{a}_\mathfrak{p} = \bar{\mathfrak{p}}^{m_\mathfrak{p}}\mathfrak{o}_\mathfrak{p}$, où $\bar{\mathfrak{p}}$ est l'idéal bilatère maximum (ou premier) de $\mathfrak{K}_\mathfrak{p}$. On désigne encore par $\bar{\mathfrak{P}}$ l'intersection de $\mathfrak{S}$ avec l'idéal $\bar{\mathfrak{p}}\mathfrak{o}_\mathfrak{p}$ de $\mathfrak{S}_\mathfrak{p}$ et avec tous les $\mathfrak{o}_\mathfrak{q}$ ($\mathfrak{q} \neq \mathfrak{p}$) . C'est l'idéal bilatère premier de $\mathfrak{k}$. On a $\mathfrak{r}_{\mathfrak{y}} = \mathfrak{P}^{m_{\mathfrak{y}}}$. Il résulte de là que : tout idéal bilatère se 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. $\mathfrak{O}$ de $\mathfrak{S}$ est de la forme $\mathfrak{r}\mathfrak{O}$, où $\mathfrak{r}$ est un idéal de $\mathfrak{k}$. Pour chaque idéal premier $\mathfrak{y}$ de k , il y a un idéal premier bilatère $\mathfrak{P}$ de $\mathfrak{S}$, et on a $\mathfrak{y} = \mathfrak{P}^{e_{\mathfrak{y}}}$, où $e_{\mathfrak{y}}$ est le degré du corps gauche semblable à $\mathfrak{S}_{\mathfrak{y}}$.