SÉMINAIRE DE MATHÉMATIQUES

A. WEIL

Corps gauches p-adiques

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. n° 9, p. 1-12

<http://www.numdam.org/item?id=SMJ_1933-1934__1__A9_0>

SEMINAIRE DE MATHEMATIQUES

Première année 1933-1934

Théorie des Groupes et des Algèbres

-I- Corps Gauches $\mathfrak{p}$ - adiques

Exposé fait par M. WEIL, le 16 Avril 1934

D'après des théorèmes connus, tout système hypercomplexe semi-simple sur un corps $\mathcal{G}$ -adique est somme directe de systèmes simples, qui sont à leur tour, représentables comme algèbres complètes de matrices sur des corps gauches dont les centres contiennent le corps $\mathcal{G}$-adique donné . L'étude de ces systèmes se ramène donc à celle des corps gauches sur les corps $\mathcal{G}$-adiques : c'est cette étude que nous allons entreprendre .

I.- Nous désignerons par k un corps $\mathcal{G}$-adique , par K un corps gauche de rang m sur k, c'est à dire que tout élément Ξ de K pourra être mis , d'une manière et d'une seule, sous la forme $\Xi = \xi_1 \Xi_1 + \ldots + \xi_m \Xi_m$, les ξ_i étant dans k, et $\Xi_1 \ldots \Xi_m$ formant une k-base de K . Soit $\varphi(\xi)$ la valeur absolue ($\mathcal{G}$-adique) de ξ dans k ; soit $\mathcal{G} = (\pi)$ l'idéal premier (unique) dans l'anneau des entiers de k, et soit $\varphi(\pi) = w$.

On obtient , comme on sait, une représentation de K par des matrices sur k (représentation régulière) en écrivant $\Xi_i \Xi = \sum_{j=1}^{m} \xi_{ij} \Xi_j$ et en faisant correspondre à Ξ la matrice $\| \xi_{ij} \|$; on sait aussi que Ξ est alors racine de l'équation caractéristique

$$F(\Xi) = \left| \xi_{ij} - \delta_{ij} \Xi \right| = 0 \qquad \left(\delta_{ij} = \begin{matrix} 0 \text{ si } i \neq j \\ 1 \text{ si } i = j \end{matrix} \right)$$

équation de degré m, qui est indépendante de la base $\Xi_1, \ldots \ldots \Xi_m$ choisie ; le terme constant $n\Xi = |\xi_{ij}|$ et le coefficient

de Ξ^{m-1}, s $\Xi = \sum_i \xi_{ii}$, seront appelés respectivement la norme et la trace de Ξ. Il est clair que

$$n(\Xi \cdot \Xi') = n(\Xi) \cdot n(\Xi') .$$

De plus, si K est corps gauche, Ξ est racine, dans k d'un unique polynome irréductible, dont F(x) est une puissance exacte. Soit en effet f(x) le polynome normé, de plus bas degré, à coefficients dans k, dont Ξ soit racine : il est bien irréductible, car sinon, K étant sans diviseurs de zéro, l'un de ses facteurs admettrait la racine Ξ ; soit d son degré. $k(\Xi)$ est alors, dans K, un corps commutatif extension algébrique de k de degré d, et K est, par rapport à $k(\Xi)$, un module (à droite par exemple) de rang $\frac{m}{d}$; soit $A_1, A_2 \ldots A_{\frac{m}{d}}$, une base de ce module : les m éléments $A_\nu \Xi^k$ ($k = 0,1, \ldots, d-1$; $\nu = 1,2 \ldots \frac{m}{d}$) forment une k-base de K, qu'on peut utiliser pour écrire l'équation caractéristique de Ξ : celle-ci apparait bien alors comme $F(x) = \pm [f(x)]^{\frac{m}{d}}$.

2.- Ξ sera dit entier si les coefficients de f(x), ou, ce qui revient au même, ceux de F(x), sont des entiers de k. Posons $\varphi(\Xi) = [\varphi(n\Xi)]^{\frac{1}{m}}$: pour $\Xi = \xi$ dans k, cette fonction coincide bien avec la valeur absolue ; on aura $\varphi(\Xi \cdot \Xi') = \varphi(\Xi)\,\varphi(\Xi')$.

Nous démontrerons les théorèmes suivants :

I°- Pour que Ξ soit entier, il faut et il suffit que $\varphi(\Xi) \leq 1$, c'est à dire que $n\Xi$ soit entier.

2°- Si $\varphi(\Xi) \leq \varphi(\Xi')$, $\varphi(\Xi + \Xi') \leq \varphi(\Xi')$.

La démonstration est la même que dans le cas particulier

où K était commutatif (conférence précédente, prg.9) et s'appuie sur le lemme (ib. prg.8) : un polynome irréductible dans k est irréductible ou puissance de polynome irréductible modulo $\mathfrak{p}$. Alors : I° la condition est évidemment nécessaire ; soit donc, réciproquement, n Ξ entier, et soit π^h le plus petit dénominateur commun des coefficients de F(x) ; si h > 0 , $\pi^h . F(x)$ serait $\equiv x^r . G(x)$ ($\mathfrak{p}$) , x^r et G(x) étant premiers entre eux mod. $\mathfrak{p}$, et r > 0 : F(x) aurait donc, d'après le lemme, deux facteurs premiers entre eux , ce qui est impossible ; par suite, h = 0 et Ξ est entier .

2°- On aura $\varphi\left(\frac{\Xi}{\Xi'}\right) \leq 1$, donc $\frac{\Xi}{\Xi'}$ est entier et son équation caractéristique F(x) = 0 est à coefficients entiers : il en est de même alors de F(x-1)= 0 et $1 + \frac{\Xi}{\Xi'}$ est entier , donc $\varphi\left(1 + \frac{\Xi}{\Xi'}\right) \leq 1$, ou $\varphi(\Xi + \Xi') \leq \varphi(\Xi')$.

Il en résulte d'abord que les entiers de K forment un anneau, contenant l'anneau des entiers de k . Cet anneau est un ordre ; on entend par là tout anneau d'éléments de K contenant l'anneau des entiers de k, et qui possède, par rapport à ce dernier, une base minima de m éléments linéairement indépendants : c'est à dire que l'on peut trouver m éléments de l'anneau, $\Omega_1, \Omega_2, \ldots\ldots, \Omega_m$, formant en même temps une k-base de K, et tel que tout élément de l'anneau soit de la forme $\Omega = \sum_{j=1}^{m} \omega_i \Omega_i$, les ω_i étant des entiers de k . Or, Ξ étant dans K, $\pi^h \Xi$ est entier pour h assez

grand ; on peut donc trouver une k-base de K formée d'entiers $A_1, A_2, \ldots A_m$. Soit alors $A = \sum_{j=1}^{m} \lambda_j A_j$ un entier quelconque ; on aura $s(A_i A) = \sum_{1}^{m} \lambda_j \cdot s(A_i A_j)$: les coefficients de ce système, étant traces d'entiers, sont des entiers de k, et le déterminant $\delta = |s(A_i A_j)|$ est $\neq 0$, car sinon, on pourrait déterminer les λ_j de façon que $s(A_i A) = 0$ pour tout i, donc $s(\Xi A) = 0$ quel que soit Ξ, ce qui est faux, par exemple pour $\Xi = A^{-1}$. Donc on peut résoudre par rapport aux λ_j, et l'on a $\lambda_j = \frac{\alpha_j}{\delta}$, les α_j étant entiers. Tout entier de K est donc de la forme $A = \frac{1}{\delta} \sum_{j} \alpha_j A_j$; il suffit alors de raisonner comme dans la théorie des corps algébriques finis, pour déterminer une base minima de l'anneau des entiers de K.

De plus, il résulte de la définition d'un ordre que tout élément d'un ordre est entier : tout ordre est donc contenu dans l'anneau des entiers : celui-ci est un ordre <u>maximum</u>, et c'<u>est le seul ordre maximum</u> dans K. Nous le désignerons par $\mathcal{V}$ et par $\Omega_1, \Omega_2, \ldots \Omega_m$, une base de $\mathcal{V}$.

3.- $|\log \varphi(\Xi)|$ est toujours un multiple entier de $\frac{1}{m} \log \frac{1}{w}$: soit $\log \frac{1}{W}$ sa plus petite valeur non nulle, et soit Π tel que $\varphi(\Pi) = W$. Appelons <u>unité</u> tout élément E tel que $\varphi(E) = 1$, donc tel que E et E^{-1} soient deux entiers : tout Ξ pourra être mis sous la forme $\Xi = \Pi^h . E$, et h (l'<u>exposant</u> de Ξ) sera déterminé par

$\varphi(\Xi) = W^h$.

Un $\mathcal{V}$-idéal à droite dans K, est un ensemble d'éléments tel que : I°- s'il contient Ξ , Ξ' , il contient aussi $\Xi \pm \Xi'$ et $\Xi . \Omega$, Ω étant un entier quelconque 2°- Il existe un entier α de k tel que $\alpha . \Xi$ soit entier quel que soit Ξ dans l'idéal . De même, pour un idéal à gauche ; un ensemble qui est idéal à gauche et à droite est dit idéal bilatère . Il est clair que les éléments Ω de K pour lesquels $\varphi(\Omega) < 1$ forment, dans $\mathcal{V}$, un idéal bilatère $\mathfrak{p} = (\Pi)$: c'est un idéal premier (même définition que pour les corps commutatifs). Soit $\mathcal{U}$ un idéal à droite : soit $A = \Pi^h E$ l'élément de $\mathcal{U}$ qui ait le plus petit exposant h (il existe, car si h_o est l'exposant du nombre α figurant dans la définition d'un idéal, $h \geq h_o$): tous les éléments H d'exposant $\geq h$ sont dans $\mathcal{U}$, car $\Xi^{-1} . H$ est entier ; donc $\mathcal{U} = \mathfrak{p}^h = (\Pi^h)$: tout idéal dans K est puissance de $\mathfrak{p}$, et par suite bilatère et principal . En particulier, l'idéal $\mathfrak{y} = (\pi)$ sera $= \mathfrak{p}^e$: e s'appellera l'ordre de ramification de $\mathfrak{y}$ dans K .

Soit k^* le corps des classes de restes de k mod. $\mathfrak{y}$: c'est un champ de Galois à q éléments . Soit K^* l'anneau des classes de restes des entiers de K mod. $\mathfrak{p}$; de l'existence d'une base minima $\Omega_1, \Omega_2 \ldots\ldots \Omega_n$, de $\mathcal{V}$, il résulte que K^* est un k^*-module fini de rang $f \leq m$, donc il contient q^f éléments ; $\mathfrak{p}$ étant premier, K^* est sans diviseurs de zéro : c'est un corps fini , et par suite(d'a-

près un théorème de Wedderburn) il est commutatif, extension algébrique de degré f de k^* . f est appelé le <u>degré relatif</u> de $\mathfrak{p}$ par rapport à k.

4.- Soit $\Xi = \sum_{i=1}^{m} \xi_i \Omega_i$; pour que $\Xi \equiv 0 \ (\mathfrak{p}^h)$ il faut et il suffit que $\pi^{-h}\Xi$ soit entier , donc (puisque les Ω_i forment une base de $\mathfrak{o}$) que les $\pi^{-h}\xi_i$ soient entiers, ou bien que $\xi_i \equiv 0 \ (\mathfrak{p}^h)$: en particulier, on obtient , dans $\mathfrak{o}$, un système complet de restes mod. $\mathfrak{p}$ en donnant à chacun des ξ_i q valeurs incongrues mod. $\mathfrak{p}$. donc il y a , dans K, q^m entiers incongrus mod. $\mathfrak{p}$. D'autre part, la convergence étant définie dans K au moyen de la valeur absolue φ (exactement comme dans les corps $\mathfrak{p}$ -adiques) on voit que la condition nécessaire et suffisante pour qu'une suite de Ξ dans K converge vers une limite est que chacune des "coordonnées" ξ_i tende vers une limite . Il en résulte pour K, un "principe de Bolzano" .

De ce qui précède résulte encore la possibilité de développer tout Ξ dans K en série suivant les puissances croissantes de Π . Si Ξ est entier, on aura :

$$\Xi = A_0 + \Pi A_1 + \Pi^2 A_2 + \ldots\ldots + \Pi^{\nu} A_{\nu} + \ldots\ldots$$

et l'on obtiendra tous les entiers une fois et une seule en donnant à chacun des coefficients A_ν les q^f valeurs d'un système complet de restes mod. $\mathfrak{p}$. Si Ξ est quelconque, d'exposant h, on aura : $\Xi = \sum_{\nu=0}^{\infty} \Pi^{h+\nu} A_\nu$.

En particulier, on obtiendra , dans K, un système com-

plet de restes mod. $\mathfrak{p} = \mathfrak{P}^e$ en donnant à chacun des A_ν , dans l'expression $A_0 + \Pi A_1 + \ldots\ldots + \Pi^{e-1} A_{e-1}$, q^f valeurs incongrues mod. $\mathfrak{P}$: on obtient ainsi $(q^f)^e$ valeurs, et l'on voit que l'on a : $e f = m$.

5.- Nous n'avons rien supposé, jusqu'ici, sur le centre de K; et, par exemple, tous nos résultats comprenaient comme cas particulier ceux de la conférence précédente, où K était commutatif, c'est à dire son propre centre . Mais le centre de K est une extension algébrique finie de k, donc encore un corps $\mathfrak{p}$-adique, et nous pouvons supposer, sans diminuer la généralité, que l'on a pris pour corps de base k ce centre même .

k étant donc désormais le centre de K, l'on sait que le rang m est un carré parfait $m = n^2$, et que tout corps commutatif contenu dans K est une extension algébrique de k de degré $\leq n$.

K^* étant extension de k^* de degré f, soit H^* un élément générateur de cette extension, de sorte que $K^* = k^*(H^*)$; H^* sera reste mod. $\mathfrak{P}$ d'un entier H de K, racine d'une équation irréductible dans k de degré $\geq f$ (sinon H^* serait a fortiori de degré $< f$ sur k^*) , mais nécessairement $\leq n$. Donc $f \leq n$.

D'autre part, dans le corps $k(\Pi)$, contenu aussi dans K, $\mathfrak{p}$ a un ordre de ramification $\geq e$, donc ce corps est de degré $\geq e$ sur k , d'où $e \leq n$. Mais $e.f = n^2$, d'où $\underline{e = f = n}$.

$k(H)$ est donc de degré n sur k ; tout entier de K est congru à un entier de $k(H)$ module $\mathfrak{P}$: le degré relatif de l'idéal premier de $k(H)$ par rapport à k est donc n; l'ordre de ramification de $\mathfrak{p}$ dans $k(H)$ est alors $\frac{n}{n} = 1$, et l'idéal premier de $k(H)$ n'est autre que $\mathfrak{p}$. On dit que $k(H)$ est un corps d'inertie de K.

Le corps des classes de restes de $k(H)$ mod. $\mathfrak{p}$, qui n'est autre que K^* , est un champ de Galois dont les q^n éléments sont, comme on sait, les racines de la congruence $x^{q^n} - x \equiv 0 \ (\mathfrak{p})$. Mais , par le lemme déjà cité (prg.8 de la conférence précédente), qui est applicable au corps commutatif $k(H)$, le polynome $x^{q^n} - x$, qui est décomposable modulo $\mathfrak{p}$ en q^n facteurs linéaires premiers entre eux, possède dans le corps $k(H)$ q^n racines distinctes . En particulier, on peut supposer que l'on a pris pour H l'une quelconque de ces racines, de degré n par rapport à k, et par exemple, une racine primitive $(q^n - 1)$ème de l'unité . Soit donc $\phi(x)$ l'un quelconque des facteurs de degré n de $x^{q^n} - x$, irréductibles dans k, qui ait pour racine une telle racine primitive H : ses autres racines, les conjugués de H , seront H^q , H^{q^2} , ... $H^{q^{n-1}}$; le groupe de Galois de $k(H)$ sur k sera cyclique, engendré par la substitution ($H \to H^q$) : c'est le même que celui de K^* sur k^* . Les H^ν ($\nu = 1, 2 \ldots q^n - 1$) forment un système complet de restes $\not\equiv 0$ (mod. $\mathfrak{p}$) dans $k(H)$, ou

dans K, et parmi eux les $H^{\nu\frac{q^n-1}{q-1}}$ ($\nu = 1;2 \ldots\ldots q-1$) forment un système complet de restes $\not\equiv 0$ (mod. $\mathfrak{y}$) dans k (ils sont bien dans k, car le polynome $x^q - x$ a q racines distinctes dans k^* , donc dans k, et k contient bien toutes les racines (q-1)ièmes de l'unité).

Démontrons encore que <u>toute unité $\mathcal{E}$ dans k est norme d'une unité E dans k(H)</u> . On aura en effet : $\mathcal{E} \equiv H^{\nu\frac{q^n-1}{q-1}}$ ($\mathfrak{y}$) , avec $1 \leq \nu \leq q-1$. Considérons H^ν et ses conjugués, $H^{\nu q}, H^{\nu q^2} \ldots\ldots H^{\nu q^{n-1}}$: ils sont tous distincts, ce sont les racines d'une équation irréductible dans k, $x^n + \alpha_1 x^{n-1} + \ldots\ldots + \alpha_{n-1} x + \alpha_n = 0$.
Mais $\alpha_n = n(H^\nu) = H^{\nu\frac{q^n-1}{q-1}} \equiv \mathcal{E}$ ($\mathfrak{y}$) .
Considérons alors l'équation $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_{n-1} x + \mathcal{E} = 0$ elle possède n facteurs linéaires premiers entre eux dans K^* donc, d'après le lemme, dans k(H) ; soit E l'une de ses racines dans k(H) , on aura bien $n E = \mathcal{E}$.

Enfin, observons que dans le développement en série d'un entier quelconque de K :

$$\Omega = A_0 + \Pi A_1 + \Pi^2 A_2 + \ldots\ldots + \Pi^\nu A_\nu + \ldots\ldots$$

on peut prendre tous les A_ν égaux, soit à 0, soit à une puissance de H . Il en résulte en particulier que tout élément de K échangeable avec Π et H appartient au centre k.

6.- k(H) étant corps commutatif maximum dans K, il résulte des théorèmes généraux que c'est un corps de <u>décomposition</u> pour K ; et l'on en déduit la représentation de

K comme produit croisé . Nous allons retrouver ces résultats directement .

En effet, la transformation ($\Lambda \to \pi \Lambda \pi^{-1}$) laisse k invariant, et transforme toute classe mod. $\mathfrak{p}$ en classe mod. $\mathfrak{p}$, elle engendre donc un automorphisme du groupe de Galois de K^* sur k^* et l'on a : $\pi^\nu . H . \pi^{-\nu} \equiv H^{q^r} \ (\mathfrak{p})$ d'où $\pi^\nu . H . \pi^{-\nu} \equiv H^{q^{\nu r}} \ (\mathfrak{p})$: en particulier, $\pi^\nu . H . \pi^{-\nu} \equiv H \ (\mathfrak{p})$ si $\nu r \equiv 0 \ (n)$, et dans ce cas seulement ; soit ν_0 la plus petite solution de cette congruence .

Nous allons déterminer un élément $\pi' = \pi + \pi^2 A_2 + \ldots + \pi^\nu A_\nu + \ldots$ de façon que l'on ait $\pi' . H . \pi'^{-1} = H^{q^r}$, c'est à dire $\pi' . H = H^{q^r} \pi'$. Posons , pour cela, $\pi_\nu = \pi + \pi^2 A_2 + \ldots + \pi^\nu A_\nu$, et supposons que l'on ait déterminé $A_2 , A_3 , \ldots A_\nu$ de façon que $\pi_\nu H \equiv H^{q^r} \pi_\nu \ (\mathfrak{p}^{\nu+1})$ montrons alors que l'on pourra déterminer $A_{\nu+1} = A$ satisfaisant à l'équation :

$$(\pi_\nu + \pi^{\nu+1} A) H \equiv H^{q^r} (\pi_\nu + \pi^{\nu+1} A) \quad (\mathfrak{p}^{\nu+2})$$

ou bien :

$$A H - \pi^{-\nu-1} H^{q^r} \pi^{\nu+1} . A \equiv \pi^{-\nu-1} (H^{q^r} \pi_\nu - \pi_\nu H) \quad (\mathfrak{p})$$

Mais, puisque K^* est commutatif, $AH = HA \ (\mathfrak{p})$; d'ailleurs $\pi^{-\nu-1} H^{q^{\nu+1}} \pi^{\nu+1} \equiv H^{q^{-\nu-1}} \ (\mathfrak{p})$, d'où :

$$(H - H^{q^{-\nu-1}}) A \equiv \pi^{-\nu-1} (H^{q^r} \pi_\nu - \pi_\nu H) \quad (\mathfrak{p})$$

Cette équation détermine bien A , sauf si $\nu = 0 \ (\nu_0)$. Mais dans ce cas, elle est identiquement vérifiée, et l'on peut prendre A quelconque .

Car alors $\pi^\nu H \pi^{-\nu} \equiv H \ (\mathfrak{p})$, ou $\pi^\nu H \equiv H \pi^\nu \ (\mathfrak{p}^{\nu+1})$.
De plus, soit $\pi_\nu \cdot H \cdot \pi_\nu^{-1} = H^{q^r} + \pi^\nu \Omega$; en élevant les deux membres à la puissance q^n , on aura :

$$\pi_\nu \cdot H \cdot \pi_\nu^{-1} \equiv H^{q^r} + \sum_{\lambda+\mu=q^n-1} (H^{q^r})^\lambda \cdot \pi^\nu \Omega \cdot (H^{q^r})^\mu \ (\mathfrak{p}^{\nu+1})$$

d'où puisque $\pi^\nu H \equiv H \pi^\nu \ (\mathfrak{p}^{\nu+1})$.
et $\Omega H \equiv H \Omega \ (\mathfrak{p})$:

$$\pi_\nu H \pi_\nu^{-1} \equiv H^{q^r} + q^n \cdot \pi_\nu \Omega \cdot H^{q^r(q^n-1)} \equiv H^{q^r} \ (\mathfrak{p}^{\nu+1})$$

puisque $q \equiv 0 \ (\mathfrak{p})$.

Remplaçons alors, une fois pour toutes, π par π' . Nous aurons $\pi \cdot H \cdot \pi^{-1} = H^{q^r}$. d'où $\pi^{\nu_0} \cdot H \cdot \pi^{-\nu_0} = H$: π^{ν_0} sera échangeable avec H , et, bien entendu , avec π ; il appartiendra donc à k . D'ailleurs le corps $k(\pi)$ doit être de degré n sur k, par suite $\nu_0 = n$, et r est premier avec n ; puisque d'ailleurs ~~par suite~~, $\mathfrak{y} = \mathfrak{p}^n$, on aura $\pi^n = \varepsilon \pi^{-1}$, ε étant une unité de k . Mais alors, ε est norme d'une unité E de $k(H)$, produit de E par ses conjugués E', E" ..... $E^{(n-1)}$. Remplaçons π par $\pi_1 = \pi E$: on aura encore $\pi_1 H \pi_1^{-1} = H^{q^r}$, et $\pi_1^n = (\pi E)^n = \pi^n . E E' E'' \ldots . E^{(n-1)} = \pi$. Nous obtenons le résultat final suivant :

Soit k un corps $\mathfrak{y}$-adique, $\mathfrak{y} = (\pi)$ son idéal premier q le nombre de classes de restes de k mod. $\mathfrak{y}$. et H une racine primitive (q^n-1) ièmes de l'unité, de degré n sur k . Tout corps gauche de rang $m = n^2$ sur le centre k peut être représenté comme produit croisé sur $k(H)$, engendré par

un élément Π satisfaisant aux relations :

$$\Pi^n = \pi \quad , \qquad \Pi . H . \Pi^{-1} = H^{q^r} ,$$

r étant un nombre quelconque premier à n.

Soit s tel que $r.s \equiv 1 \ (n)$: on peut encore engendrer K au moyen de l'élément $P = \Pi^s$, satisfaisant aux relations $P^r = \pi^s$, $P . H . P^{-1} = H^q$.

Autrement dit, si l'on désigne par σ l'automorphisme $(H \to H^q)$ générateur du groupe de Galois de $k(H)$ sur k, K est produit croisé $(K(H), \sigma, \pi^s)$; s peut prendre toutes les valeurs premières à n . En utilisant la notion de produit de classes d'algèbres sur k, on voit que ces classes forment un groupe cyclique .

BIBLIOGRAPHIE

1. Hensel , passim, et en particulier Eine neue Théorie der algebraischen Zahlen, Math.Zeitschr.2 (1918).

2. Hasse, Ueber $\mathfrak{p}$-adische Schiefkörper ... Math. Ann. 104 (1931)

3. Artin, Ueber die Bewertungen algebraischer Zahlkörper K J de Crelle t.167 .

4. Chevalley, Thèse , Chap. V .