FORMES DIFFERENTIELLES ET CORPS DE NOMBRES

SAMUEL VIDAL

"À notre époque, pour l'âme de chaque théorie mathématique, se battent le démon de l'algèbre et l'ange de la géométrie."

Hermann Weyl

0. Introduction

Exemple introductif. Soit X un ouvert de $\mathbf{R}^n$, on note A la $\mathbf{R}$-algèbre des fonctions lisses à valeur dans $\mathbf{R}$. Les champs de vecteurs sur X sont par définition les sections globales du fibré tangent de X, ils constituent un A-module qui s'identifie à celui des dérivations de A à valeur dans A. Il est facile de vérifier que c'est un A-module libre de rang n engendré par les opérateurs de dérivée partielle, $\partial/\partial x_i$ pour $i = 1, ..., n$. Le module des formes différentielles de X est par définition le A-module dual de celui des champs de vecteurs, il s'identifie à celui des sections globales du fibré cotangent et l'on voit tout de suite qu'il est libre et que les formes $\mathrm{d}x_i$ définies par $(\mathrm{d}x_i)(\partial/\partial x_j) = \delta_{ij}$ en constituent une base.

Organisation de l'exposé. Dans ce travail, nous tâcherons de traiter une généralisation algébrique de cette situation et l'une de ses applications aux corps de nombres, notamment grâce à la *différente* d'une extension algébrique (notion due à D. Hilbert). L'objectif étant, entre autre, d'approfondir la courte note d'A. Weil [7] et ce faisant, nous tâcherons d'éclaircir l'analogie frappante qu'il existe entre corps de fonctions et corps de nombres à l'aide d'exemples empruntés à la *géométrie* d'une part et à l'*arithmétique* d'autre part.

1. Module des Formes Différentielles

Dans ce qui suit, k désigne un anneau commutatif unitaire et A désigne une k-algèbre commutative unitaire. L'objectif de cette section est de définir le A-module $\Omega_k(A)$ des formes différentielles de Kähler.

1.1. **Généralités.** On notera $\mu : A \otimes_k A \to A$ la multiplication de A. On posera $I = \mathrm{Ker}(\mu)$; c'est un idéal de l'algèbre $B = A \otimes_k A$. On a sur I une structure de

A-bimodule induite par sa structure de B-module,

$$x.(a \otimes b) = (xa) \otimes b$$
$$(a \otimes b).y = a \otimes (by)$$

Le A-module des k-dérivations de A à valeurs dans un A-module M est noté $D_k(A, M)$, il s'agit des applications k-linéaires $\mathrm{d} : A \to M$ vérifiant la condition de Leibniz :

$$\mathrm{d}(ab) = a.\mathrm{d}(b) + b.\mathrm{d}(a) \qquad\qquad (a, b \in A)$$

Le noyau d'une telle dérivation est un sous-anneau de A qui contient k, et si A est un corps, c'est de plus un sous-corps.

Le module $D_k(A)$ muni du crochet $[\,\gamma, \eta\,] = \gamma\eta - \eta\gamma$ est une algèbre de Lie, ceci revient à dire qu'il est alterné et que l'on a l'identité de Jacobi :

$$[\,\gamma, [\,\eta, \nu\,]\,] + [\,\eta, [\,\nu, \gamma\,]\,] + [\,\nu, [\,\gamma, \eta\,]\,] = 0$$

quels que soient $\gamma, \eta, \nu \in D_k(A)$.

Lemme 1.1. *Les deux structures de A-modules sur I/I^2 (celle provenant du premier facteur et celle provenant de second facteur) sont identiques.*

Démonstration. On calcule dans I modulo I^2,

$$\begin{aligned} x.(a \otimes 1 - 1 \otimes a) &\equiv xa \otimes 1 - x \otimes a \\ &\equiv xa \otimes 1 - x \otimes a - (x \otimes 1 - 1 \otimes x)(a \otimes 1 - 1 \otimes a) \\ &\equiv a \otimes x - 1 \otimes xa \\ &\equiv (a \otimes 1 - 1 \otimes a).x \end{aligned}$$

Fin de la démonstration.

Remarque. On considère désormais I/I^2 comme un A-module.

Lemme 1.2. *L'application $\mathrm{d}_{A/k} : a \mapsto a \otimes 1 - 1 \otimes a \mod I^2$ de A dans I/I^2 est une k-dérivation de A et son image engendre I/I^2 comme A-bimodule.*

Démonstration. Le premier point se vérifie facilement,

$$\begin{aligned} \mathrm{d}_{A/k}(ab) &= (ab \otimes 1 - 1 \otimes ab) \\ &= ab \otimes 1 - a \otimes b + a \otimes b - 1 \otimes ab \\ &= a.(b \otimes 1 - 1 \otimes b) + (a \otimes 1 - 1 \otimes a).b \\ &= a.\mathrm{d}_{A/k}(b) + b.\mathrm{d}_{A/k}(a) \end{aligned}$$

Pour vérifier le second point il suffit de montrer que les éléments $\{a \otimes 1 - 1 \otimes a\}_{a \in A}$ engendrent I comme B-module. Un élément u de I s'écrit par définition $\sum_i a_i \otimes b_i$

avec $\sum_i a_i b_i = 0$, d'où,

$$u = \sum_i (a_i \otimes 1).(1 \otimes b_i - b_i \otimes 1)$$

Fin de la démonstration.

Théorème 1.3. *On a un isomorphisme canonique de A-modules,*

$$I/I^2 \xrightarrow{\sim} A \otimes_B I$$

La structure de A-module sur $A \otimes_B I$ provenant du premier facteur.

Remarque. On dit que le A-module I/I^2 s'obtient à partir du B-module I par *extension des scalaires* (suivant le morphisme d'algèbres μ).

Démonstration. De façon générale si I est un idéal de B et si M est un B-module quelconque, le B/I-module M' obtenu à partir de M par extension des scalaires suivant la projection canonique $B \to B/I$ est $M/IM \simeq B/I \otimes_B M$ et notre théorème est démontré en posant $M = I$ et $A = B/I$. Nous explicitons maintenant la construction de l'isomorphisme dans le cas particulier qui nous intéresse.

On tensorise pour cela la suite exacte $0 \to I \to B \xrightarrow{\mu} A \to 0$ par I et l'on obtient le diagramme suivant à lignes exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I \otimes_B I & \longrightarrow & B \otimes_B I & \longrightarrow & A \otimes_B I & \longrightarrow & 0 \\
 & & \downarrow \simeq & & \downarrow \simeq & & \downarrow = & & \\
0 & \longrightarrow & I^2 & \longrightarrow & I & \longrightarrow & A \otimes_B I & \longrightarrow & 0
\end{array}$$

L'exactitude en I et en $A \otimes_B I$ provient de l'exactitude à droite du foncteur $(\cdot \otimes_B I)$, l'injectivité de $I^2 \to I$ est claire. Fin de la démonstration.

On définit l'espace des 1-formes différentielles, noté $\Omega_k(A)$ de la manière suivante,

$$\Omega_k(A) = I/I^2 = A \otimes_B I$$

(Définition due à E. Kähler). Signalons que l'on peut définir plus généralement le module des formes différentielles extérieures de degré r, noté $\Omega_k^r(A)$, en posant,

$$\Omega_k^r(A) = \wedge^r \Omega_k(A)$$

et que le produit de deux formes $\omega_r \in \Omega_k^r(A)$ et $\omega_s \in \Omega_k^s(A)$, noté $\omega_r \, \omega_s$, est simplement le produit extérieur $\omega_r \wedge \omega_s \in \Omega_k^{r+s}(A)$. C'est ainsi que l'on a une *algèbre différentielle graduée* qui est en particulier un complexe de cochaînes

pour la différentiation standard, et dont on définit le n-ième groupe de cohomologie $H_k^n(A)$ en quotientant comme d'habitude *cocycles* par *cobords* :

$$\begin{aligned} H_k^0(A) &= \mathrm{Ker}(\mathrm{d}_{A/k}) \quad \text{et pour } n \geq 1 : \\ Z_k^n(A) &= \mathrm{Ker}(\mathrm{d}_{A/k}^n) \\ B_k^n(A) &= \mathrm{Im}(\mathrm{d}_{A/k}^{n-1}) \\ H_k^n(A) &= Z_k^n(A)/B_k^n(A) \end{aligned}$$

Remarque. Tout anneau commutatif unitaire est d'une unique façon une algèbre sur l'anneau $\mathbf{Z}$ des entiers relatifs. On abrège alors la notation en posant $\Omega(A)$ au lieu de $\Omega_{\mathbf{Z}}(A)$.

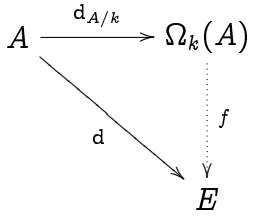
Exemple 1. Si $A = k[x_1, ..., x_n]$ est un anneau de polynômes sur k, alors $\Omega_k(A)$ est le A-module libre de rang n engendré par les formes $\mathrm{d}x_1, ..., \mathrm{d}x_n$. Avec $n = 1$ on a $\mathrm{d}f(x) = f'(x)\,\mathrm{d}x$ pour tout polynôme f et tout $x \in A$, et plus généralement, si f est un polynôme en n variables $x_1, ..., x_n$, on a comme de juste,

$$\mathrm{d}f(u_1, ..., u_n) = \frac{\partial f}{\partial x_1}(u_1, ..., u_n)\,\mathrm{d}u_1 + ... + \frac{\partial f}{\partial x_n}(u_1, ..., u_n)\,\mathrm{d}u_n$$

quels que soient $u_1, ..., u_n \in A$.

Le théorème suivant exprime l'*universalité* de la paire $(\Omega_k(A), \mathrm{d}_{A/k})$:

Théorème 1.4. *Soit E un A-module et soit d une k-dérivation de A à valeurs dans E. Il existe un et un seul morphisme de A-modules f rendant commutatif le diagramme suivant.*



Démonstration. Le fait que l'image de $\mathrm{d}_{A/k}$ engendre I/I^2 et la condition $\mathrm{d} = f \circ \mathrm{d}_{A/k}$ entraînent l'unicité de f par linéarité : soit $u \in I$ c'est-à-dire $u = \sum_i x_i \otimes y_i$ avec $\sum_i x_i y_i = 0$ alors,

$$\begin{aligned} f(u) &= f(\sum_i x_i.(1 \otimes y_i - y_i \otimes 1)) \\ &= \sum_i x_i.f(1 \otimes y_i - y_i \otimes 1) \\ &= \sum_i x_i.f(\mathrm{d}_{A/k}(-y_i)) \\ &= \sum_i x_i.\mathrm{d}(-y_i) \end{aligned}$$

Pour montrer que f est bien définie (l'*existence*) il suffit de voir que sa définition passe au quotient :

$$\begin{aligned} f[(a\otimes 1-1\otimes a)(b\otimes 1-1\otimes b)] &= f(ab\otimes 1-a\otimes b-b\otimes a+1\otimes ab)\\ &= f(b.(a\otimes 1-1\otimes a)-(a\otimes 1-1\otimes a).b)\\ &= b.f(\mathrm{d}_{A/k}(a))-b.f(\mathrm{d}_{A/k}(a))=0 \end{aligned}$$

Fin de la démonstration.

Corollaire 1. *On a un isomorphisme naturel de A-modules,*

$$\mathrm{Hom}_A(\Omega_k(A),E)\xrightarrow{\sim} D_k(A,E)$$

donné par $f\mapsto f\circ \mathrm{d}_{A/k}$.

L'énoncé précédent résulte immédiatement de la propriété universelle il exprime que la paire $(\Omega_k(A),\mathrm{d}_{A/k})$ *représente* le foncteur $D_k(A,\cdot)$. Pratiquement, cela permet de traiter la question des dérivations en terme d'homomorphismes. C'est en ce sens que l'on peut dire que la construction $\Omega_k(A)$ *linéarise* le problème.

En posant $E=A$ on met en dualité le module des champs vectoriels avec celui des formes différentielles. Ceci est en parfait accord avec ce qui a cours en géométrie différentielle et justifie la terminologie.

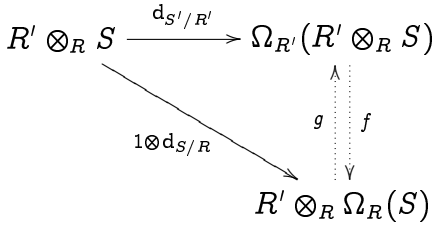
2. Localisation et Complétion

Le comportement du module des différentielles vis-à-vis des opérations de changement d'anneaux est explicité par le théorème d'application générale suivant.

Théorème 2.1 (Changement d'anneaux). *Soient R' et S deux R-algèbres et soit $S'=R'\otimes_R S$ alors,*

$$\Omega_{R'}(R'\otimes_R S)\simeq R'\otimes_R \Omega_R(S)$$

Démonstration. Considérons le diagramme suivant,



L'application $1\otimes \mathrm{d}_{S/R}$ est une R'-dérivation, il existe donc un unique homomorphisme $f:\Omega_{R'}(S')\to R'\otimes_R\Omega_R(S)$ rendant commutatif le diagramme. Dans l'autre

sens, on remarque que l'application $\phi : S \to \Omega_{R'}(S')$ obtenue par compositions des applications suivantes,

$$S \simeq R \otimes_R S \xrightarrow{\rho \otimes 1} R' \otimes_R S \xrightarrow{\mathrm{d}_{S'/R'}} \Omega_{R'}(R' \otimes_R S)$$

(où l'on a noté $\rho : R \to R'$ le morphisme structural), est une R-dérivation. Il existe donc un unique homomorphisme de S-modules $h : \Omega_R(S) \to \Omega_{R'}(R' \otimes_R S)$ tel que $\phi = h \circ \mathrm{d}_S$. L'application $g : R' \otimes_R \Omega_R(S) \to \Omega_{R'}(R' \otimes_R S)$ réciproque de f est induite de h par la propriété universelle du produit tensoriel. Fin de la démonstration.

L'utilité principale du théorème précédent est qu'il permet de montrer comme cas particulier que la formation du module des différentielles commute aux procédés de *localisation* et de *complétion* :

Application 1 (Localisation)**.** En posant, $S = A$, $R = k$ et $R' = A_{\mathfrak{p}}$ où $\mathfrak{p}$ est un idéal premier quelconque d'une k-algèbre A, on obtient l'isomorphisme,

$$\Omega_A(A_{\mathfrak{p}}) \simeq (\Omega_k(A))_{\mathfrak{p}}$$

Application 2 (Complétion)**.** En posant $S = A$, $R = k$ et $R' = \widehat{A}_{\mathfrak{p}}$ où $\widehat{A}_{\mathfrak{p}}$ désigne le complété de l'anneau local $A_{\mathfrak{p}}$ pour la topologie $\mathfrak{p}$-adique, on a l'isomorphisme,

$$\Omega_A(\widehat{A}_{\mathfrak{p}}) \simeq ((\Omega_k(A))_{\mathfrak{p}})\widehat{} \simeq (\Omega_A(A_{\mathfrak{p}}))\widehat{}$$

3. Les Deux Suites Exactes Fondamentales

Les deux suites exactes suivantes sont fort utiles pour aboutir à des théorèmes de structure concernant le module des différentielles. Nous nous bornons ici à les énoncer et nous renvoyons le lecteur à l'ouvrage de Matsumura [5, th. 25.1 et 25.2 p. 193-195] pour les démonstrations.

Théorème 3.1 (Première suite exacte)**.** *Soient $k \xrightarrow{\phi} A \xrightarrow{\psi} B$ des morphismes d'anneaux, alors,*

(1) On a une suite exacte naturelle de B-modules,

$$\Omega_k(A) \otimes_A B \xrightarrow{\eta} \Omega_k(B) \xrightarrow{\tau} \Omega_A(B) \to 0$$

(2) L'application η admet une rétraction si et seulement si toute k-dérivation de A à valeur dans un B-module M se prolonge en une k-dérivation de B.

Remarque. Dire que η admet une rétraction revient à dire que η est injective et que son image est facteur direct de $\Omega_k(B)$.

Théorème 3.2 (Seconde suite exacte). *Soit A une k-algèbre, et soit $B = A/\mathfrak{a}$ où $\mathfrak{a}$ est un idéal de A. Alors on a une suite exacte de B-modules :*

$$\mathfrak{a}/\mathfrak{a}^2 \xrightarrow{\delta} \Omega_k(A) \otimes_A B \to \Omega_A(B) \to 0$$

avec $\delta(a) = \mathrm{d}_{A/k}(a) \otimes 1$.

4. Corps de Nombres et Corps de Fonctions

Pour effectuer ce travail nous nous sommes appuyé sur les premiers chapitres de l'ouvrage de Serre *Corps Locaux* cité [6] dans la bibliographie. Nous y avons découvert un message crypté ; au lecteur attentif il dit ceci : les anneaux de Dedekind constituent une pierre de Rosette entre Arithmétique et Géométrie. Elle ne concerne pas l'intégralité de ces disciplines, seulement l'arithmétique des corps de nombres et la géométrie des courbes algébriques, mais c'est un terrain solide sur lequel ériger un dictionnaire plus vaste encore.

4.1. Anneaux de Dedekind.

Cette section est consacré à quelques rappels de propriétés concernant les anneaux de Dedekind. Tout d'abord la définition.

Définition 4.1. Un anneau intègre noethérien A est de Dedekind s'il vérifie l'une des propriétés équivalentes suivantes :

(1) Le *localisé* en $\mathfrak{p}$ de A, noté $A_\mathfrak{p}$, est un anneau de valuation discrète, pour tout idéal premier non-nul $\mathfrak{p}$ de A.

(2) A est intégralement clos et de dimension ≤ 1 (*i.e.* tout idéal premier non-nul est maximal).

(3) Tout idéal de A se décompose de façon unique comme produit fini d'idéaux premiers.

Remarques. Toute l'importance en arithmétique du procédé de localisation provient en effet du premier point de la définition. Le dernier point correspond à ce qu'il est d'usage d'appeller, le théorème fondamental de la théorie classique des idéaux.

Proposition 4.1. *Soit A un anneau commutatif intègre, les propriétés suivantes sont équivalentes :*

(1) A est de Dedekind.

(2) Tout idéal de A est projectif.

Exemple 2. C'est ainsi que tout anneau *principal* est de Dedekind, puisqu'un idéal principal d'un anneau intègre est libre de rang *un* et donc projectif. En particulier, $\mathbf{Z}$ est de Dedekind.

Exemple 3. L'anneau $k[V]$ des coordonnées d'une variété algébrique affine V définie sur un corps algébriquement clos k, est un anneau de Dedekind si et seulement si V est irréductible, non-singulière et de dimention *un*. Le corps K est alors le *corps des fonctions* de la variété. Cet anneau dépend ici d'un plongement que l'on se donne de V dans un espace affine A^n. Une façon plus *intrinsèque* de le caractériser est qu'il est isomorphe à l'anneau $\mathscr{O}_k[V] \subset K$ des fonctions partout régulières de V [1, p. 17, th. 3.2].

4.2. **Idéaux fractionnaires.** On se donne A un anneau commutatif intègre et on note K son corps des fractions.

Lemme 4.2. *Soit $\mathfrak{F}$ un idéal fractionnaire de A, les propriétés suivantes sont équivalentes :*

(1) *$\mathfrak{F}$ est inversible.*

(2) *$\mathfrak{F}$ est de type fini et pour tout idéal premier $\mathfrak{p}$, $\mathfrak{F}_\mathfrak{p}$ est inversible.*

(3) *$\mathfrak{F}$ est de type fini et pour tout idéal maximal $\mathfrak{m}$, $\mathfrak{F}_\mathfrak{m}$ est inversible.*

Remarque. On dit pour cette raison que (1) ci-dessus est une propriété *locale*.

Démonstration. Montrons que (1) implique (2) : $\mathfrak{F}$ est de type fini puisqu'il est inversible et donc $A_\mathfrak{p} = (\mathfrak{F}(A : \mathfrak{F}))_\mathfrak{p} = \mathfrak{F}_\mathfrak{p}(A_\mathfrak{p} : \mathfrak{F}_\mathfrak{p})$.

Montrons que (3) implique (1) : Posons $\mathfrak{G} = \mathfrak{F}(A : \mathfrak{F})$, c'est un idéal entier et pour chaque idéal maximal $\mathfrak{m}$ on a $\mathfrak{G}_\mathfrak{m} = \mathfrak{F}_\mathfrak{m}(A_\mathfrak{m} : \mathfrak{F}_\mathfrak{m})$ puisque $\mathfrak{F}_\mathfrak{m}$ est inversible. De là $\mathfrak{G} \not\subseteq \mathfrak{m}$ et donc $\mathfrak{G} = A$. Finalement $\mathfrak{F}$ est bien inversible. Fin de la démonstration.

Lemme 4.3. *Soit A un anneau local intègre, les deux points suivants sont équivalents,*

(1) *A est un anneau de valuation discrète.*

(2) *Tout idéal fractionnaire de A est inversible.*

Démonstration. Montrons que (1) implique (2) : On note $\mathfrak{m}$ l'unique idéal maximal de A. Soit $\mathfrak{F} \neq 0$ un idéal fractionnaire de A, il existe donc par définition un élément a de A tel que $a\mathfrak{F} \subseteq A$. Les idéaux (a) et $a\mathfrak{F}$ sont entiers donc de la forme $\mathfrak{m}^r$ et $\mathfrak{m}^s$ de sorte que $\mathfrak{F} = \mathfrak{m}^{s-r}$ est inversible.

Montrons que (2) implique (1) : Il suffit de démontrer que tout idéal entier est une puissance de $\mathfrak{m}$ puisque d'après le premier lemme, A est noethérien. Notons à cette fin Λ l'ensemble des idéaux de A qui ne soient pas des puissances de $\mathfrak{m}$. Supposons-le non-vide en vue d'une contradiction. Soit donc $\mathfrak{a}$ un élément maximal de Λ, on a $\mathfrak{a} \neq \mathfrak{m}$ donc $\mathfrak{a} \subset \mathfrak{m}$ puis comme $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = A$, $\mathfrak{m}^{-1}\mathfrak{a}$ est un idéal propre de A et $\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{a}$. La contradiction provient de ce que l'inclusion est propre en appliquant le lemme de Nakayama. Fin de la démonstration.

En vertu du premier lemme, on peut éliminer l'hypothèse de localité, et l'on a démontré le théorème suivant :

Théorème 4.4. *Soit A un anneau intègre, les deux points suivants sont équivalents,*

(1) A est un anneau de Dedekind.

(2) Tout idéal fractionnaire de A est inversible.

4.3. **Extensions.** Soit A un anneau *noethérien* dont on note K le corps de fraction. Soit encore L une extension finie de K et soit B la clôture intégrale de A dans L

(1) Si A est de Dedekind, B l'est également.

(2) Si l'extension L/K est séparable, B est un A-module de type fini.

On suppose désormais que les deux points précédents sont vérifiés. Les deux exemples que l'on a en vue sont les suivants.

Exemple 4. On pose $A = \mathbf{Z}$ et dans ce cas, L est un *corps de nombres* dont B est l'anneau des entiers. Plus généralement si A est l'anneau des entiers d'un corps de nombres K, le corps L est un corps de nombres dont B est encore l'anneau des entiers (transitivité de la clôture intégrale).

Exemple 5. Soit k un corps algébriquement clos de caractéristique $p > 0$, soit V une courbe algébrique projective connexe, non singulière et définie sur k, (nous sommes dans les hypothèses de l'exemple 3). On se donne un groupe fini G opérant fidèlement sur V au moyen d'automorphismes notés $(\tau_g)_{g\in G}$. On désigne par $V' = V/G$ la variété quotient. Si K et L désignent respectivement les corps de fonctions rationnelles attachés à V' et V, la surjection canonique $\rho : V \to V'$ induit une structure naturelle d'extension L/K qui est galoisienne et dont le groupe de Galois est G.

4.3.1. *Ramification d'une extension.* Nous conservons les notations de l'exemple précédent. Les points fixes d'un automorphisme de V forment une sous-variété de V et comme V est de dimension *un* cette sous-variété est de dimension *nulle* ou *un*, dans le premier cas c'est un nombre fini de points et dans le deuxième cas c'est V tout entière puisqu'elle est supposée irréductible. Comme l'action est fidèle, les τ_g avec $g \neq e$ sont différents de l'identité, donc chaque τ_g n'a qu'un nombre fini de points fixes ; ce sont les *points de ramification* du revêtement. Comme G est fini il n'y a qu'un nombre fini de points de ramification. Les centralisateurs dans G des points de V sont par définition les *groupes d'inertie*, la terminologie prend alors tout son sel.

En formulant cela dans le langage des idéaux de l'anneau de Dedekind correspondant à chacune des courbes, on retrouve les définitions correspondantes relatives aux extension galoisiennes de corps de nombres (la situation de l'exemple 4). C'est là l'un des nombreux avatars de l'analogie entre corps de nombres et corps de fonctions.

4.3.2. *Différente d'une extension.* En conservant les notations précédentes, on appelle différente de l'extension L/K, et l'on note $\mathfrak{D}_{L/K}$, l'idéal de B engendré par la partie suivante :

$$\{f'(x) \,|\, x \in B, f \in A[X] \text{ et } f(x) = 0\}$$

Théorème 4.5. *On suppose que l'anneau B est engendré sur A par un unique élément x dont on note f le polynôme caractéristique. Alors, $\mathfrak{D}_{L/K} = (f'(x))$ et c'est l'annulateur de $\Omega_A(B)$ comme B-module.*

Démonstration. c'est immédiat puisque, $f(x) = 0$ entraîne $0 = \mathrm{d}(f(x)) = f'(x)\mathrm{d}x$ d'une part et que d'autre part $\mathrm{d}x$ engendre $\Omega_A(B)$.

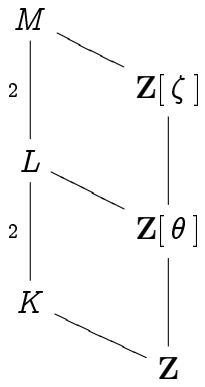
Exemple 6. Nous considérons l'extension quadratique L/K avec $L = \mathbf{Q}(i)$ et $K = \mathbf{Q}$. Les anneaux A et B correspondent respectivement aux entiers relatifs et aux entiers de Gauss. On rappelle qu'il s'agit de l'anneau engendré sur $\mathbf{Z}$ par la racine imaginaire i dont le polynôme minimal f n'est autre que le polynôme cyclotomique $\Phi_4(T) = T^2+1$. Le discriminant de l'extension est l'idéal (4) de sorte que le seul idéal premier de $\mathbf{Z}$ qui puisse être ramifié dans $\mathbf{Z}[i]$ soit (2). L'indice de ramification est nécessairement *deux* pour cet idéal et *un* partout ailleurs. Il n'y qu'un idéal premier de $\mathbf{Z}[i]$ au dessus de (2) c'est l'idéal principal $(1+i) = (1-i)$ de $\mathbf{Z}[i]$ qui est effectivement fixé par le groupe de Galois tout entier qui est donc son groupe d'inertie. La différente de l'extension est $(1+i)^2 = 2\,\mathbf{Z}[i]$, ou encore, en appliquant le théorème, $f'(i)\,\mathbf{Z}[i] = f'(-i)\,\mathbf{Z}[i]$

Exemple 7. Un exemple déjà moins trivial est le suivant. Considérons cette fois l'extension biquadratique M/K avec $M = \mathbf{Q}(\mu_5)$ et $K = \mathbf{Q}$. Les anneaux A et B sont respectivement $\mathbf{Z}$ et $\mathbf{Z}[\zeta]$, où ζ désigne une racine primitive cinquième de l'unité (autrement dit, n'importe laquelle sauf *un*). Comme il est classique, le groupe de Galois G de cette extension s'identifie au groupe multiplicatif du corps $\mathbf{F}_5$ qui est cyclique d'ordre *quatre*. On note H le sous-groupe d'ordre deux qu'il comporte. En notant σ_k l'automorphisme associé à chacune des classes de congruence $k \in \mathbf{F}_5^*$, on peut résumer l'action de G par la table suivante,

	σ_1	σ_2	σ_3	σ_4
ζ	ζ	ζ^2	ζ^3	ζ^4
ζ^2	ζ^2	ζ^4	ζ	ζ^3
ζ^3	ζ^3	ζ	ζ^4	ζ^2
ζ^4	ζ^4	ζ^3	ζ^2	ζ
a	a	b	b	a
b	b	a	a	b

où $a = \zeta + \zeta^{-1}$ et $b = \zeta^2 + \zeta^{-2}$ désignent respectivement la trace de ζ et celle de ζ^2 sur le corps intermédiaire $L = \mathbf{Q}(\mu_5)^{\sigma_4}$. On peut poser $a = 2\cos(\frac{2\pi}{5})$ et $b = 2\cos(\frac{4\pi}{5})$ mais cela revient à choisir $\zeta = e^{\pm\frac{2i\pi}{5}}$ ce qui n'a rien de canonique. On remarque en consultant la table que a et b sont conjugués sur K.

La clôture intégrale de $\mathbf{Z}$ est $\mathbf{Z}[\,\zeta\,]$ dans M et $\mathbf{Z}[\,\theta\,]$ dans L, où $\theta = \frac{1+\sqrt{5}}{2}$ désigne traditionnellement le *nombre d'or*. On résume la situation par le diagramme d'extensions suivant :



Le discriminant de l'extension M/K est l'idéal (125) d'où il résulte que seul l'idéal (5) de $\mathbf{Z}$ peut être ramifié dans $\mathbf{Z}[\,\zeta\,]$ et par conséquent aussi dans $\mathbf{Z}[\,\theta\,]$ comme on le voit de façon directe en calculant le discriminant de l'extension L/K qui est (5). L'idéal principal $(1 + 2\theta)$ de $\mathbf{Z}[\,\theta\,]$ est un idéal premier au dessus de (5) on constate qu'il est fixe sous G, tout comme l'idéal premier (5) de $\mathbf{Z}[\,\zeta\,]$. Les indices de ramification en ces idéaux sont respectivement 2 et 4. En utilisant les relations fondamentales :

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$
$$\zeta^2 + (1 - \theta)\zeta + 1 = 0$$
$$\theta^2 - \theta - 1 = 0$$

on calcule la différente de chacune des extentions,

$$\mathfrak{D}_{M/K} = 125\,\mathbf{Z}[\,\zeta\,] \qquad \mathfrak{D}_{M/L} = 25\,\mathbf{Z}[\,\zeta\,] \qquad \mathfrak{D}_{L/K} = 5\,\mathbf{Z}[\,\theta\,]$$

On rassemble pour finir les discriminants,

$$\mathfrak{d}_{M/K} = 125\,\mathbf{Z} \qquad \mathfrak{d}_{M/L} = 25\,\mathbf{Z}[\,\theta\,] \qquad \mathfrak{d}_{L/K} = 5\,\mathbf{Z}$$

5. Complément

Théorème 5.1. *Soit L un corps de fonctions à une indéterminée sur un corps K, alors*

$$\dim_L \Omega_K(L) \geq 1$$

avec égalité dans le cas séparable.

Démonstration. Nous montrons l'assertion en deux étapes. Posons $B = K[t]$. On se donne un B-module quelconque M et une dérivation $\mathrm{d} : K \to M$. On peut la prolonger en une dérivation $\mathrm{d}_+ : B \to M$ en posant $\mathrm{d}_+(f) = f^{\mathrm{d}}$ où f^{d} est obtenu à partir d'un polynôme $f = a_0 + ... + a_n t^n$ en appliquant d indépendamment à chacun des coefficients : $f^{\mathrm{d}} = \mathrm{d}(a_0) + ... + \mathrm{d}(a_n)t^n$. En vertu du deuxième point du théorème 3.1, l'application naturelle $\Omega_{\mathbf{Z}}(K) \otimes_K K[t] \to \Omega_{\mathbf{Z}}(K[t])$ admet donc une rétraction puis,

$$\Omega_{\mathbf{Z}}(K[t]) \simeq (\Omega_{\mathbf{Z}}(K) \otimes_K K[t]) \oplus K[t]\mathrm{d}t$$

En localisant suivant l'idéal nul on obtient que $\dim_{K'} \Omega_K(K') = 1$ où $K' = K(t)$. Il s'agit ensuite de vérifier que $\Omega_{K'}(L) = 0$ dans le cas où L/K' est une extension algébrique séparable. Il existe dans ce cas pour tout $a \in L$ un polynôme $f \in K'[X]$ tel que $f(a) = 0$ et $f'(a) \neq 0$ et alors $0 = \mathrm{d}(f(a)) = f'(a)\mathrm{d}(a)$ donc $\mathrm{d}(a) = 0$. si bien que d'après le lemme 1.2, $\Omega_{K'}(L) = 0$. Fin de la démonstration.

Références

[1] R. Hartshorne. *Algebraic Geometry*. Number 52 in Graduate texts in Math. Springer, 1977.

[2] M.F. Atiyah I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[3] Y. Kawada. On the derivations in number fields. *Annals of Math.*, 54(2) :303–314, 1951.

[4] E. Kähler. Algebra und differentialrechnug. *Berichte über die Mathematikertagg*, 1953.

[5] H. Matusumura. *Commutative Ring Theory*. Cambrige University Press, 1986.

[6] J.P. Serre. *Corps locaux*. Hermann, Paris, 1968.

[7] A. Weil. Differentiation in algebraic number fields. (abstract). *Bull. Amer. Math. Soc.*, 49 :41, 1943.