

LE SÉMINAIRE DE MATHÉMATIQUES 1933–1939

édition réalisée et annotée par
Michèle Audin

5. Année 1937-1938 *Fonctions algébriques*

Claude Chevalley

La théorie algébrique des fonctions algébriques – I

Séminaire de mathématiques (1937-1938), Exposé 5-CD, 17 p.

<http://books.cedram.org/MALSM/SMA_1937-1938__5__CD_0.pdf>



Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 3.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/3.0/fr/>

cedram

Exposé mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

LA THÉORIE ALGÈBRIQUE DES FONCTIONS ALGÈBRIQUES – I

par Claude Chevalley

Dans^{[1][2]} les deux précédentes conférences, on a étudié, avec les moyens de l'analyse, les corps de fonctions algébriques construits à partir du corps des nombres complexes pris comme corps des constantes.^[3] Nous allons maintenant revenir sur cette théorie du point de vue algébrique. Les avantages qu'il y a à opérer ainsi sont de plusieurs espèces :

- 1) on met en lumière le caractère algébrique des notions étudiées, et on n'utilise, pour les démonstrations, que des moyens purement algébriques ;
- 2) on permet la généralisation, et notamment l'étude des fonctions algébriques obtenues en prenant un corps quelconque comme corps de constantes, étude qui doit être intéressante du point de vue de la recherche des propriétés arithmétiques des courbes algébriques.

Avant de commencer cette étude, nous avons besoin de rappeler un certain nombre de points de la théorie abstraite des corps.

Théorie générale des corps

1. – Théorie des polynômes. k étant un corps quelconque, on peut développer la théorie des polynômes à coefficients dans k par rapport à un certain nombre de variables x_1, x_2, \dots, x_n . Étant donné deux polynômes, P, Q , il existe un polynome D qui les divise et qui est divisible par tout diviseur commun à P et à Q ; D est déterminé par ces conditions à une constante multiplicative près ; on l'appelle un p.g.c.d. de P et Q . Il résulte de là que tout polynome peut être décomposé en facteurs irréductibles (c'est-à-dire en polynômes n'admettant plus de décomposition non triviale), et ceci d'une seule manière, à des constantes multiplicatives près.

Dans le cas où $n = 1$, on a de plus le fait que D peut se mettre sous la forme $UP + VQ$, U et V étant de nouveaux polynômes. En particulier, si P et Q sont premiers entre eux, on peut mettre 1 et par suite n'importe quel polynome, sous la forme $UP + VQ$.

$f(x)$ étant un polynome, a est appelé un *zéro* de $f(x)$ si $f(a) = 0$. Dans ce cas $f(x)$ est divisible par $x - a$. S'il est divisible par $(x - a)^r$, mais non par $(x - a)^{r+1}$, r est appelé l'ordre du zéro a . Si $r > 1$, on dit que a est un zéro multiple. Dans ce cas, a est un zéro du dérivé $f'(x)$ de $f(x)$, défini comme étant le coefficient de t dans $f(x + t)$.

Quand on opère sur un corps quelconque comme corps des coefficients, il faut distinguer soigneusement la notion de polynome de celle de la fonction représentée par le polynome : nous verrons que dans certain cas, un polynome non nul peut prendre la valeur 0 quelles que soient les valeurs données aux variables.

2.— Extensions. k étant un corps, on appelle *extension* de k la notion complexe composée d'un corps K et d'une isomorphie I_k de k avec un sous-corps de K , que nous désignerons par k^* . Une extension devra donc se représenter en principe par un symbole de la forme (K, I_k) . On emploie souvent la notation défectueuse K/k ; l'emploi de cette notation sera de règle lorsqu'on supposera que I_k est l'isomorphisme identique, de sorte que $k \subset K$.

Les extensions (K, I_k) , (K', I'_k) de k ne seront considérées comme identiques que si $K = K'$ et $I_k = I'_k$. Plus importante est la notion d'*isomorphie* : les extensions précédentes seront dites isomorphes s'il existe une isomorphie J de K avec K' telle que $I'_k = JI_k$. Si L est un sous-corps de K contenant k , l'extension (L, I_k) sera dite contenue dans (K, I_k) .

E étant un ensemble d'éléments de K , on désignera par $k^*(E)$ le plus petit sous-corps de K contenant k^* et E . Quand cela ne risque pas d'entraîner de confusion, ce corps pourra aussi se noter $k(E)$. On dit qu'il résulte de l'adjonction à k des éléments de E . De même, on dit que l'extension $(k^*(E), I_k)$ est engendrée par les éléments de E .

Une extension est dite *simple* quand elle peut être engendrée par un seul élément.

L'isomorphie I_k fait correspondre à tout polynome f à coefficients dans k un polynome f^* à coefficients dans K . Si un élément de K est un zéro de f^* , on dit aussi (improprement) qu'il est zéro de f . Si un élément de K est zéro d'un polynome à coefficients dans k , on dit qu'il est algébrique sur k ; s'il en est ainsi de tous les éléments de K , on dit que l'extension (K, I_k) est algébrique; sinon, qu'elle est transcendante.

Nous aurons à considérer plus particulièrement trois sortes d'extensions d'un corps k :

- 1) les extensions transcendantes simples : on démontre que tout corps possède une extension transcendante simple, et une seule à une isomorphie près ;
- 2) les extensions algébriques simples : une telle extension est engendrée par un zéro d'un polynome irréductible dans k ; inversement, f étant un polynome irréductible dans k , on peut toujours former une extension algébrique de k qui soit engendrée par un zéro de f . Nous appellerons une telle extension, *extension de dislocation* de f .^[4] Elle est déterminée à une isomorphie près par la donnée de f .

3) f étant un polynome quelconque de degré > 0 à coefficients dans k , on peut former une extension de k engendrée par des zéros de f et dans laquelle f se décompose en facteurs linéaires. Une pareille extension est dite *extension de décomposition* de f ; elle est déterminée à une isomorphie près par la donnée de f .

4/5

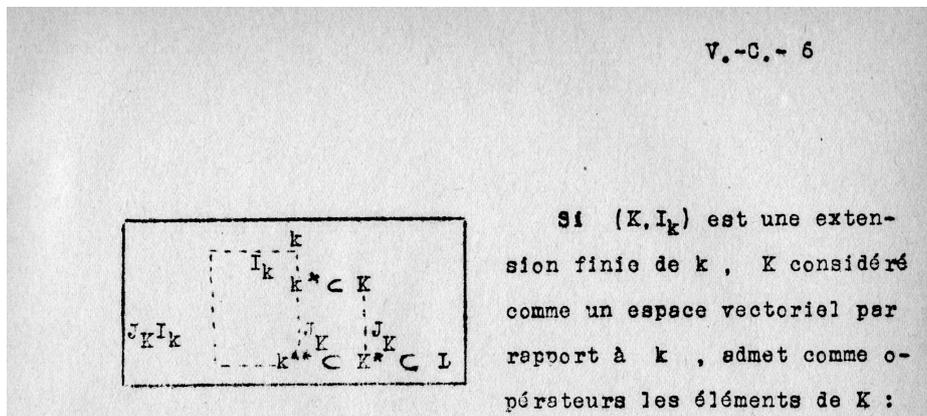
Se donner une extension (K, I_k) de k conduit à considérer les éléments de k comme des opérateurs de K (puisque les éléments de $k^* = I_k k$ sont contenus dans K). K se trouve ainsi muni d'une structure d'espace vectoriel par rapport à k . La dimension (finie ou infinie) de cet espace vectoriel s'appelle le *degré* de l'extension et se note $(K : k)$ (ce nombre est bien déterminé par les données de K et de k^* , mais non par celles de K et de k). Une extension de degré fini s'appelle finie. Toute extension finie est algébrique, et est isomorphe à une extension contenue dans une extension de décomposition d'un polynome f de k . Par contre, une extension finie n'est pas toujours simple (cf. la suite). Une extension de dislocation d'un polynome irréductible f a pour degré le degré de f .

(K, I_k) étant une extension de k , soit (L, J_K) une extension de K . Alors le symbole (L, J_K, I_k) définit une extension de k (cf. schéma ci-joint, page suivante). Le degré $(L : k)$ de cette extension est donné par la formule

$$(L : k) = (L : K)(K : k)$$

Si (K, I_k) est une extension finie de k , K considéré comme un espace vectoriel par

5/6



rapport à k , admet comme opérateurs les éléments de K : autrement dit, il fournit une représentation de K . Si on choisit une base de K par rapport à k , on obtient une représentation de K , par des matrices à coefficients dans k . Si A_α est la substitution linéaire qui correspond à un élément α de K , le polynome caractéristique f de A_α est appelé *polynome caractéristique* de α . C'est une puissance du polynome irréductible de k admettant α pour zéro.

Le déterminant de A_α s'appelle la *norme* de α , prise de K à k . On le désigne par $N_{K/k}(\alpha)$. On a donc :

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha)N_{K/k}(\beta).$$

La trace de A_α s'appelle la *trace* de α , prise de K à k . On la désigne par $S_{K/k}(\alpha)$.^[5] On a donc :

$$S_{K/k}(\alpha + \beta) = S_{K/k}(\alpha) + S_{K/k}(\beta).$$

Si (L, J_K) est une extension de K , et si $\gamma \in L$ on a :

$$N_{L/k}(\gamma) = N_{K/k}(N_{L/K}(\gamma)) \quad S_{L/k}(\gamma) = S_{K/k}(S_{L/K}(\gamma))$$

6/7

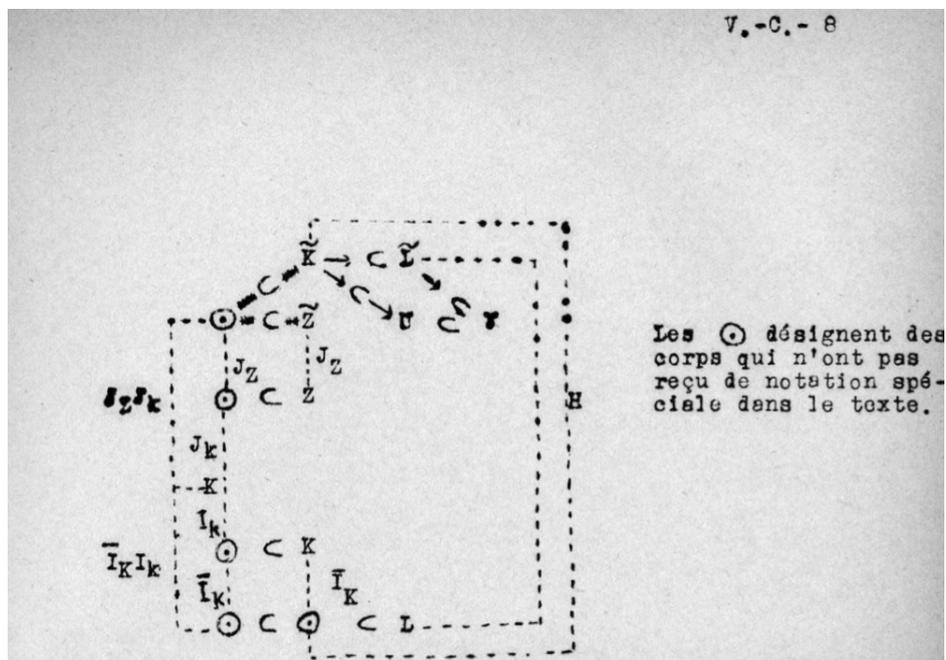
3.— Extensions composées. Considérons deux extensions (K, I_k) et (Z, J_k) d'un corps k . U étant un corps, supposons données des isomorphismes I_K, J_Z de K et de Z avec des sous-corps \tilde{K}, \tilde{Z} de U , telles que $U = \tilde{K}\tilde{Z}$ (c'est-à-dire que U soit le plus petit corps contenant \tilde{K} et \tilde{Z}), et que les isomorphismes $I_K I_k$ et $J_K J_k$ de k dans U soient identiques. Nous dirons alors que les données de U, I_K, J_Z déterminent une *extension composée* des extensions (K, I_k) et (Z, J_k) . Nous désignerons cette extension composée par le symbole (U, I_K, J_Z) .

Les extensions composées (U, I_K, J_Z) et (U', I'_K, J'_Z) seront dites isomorphes s'il existe une isomorphie G de U dans U' telle que $GI_K = I'_K$ et $GJ_Z = J'_Z$.

Nous n'aurons à nous servir de la notion d'extension composée que dans le cas où l'une au moins des extensions $(K, I_k), (Z, J_k)$ est finie ; supposons par exemple, qu'il en soit ainsi de la première. Il existe alors un polynome g à coefficients dans k tel que l'extension (K, I_k) soit engendrée par des zéros de g . Formons alors sur K et sur Z des extensions (L, \bar{I}_K) et (V, \bar{J}_Z) de décomposition de g . En vertu du choix de g , (L, \bar{I}_K, I_k) est une extension de décomposition de g sur k . D'autre part les zéros de g dans V engendrent sur k une extension de décomposition (L, \bar{J}_Z, J_k) de g . Nous avons donc deux extensions de décomposition de g sur k : nous savons qu'elles sont isomorphes. Or la première contient une extension de k isomorphe à (K, I_k) ; il en résulte qu'il existe une isomorphie H de (K, I_k) avec une extension contenue dans (V, \bar{J}_Z, J_k) . Posons $\tilde{K} = HK$, et $\tilde{Z} = J_Z Z$; soit $U = \tilde{K}\tilde{Z}$ le plus petit sous-corps de V contenant K et Z . Le symbole (U, H, \bar{J}_Z) représente une extension composée des extensions (K, I_k) et (Z, J_k) .

D'autre part, $L, V, \bar{I}_K, \bar{J}_Z$ étant fixés, il n'y a qu'un nombre fini d'isomorphismes H , car g n'a qu'un nombre fini de zéros. Soient H_i ($1 \leq i \leq s$) ces isomorphismes, et U_i les corps U correspondants. Nous allons montrer que toute extension composée (U', I'_K, J'_Z) des extensions données est isomorphe à l'une des (U, H_i, \bar{J}_Z) . Formons, en effet, sur U' une extension (V', J'_U) de décomposition de g . Alors $(V', J_{U'} J'_Z)$ est une extension de décomposition de g sur Z , donc isomorphe à (V, \bar{J}_Z) . Il existe donc une isomorphie G de V' avec V telle que $GJ_{U'} J'_Z = \bar{J}_Z$. L'extension $(GJ_{U'} I'_K K, GJ_{U'} I'_K I_k)$ est une extension de k isomorphe à (K, I_k) et contenue dans l'extension (V, \bar{J}_Z, J_k) (on

8/9



notera que $I'_K I_k = J'_Z J_k$ par hypothèse). Donc $GJ_{U'} I'_K$ est l'une des isomorphies H_i . Il en résulte que $GJ_{U'}$ est une isomorphie entre (U', I'_K, J'_Z) et (U_i, H_i, \bar{J}_Z) ce qui démontre notre assertion.

Il en résulte que si (K, I_k) est finie, il n'y a qu'un nombre fini de types d'extensions composées de (K, I_k) et (Z, J_k) .

4.- La caractéristique. k étant un corps, désignons par 1 son unité multiplicative. Deux circonstances peuvent se présenter : ou bien la somme de n éléments égaux à 1 n'est jamais nulle (n entier positif) : on dit alors que le corps est de caractéristique 0 ; - ou bien, on peut avoir $n \cdot 1 = 0$; dans ces conditions, le plus petit entier positif p pour lequel $p \cdot 1 = 0$ est un nombre premier que l'on appelle caractéristique du corps. 9/10
 a étant un élément quelconque du corps, la somme de p éléments égaux à a est nulle.

Deux corps dont l'un est contenu dans l'autre ont évidemment même caractéristique. Tout corps de caractéristique 0 contient un corps isomorphe au corps des nombres rationnels et est par suite infini. Si p est un nombre premier, la famille des classes de restes d'entiers (mod. p) donne un corps fini de caractéristique p ; tout corps de caractéristique p contient un corps isomorphe à celui-là.

Dans un corps de caractéristique p , on a la formule remarquable $(a + b)^p = a^p + b^p$. Jointe à la formule évidente $(ab)^p = a^p b^p$, elle montre que la correspondance $a \rightarrow a^p$ est une isomorphie du corps k avec un corps qui y est contenu. Nous désignerons par σ cette isomorphie et nous l'appellerons l'endomorphie fondamentale de k ; si k est

de caractéristique 0, nous désignerons par σ la transformation identique. E étant un ensemble, nous désignerons par E^σ son image par σ .

5. – Corps parfaits. Extensions séparables. Nous dirons que le corps k est *parfait* si $k^\sigma = k$. Il résulte de là que tout corps de caractéristique 0 est parfait ; il en est de même des corps finis (puisque k^σ a autant d'éléments que k). Par contre, on voit facilement que le corps $k(x)$ qui résulte de l'adjonction à un corps k de caractéristique $p \neq 0$ d'une transcendante x , n'est pas parfait.

Une extension K/k , de degré fini, est dite *séparable* si $K = k(K^\sigma)$. En tenant compte de ce que $(K^\sigma : k^\sigma) = (K : k)$, on voit que toute extension finie d'un corps parfait est séparable.

Si K/k est une extension séparable, de degré fini, et si L est un corps intermédiaire entre k et K , les extensions K/L et L/k sont séparables. Pour la première, c'est évident ; pour la seconde, cela résulte de la formule

$$(K : k(L^\sigma)) = (k(K^\sigma) : k(L^\sigma)) \leq (K^\sigma : L^\sigma) = (K : L).$$

α étant un élément algébrique par rapport à k soit $f(X)$ le polynôme irréductible dans k admettant α pour zéro. Nous allons montrer qu'une condition nécessaire et suffisante pour que $k(\alpha)/k$ soit séparable est que α soit zéro simple de $f(x)$.

En effet, si α est zéro multiple de $f(x)$, on a $f'(\alpha) = 0$. f étant irréductible, cela n'est possible que si $f'(x) = 0$, c'est-à-dire si $f(x)$ peut se mettre sous la forme $g(x^p)$, g étant un polynôme de degré plus petit que celui de f et p la caractéristique de k . On a alors $g(\alpha^p) = 0$, d'où $(k(\alpha^p) : k) < (k(\alpha) : k)$. Or, si on pose $k(\alpha) = K$, on a $k(\alpha^p) = k(K^\sigma)$: l'extension K/k n'est donc pas séparable dans le cas envisagé. Si, au contraire, α est zéro simple de $f(x)$, $x - \alpha$ est p.g.c.d. de $f(x)$ et de $(x - \alpha)^p = x^p - \alpha^p$, d'où $\alpha \in k(\alpha^p)$, et $k(K^\sigma) = K$.

D'autre part, si une extension K/k de k , de degré fini, se met sous la forme $k(E)$, une condition nécessaire et suffisante pour que E/k soit séparable est que, pour tout $\alpha \in E$, $k(E)/k$ soit séparable. La condition est évidemment nécessaire ; inversement, si elle est remplie, on a $k(E^\sigma) = k(E) = K$; comme $k^\sigma(E^\sigma) = K^\sigma$ on a aussi $k(K^\sigma) = K$.

Les deux précédents résultats permettent de reconnaître si une extension est séparable dès qu'on connaît un système de générateurs de cette extension. On voit notamment que toute extension algébrique finie d'un corps parfait est séparable. Par contre, si k n'est pas parfait, et si $a \in k \rightarrow k^\sigma$, l'extension $k(\sqrt[p]{a})/k$ n'est pas séparable. Par suite, une condition nécessaire et suffisante pour qu'un corps soit parfait est que toutes ses extensions finies soient séparables. On en déduit tout de suite que toute extension algébrique (finie ou non) d'un corps parfait est un corps parfait.

K étant une extension finie du corps k , formons la suite

$$K = k(K^{\sigma^0}), k(K^\sigma), k(K^{\sigma^2}), \dots, k(K^{\sigma^n}), \dots$$

Ces corps sont emboîtés les uns dans les autres ; il en résulte qu'il existe un entier

f tel que $k(K^{\sigma^f}) = k(K^{\sigma^{f+1}})$. Tous les corps de la suite à partir du rang f sont alors identiques. L'entier f étant choisi le plu petit possible, on l'appelle l'*exposant* de l'extension K/k . L'extension $k(K^{\sigma^f})/k$ est séparable : son degré n est appelé *degré réduit* de l'extension K/k . On voit tout de suite que $(k(K^{\sigma^i}) : k(K^{\sigma^{i+1}}))$ est une puissance de p ; il en résulte que le degré de l'extension K/k est de la forme np^{f+x} ($x \geq 0$).

6. – Extensions simples. Une extension K/k du corps k est dite *simple* si K résulte de l'adjonction à k d'un seul élément. Nous nous proposons de démontrer le théorème suivant :

K/k étant une extension algébrique finie de degré réduit n et d'exposant f , une condition nécessaire et suffisante pour qu'elle soit simple est que $(K : k) = np^f$ (p étant la caractéristique de k ; remplacer p^f par 1 si $p = 0$).

Nous poserons au cours de la démonstration $k(K^{\sigma^i}) = K_i$ ($1 \leq i \leq f$), $K_0 = K$.

1) Si $K = k(\alpha)$, on a $K_i = k(\alpha^{p^i})$; on en déduit $(K_i : K_{i+1}) = p$ et par suite $(K : k) = np^f$, ce qui démontre que la condition est nécessaire. 13/14

2) Pour montrer qu'elle est suffisante, supposons d'abord que k contienne une infinité d'éléments. Soient α, β deux éléments de K , zéros de polynômes irréductibles $f(x), g(x)$ dans k . Soient, dans une extension algébrique convenable de k , $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$, les zéros distincts de f , $\beta_1 = \beta, \beta_2, \dots, \beta_s$ ceux de g . Nous allons montrer que, si $k(\beta)/k$ est une extension séparable, on peut choisir un $a \in k$ tel qu'en posant $\vartheta = \alpha + a\beta$ on ait $k(\alpha, \beta) = k(\vartheta)$. En effet, choisissons a de telle manière que les rs éléments $\alpha_i + a\beta_j$ ($1 \leq i \leq r, 1 \leq j \leq s$) soient tous distincts les uns des autres. Le polynôme $f(\vartheta - ax)$ admet le zéro β , mais n'a aucun autre zéro commun avec $g(x)$. Comme β est zéro simple de $g(x)$, $x - \beta$ est un p.g.c.d. de $f(\vartheta - ax)$ et de $g(x)$. On a donc $\beta \in k(\vartheta)$, d'où $\alpha = \vartheta - a\beta \in k(\vartheta)$, ce qui démontre la proposition.

Ceci dit, choisissons dans $K - K_1$ (dans K si $f = 0$) un élément α pour lequel $(k(\alpha) : k)$ soit aussi grand que possible. Si $\beta \in K_f$, l'extension $k(\beta)/k$ est séparable, et par suite $k(\alpha, \beta)/k$ est simple ; en vertu du choix de α , il en résulte $k(\alpha, \beta) = k(\alpha)$, $\beta \in k(\alpha)$, $k(\alpha)$ contient K_f . Montrons qu'il est impossible qu'il existe un $i < f$ tel que $k(\alpha)$ contienne K_{i+1} mais non K_i . En effet, en tenant compte de ce que $(K : K_1)$ égale p et de ce que $\alpha \in K_1$, on voit que $K = K_1(\alpha)$, d'où $k(K^\sigma, \alpha) = K$. On en déduit $k^{\sigma^i}(K^{\sigma^{i+1}}, \alpha^{p^i}) = K^{\sigma^i}$, et par suite $K_i = k(K_{i+1}, \alpha^{p^i})$, ce qui prouve notre assertion. On a donc $K_0 = K \subset k(\alpha)$. 14/15

Remarque. Il nous a suffi pour démontrer la réciproque dans le cas où k est de caractéristique $p \neq 0$, de supposer $(K : k(K^\sigma)) = p$; cette condition est donc équivalente à la condition $(K : k) = np^f$. Elle est notamment toujours remplie

si $(k : k^\sigma) = p$. Par suite : si k est un corps parfait, et si x est transcendant sur k , toute extension finie de $k(x)$ est simple.

- 3) Si k est fini, il en est de même de K . Le théorème résulte alors de la proposition suivante : le groupe multiplicatif K^* des éléments $\neq 0$ d'un corps fini K est cyclique. Choisissons en effet dans K^* un élément α d'ordre maximum m . Soit β un élément quelconque de K , d'ordre n . q étant un nombre premier, posons $m = q^r \bar{m}$, $n = q^s \bar{n}$, avec \bar{m}, \bar{n} , premiers à q . l'élément $\alpha^{q^r} \beta^{\bar{n}}$ est d'ordre $q^s \bar{m}$; en vertu du choix de m , on a $s \leq r$. Ceci étant vrai pour chaque q , on en conclut que n divise m . Tous les éléments de K^* sont donc des zéros de $x^m - 1$; K^* ne peut donc contenir plus de m éléments, ce qui démontre la proposition.

Diviseurs premiers

k étant le corps des nombres complexes,^[6] K un corps de fonctions algébriques sur k , on a vu comment on pouvait associer à un point P de la surface de Riemann de K une fonction $\nu_P(x)$, définie pour $x \neq 0$ dans K , et telle que $\nu_P(xy) = \nu_P(x) + \nu_P(y)$. Cette fonction jouit de plus de la très importante propriété suivante si x, y sont des éléments de K , avec $x \neq 0, y \neq 0, x + y \neq 0$ on a

$$\nu_P(x + y) = \underline{\text{borne}}(\nu_P(x), \nu_P(y))$$

K étant maintenant un corps quelconque, nous appellerons *valuation* de K une fonction ν définie sur le groupe multiplicatif K^* des éléments $\neq 0$ de K et possédant les propriétés suivantes :

- I. ν est une homomorphie de K^* sur le groupe additif des entiers;
- II. Si $x \neq 0, x \neq -1$, la condition $\nu(x) \geq 0$ entraîne $\nu(1 + x) \geq 0$.

On complète souvent la définition d'une valuation en posant $\nu(0) = +\infty$. La formule $\nu(x + y) = \nu(x) + \nu(y)$ reste vraie avec les conventions habituelles de calcul sur $_{16/17} +\infty$. De plus, les conditions I. II. entraînent l'inégalité

$$\nu(x + y) \geq \underline{\text{borne}}(\nu(x), \nu(y))$$

et on voit tout de suite que cette inégalité peut être transformée en égalité si $\nu(x) \neq \nu(y)$.

À toute valuation ν d'un corps K , nous associerons un nouvel objet que nous appellerons un *diviseur premier* du corps K (cf. cependant plus loin une restriction en ce qui concerne les corps de fonctions algébriques).

Supposons connu dans le corps K un anneau $\mathcal{O} \neq 0$, tel que :

- 1) tout élément de K soit quotient de deux éléments de \mathcal{O} ;

2) le théorème de décomposition unique des idéaux en facteurs premiers soit vrai dans \mathcal{O} .

Dans ces conditions, x étant un élément quelconque $\neq 0$ de K , l'idéal $\mathcal{O}x$ se met sous la forme $\prod \mathfrak{P}^{\nu_{\mathfrak{P}}(x)}$, le produit étant étendu aux idéaux premiers \mathfrak{P} de \mathcal{O} et les $\nu_{\mathfrak{P}}(x)$ étant des exposants entiers, nuls sauf un nombre fini. Chacune des fonctions $\nu_{\mathfrak{P}}$ est une valuation de K , et par suite, à chaque idéal premier \mathfrak{P} de \mathcal{O} correspond un diviseur premier de K . Les valuations $\nu_{\mathfrak{P}}$ sont toutes ≥ 0 sur \mathcal{O} . Inversement, si ν est une valuation de K toujours ≥ 0 sur \mathcal{O} , l'ensemble des x de \mathcal{O} tels que $\nu(x) > 0$ est un idéal premier \mathfrak{P} de \mathcal{O} ; p étant un élément de \mathcal{O} divisible par \mathfrak{P} , mais non par \mathfrak{P}^2 , tout $x \neq 0$ de K se met sous la forme $p^{\nu_{\mathfrak{P}}(x)} \frac{y}{z}$, y et z étant des éléments de \mathcal{O} non contenus dans \mathfrak{P} . On en déduit tout de suite que $\nu = \nu_{\mathfrak{P}}$.

17/18

Ceci s'applique notamment dans le cas où K est un corps de nombres algébriques de degré fini. L'anneau \mathcal{O} des entiers du corps possède les propriétés 1), 2). De plus, dans ce cas, on voit tout de suite que toute valuation est nécessairement ≥ 0 sur \mathcal{O} : il y a donc correspondance biunivoque entre les idéaux premiers de \mathcal{O} et les diviseurs premiers de K .

Considérons maintenant un corps k et un sur-corps $K = k(x)$ simplement transcendant sur k . Soit $\mathcal{O} = k[x]$ l'anneau des polynômes à coefficients dans k . Les idéaux premiers de \mathcal{O} sont les \mathcal{O}_f , f désignant les polynômes irréductibles dans k , et \mathcal{O} satisfait aux conditions 1), 2). À tout polynôme irréductible f correspond ainsi un diviseur premier de K . Si k est algébriquement fermé, les polynômes f sont de la forme $x - a$ ($a \in k$) et correspondent bi-univoquement aux éléments de k . Les valuations que nous venons d'obtenir dans K prennent la valeur 0 sur le groupe k^* des constantes $\neq 0$. Inversement, si ν est une valuation de K , nulle sur k^* , et si $\nu(x) \geq 0$, ν est ≥ 0 sur \mathcal{O} et coïncide avec une des valuations que nous venons de trouver. Si au contraire $\nu(x) < 0$, ν est la valuation qui correspond à l'idéal premier $x^{-1}\mathcal{O}'$ de l'anneau $\mathcal{O}' = k[x^{-1}]$.

18/19

ν étant maintenant une valuation quelconque d'un corps K , P le diviseur premier qui lui correspond, l'ensemble \mathcal{O}_P des x tels que $\nu(x) \geq 0$ constitue un anneau, dont les éléments s'appellent les *entiers* de K (pour P , ou pour ν). L'ensemble de x tels que $\nu(x) > 0$ constitue dans \mathcal{O} un idéal premier \mathfrak{P}_P . Si p est tel que $\nu(p) = 1$, on a $\mathfrak{P} = p\mathcal{O}$, et \mathfrak{P} est le seul idéal premier de \mathcal{O} . L'anneau \mathcal{O} satisfait évidemment aux conditions 1), 2). L'anneau \mathcal{O}/\mathfrak{P} est un corps \mathbb{P} qu'on appelle *corps des restes* de K (par rapport à P ou à ν). Si, par exemple, $K = k(x)$, et si P correspond à un polynôme irréductible f de $k[x]$, le corps des restes définit une extension de dislocation de f sur k , de degré relatif égal au degré de f .

Plus généralement, considérons un nombre fini de valuations différentes $\nu_1, \nu_2, \dots, \nu_h$ d'un corps K . Soit \mathcal{O} l'anneau des x tels que l'on ait simultanément $\nu_1(x) \geq 0$, $\nu_2(x) \geq 0, \dots, \nu_h(x) \geq 0$. Nous allons montrer que \mathcal{O} satisfait aux conditions 1), 2). Nous avons besoin pour cela du lemme suivant (Ostrowski) :^[7]

19/20

Lemme. *Il existe un $x \in K$ tel que $\nu_1(1 - x) > 0$, $\nu_2(x) > 0, \dots, \nu_h(x) > 0$.*

- a) pour $h = 2$, il existe un x_1 tel que $\nu_1(x_1) = 0$, $\nu_2(x_1) \neq 0$, car sinon la valeur de ν_2 ne dépendrait que de celle de ν_1 , et on aurait $\nu_1 = \nu_2$, en vertu de la condition I. En remplaçant éventuellement x_1 par son inverse, on peut supposer que $\nu_2(x_1) > 0$. De même, il existe un x_2 tel que $\nu_1(x_2) > 0$, $\nu_2(x_2) = 0$. L'élément $x = x_1/x_1 + x_2$ satisfait aux conditions.
- b) pour $h > 2$, par récurrence sur h . Le théorème étant supposé vrai pour $h - 1$, il existe x_1, x_2 tels que $\nu_1(1 - x_1) > 0$, $\nu_3(x_1) > 0$, $\nu_i(x_1) > 0$ pour $i \geq 3$; $\nu_1(1 - x_2) > 0$, $\nu_2(x_2) > 0$, $\nu_i(x_2) > 0$ pour $i > 3$; dans le cas où $\nu_2(x_1) > 0$ et $\nu_3(x_2) > 0$, nous poserons $x = x_1/1 + x_1(1 - x_1)$; enfin, si $\nu_2(x_1) \geq 0$, $\nu_3(x_2) < 0$ nous poserons $x = x_2/1 + x_2(1 - x_2)$. L'élément x ainsi obtenu satisfait aux conditions imposées.

Il résulte de là que, sur le groupe multiplicatif des x tels que $\nu_j(x) = 0$ pour $j \neq i$, ν_1 n'est pas identiquement nulle. Soit p_i un élément pour lequel ν_i prenne sa plus petite valeur positive. Les p_i sont dans \mathcal{O} , et tout élément de K peut être amené dans \mathcal{O} par multiplication par un produit de puissances de p_i . \mathcal{O} satisfait donc à 1); de plus on voit, en prenant un x tel que $\nu_i(x) = 1$, que l'on a nécessairement $\nu_i(p_i) = 1$. Tout élément x se met sous la forme $\prod_{i=1}^n p_i^{\nu_i(x)} \cdot e$ où e est une unité de \mathcal{O} , c'est-à-dire un élément de \mathcal{O} dont l'inverse est encore dans \mathcal{O} . L'anneau \mathcal{O} satisfait donc aussi à 2), et on voit de plus que tous ses idéaux premiers sont principaux.

D'autre part, N étant un entier quelconque, x étant un élément satisfaisant aux conditions du lemme, on peut choisir n assez grand pour que l'élément $u_1 = 1 - (1 - x^n)^n$ satisfasse aux conditions $\nu_1(1 - u_1) \geq N$, $\nu_j(u_1) \geq N$ pour $j \neq 1$. De même, on peut, pour chaque i , trouver un u_i tel que $\nu_i(1 - u_i) \geq N$ et $\nu_j(u_i) \geq N$ pour $j \neq i$. On en déduit tout de suite le

Théorème d'indépendance (Ostrowski). $\nu_1, \nu_2, \dots, \nu_h$ étant des valuations distinctes d'un corps K , y_1, y_2, \dots, y_h des éléments de K , A un entier, il existe un $x \in K$ tel que l'on ait simultanément $\nu_i(x - y_i) \geq A$ ($1 \leq i \leq h$).^[8]

Projection d'un diviseur premier. Nous allons maintenant étudier ce que deviennent les diviseurs premiers d'un corps quand on fait une extension algébrique finie de ce corps.

Soit donc un corps L , et soit K un sur-corps de degré fini de L . Soit P un diviseur premier de K . La valuation correspondante ν_P ne peut être identiquement nulle sur L . Il en résulte qu'il existe un entier $e > 0$ bien déterminé tel que $\frac{\nu_P}{e}$ soit une valuation de L . Le diviseur premier correspondant Q s'appelle la *projection* de P sur L . Le nombre e s'appelle l'*ordre de ramification* de P par rapport à L .

Avant de passer à l'étude du problème inverse, c'est-à-dire à la question de trouver quels sont les diviseurs premiers de K qui se projettent sur un diviseur premier donné

de L , nous avons besoin d'introduire des considérations topologiques, liées à l'étude des valuations.

Corps complets. P étant un diviseur premier d'un corps K , on peut associer à P une structure topologique uniforme de K en appelant voisinage d'indice n d'un élément x l'ensemble des y tels que $\nu_P(y - x) \geq n$: on vérifie facilement que les axiomes des structures uniformes sont vérifiés.^[9] D'ailleurs, cette structure uniforme peut être définie par une métrique, qu'on obtient en posant, par exemple, $\rho(x, y) = e^{-\nu_P(y-x)}$. On remarquera que les voisinages de 0 sont des sous-groupes additifs à la fois ouverts et fermés. 22/23

On dit que le corps K est complet par rapport à P si l'espace uniforme ainsi obtenu est complet.

S'il n'en est pas ainsi, on peut le compléter : soit K_P l'espace uniforme complet obtenu. Il existe une isomorphie I_P entre K et un sous-ensemble dense de K_P . En vertu de la remarque faite sur les voisinages de 0 dans K , K_P peut être considéré comme un groupe additif complet, I_P étant une isomorphie additive de K dans K_P . Le produit xy , considéré comme fonction du couple (x, y) , est une fonction uniformément continue au voisinage de chaque point de $K \times K$, comme il résulte de l'inégalité

$$\nu_P(xy - x'y') \geq \underline{\text{borne}} \{ \nu_P(x) + \nu_P(y - y'), \nu_P(y) + \nu_P(x - x') \}$$

qui est valable dès que $\nu_P(y - y') > \nu_P(y)$. Il en résulte que cette fonction peut se prolonger dans $K_P \times K_P$, et que K_P reçoit ainsi une structure d'anneau, I_P devenant ainsi une isomorphie d'anneaux. La fonction $1/x$ est uniformément continue au voisinage de chaque $x \neq 0$ de K : on en déduit tout de suite que K_P est un corps. Le symbole (K_P, I_P) représente donc une extension de K , déterminée à une isomorphie près par les données de K et de P , et qu'on appelle extension P -adique de K . Le corps K_P lui-même s'appelle le corps des éléments P -adiques de K . 23/24

La fonction $e^{-\nu_P}$ est uniformément continue dans K . Elle se prolonge donc dans K_P par une fonction $e^{-\nu}$. On voit tout de suite que ν est une valuation de K_P : elle y définit un diviseur premier qu'il y a tout intérêt à ne pas distinguer de P lui-même dans les notations : on le désignera donc encore par P . Si o est l'anneau des entiers de K (pour P), celui de K_P est le plus petit ensemble fermé contenant $I_P o$. Le corps des restes de K_P est donc le même (à une isomorphie près) que celui de K .

Supposons par exemple que $K = k(x)$, x transcendant sur k , et que P soit le diviseur premier nul sur k^* défini par $\nu(x) = 1$, les éléments de K_P sont alors les

séries formelles $\sum_{i_0}^{+\infty} a_i x^i$ à coefficients dans k (exposants entiers et positifs sauf pour

un nombre fini d'entre eux). On a $\nu\left(\sum_{i_0}^{+\infty} a_i x^i\right) = i_0$ si $a_{i_0} \neq 0$. 24/25

Le lemme de HENSEL. La théorie des polynômes dont les coefficients sont dans un corps complet comporte un résultat très remarquable dû à Hensel. Pour le formuler et le démontrer, nous avons besoin d'étendre à une extension transcendante une valuation donnée dans un corps. Soit donc K un corps, P un diviseur premier de K , \mathbb{P} le corps des restes de K . Soit $K(t)$ un sur-corps simplement transcendant de K . $f = \sum x_i t^i$ étant un polynôme à coefficients dans K , posons $\nu'(f) = \underline{\text{borne}} \{\nu_{\mathbb{P}}(x_i)\}$. f/g étant une fraction rationnelle de $K(t)$, posons $\nu'(f/g) = \nu'(f) - \nu'(g)$. La fonction ν' ainsi obtenue est une valuation de $K(t)$. Si \mathbb{P}' est le corps des restes de $K(t)$ par rapport à ν' , il existe une isomorphie J entre \mathbb{P} et un sous-corps de \mathbb{P}' , et le reste \bar{t} qui correspond à t est transcendant sur $J\mathbb{P}$: on a $\mathbb{P}' = J\mathbb{P}(\bar{t})$. f étant un polynôme de $K(t)$ à coefficients entiers, nous désignerons par \bar{f} l'élément de \mathbb{P}' qui lui correspond. Ceci dit, nous arrivons au

Lemme de Hensel. *Supposons le corps K complet par rapport à P . Si f est un polynôme irréductible dans K à coefficients entiers, et si \bar{f} peut se décomposer en le produit $\bar{g} \cdot \bar{h}$ de deux polynômes à coefficients dans \mathbb{P} premiers entre eux, f peut se décomposer en le produit de deux polynômes $g \cdot h$ à coefficients entiers appartenant respectivement aux classes \bar{g}, \bar{h} .*

Soient a, b, c , les degrés de f, \bar{g}, \bar{h} . Il existe par hypothèse des polynômes g_1, h_1 , à coefficients entiers, de degrés b, c , tels que $\nu'(f - g_1 h_1) \geq 1$ et $\bar{g}_1 = \bar{g}, \bar{h}_1 = \bar{h}$. Nous allons construire par récurrence sur n [des] polynômes g_n, h_n à coefficients entiers, tels que $\nu'(f - g_n h_n) \geq n$ et que $d^o g_n \leq a - c, d^o h_n \leq c$. Supposons g_n, h_n déjà construits ; p désignant un élément de K , tel que $\nu_{\mathbb{P}}(p) = 1$, posons $r_n = p^{-n}(f - g_n h_n)$, r_n est un polynôme à coefficients entiers de degré $\leq a$. \bar{g} et \bar{h} étant premiers entre eux, nous pouvons trouver des polynômes u_n, v_n à coefficients entiers, tels que $\bar{r}_n = \bar{g} \cdot \bar{u}_n + \bar{h} \cdot \bar{v}_n$, les degrés de u_n, v_n étant respectivement $\leq c$ et $a - c$. Nous poserons

$$g_{n+1} = g_n - p^n v_n \quad h_{n+1} = h_n - p^n u_n$$

On voit tout de suite que g_{n+1}, h_{n+1} , satisfont aux conditions imposées pour $n + 1$. De plus, les formules de récurrence montrent que g_n, h_n tendent, quand n augmente indéfiniment, vers des polynômes g, h , qui satisfont aux conditions imposées.

Une conséquence du lemme de Hensel, que nous allons utiliser tout à l'heure, est la suivante :

K étant complet, si un polynôme irréductible f de K a pour premier coefficient 1 et pour dernier coefficient un entier, il est à coefficients entiers.

En effet, s'il n'en était pas ainsi, il existerait un exposant u tel que $p^u f$ puisse se mettre sous la forme $t^i g + ph$, avec $i > 0$, g et h étant des polynômes à coefficients entiers, le dernier coefficient de g n'étant pas divisible par p . Les polynômes \bar{t}^i, \bar{g} seraient premiers entre eux, et on pourrait en vertu du lemme de Hensel, en déduire une décomposition de f , contrairement à l'hypothèse.

Extensions finies d'un corps complet. Soit L un corps parfait par rapport à un diviseur premier Q , et soit K un sur-corps de degré relatif fini de L . Nous allons montrer qu'il existe un diviseur premier et un seul de K , qui se projette en Q sur L . x étant un élément de K , posons

$$\nu'(x) = \nu_Q(N_{K/L}(x))$$

On a $\nu'(xy) = \nu'(x) + \nu'(y)$. De plus, si $\nu'(x) \geq 0$, x est zéro d'un polynôme irréductible $f(t)$ à coefficients entiers dans L dont le premier coefficient est 1 et dont le dernier est entier pour Q ; il en résulte que tous les coefficients de ce polynôme sont entiers; il en est donc de même pour le polynôme caractéristique g de x qui est une puissance de f . Or le polynôme caractéristique de $1+x$ est $g(1+t)$; il en résulte que $N_{K/L}(1+x)$ est entier, et que $\nu'(1+x) \geq 0$. Si d est le p.g.c.d. des valeurs prises par ν' , la fonction $\frac{\nu'}{d}$ est une valuation de K qui définit un diviseur premier P qui se projette en Q sur L . Les entiers de K pour P sont les éléments dont les polynômes caractéristiques sont à coefficients entiers. 27/28

Il résulte de là que si P' est un diviseur premier quelconque de K qui se projette en Q sur L , les entiers pour P sont aussi entiers pour P' ; la condition $\nu_P \geq 0$ entraîne $\nu_{P'} \geq 0$, ce qui n'est possible que si $P = P'$. Donc :

Si L est un corps complet par rapport à un diviseur premier Q , il y a dans un sur-corps de degré fini de L un diviseur premier et un seul qui se projette en Q sur L .

Soit q un élément de L tel que $\nu_Q(q) = 1$ et p un élément de K tel que $\nu_P(p) = 1$. De l'égalité $\nu'(q) = (K : L)$ résulte que le nombre d , qui s'appelle le *degré relatif* de P par rapport à L , divise $(K : L)$. De plus, on a $\nu_P(q) = (K : L)/d$, et par suite $(K : L)$ est le produit du degré relatif d par l'ordre de ramification e de P par rapport à L . 28/29

Désignons par o l'anneau des entiers de L par rapport à Q et par \mathcal{O} celui des entiers de K par rapport à P . Le corps des restes de K est $\mathcal{O}/p\mathcal{O}$. En prenant les classes qui contiennent des éléments de o on obtient une isomorphie du corps des restes o/qo de L dans $\mathcal{O}/p\mathcal{O}$. On voit facilement que si des éléments $x_1, x_2, \dots, x_\delta$ de \mathcal{O} sont tels que leurs classes (mod. $p\mathcal{O}$) soient linéairement indépendantes par rapport à o/qo , ces éléments sont eux-mêmes linéairement indépendants par rapport à L . Il en résulte que le corps des restes de K est une extension finie de celui de L . δ étant pris égal au degré de cette extension, on voit facilement que les éléments $p^i x_j$ ($0 \leq i \leq e, 1 \leq j \leq \delta$) forment une *base* de \mathcal{O} par rapport à o , c'est-à-dire que tout élément de \mathcal{O} se met et d'une seule manière sous la forme d'une combinaison linéaire de ces éléments à coefficients dans o . Il en résulte que $e\delta = (K : L)$ et que, par suite, *le corps des restes de K est une extension du corps des restes de L de degré égal au degré relatif d de P .* 29/30

D'autre part, si nous mettons un élément de K sous la forme $\sum u_{i,j} p^i x_j$, nous obtenons une topologie uniforme complète dans K en prenant pour voisinage V_n de \mathcal{O} l'ensemble des éléments pour lesquels $\nu_Q(U_{i,j}) \geq n$ pour toutes les combinaisons (i, j) .

Mais cette condition est équivalente à la condition $\nu_P(x) \geq ne$. Il en résulte que la topologie définie par P dans K est complète.

Extensions finies d'un corps quelconque. Considérons maintenant un corps L dans lequel on connaît un diviseur premier Q et un sur-cors de degré fini K de L . Formons l'extension Q -adique (L_Q, I_Q) de L , et considérons une extension composée (U, H_{L_Q}, J_K) des extensions (L_Q, I_Q) et K/L . (U, H_{L_Q}) est le symbole d'une extension finie de L_Q . On y peut donc définir un diviseur premier P_0 et une valuation correspondante ν_0 . Le corps $J_K K$ est partout dense dans U ; il en résulte tout de suite, que la fonction $\nu(x) = \nu_0(J_K x)$ est une valuation de K ; elle y définit un diviseur premier P qui se projette en Q sur L . De plus J_K peut se prolonger par une isomorphie entre K_P et U , l'ordre de ramification de P par rapport à L est égal à celui de P_0 par rapport à $H_Q L_Q$; le corps des restes de K par rapport à P est une extension finie de celui de L par rapport à Q de degré égal au degré relatif de P_0 par rapport à $H_Q L_Q$. Ce nombre s'appelle encore le *degré relatif* de P par rapport à L .

Deux extensions composées isomorphes donnent évidemment par ce procédé le même diviseur premier de K .

Soit maintenant, inversement, P un diviseur premier de K qui se projette en Q . Soit (K_P, I_P) l'extension P -adique de K ; soit L_Q le plus petit ensemble fermé de K_P contenant $I_P L$. (L_Q, I_P) est une extension Q -adique de L . Soit U le sous-cors de K_P engendré par L_Q et $I_P K$: il n'y a dans U qu'un seul diviseur premier qui se projette en Q sur L_Q , et U est complet par rapport à ce diviseur premier. On a donc $U = K_P$, de sorte que tout diviseur premier de K qui se projette en Q peut être obtenu par le procédé indiqué plus haut. Il en résulte *qu'il n'y a qu'un nombre fini de diviseurs premiers de K qui se projettent en Q sur L .*

Soient P_1, P_2, \dots, P_g ces diviseurs premiers. Désignons par \mathcal{O} l'anneau des éléments x de K tels que l'on ait simultanément $\nu_i(x) \geq 0$ ($1 \leq i \leq g$), et par o l'anneau des entiers pour Q de L . Il est clair que \mathcal{O} contient les éléments de K qui sont entiers par rapport à o . Inversement, soit x un élément de \mathcal{O} , zéro d'un polynôme f irréductible dans L dont le premier coefficient est 1. On obtient les extensions composées de $L(x)/L$ et de L_Q/L en décomposant f en facteurs irréductibles dans L_Q : soit $f = \prod_{i=1}^{g'} f_i^{u_i}$ cette décomposition; si P'_1, P'_2, \dots, P'_g sont les diviseurs premiers de $L(x)$ qui se projettent en Q , les corps $(L(x))_{P'_i}$ sont des extensions de dislocation des f_i sur L_Q . Les $\nu_{P'_i}(x)$ étant ≥ 0 , il en résulte que les f_i sont à coefficients entiers dans L_Q , et que f est à coefficients entiers dans L : \mathcal{O} se confond avec l'anneau des entiers de K par rapport à o .

Soient d_i les degrés relatifs des P_i par rapport à L , et e_i leurs ordres de ramification ($1 \leq i \leq g$). Nous pouvons choisir d_i éléments $x_{i,j}$ ($1 \leq j \leq d_i$) de K entiers pour P_i , et dont les classes (mod. P_i) soient linéairement indépendantes par rapport à o/Q . En utilisant le théorème d'indépendance, on voit qu'on peut sans restriction supposer que l'on a $\nu_{P_\ell}(X_{i,j}) \geq e_P$ pour $1 \leq \ell \leq g$, $\ell \neq i$. Choisissons d'autre part un p_i tel que $\nu_{P_i}(p_i) = 1$, $\nu_{P_j}(p_i) = 0$ si $j \neq i$. Posant $n' = \sum_{i=1}^g d_i e_i$, désignons par $z_1, z_2, \dots, z_{n'}$, les éléments $x_{i,j} p_i^\alpha$ ($1 \leq i \leq g$, $1 \leq j \leq d_i$, $0 \leq \alpha < e_i$). Il est facile de voir qu'un élément de la forme $\sum_1^{n'} a_i z_i$, les a_i étant dans L , ne peut être dans \mathcal{O} que si les a_i sont tous dans o , et que les z_i sont linéairement indépendants par rapport à k . On en conclut l'inégalité

$$\sum_1^g d_i e_i \leq (K : k)$$

Si cette inégalité est une égalité, les z_i constituent une base de K/L . En vertu du choix des premiers z_i , on peut pour chaque entier m positif, trouver des $a_{i,m} \in o$ ($1 \leq i \leq n'$)

tels que $\nu_{P_\ell} \left(z_{n'+1} - \sum_1^{n'} a_{i,m} z_i \right) \geq m e_\ell$ ($1 \leq \ell \leq g$), donc que $\frac{z_{n'+1} - \sum_1^{n'} a_{i,m} z_i}{q^m}$ soit dans \mathcal{O} . Il en résulte que \mathcal{O} ne possède pas de base finie par rapport à o . Donc :

33/34

Une condition nécessaire et suffisante pour que \mathcal{O} possède une base finie par rapport à o est que

$$\sum_1^g d_i e_i = (K : k)$$

Il en est toujours ainsi, en vertu d'un théorème bien connu de Mlle Noether, dans le cas des extensions séparables. Il en est encore de même, comme on verra dans la prochaine conférence, dans le cas où L est un corps de fonctions algébriques. Par contre, on peut donner des exemples dans lesquels la condition n'est pas réalisée.

Structure des corps complets. Soit K un corps complet par rapport à une valuation, ν , correspondant à un diviseur premier P . Hasse et Schmidt (Crelle, 1933), puis, plus simplement, Witt et Teischmüller [sic] (Crelle, 1936) ont montré que la structure du corps K était bien déterminée par la donnée de celle du corps des restes \mathfrak{K} de K : c'est-à-dire que si deux corps complets ont des corps de restes isomorphes, on peut établir entre eux une isomorphie conservant la valuation. Les auteurs cités ont montré comment construire K quand on connaît \mathfrak{K} . Le résultat est particulièrement simple dans le cas où K et \mathfrak{K} ont même caractéristique : K est alors isomorphe au corps des séries formelles à coefficients dans \mathfrak{K} .

34/35

Les diviseurs premiers des corps de fonctions algébriques

k étant un corps, soit $k(x)$ une extension transcendante simple de k . Un corps K contenant $k(x)$ et tel que l'extension $K/k(x)$ soit finie est appelé un corps de fonctions algébriques sur k . Le corps k' des éléments de K qui sont algébriques sur k s'appelle le *corps des constantes* de K . K est encore un corps de fonctions algébriques sur k' . il n'y aura dans la suite aucun inconvénient à supposer toujours que $k = k'$: c'est ce que nous ferons.

Dans le cas où k est parfait, nous savons que l'extension $K/k(x)$ est simple : on a $K = k(x, y)$, où y satisfait à une équation irréductible $f(x, y) = 0$. Le premier nombre ne peut pas être un polynôme en x^p, y^p (où p est la caractéristique de k) car il serait alors une puissance $p^{\text{ième}}$. Donc l'une au moins des extensions $K/k(x), K/k(y)$ est séparable. Il en résulte que si k est parfait, K contient toujours des *fonctions*
35/36 *séparantes* t , c'est-à-dire des fonctions telles que $K/k(t)$ soit séparable. Si k n'est pas parfait, il n'en est plus nécessairement ainsi.

Dans l'étude des corps de fonctions algébriques on se restreint systématiquement à l'étude des diviseurs premiers P correspondant à des valuations ν_P prenant la valeur 0 sur le corps des constantes $\neq 0$. Quand nous parlerons de diviseurs premiers, nous supposerons toujours cette condition réalisée.

Le corps des restes d'un corps de fonctions algébriques K par rapport à un diviseur premier P est une extension finie du corps des constantes : le degré de cette extension est appelé le *degré absolu* de P . Si x est un élément de K tel que $\nu_P(x) \neq 0$, le degré absolu de P est égal à son degré relatif par rapport à $k(x)$.

Le corps des restes \mathfrak{K} d'un corps de fonctions algébriques K par rapport à un diviseur premier P a toujours même caractéristique que K ; et par suite K est isomorphe à un sous-corps du corps des séries formelles à coefficients dans \mathfrak{K} . Inversement, toute isomorphie de K dans un corps de séries formelles détermine un diviseur premier de K (à condition qu'à un élément au moins $\neq 0$ de K corresponde une série formelle à terme constant nul). On peut donc trouver les diviseurs premiers de K en recherchant les isomorphismes de K dans le corps des séries formelles à coefficients dans un sur-corps
36/37 algébriquement fermé \bar{k} de k . Si le corps est parfait, aux éléments de k correspondent nécessairement des éléments de \bar{k} , et de plus deux isomorphismes ne donnent le même diviseur premier que si on peut passer de l'une à l'autre par une automorphie du corps des séries formelles conservant \bar{k} (dans son ensemble). Ces deux propriétés ne sont plus vraies si k n'est pas parfait.

Notes

1. Il s'agit de deux exposés. La rédaction a peut-être été faite en deux étapes. C'est certainement le cas de la frappe : les premières pages sont numérotées V.-C.- x ($1 \leq x \leq 21$) et les suivantes V.-C+D.- y ($22 \leq y \leq 37$).
2. Il n'y a pas de bibliographie. Sont cités dans cet exposé les articles de Hasse et Schmidt [HS33], de Witt [Wit36] et de Teichmüller [Tei36].
3. Les deux exposés précédents portaient en effet sur les surfaces de Riemann.
4. Dislocation est, depuis, devenu rupture.
5. Le S est pour *Spur*, comme au début du séminaire.
6. Il n'y a toujours pas de notation standardisée pour les ensembles de nombres usuels.
7. L'article [Ost17] d'Ostrowski a déjà été cité dans l'exposé 1-H, sur les corps p -adiques.
8. Ici s'arrête l'exposé C... et commence l'exposé C+D, la pagination continuant. Voir la note 1.
9. Les structures uniformes, introduites par Weil (et par Bourbaki) venaient de faire l'objet du fascicule [Wei37] (et feraient l'objet du chapitre 2 de [Bou40]). Chevalley les utilisa immédiatement. Rappelons qu'une structure uniforme sur E est... un filtre de $E \times E$ ou, si l'on préfère, une famille d'entourages de la diagonale de $E \times E$: elles sont donc bien adaptées à la description des espaces complets (la définition d'une suite de Cauchy fait intervenir des couples). Quelques années auparavant, lorsqu'il donna l'exposé 1-H, Weil ne disposait pas encore des structures uniformes!

Références

- [Bou40] N. BOURBAKI – *Éléments de mathématique. Les structures fondamentales de l'analyse. 3. Topologie générale. 1. Structures topologiques. 2. Structures uniformes*, Hermann, Paris, 1940.
- [HS33] H. HASSE & F. K. SCHMIDT – « Die Struktur diskret bewerteter Körper », *J. Reine Angew. Math.* **170** (1933), p. 4–63.
- [Ost17] A. OSTROWSKI – « Über einige Lösungen der Funktionalgleichung $\varphi(x) \cdot \varphi(y) = \varphi(xy)$ », *Acta Math.* **41** (1917), p. 271–284.
- [Tei36] O. TEICHMÜLLER – « Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper », *J. Reine Angew. Math.* **176** (1936), p. 141–152.
- [Wei37] A. WEIL – *Sur les espaces à structure uniforme et sur la topologie générale*, Publications de l'Institut de mathématiques de l'université de Strasbourg, Hermann, Paris, 1937.
- [Wit36] E. WITT – « Zyklische Körper und Algebren der Charakteristik p vom Grad p^n . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p », *J. reine angew. Math.* **176** (1936), p. 126–140.