Courbes algébriques et applications aux courbes elliptiques

1 Introduction

1.1 Référence

- W. Fulton, Algebraic curves, Benjamin 1969.
- R. Hartshorne, Algebraic Geometry Springer 1977.
- J. Silverman, The arithmetic of elliptic curves, Springer-Verlag, 1986.
- H. Stichtenoth, Algebraic function fields and codes, Springer, 1993.
- R.J. Walker, Algebraic curves Princeton University Press.
- S. Lang, Algebra.
- J.-P. Serre, Corps locaux.
- D. Perrin, Introduction à la géométrie algébrique.

1.2 Plan du cours

Topologie de Zariski, variétés affines.
Variétés projectives, morphisme de variétés projectives.
Cas des courbes algébriques.
Corps de fonctions.
Diviseurs, théorème de Riemann.
Théorème de Riemann-Roch.

2 Variétés affines, topologie de Zariski

Les premières propriétés sur les anneaux (voir Algebra Lang) sont supposées connues. Tous les anneaux considérés sont commutatifs et unitaires. On présente néanmoins 4 rappels

sur les idéaux, les anneaux locaux, la topologie et les groupes de Galois.

2.1 Rappel : Idéaux premiers et maximaux

Définition 2.1 *Un* **idéal premier** $\mathbf{p}$ *est un idéal (sous-groupe stable par la multiplication par les éléments de A) tel que $\mathbf{p} \neq A$ et $\mathbf{p}$ satisfait l'une des conditions équivalentes :*
i. $\forall (a,b) \in A$, $ab \in \mathbf{p}$ implique a ou $b \in \mathbf{p}$,
ii. L'anneau $A/\mathbf{p}$ est intègre.
ii. Soient $\mathbf{a}, \mathbf{b}$ idéaux, notons $\mathbf{ab} = \{ab, (a,b) \in \mathbf{ab}\}$. Si $\mathbf{ab} \subset \mathbf{p}$, alors $\mathbf{a}$ ou $\mathbf{b} \subset \mathbf{p}$.

Dans la suite $\mathbf{p}$ désignera toujours un idéal premier de A.

Définition 2.2 *Un idéal $\mathbf{m}$ est dit* **maximal** *si $\mathbf{m} \neq A$ et s'il est maximal pour l'inclusion.*

On montre qu'un idéal $\mathbf{m}$ est maximal si et seulement si $A/\mathbf{m}$ est un corps.

Remarque 2.1.1 *i. Si A intègre alors (0) est un idéal premier.*
ii. D'après le théorème de Krull, tout idéal est inclus dans un idéal maximal. Il existe donc toujours des idéaux maximaux (lemme de Zorn).
iii. Il existe des idéaux premiers dans A, car tout idéal maximal est premier.

Revoir les anneaux noetheriens.

2.2 Rappel : Anneaux locaux localisation

Définition 2.3 *Un anneau A est dit* **local** *s'il possède un seul idéal maximal.*

Exemple 2.2.1 $k[[X]]$.

Définition 2.4 *Soit A un anneau et S une partie multiplicative de A ($0 \notin S$, $1 \in S$ et si $s, s' \in S$ alors $ss' \in S$. La relation*

$$(a,s) \equiv (a',s') \text{ ssi } as' = a's$$

est une relation d'équivalence sur $A \times S$ et l'ensemble des classes d'équivalence est muni d'une structure d'anneau noté $S^{-1}A$ via les opérations

$$[a, s] + [a', s'] = [as' + a's, ss'], [a, s][a', s] = [aa', ss']$$

Voir MMD.
• Pour A intègre, $S = A - \{0\}$ est multiplicative et $S^{-1}A$ est un corps appelé **corps des fractions** de A.
• Si $\mathbf{p}$ est un idéal premier $S = A - \mathbf{p}$ est multiplicative et $S^{-1}A = A_{\mathbf{p}}$ est dit **localisé** de A en $\mathbf{p}$. C'est un anneau local d'idéal maximal $\mathbf{p}A_{\mathbf{p}}$.

2.3 Rappel : Topologie

Définition 2.5 *Soit X un ensemble. On appelle* **topologie** *sur X la donnée d'un ensemble $\mathcal{O}$ de partie de X possédant les propriétés suivantes :*
i. $\mathcal{O}$ contient $\emptyset$ et X,
ii. la réunion quelconque d'éléments de $\mathcal{O}$ est encore dans $\mathcal{O}$,
iii. l'intersection finie d'éléments de $\mathcal{O}$ est encore dans $\mathcal{O}$.
Les éléments de $\mathcal{O}$ sont appelés **ouverts** *et les complémentaires sont appelés* **fermés**. *Le couple $(X, \mathcal{O})$ est appelé* **espace topologique**.

Par exemple, un espace métrique est un espace topologique.
Si $\mathcal{O} = \{\emptyset, X\}$, X est dit muni de la **topologie grossière**.
On peut définir de façon duale une topologie sur X en donnant l'ensemble de ses fermés.

Définition 2.6 *Soit $(X, \mathcal{O})$ un espace topologique. Une* **base d'ouverts** *de $\mathcal{O}$ est un sous-ensemble $\mathcal{O}'$ de $\mathcal{O}$ tel que $\mathcal{O}$ soit le plus petit ensemble contenant $\mathcal{O}'$ qui soit une topologie (on dit encore que $\mathcal{O}'$ engendre la topologie $\mathcal{O}$).*

Si $\{\{x\}, x \in X\}$ est une base de la topologie de X, X est dit muni de la **topologie discrète**.

Définition 2.7 *Un* **groupe toplogique** *est un groupe muni d'une topologie telle que la loi de groupe soit continue.*

Pour définir un groupe topologique, il suffit de ce donner un groupe et une base de voisinage de 1.

2.4 Rappel : Groupe de Galois

Définition 2.8 *Soit L une extension du corps K. Le* **degré de transcendance** *de L sur K est le plus petit m tel que L soit une extension algébrique d'un corps $K(x_1, \dots, x_n)$.*

Exemple 2.4.1 *Si L/K est algébrique $degtr_{L/K} = 0$.*

Définition 2.9 *Un corps k est dit* **parfait** *si toute extension algébrique de k est séparable.*
L'extension E/k est dite **algébrique** *si tout élément x de E est solution d'un polynôme minimal P_x non nul à coefficients dans k.*
L'extension E/k est dite **séparable** *si pour tout $x \in E$, P_x a des racines simples.*

Exemples 2.4.2 • *Si la caractéristique de k est nulle, alors k est parfait (car P_x est premier à P'_x).*
• *Si k est fini, k est parfait. En effet notons $p = cark$. Soit $f(X) = \sum_{j=0}^{m} b_j X^j \in k[X]$ un polynôme irréductible inséparable. Le morphisme $k \to k, x \mapsto x^p$ est surjectif donc il existe $a_j \in k$ avec $b_j = a_j^p$. Alors $f(X) = (\sum_j a_j X^j)^p$ qui n'est pas irréductible.*
• *Si k est algébriquement clos, alors k est parfait. (Même raisonnement qu'avant en car p).*

Définition 2.10 *L'extension E/k est dite* **normale** *si tout morphisme de corps de E qui laisse fixe k est un automorphisme. (Si l'extension est finie, cela signifie que tous les polynômes irréductible coefficients dans k ayant une racine dans E ont toutes ses racines dans E).*
Une E/k une extension séparable et normale algébrique est dite **galoisienne**.

Soit E/k une extension finie galoisienne. On note $\mathrm{Gal}(E/k) = \mathrm{Aut}_k E$ le groupe des E-automorphisme qui laisse fixe k.

Soit $(G_i)_i \in I$ un système projectif de groupes : pour tous $i, j, k \in I$ avec $i \leq j \leq k$, on a des morphismes de groupes $\varphi_{i,j} : G_j \to G_i$, tels que $\varphi_{i,i} = Id$, $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$. La limite projective de $(G_i)_i \in I$ est le groupe G

$$G = \{(g_i) \in \Pi G_i, \forall i \leq j, g_i = \varphi_{i,j}(g_j)\}$$

Il peut être défini par la propriété universelle suivante : si Y groupe avec morphismes compatibles dans les G_i, alors il existe un morphisme de $Y \to G$ qui induit tout.
On note $\mathrm{Gal}(\overline{k}/k)$ la limite projective des $\mathrm{Gal}(E/k)$ avec E/k extension galoisienne finie.

Proposition 2.4.3 *Soit Ω/k une extension galoisienne (i.e. normale et séparable) de groupe $G = \mathrm{Gal}(\Omega/k)$. Soit S un sous ensemble fini de Ω et*

$$G(S) = \{\sigma \in G, \sigma(s) = s, \forall s \in S\}$$

Il existe une unique structure de groupe topologique sur G pour laquelle les ensembles $G(S)$ forment une base de voisinage de 1. Cette topologie est dite **topologie de Krull**.

Si G est fini, la topologie de Krull est la topologie discrète.

Proposition 2.4.4 *Soit Ω/k une extension galoisienne de groupe G.*
i. Pour tout $k \subset M \subset \Omega$, Ω/M est galoisienne et $\mathrm{Gal}(\Omega/M)$ est un fermé de G avec $\Omega^{\mathrm{Gal}(\Omega/M)} = M$.
ii. Pour tout sous-groupe H de G, l'adhérence $\overline{H} = \mathrm{Gal}(\Omega/\Omega^H)$.

2.5 Ensembles algébriques affines, topologie de Zariski

Dans ce chapitre, k désigne un corps parfait et $\overline{k}$ une clôture algébrique de k.

Définition 2.11 *Un n-espace affine (sur k) est l'ensemble des n-uplets*

$$\mathbf{A}^n = \mathbf{A}^n(\overline{k}) = \{P = (x_1, \ldots, x_n), x_i \in \overline{k}\}.$$

L'ensemble des points k-rationnels de $\mathbf{A}^n$ est l'ensemble

$$\mathbf{A}^n(k) = \{P = (x_1, \ldots, x_n), x_i \in k\}.$$

Remarque 2.5.1 *Le groupe de Galois* $\mathrm{Gal}(\overline{k}/k)$ *agit sur* $\mathbf{A}^n$ *: pour* $P \in \mathbf{A}^n$, $\sigma \in \mathrm{Gal}(\overline{k}/k)$,

$$P^\sigma = (x_1^\sigma, \dots, x_n^\sigma).$$

L'ensemble $\mathbf{A}^n(k)$ *satisfait donc*

$$\mathbf{A}^n(k) = \{P \in \mathbf{A}^n, P = P^\sigma, \sigma \in \mathrm{Gal}(\overline{k}/k)\}.$$

Notons $\overline{k}[X] = \overline{k}[X_1, \dots, X_n]$ l'anneau des polynômes en n variables à coefficients dans $\overline{k}$. A tout partie S de $\overline{k}[X]$, on associe le sous-ensemble de $\mathbf{A}^n$,

$$V(S) = \{P \in \mathbf{A}^n, f(P) = 0, f \in I\}.$$

Définition 2.12 *Un* **ensemble algébrique** *(affine) est un ensemble de la forme* $V(S)$. *Si* V *est un ensemble affine,* **l'idéal de** V *est défini par*

$$I(V) = \{f \in \overline{k}[X] : f(P) = 0, P \in V\}.$$

Proposition 2.5.2 *i.* $I(V)$ *est un idéal.*
ii. $V = V(I(V))$.
iii. $I(V)$ *admet un nombre fini de générateurs.*

Preuve : i. $0 \in I(V)$, $f - g \in I(V)$, $hf \in I(V)$, $h \in \overline{k}[X]$.
ii. $V = V(S)$ donc $S \subset I(V)$ donc $V(I(V)) \subset V$. Réciproquement si $P \in V(S)$, $f(P) = 0$, $f \in I(V)$ donc $f \in V(I(V))$.
iii. L'anneau $\overline{k}[X]$ est noetherien. Ainsi, tout idéal est engendré par un nombre fini d'éléments (théorème de la base d'Hilbert, voir cours d'algèbre formelle de M. Martin-Deschamps). ∎

Définition 2.13 *Un ensemble algébrique* V *est dit défini sur* k *si son idéal* $I(V)$ *est engendré par des polynômes de* $k[X]$. *On note alors* V/k. *Si* V *est défini sur* k, *alors l'ensemble des points* k*-rationnels de* V *est*

$$V(k) = V \cap \mathbf{A}^n(k).$$

Exemples 2.5.3 • *$V(1) = \emptyset$ et $V(0) = \overline{k}[X]$ sont des ensembles algébriques.*
• *$V(x^4 - 2) = \{\pm 2^{1/4}, \pm i 2^{1/4}\}$, $V(x^4 - 2)(\mathbf{R}) = \{\pm 2^{1/4}\}$, $V(x^4 - 2)(\mathbf{Q}) = \emptyset$.*
• *Un point de $\overline{k}$ est un ensemble algébrique car $V(X_1 - x_1, \ldots, X_n - x_n) = \{(x_1, \ldots, x_n)\}$.*
• *Dans $\overline{k}^2$, $V(X_1^2) = V(X_1)$ c'est l'axe des X_2. On a $I(V) = (X_1)$.*
• *Tout sous-espace affine de $\mathbf{A}^n$ est un ensemble algébrique.*

Remarque 2.5.4 • *Soit S une partie de $\overline{k}[X]$. Notons $< S >$ l'idéal engendré par S dans $\overline{k}[X]$. Il est clair que $V(S) = V(< S >)$. En général $I(V(S)) \neq S$ même si S est un idéal.*

Exemples 2.5.5 • *Soit $S = \{f_1, \ldots, f_d\} \subset \overline{k}[X]$. Alors V est vide si et seulement si 1 est combinaison des f_i.*
• *Soit $V = V(X_1^2 + X_2^2 + 1)$ avec $k = \mathbf{R}$. On a $V = V(\mathbf{C})$ est un cercle mais $V(\mathbf{R}) = \emptyset$.*

Proposition 2.5.6 *i. Toute intersection d'ensembles algébriques est un ensemble algébrique.*
ii. Toute réunion finie d'ensembles algébriques est un ensemble algébrique.

Preuve : i. $\cap_\alpha V(S_\alpha) = V(\cup_\alpha S_\alpha)$.
ii. $V(S_1) \cup V(S_2) = V(S_1 S_2)$ où $S_1 S_2$ est l'ensemble des produits d'un élément de S_1 et d'un élément de S_2. (si $x \notin V(S_1) \cup V(S_2)$, $\exists F_1 \in S_1$ et $F_2 \in S_2$ avec $F_1(x) F_2(x) \neq 0$ donc $x \notin V(S_1 S_2)$). ∎

La proposition permet de définir une topologie dite **de Zariski** sur $\mathbf{A}^n(k)$ en prenant pour fermés les ensembles algébriques. Cette topologie n'est pas séparée. Pire, si k est infini, tous ouverts non vides quelconques se rencontrent (la topologie de Zariski sur $\mathbf{A}^n(k)$ où k est fini est discrète). Les ouverts sont très gros, et les fermés très petits. Dans k, les fermés sont $\emptyset$, k et les ensembles finis. On munit tout ensemble algébrique de la topologie induite par la topologie de Zariski de k^n.

Remarque 2.5.7 *Plus généralement, soit A un anneau, le* **spectre** *de A est l'ensemble des idéaux premiers de A :*

$$\operatorname{Spec} A = \{\mathbf{p} \text{ idéal premier de } A\}$$

L'ensemble $\operatorname{Spec} A$ *est muni d'un topologie, dite* **topologie de Zariski** *définie par ses fermés : les fermés de* $\operatorname{Spec} A$ *sont :*

$$V(I) = \{\mathbf{p} \in SpecA, I \subset \mathbf{p}\}, I \text{ idéal (quelconque) de } A$$

Proposition 2.5.8 *i. On a $V \subset V(I(V))$ (vous verrez dans le cours de Mireille Martin-Deschamps que $V(I(V))$ est l'adhérence de V pour la topologie de Zariski donc égalité ssi V affine).*
ii. $S \subset I(V(S))$ mais en général, on n'a pas l'égalité ($I(V(T^2)) = (T)$) même si S est un idéal. La relation entre I et $I(V(I))$ est l'objet du Nullstellensatz.

Remarque 2.5.9 • *Soit V un ensemble algébrique, on considère l'idéal*

$$I(V/K) = \{f \in k[X], f(P) = 0, P \in V\} = I(V) \cap k[X]$$

Alors V est définie sur k si et seulement si

$$I(V) = I(V/k)\overline{k}[X].$$

• *Si $f(X) \in k[X]$ et $P \in \mathbf{A}^n$ alors pour tout $\sigma \in \operatorname{Gal}(\overline{k}/k)$,*

$$f(P^\sigma) = f(P)^\sigma$$

Donc si V est définie sur k, alors l'action de $\operatorname{Gal}(\overline{k}/k)$ sur $\mathbf{A}^n$ insuit une action sur V et

$$V(k) = \{P \in V, P^\sigma = P, \sigma \in \operatorname{Gal}(\overline{k}/k)\}.$$

Déterminer V/k c'est résoudre les équations polynômiales et c'est un problème central en arithmétique.

Exemples 2.5.10 • *L'ensemble algébrique $V(Y^2 - X^3 - 17)$ est une infinité de points $\mathbf{Q}$-rationnels (courbe elliptique semestre 2).*
• *Le théorème de Fermat dit que si $n \geq 3$*

$$V(X^n + Y^n - 1)(\mathbf{Q}) = \begin{cases} \{(1,0),(0,1)\} & n \text{ impair} \\ \{(\pm 1,0),(0,\pm 1) & n \text{ pair} \end{cases}$$

2.6 Variétés algébriques affines

Définition 2.14 *Une ensemble algébrique V est dit variété (affine) si $I(V)$ est un idéal premier dans $\overline{k}[X]$.*

Remarque 2.6.1 • *Si V est définie sur k, il ne suffit pas de vérifier que $I(V/K)$ est premier. En effet Soit $k = \mathbf{Q}$ et $V = V(x^2+y^2)$. Alors $A = \mathbf{Q}[X,Y](X^2+Y^2)$ est intègre donc (X^2+Y^2) est un idéal premier de $\mathbf{Q}[X,Y]$. Mais $(X^2+Y^2) = (X+iY)(X-iY)$ n'est pas premier dans $\overline{\mathbf{Q}}[X,Y]$.*

Définition 2.15 *Un espace topologique est* **irréductible** *si $\forall F_1, F_2$ fermés propres de X, $F_1 \cup F_2 \neq X$.*

Exemples 2.6.2 • $\mathbf{R} =]-\infty, 0] \cup [0, +\infty[$ *n'est pas irréductible.*
• *X est irréductible si et seulement si tout ouvert non vide est partout dense (exercice).*

Définition 2.16 *Soit X un espace topologique une partie $Z \subset X$ est dite* **irréductible**, *si le sous-espace topologique Z est irréductible.*

Les ouverts de Z sont les intersections d'ouverts de X avec Z. La partie Z est irréductible si et seulement si $\overline{Z}$ est irréductible. C'est pourquoi, on s'interesse surtout aux fermés irréductibles.

Les variétés affines sont les ensembles algébriques irréductibles pour la topologie de Zariski (voir MMD).

2.7 Corps de fonctions des variétés affines

Soit V/k une variété (V est définie sur k).

Définition 2.17 *L'anneau de coordonnées affines de V/k est*

$$k[V] = \frac{k[X]}{I(V/k)}$$

C'est un anneau intègre. Son corps des fractions $k(V)$ est dit **corps des fonctions** *de V/k.*

Exemple 2.7.1 *$V = V(y^2 - x^3 + x)$. On montre que $(y^2 - x^3 + x)$ est irréductible dans $\mathbf{R}[x, y]$. Ainsi $\mathbf{R}[V] = \mathbf{R}[x, y]/(y^2 - x^3 + x)$ (voir plus tard).*

Remarque 2.7.2 • *Le groupe $\mathrm{Gal}(\overline{k}/k)$ agit sur $\overline{k}[V]$ et sur $\overline{k}(V)$ (en effet si V est définie sur k, $\mathrm{Gal}(\overline{k}/k)$ laisse stable $I(V)$). On peut même démontrer (cohomologie des groupes)*

$$k[V] = \{f \in \overline{k}[X], f^\sigma = f, \sigma \in \mathrm{Gal}(\overline{k}/k)\}.$$

Définition 2.18 *Soit V une variété. La* **dimension** *de V, notée $\dim V$ est le degré de transcendance de $\overline{k}(V)$ sur $\overline{k}$.*

Exemples 2.7.3 • $\dim A^n = n$ *car* $\overline{k}(A^n) = \overline{k}[X_1, \ldots, X_n]$.
• *Si $f \in \overline{k}[X]$ non constant alors la dimension de l'hypersurface $V(f)$* $\dim V(f) = n - 1$.

Définition 2.19 *Soit V une variété, $P \in V$, $f_1, \ldots, f_m \in \overline{k}[X]$ des générateurs de $I(V)$. Alors V est lisse en P si la matrice jacobienne $m \times n$*

$$(\partial f_i/\partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$$

est de rang $n - \dim(V)$. Si V est lisse en tout point alors on dit que V est lisse.

Remarque 2.7.4 • *La notion de dérivée partielle par rapport à une variable est définie pour n'importe quel corps k avec les règles usuelles de dérivation. (Attention en caractéristique p, $dx^p/dx = px^{p-1} = 0$).*
• *La définition de la lissité ne dépend pas du système de générateurs de $I(V)$ choisi (voir plus loin).*

3 Variétés projectives, morphisme de variétés projectives

3.1 Variétés projectives

Définition 3.1 *L'***espace projectif** *de dimension n, noté $\mathbf{P}^n$ ou $\mathbf{P}^n(\overline{k})$ est l'ensemble des $(n+1)$-uplets*

$$(x_0, \ldots, x_n) \in \mathbf{A}^{n+1}$$

avec au moins un x_i non nul, modulo la relation d'équivalence

$$(x_0, \dots, x_n) \simeq (y_0, \dots, y_n)$$

si $\exists \lambda \in \overline{k}^*$ tel que $x_i = \lambda y_i$, $\forall i$.
Une classe d'équivalence $\{(\lambda x_0, \dots, \lambda x_n)\}$ est notée $[x_0, \dots, x_n]$ et $x_0, \dots, x_n$ sont dits **coordonnées homogènes** *pour les points $[x_0, \dots, x_n] \in \mathbf{P}^n$.*
L'ensemble des **points k-rationnels** *de $\mathbf{P}^n$ est*

$$\mathbf{P}^n(k) = \{[x_0, \dots, x_n] \in \mathbf{P}^n \text{ avec } x_i \in k\}.$$

Remarque 3.1.1 *Le groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ agit sur $\mathbf{P}^n(k)$ via*

$$[x_0, \dots, x_n]^\sigma = [x_1^\sigma, \dots, x_n^\sigma]$$

Définition 3.2 *Un polynôme $f \in \overline{k}[X] = \overline{k}[X_0, \dots, X_n]$ est dit* **homogène** *de degré d si*

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n), \quad \forall \lambda \in \overline{k}.$$

Un idéal $I \subset \overline{k}[X]$ est dit **homogène** *s'il est engendré par des polynômes homogènes.*

Remarque 3.1.2 *Si $f \in \overline{k}[X]$ est homogène, la condition $f(P) = 0$, $P \in \mathbf{P}^n$ ne dépend pas du représentant de la classe d'équivalence.*

Définition 3.3 *A un idéal homogène I, on associe le sous-ensemble de $\mathbf{P}^n$,*

$$V_I = \{P \in \mathbf{P}^n, f(P) = 0, \forall f \text{ homogène } \in I\}.$$

Un **ensemble (algébrique) projectif** *est un ensemble de la forme V_I.*
Si V est un ensemble projectif, on définit **l'idéal homogène** *de V comme l'idéal de $\overline{k}[X]$ engendré par*

$$\{f \in \overline{k}[X], f \text{ homogène et } f(P) = 0, \forall P \in V\}.$$

La variété V est dite **définie sur** *k si $I(V)$ peut-être engendrée par des polynômes homogènes dans $k[X]$.*

De façon analogue au cas affine,

Proposition 3.1.3 *La réunion de deux ensembles projectifs est un ensemble projectif. L'intersection d'une famille d'ensembles projectifs est un ensemble projectif. L'ensemble vide et* $\mathbf{P}^n$ *sont des ensembles projectifs.*

En corollaire, on peut définir la topologie de Zariski sur $\mathbf{P}^n$ en prenant comme ouverts les complémentaires des ensemble projectifs.

Définition 3.4 *Un ensemble algébrique projectif est dit* **variété projective** *si son idéal homogène* $I(V)$ *est premier dans* $\overline{k}[X]$.

Remarque 3.1.4 *Les variétés projectives sont les ensembles algébriques irréductibles pour la topologie induite de la topologie de Zariski (voir Cours de Mireille Martin-Deschamps).*

3.2 Lien affine/projectif

Pour $0 \leq i \leq n$, soit

$$\phi_i : \mathbf{A}^n \to \mathbf{P}^n, (y_1, \dots, y_n) \mapsto [y_1, \dots, y_{i-1}, 1, y_i, \dots, y_n]$$

et on pose $U_i = \{P = [x_0, \dots, x_n] \in \mathbf{P}^n, x_i \neq 0\}$. On a ainsi un recouvrement $\mathbf{P}^n = \cup_{i=0}^n U_i$.

Proposition 3.2.1 *On a un homéomorphisme :* $\phi_i^{-1} : U_i \to \mathbf{A}^n$ *où* $\mathbf{A}^n$ *est muni de la topologie de Zariski et* U_i *de la topologie induite de la topologie de Zariski sur* $\mathbf{P}^n$

Preuve : • C'est un isomorphisme car

$$\phi_i^{-1}[x_0, \dots, x_n] = \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right)$$

Montrons que les ensembles fermés de U_i s'envoient sur les ensembles fermés de $\mathbf{A}^n$ (et réciproquement). Pour fixer les notations, supposons $i = 1$. Notons S^h les polynômes homogènes de $\overline{k}[x_0, \dots, x_n]$. Soit

$$\alpha : S^h \to \overline{k}[y_1, \dots, y_n], \alpha(f) = f(1, y_1, \dots, y_n)$$

$$\beta : \overline{k}[y_1, \dots, y_n] \to S^h, \beta(g) = x_0^e g(x_1/x_0, \dots, x_n/x_O) \text{ où } e = \deg g$$

• Soit $Y \subset U_1$ un ensemble fermé et $\overline{Y}$ sa clôture dans $\mathbf{P}^n$. L'ensemble fermé $\overline{Y}$ est un ensemble projectif, donc il est défini par un idéal homogène $I(\overline{Y})$ engendré par une famille $f_1, \dots, f_r$ de polynômes homogènes de S^h. Soit I l'idéal engendré par la famille $(\alpha(f_i))_{1 \leq i \leq r}$. On a $\phi_1(Y) = V(I)$ est donc fermé.
• Réciproquement si W est un fermé de $\mathbf{A}^n$, alors $W = V(I)$ pour I un idéal de $\overline{k}[y_1, \dots, y_n]$. On a alors $\phi_1^{-1}(W) = V(\beta(I)) \cup U_1$. Donc ϕ_1 et ϕ_1^{-1} sont des applications fermées et ϕ_1 est un homéomorphisme. ∎

Corollaire 3.2.2 *Soit V un ensemble projectif algébrique d'idéal homogène $I(V) \subset \overline{k}[X]$. On a $V = \cup_{i=0}^n V \cap U_i$ et $\phi_i^{-1}(V \cap U_i)$ est un ensemble algébrique affine d'idéal engendré par*

$$\{f(Y_1, \dots, Y_{i-1}, 1, Y_i, \dots, Y_n), \quad f(X_0, \dots, X_n) \text{ homogène } \in I(V)\}.$$

Preuve : C'est le deuxième • de la démonstration précédente. ∎

Définition 3.5 *Le polynôme $\tilde{f}(Y_1, \dots, Y_n) = f(Y_1, \dots, Y_{i-1}, 1, Y_i, \dots, Y_n)$ est dit* **deshomogénéisati** *de $f(X_0, \dots, x_n)$.*

Réciproquement

Définition 3.6 *Si $f(Y) \in \overline{k}[Y]$, on pose*

$$f^*(X_0, \dots, X_n) = X_i^d f(X_0/X_i, \dots, X_{i-1}/X_i, X_{i+1}/X_i, \dots, X_n/X_i)$$

où $d = \deg f$ est le plus petit entier tel que f^* est un polynôme. On appelle f^*, **l'homogénéisation** *de f par rapport à la variable X_i.*

Remarque 3.2.3 *Le polynôme f^* ainsi construit est homogène de degré d car si $g(Y_1, \dots, Y_n) = Y_1^{\alpha_1} \cdots Y_n^{\alpha_n}$ est un monôme de f, on a $d \geq \alpha_1 + \cdots \alpha_n$ et*

$$g^*(X_0, \dots, X_n) = X_i^{d-\alpha_1-\alpha_r} X_0^{\alpha_1} \cdots X_{i-1}^{\alpha_i} X_{i+1}^{\alpha_{i+1}} \cdots X_n^{\alpha_n}$$

homogène de degré d.

Les applications ϕ_i permettent de définir des variétés affines à partie de variétés projectives. Voyaons l'opération inverse qui permet de passer d'une variété affine à une variété projective.

Définition 3.7 *Soit V une variété algébrique affine d'idéal $I(V)$. La* **clôture projective** *de V notée $\overline{V}$ est l'ensemble projectif d'idéal homogène $I(\overline{V})$ engendré par $\{f^*, f \in I(V)\}$.*

Proposition 3.2.4 *i. Si V est une variété affine alors $\overline{V}$ est une variété projective et $V = \phi_i^{-1}(\overline{V} \cap U_i)$.*
ii. Si V est une variété projective, alors $\phi_i^{-1}(V \cap U_i)$ est une variété affine et

$$\phi_i^{-1}(V \cap U_i) = \emptyset \text{ ou } V = \overline{\phi_i^{-1}(V \cap U_i)}.$$

iii. Si la variété affine (resp. proj.) V est définie sur k alors $\overline{V}$ (resp. $\phi_i^{-1}(V \cap U_i)$) est définie sur k.

Preuve : i. Soit V une variété affine. Par définition $\overline{V}$ est un ensemble projectif. Pour voir que $\overline{V}$ est une variété projective, il s'agit de montrer que $I(\overline{V})$ est premier. Comme $I(\overline{V})$ est homogène, il suffit de vérifier que si f, g sont homogènes et $fg \in I(\overline{V})$ alors f ou $g \in I(\overline{V})$. Or la deshomogénéisation $\tilde{f}g \in I(V)$ idéal premier donc $\tilde{f}$ ou $\tilde{g} \in I(V)$ et en homogénéisant, on obtient f ou $g \in I(\overline{V})$.
Par définition $V = \phi_i^{-1}(\overline{V} \cap U_i)$.
ii. Si V est une variété projective, $V \cap U_i$ est irréductible et $\phi_i^{-1}(V \cap U_i)$ aussi. Donc $\phi_i^{-1}(V \cap U_i)$ est une variété affine.
De plus $(V \cap U_i)$ est un ouvert de V irréductible donc il est vide ou dense. S'il est vide $\phi_i^{-1}(V \cap U_i) = \emptyset$. S'il est dense $\overline{\phi_i^{-1}(V \cap U_i)}$ est un fermé de V qui contient un ouvert dense donc $V = \overline{\phi_i^{-1}(V \cap U_i)}$.
iii. Si V est une variété affine définie sur k alors $I(V)$ est engendré par des polynômes $f_1, \ldots, f_r$ de $k[Y_1, \ldots, Y_n]$ donc $I(\overline{V})$ est engendré par $(f_i^*)_{1 \leq i \leq r}$ des polynômes homogènes à coefficients dans k donc $\overline{V}$ est définie sur k.
Si V est une variété projective définie sur k, alors son idéal homogène est engendré par des polynômes homogènes $g_i \in k[X_0, \ldots X_n]$, $1 \leq i \leq s$. L'ensemble algébrique $\phi_i^{-1}(V \cap U_i)$ d'idéal défini sur k car engendré par $g_i(Y_1, \ldots, Y_{i_1}, 1, Y_i, \ldots, Y_n) \in k[Y_1, \ldots, Y_n]$, $1 \leq i \leq s$.
∎

Définition 3.8 *Le* **corps de fonctions** $\overline{k}(V)$ *de la variété projective* V *est*

$$k(V) = \{f/g \text{ où } f, g \in \overline{k}[X_0, \dots, X_n] \text{ homogènes de même degré } g \notin I(V)\}/\simeq$$

où $f/g \simeq f'/g'$ *si* $fg' - f'g \in I(V)$.

Proposition 3.2.5 *Soit* V *une variété projective. Soit* i *avec* $V \cap U_i \neq \emptyset$. *Alors le corps de fonctions* $\overline{k}(V)$ *est isomorphe au corps de fonctions de* $\phi_i^{-1}(V \cap U_i)$.

Preuve : Soit V une variété projective et $I(V)$ son idéal homogène engendré par les polynômes homogènes $f_1, \dots, f_r$. Notons $V' = \phi_i^{-1}(V \cap U_i)$ la variété affine d'ideal $I(V')$ engendré par $f_i(Y_1, \dots, Y_{i-1}, 1, \dots, Y_n)$. Alors

$$\overline{k}(V') = \{f/g \in \overline{k}[Y_1, \dots, Y_n], g \notin I(V')\}/\simeq \text{ avec } f/g \simeq f'/g' \text{ si } fg' - f'g \in I(V')\}$$

L'application d'homogénéisation induit alors un isomorphisme de $\overline{k}(V')$ sur $\overline{k}(V)$. ∎

Définition 3.9 *i. Soit* V *une variété projective et* i *tel que* $V \cap U_i \neq \emptyset$. *La* **dimension** *de* V *est la dimension de* $\phi_i^{-1}(V \cap U_i)$.
ii. Soit $P \in V \cap U_i$, P *est dit* **lisse** *si* $\phi_i^{-1}(P) \in \phi_i^{-1}(V \cap U_i)$ *est lisse. La variété* V *est dite* **lisse** *si tous ses points sont lisses.*

Définition 3.10 *Une courbe est une variété projective de dimension 1.*

3.3 Morphisme de variétés projectives

Définition 3.11 *Soit* $V_1, V_2 \subset \mathbf{P}^n$ *deux variétés projectives. Une* **application rationnelle** *de* V_1 *dans* V_2 *est une application de la forme*

$$\phi : V_1 \to V_2, \quad \phi = [f_0, \dots, f_n],$$

où $f_0, \dots, f_n \in \overline{k}(V_1)$ *satisfont en tout point* $P \in V_1$, $f_0, \dots, f_n$ *sont définies et* $\phi(P) = [f_0(P), \dots, f_n(P)] \in V_2$.

Définition 3.12 *Une application rationnelle*

$$\phi = [f_0, \dots, f_n] : V_1 \to V_2$$

est dite **régulière** *en $P \in V_1$ s'il existe une fonction $g \in \overline{k}(V_1)$ tel que*
i. $\forall i$, gf_i est régulière en P,
ii. pour un i, $(gf_i)(P) \neq 0$.
Une application rationnelle qui est régulière en tout point est dite **morphisme**.

Définition 3.13 *On dit que V_1 et V_2 sont isomorphes , s'il existe des morphismes $\phi : V_1 \to V_2$ et $\psi : V_2 \to V_1$ tels que $\psi \circ \phi$ et $\phi \circ \psi$ sont l'identité. Elles sont isomorphes sur k si ϕ et ψ peuvent être définies sur k.*

Exemples 3.3.1 • *char $k \neq 2$.*
$V : X^2 + Y^2 = Z^2$.
$\phi : V \to \mathbf{P}^1, \phi = [X + Z, Y]$
ϕ est régulière en tout point de V sauf éventuellement en $[1, 0, -1]$ ($\phi([1, 0, -1]) = (0, 0)$). Or $\phi = [X + Z, Y] = [X^2 - Z^2, Y(X - Z)] = [-Y^2, Y(X - Z)] = [-Y, X - Z]$. Donc $\phi([1, 0, -1]) = [0, 2] = [0, 1]$. Donc ϕ est régulière. De plus $\psi : \mathbf{P}^1 \to V, [S^2 - T^2, 2ST, S^2 + T^2]$ est un inverse de ϕ donc V et $\mathbf{P}^1$ sont isomorphes.
• *Supposons $k = \mathbf{F}_q$ et $V \subset \mathbf{P}^n$ une variété définie sur k. Alors l'application*

$$\phi : [X_0, \dots, X_n] \mapsto [X_0^q, \dots, X_n^q]$$

est un morphisme $\phi : V \to V$ dit **morphisme de Frobenius**.

4 Corps de Fonctions

4.1 Anneau de valuation

Soit k un corps.

Définition 4.1 *Un* **corps de fonctions** *algébrique en une variable sur k est une extension de corps F/k telle que F soit une extension algébrique finie de $k(x)$ pour un élément*

x transcendant sur k.
Un tel corps de fonctions est dit **corps des fonctions rationnelles** *si $F = k(x)$ pour un $x \in F$ transcendant sur k.*
Le sous-corps de F des éléments de F algébriques sur k est appelé **corps des constantes** *de F/k.*

Il s'agit de voir que les éléments de F algébriques sur k forment un corps (voir Algebra Lang).

Exemples 4.1.1 • *Le corps des fonctions d'une courbe projective est un corps de fonctions.*
• *Si $\overline{k}/k$ est infinie, $\overline{k}(x)$ n'est pas un corps de fonctions sur k.*

Définition 4.2 *Un* **anneau de valuation** *d'un corps de fonctions F/k est un anneau $\mathcal{O} \subset F$ tel que*
- $k \subset\neq \mathcal{O} \subset\neq F$
- $\forall z \in F$, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Exemple 4.1.2 *Soit le corps des fonctions rationnelles $k(x)$ et $p(x) \in k[x]$ un polynôme irréductible. L'anneau (localisé en (p))*

$$\mathcal{O}_p = \left\{ \frac{f(x)}{g(x)}, f(x), g(x) \in k[x], p(x) \not| g(x) \right\}$$

est un anneau de valuation de $k(x)/k$ ($k \subset\neq \mathcal{O} \subset\neq F$). Si $q(x)$ est un polynôme irréductible non associé à $p(x)$ alors $\mathcal{O}_p \neq \mathcal{O}_q$.

Proposition 4.1.3 *Soit $\mathcal{O}$ un anneau de valuation d'un corps de fonctions F/k. On note $\mathcal{O}^*$ le groupe des unités (éléments inversibles) de $\mathcal{O}$. Alors*
i. $\mathcal{O}$ est un anneau local d'idéal maximal $P = \mathcal{O} - \mathcal{O}^*$.
ii. Si $\tilde{k}$ désigne le corps des constantes de F/k, $\tilde{k} \subset \mathcal{O}$ et $\tilde{k} \cap P = \{0\}$.

Preuve : i. On démontre facilement que P est un idéal de $\mathcal{O}$ ($x \in P$, $z \in \mathcal{O}$ $xz \notin \mathcal{O}^*$ donc $xz \in P$. Pour tous $x, y \in P$ $1 + x/y \in \mathcal{O}$ donc $x + y = y(1 + x/y) \in P$). Il est

maximal et il est unique car contient tous les idéaux stricts de $\mathcal{O}$.
ii. Soit $z \in \tilde{k}$. Si $z \notin \mathcal{O}$ alors $z^{-1} \in \mathcal{O}$ car $\mathcal{O}$ est de valuation. Comme z^{-1} est algébrique sur k, on a $a_r z^{-r} + \cdots + a_1 z^{-1} + 1 = 0$ donc $z^{-1}(a_r z^{-r+1} + \cdots + a_1) = -1$ donc $z = -(a_r z^{-r+1} + \cdots + a_1) \in k[z^{-1}] \subset \mathcal{O}$ donc $z \in \mathcal{O}$. $\tilde{k} \cap P = \{0\}$ est clair. ∎

Commençons par un lemme technique utile :

Lemme 4.3 *Soit $\mathcal{O}$ un anneau de valuation d'un corps de fonctions F/k, P son idéal maximal et $x \in P - \{0\}$. Soit $x_1, \ldots, x_n \in P$ tels que $x_1 = x$ et $x_i \in x_{i+1}P$. Alors $n \leq [F : k(x)] < \infty$.*

Preuve : Comme $x \in P$, et $P \cap \tilde{k} = \{0\}$, on a x transcendant sur k. Comme F/k est de degré de transcendance 1, $[F : k(x)] < \infty$. Pour montrer $n \leq [F : k(x)]$, il suffit de montrer que les éléments $x_1, \ldots, x_n$ sont linéairement indépendants sur $k(x)$. Raisonnons par l'absurde et supposons qu'il existe $\varphi_1, \ldots, \varphi_n \in k(x)$ avec $\sum_{i=1}^n \varphi_i x_i = 0$ ($x | \varphi_i$ si $i > j$). Quitte à multiplier l'expression par un élément de $k(x)$, on peut supposer que tous les φ_i sont des polynômes en x et que x ne les divise pas tous. Posons $a_i = \varphi_i(0)$ et soit j le plus grand indice pour lequel $a_j \neq 0$. Alors

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i$$

avec $\varphi_i \in k[x]$, $x_i \in x_j P$ pour $i < j$ et $\varphi_i = x g_i$ pour $i > j$ ($x \in x_j P$) et $g_i \in k[x]$. Ainsi

$$-\varphi_j = \sum_{i<j} \varphi_i \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i x_i$$

Tous les termes de droite appartiennent à P donc $\varphi_j \in P$. Or $\varphi_j = a_j + x g_j$ avec $g_j \in k[x] \subset \mathcal{O}$ et $x \in P$ donc $a_j = \varphi_j - x g_j \in P \cap k$ donc $a_j = 0$. Absurde ! ∎

Théorème 4.4 *Soit $\mathcal{O}$ un anneau de valuation d'un corps de fonctions F/k, P son idéal maximal et $x \in P - \{0\}$. Alors*
i. P est un idéal principal.
ii. Si $P = t\mathcal{O}$, tout $z \in F - \{0\}$ s'écrit de manière unique $z = ut^n$ avec $n \in \mathbf{Z}$ et $u \in \mathcal{O}^*$.
iii. $\mathcal{O}$ est un anneau principal.

Preuve : i. Si P n'est pas principal. Il existe $x_1, x_2 \in P$ avec $x_2 \in P - x_1\mathcal{O}$. Comme $\mathcal{O}$ est de valuation $x_2x_1^{-1} \notin \mathcal{O}$ implique $x_1x_2^{-1} \in P$ donc $x_1 \in x_2P$. Par récurrence, on construit donc une suite infinie (x_n) d'éléments de P avec $x_i \in x_{i+1}P$ ce qui est exclut par le lemme.
ii. L'unicité est claire. Montrons l'existence. Soit $z \in F - \{0\}$. Comme z ou $z^{-1} \in \mathcal{O}$, on peut supposer $z \in \mathcal{O}$. Si $z \in \mathcal{O}^*$ le résultat est clair. Sinon $z \in P$. D'après le lemme la suite $z, t^{m-1}, \dots, t$ (avec $z \in t^m\mathcal{O}$) est bornée. On prend m maximal tel que $z \in t^m\mathcal{O}$. Il existe alors $u \in \mathcal{O}$ tel que $z = ut^m$.
Si $u \in P = t\mathcal{O}$ alors $z \in t^{m+1}\mathcal{O}$ absurde. Donc $u \in \mathcal{O}^*$.
iii. Soit I un idéal non nul de $\mathcal{O}$. Soit $n = \min\{r \in \mathbf{N}, t^r \in I\}$. On a $t^n \in I$ donc $t^n\mathcal{O} \subset I$. Soit $y \in I - \{0\}$, $y = t^s u$, $u \in \mathcal{O}^*$ donc $t^s \in I$ donc $s \leq n$ donc $y \in t^n\mathcal{O}$. D'où $I = t^n\mathcal{O}$ ∎

4.2 Places et valuation discrète

Rappel : pour un F/k corps de fonctions, (i.e $k(x)/k$ transcendante et $F/k(x)$ algébrique finie), on a défini la notion d'anneau de valuation $\mathcal{O} \subset F$ avec $k \subset\neq \mathcal{O} \subset\neq F$ tel que si $z \in F - \{0\}$, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. On a vu que $\mathcal{O}$ est un anneau local principal d'idéal maximal $P = \mathcal{O} - \mathcal{O}^* = (t)$. Les éléments non nuls de F s'écrivent alors $z = ut^n$ avec $n \in \mathbf{Z}$ et $u \in \mathcal{O}^*$, $z \in \mathcal{O}$ ssi $n \in \mathbf{N}$ et $z \in P$ ssi $n > 0$.

Définition 4.5 *Une* **place** *P d'un corps de fonctions F/k est l'idéal maximal d'un anneau de valuation quelconque de F/k. Une* **uniformisante** *de P est un $t \in P$ avec $P = t\mathcal{O}$. On note $\mathcal{P}_F$ l'ensemble des places de F/k.*

Définition 4.6 *Une* **valuation discrète** *de F/k est une fonction $v : F \to \mathbf{Z} \cup \{\infty\}$ telle que*
1. $v(x) = \infty$ ssi $x = 0$,
2. $\forall x, y \in F$, $v(xy) = v(x) + v(y)$,
3. $\forall x, y \in F$, $v(x + y) \geq \min(v(x), v(y))$,
4. il existe un élément $z \in F$ tel que $v(z) = 1$,
5. $\forall a \in k - \{0\}$, $v(a) = 0$.

Remarque 4.2.1 *(Inégalité triangulaire stricte) Si v est une valuation discrète de F/k et si $x, y \in F$ avec $v(x) \neq v(y)$ alors $v(x+y) = \min(v(x), v(y))$. (preuve classique : on remarque que $v(ax) = v(x), a \in k - \{0\}$ donc $v(-x) = v(x)$. On peut supposer $v(x) > v(y)$. Si $v(x+y) > v(y)$ alors $v(y) = v(x+y) - x) \geq \min(v(x+y), v(x)) > v(x)$ absurde !).*

Définition 4.7 *A une place $P \in \mathcal{P}_F$, on peut associer une valuation v_P en choisissant une uniformisante t pour P et en posant :*
i. $v_P(0) = \infty$,
ii. $v_P(z) = n$ si $z = t^n u$ avec $u \in \mathcal{O}^*$.

Seule la propriété 3 pour v_P nécessite une démontration. Soit $x, y \in F - \{0\}$ avec $v_P(x) = n$ et $v_P(y) = m$. On suppose $n \leq m$. On écrit $x = ut^n$ et $v = u't^m$. Ainsi $x + y = t^n(u + u't^{m-n}) = t^n z$. Si $z = 0$, $v_P(x+y) = \infty \geq \min(v_P(x), v_P(y))$. Sinon $z = u''t^r$ avec $u'' \in \mathcal{O}^*$ et $v_P(x+y) = n + r \geq n = \min(v_P(x), v_P(y))$.

Remarquez que cette définition ne dépend pas du choix de t (car $t' = tu$) mais seulement de P. Le théorème suivant permet de montrer que la donnée d'un anneau de valuation ou d'une valuation discrète d'un corps de fonctions sont équivalentes.

Théorème 4.8 *Soit F/k un corps de fonctions.*
i. Pour toute place P de F/k, v_P est une valuation discrète de F/k et on a $\mathcal{O}_P = \{z \in F, v_P(z) \geq 0\}$, $\mathcal{O}_P^* = \{z \in F, v_P(z) = 0\}$ et $P = \{z \in F, v_P(z) > 0\}$.
ii. Si v est une valuation discrète, alors $P = \{z \in F, v(z) > 0\}$ est une place de F/k d'anneau de valuation $\mathcal{O}_P = \{z \in F, v(z) \geq 0\}$.
iii. Tout anneau de valuation de F/k est un sous-anneau maximal propre de F.

Preuve : i. Comme $P = t\mathcal{O}$, $P = \{z \in F | v(z) > 0\}$. Par définition de v_P, $\mathcal{O}^* = \{z \in F, v_P(z) = 0\}$ et $\mathcal{O} = \mathcal{O}^* \cup P$ donne la dernière égalité.
ii. L'anneau $\mathcal{O}_P$ est un sous-anneau de F de valuation car si $z \in F - \{0\}$, $v(z) = -v(z^{-1})$. La place associée est $P = \{z \in F, v(z) > 0\}$.
iii. Soit $\mathcal{O}$ un anneau de valuation d'idéal maximal P et $z \in F - \mathcal{O}$. Il est propre. Il s'agit de montrer qu'il est maximal. Soit $y \in F$. Pour ℓ assez grand $v(yz^{-\ell}) = v(y) - \ell v(z) \geq 0$ (car $v(z) < 0$) donc $yz^{-\ell} \in \mathcal{O}$. Ainsi $y = (yz^{-\ell})z^\ell \in \mathcal{O}[z]$. Donc $\mathcal{O}[z] = F$ et $\mathcal{O}$ est maximal. ∎

4.3 Degré, zéros et pôles d'une place

Définition 4.9 *Soit P une place et $\mathcal{O}_P$ son anneau de valuation. Comme P est un idéal maximal de $\mathcal{O}_P$, $F_P = \mathcal{O}_P/P$ est un corps, dit* **corps résiduel des classes**.
L'entier $degP = [F_P : k]$ est appelé **degré** *de P.*

Le degré est fini d'après la proposition suivante :

Proposition 4.3.1 *Si P est une place de F/k et $0 \neq x \in P$, alors*

$$\deg P \leq [F : k(x)] < \infty$$

Preuve : Comme $x \neq 0$ et $x \in P$, on a $x \notin \tilde{k}$ donc x est transcendant sur k et $[F : k(x)] < \infty$. Soit $z_1, \ldots, z_n$ des éléments de $\mathcal{O}_P$ dont les classes dans F_P sont k-linéairement indépendantes. Montrons alors que $z_1, \ldots, z_n$ sont $k(x)$-linéairement indépendants. Soit une combinaison linéaire non triviale $\sum_{i=1}^{n} \varphi_i z_i = 0$ avec $\varphi_i \imath nk(x)$. Quitte à multiplier, on peut supposer que tous les $\varphi_i \in k[x]$ et qu'ils ne sont pas tous divisibles par x : il existe j avec $\varphi_j = a_j + xg_j$ avec $a_j \in k - \{0\}$. Or $x \in P$, donc modulo P, on obtient une combinaison linéaire non triviale $\sum_{i=1}^{n} a_i z_i \equiv 0 \mod P$ ce qui contredit que les classes dans F_P sont linéairement indépendantes. Absurde ! ∎

Remarque 4.3.2 *Si deg(P)=1 alors $F_P = k$.*
Si k est algébriquement clos, on a toujours $degP = 1$ (F_P/k est algébrique).

Définition 4.10 *Soit $z \in F$ et $P \in \mathcal{P}_F$. On dit que P est un* **zéro** *d'ordre m de z ssi $v_P(z) = m > 0$, P est un* **pôle** *d'ordre m de z ssi $v_P(z) = m < 0$.*

On conclut ce paragraphe en montrant que l'ensemble des places de F/k n'est pas vide et que tout élément $z \in F$ transcendant sur k admet un pôle et un zéro.

Théorème 4.11 *Soit F/k un corps de fonctions et R un sous-anneau de F contenant k. Soit $\{0\} \subset\neq I \subset\neq R$ un idéal propre de R. Il existe alors une place $P \in \mathcal{P}_F$ avec $I \subset P$ et $R \subset \mathcal{O}_P$.*

Preuve : Soit $\mathcal{F} = \{$ sous-anneau $S \subset F | R \subset S$ et $IS \neq S\}$. C'est un ensemble inductivement ordonné pour l'inclusion. En effet si $H \subset \mathcal{F}$ est une partie totalement ordonnée pour l'inclusion, alors $T = \cup_{S \in H} S \in F$ (T sous-anneau de F, $R \subset T$, si $IT = T$ ($1 \in T$ car T anneau) alors $1 = \sum a_i s_i \in IS'$ absurde). D'après le lemme de Zorn, $\mathcal{F}$ admet un élément maximal $\mathcal{O}$. Comme $I \neq \{0\}$ et $I\mathcal{O} \neq \mathcal{O}$ ($I \cup \mathcal{O}^* = \emptyset$), $I \subset \mathcal{O} - \mathcal{O}^*$ et $\mathcal{O} \subset\neq F$. Supposons qu'il existe $z \in F$ avec $z \notin \mathcal{O}$ et $z^{-1} \notin \mathcal{O}$. Alors par maximalité de $\mathcal{O}$, $I\mathcal{O}[z] = \mathcal{O}[z]$ et $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$, donc $1 = \sum_{i=0}^{n} a_i z^i = \sum_{i=0}^{m} b_i z^{-i}$ ($a_i, b_i \in I\mathcal{O}$). On peut supposer n et m minimaux. Comme $1 \notin I\mathcal{O}$, $m, n \geq 1$, supposons $m \leq n$. Mais alors

$$1 - b_0 = (1 - b_0) \sum a_i z^i = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n$$

$$(1 - b_0)a_n z^n = \sum_{i=1}^{m} b_i z^{n-i} a_n$$

$$(1 - b_0)a_n z^n = b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}$$

Donc $1 = c_0 + \cdots + c_{n-1} z^{n-1}$ absurde. Donc $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$ et $\mathcal{O}$ anneau de valuation. ∎

Corollaire 4.3.3 *Soit F/k un corps de fonctions et soit $z \in F$ transcendant sur k. Alors z a au moins un pôle et un zéro. En particulier $\mathcal{P}_F \neq \emptyset$.*

Preuve : On considère $R = k[z]$ et $I = zk[z]$. D'après le théorème, il existe une place $P \in \mathcal{P}_F$ avec $z \in P$. Donc P est un zéro de z. Le même argument montre que z^{-1} a un zéro $Q \in \mathcal{P}_F$. Donc Q est un pôle de z. ∎

Exemple 4.3.4 *On reprend $F = k(x)$. Si p est un polynôme irréductible unitaire, on peut considérer l'anneau de valuation*

$$\mathcal{O}_p = \{f/g \in k(x), f, g \in k[x] \text{ et } p \not| g\}.$$

Son idéal maximal est

$$P = \{f/g \in k(x), f, g \in k[x], p | f \text{ et } p \not| g\}.$$

Alors $OO_P/P = k[x]/(p(x))$ *et* $\deg P = \deg p$. *On a une autre place dans* $k(x)$ *dite place à l'infini d éfinie par l'anneau de valuation*

$$\mathcal{O}_\infty = \{f/g, f, g \in k[x] \deg f \leq \deg g\}$$

$$P_\infty = \{f/g, f, g \in k[x] \deg f < \deg g\}$$

Alors $\mathcal{O}_\infty/P_\infty = k$ *et* $\deg P_\infty = 1$. *On peut montrer qu'il n'y a pas d'autres places. Soit* $z \in k(x)$ *transcendant sur* k. *Alors*

$$z = \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}{q_1^{\beta_1} \cdots q_s^{\beta_s}}$$

a un pôle et un zéro.

4.4 Théorème d'approximation faible

Dans ce paragraphe, F/k désigne un corps de fonctions et on suppose que k est le corps des constantes de F/k. On va montrer qu'un élément $x \in F - k$ n'a qu'un nombre fini de pôles et de zéros.

Théorème 4.12 Théorème d'approximation faible. *Soit* F/k *un corps de fonctions,* $P_1 \ldots, P_n \in \mathcal{P}_F$ *des places distinctes de* F/k, $x_1, \ldots, x_n \in F$ *et* $r_1, \ldots, r_n \in \mathbf{Z}$. *Alors il existe* $z \in F$ *tel que*

$$v_{P_i}(z - x_i) = r_i, \quad 1 \leq i \leq n.$$

Preuve : • Montrons par récurrence sur n qu'il existe $u \in F$ avec $v_{P_1}(u) > 0$ et $v_{P_i}(u) < 0$, $2 \leq i \leq n$.
Si $n = 2$, comme les anneaux de valuation sont maximaux, $\mathcal{O}_{P_1} \not\subset \mathcal{O}_{P_2}$ et $\mathcal{O}_{P_2} \not\subset \mathcal{O}_{P_1}$. Donc il existe $y_1 \in \mathcal{O}_{P_1} - \mathcal{O}_{P_2}$ et $y_2 \in \mathcal{O}_{P_2} - \mathcal{O}_{P_1}$. L'élément $u = y_1/y_2$ convient ($v_{P_1}(y_1) \geq 0$, $v_{P_2}(y_1) < 0$, $v_{P_1}(y_1) < 0$ et $v_{P_2}(y_2) \geq 0$ donc $v_{P_1}(y_1/y_2) > 0$ et $v_{p_2}(y_1/y_2) < 0$).
Supposons le résultat vrai pour $n - 1 \geq 2$. Il existe $y \in F$ avec $v_{P_1}(y) > 0$ et $v_{P_i}(y) < 0$, $2 \leq i \leq n - 1$. Si $v_{P_n}(y) < 0$ la preuve est terminée. Sinon soit $z \in F$ avec $v_{P_1}(z) > 0$ et $v_{P_n}(z) < 0$ et posons $u = y + z^r$ avec $r \geq 1$ tel que $rv_{P_i}(z)) \neq v_{P_i}(y)$, $1 \leq i \leq n$. Alors

$v_{P_1}(u) \geq \min(v_{P_1}(y), rv_{P_1}(z)) > 0$ et $v_i(u) = \min\{v_{P_i}(y), rv_{P_i}(z)\} < 0$, $2 \leq i \leq n$.

• Montrons qu'il existe $w \in F$ tel que $v_{P_1}(w-1) > r_1$ et $v_{P_i}(w) > r_i$, $2 \leq i \leq n$.
On prend le u de l'étape précédente. Soit $w = (1+u^s)^{-1}$. Pour $s \in \mathbf{N}$ assez grand,

$$v_{P_1}(w-1) = v_{P_1}(-u^s(1+u^s)^{-1}) = sv_{P_1}(u) > r_1$$

et $v_{P_i}(w) = -v_{P_i}(1+u^s) = -sv_{P_i}(u) > r_i$, $2 \leq i \leq n$.

• Montrons que pour $y_1, \ldots, y_n \in F$, il existe $z \in F$ avec $v_{P_i}(z - y_i) > r_i$, $1 \leq i \leq n$.
Soit $s \in \mathbf{Z}$ avec $v_{P_i}(y_j) \geq s$, $1 \leq i, j \leq n$. Il existe $w_1, \ldots, w_n$ avec

$$v_{P_i}(w_i - 1) > r_i - s, \quad v_{P_i}(w_j) > r_i - s, j \neq i$$

Alors $z = \sum_{i=1}^n y_j w_j$ convient.

• Soit $z \in F$, $v_{P_i}(z - x_i) > r_i$, $1 \leq i \leq n$. Soit z_i avec $v_{P_i}(z_i) = r_i$. Il existe $z' \in F$ avec $v_{P_i}(z' - z_i) > r_i$, $1 \leq i \leq n$. D'où

$$v_{P_i}(z') = v_{P_i}((z' - z_i) + z_i) = \min(v_{P_i}(z - z_i), v_{P_i}(z_i)) = r_i$$

Soit $x = z + z'$. alors

$$v_{P_i}(x - x_i) = v_{P_i}((z - x_i) + z') = \min(v_{P_i}(z - x_i), v_{P_i}(z')) = r_i.$$

∎

Proposition 4.4.1 *Soit F/k un corps de fonctions et $P_1, \ldots, P_r \in \mathcal{P}_F$ des zéros d'un éléments x de F. Alors*

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \deg(P_i) \leq [F : k(x)]$$

Preuve : Pour tout $1 \leq i \leq r$, il existe $t_i \in F$ avec $v_{P_j}(t_i) = \delta_{ij}$, $1 \leq j \leq r$.
Par ailleurs, soit $s_{i,1}, \ldots, s_{i,\deg P_i} \in \mathcal{O}_{P_i}$ tels que $s_{i,1}, \ldots, s_{i,\deg P_i}$ mod P_i est une k-base du corps résiduel $F_{P_i} = \mathcal{O}_{P_i}/P_i$. D'après le théorème d'approximation faible, il existe $z_{ij} \in F$ tels que

$$v_{P_i}(s_{i,j} - z_{ij}) > 0, \text{ et } v_{P_k}(z_{ij}) \geq v_{P_k}(x), k \neq i$$

Nous allons montrer que les éléments

$$t_i^a z_{ij}, 1 \leq i \leq r, 1 \leq j \leq \deg P_i, 0 \leq a < v_{P_i}(x)$$

sont $k(x)$-linéairement indépendants ce qui démontrera le théorème car on aura ainsi une famille de $\sum_{i=1}^r v_{P_i}(x) \cdot \deg(P_i)$ éléments de F indépendants sur $k(x)$. D'où

$$\sum_{i=1}^r v_{P_i}(x) \cdot \deg(P_i) \leq [F : k(x)].$$

Raisonnons par l'absurde, s'ils sont liés, on a

$$\sum_{i=1}^r \sum_{j=1}^{\deg P_i} \sum_{a=0}^{v_{P_i}(x)-1} \varphi_{ija} t_i^a z_{ij} = 0 \text{ avec } \varphi_{ija} \in k(x) \text{ non tous nuls .}$$

Quitte à diviser ou multiplier par x, on peut supposer que les $\varphi_{ija} \in k[x]$ ne sont pas tous divisibles par x. On note $k \in \{1, \ldots, r\}$, $c \in \{0, \ldots, v_{P_k}(x) - 1\}$ les indices tels que

$$\forall a < c, \forall i \in \{1, \ldots, \deg P_k\}, x | \varphi_{kja}, \text{ et } \exists j \{1, \ldots, \deg P_k\}, x \not| \varphi_{kjc}$$

Or $\sum_{i=1}^r \sum_{j=1}^{\deg P_i} \sum_{a=0}^{v_{P_i}(x)-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0$.
Pour $i \neq k$, $v_{P_k}(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) = v_{P_k}(\varphi_{ija}) + a v_{P_k}(t_i) - c v_{P_k}(t_k) + v_{P_k}(z_{ij}) \geq 0 + 0 - c + v_{P_k}(x) > 0$.
Car $v_{P_k}(\varphi_{ija}) \geq 0$ car P_k zéro de x donc P_k ne peut pas être un pôle d'un polynôme en x.
$v_{P_k}(t_i) = 0$ par définition de t_i vu que $i \neq k$.
et $v_{P_k}(z_{ij} \geq v_{P_k}(x)$ si $i \neq k$.
Pour $i = k$ et $a < c$, $v_{P_k}(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) \geq v_{P_k}(x) + a - c > 0$ ($x | \varphi_{kja}$ donc $v_{P_k}(\varphi_{kja}) \geq v_{P_k}(x)$ et $v_{P_i}(z_{ij}) \geq \min(v_{P_i}(s_{ij} - z_{ij}), v_{P_i}(s_{ij})) \geq 0$).
Pour $i = k$ et $a > c$, $v_{P_k}(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) \geq a - c > 0$ (pareil).
Donc tous ces éléments appartiennent à P_k. Donc (pour $a = c$ et $i = k$)

$$\sum_{j=1}^{\deg P_k} \varphi_{kjc} z_{kj} \in P_k.$$

La classe de φ_{kjc} modulo P_k appartient à k (car c'est un polynôme de $k(x)$ et $x \in P_k$) et il existe $j \in \{1, \ldots, \deg P_k\}, x \not| \varphi_{kjc}$, donc $\varphi_{kjc} \notin P_k$. Nous obtenons donc une k-combinaison linéaire non triviale

$$\sum_{j=1}^{\deg P_k} \varphi_{kjc}(P_k) z_{kj} = 0 \mod P_k$$

ce qui est exclu car z_{kj} mod P_k forment une base de F_{P_k}/k. ∎

Corollaire 4.4.2 *Un élément x non nul d'un corps de fonctions F/k ne peut avoir qu'un nombre fini de zéros et de pôles.*

Preuve : Si x est constant, il n'a ni pôle, ni zéro. Si x est transcendant sur k, le nombre de ses zéros est $\leq [F : k(x)]$ d'après la proposition 4.4.1. Le même argument pour x^{-1} permet de montrer la finitude du nombre de pôles. ∎

5 Diviseurs, théorème de Riemann

5.1 Groupe de Picard, dimension

Définition 5.1 *Le groupe abelien libre engendré par les places de F/k est noté $\mathcal{D}_F$ et est appelé* **groupe des diviseurs** *de F/k. Ses éléments sont appelés les* **diviseurs** *de F/k. Un diviseur est donc une somme formelle $D = \sum_{P \in \mathcal{P}_F} n_P P$ où les $n_P \in \mathbf{Z}$ sont presque tous nuls. • Étant donné $Q \in \mathcal{P}_F$ et un diviseur $D = \sum_{P \in \mathcal{P}_F} n_P P$, on pose $v_Q(D) = n_Q$. Le* **degré** *d'un diviseur est*

$$\deg(D) = \sum_{P \in \mathcal{P}_F} v_P(D) \cdot \deg P$$

Ceci définit un morphisme $\deg : \mathcal{D}_F \to \mathbf{Z}$.
• *On définit un ordre partiel sur $\mathcal{D}_F$ via $D_1 \leq D_2$ si $\forall P \in \mathcal{P}_F$, $v_P(D_1) \leq v_P(D_2)$. Un diviseur D est dit* **effectif** *si $D \geq 0$.*

D'après corollaire 4.4.2 si $x \in F - \{0\}$, z n'a qu'un nombre fini de zéros et de pôles. La définition suivante a donc un sens :

Définition 5.2 *Soit $x \in F - \{0\}$. Le* **diviseur principal** *associé à x est $(x) = \sum_{P \in \mathcal{P}_F} v_P(x)P$. Le groupe $\mathbf{P}_F = \{(x), x \in F - \{0\}\}$ est le* **groupe des diviseurs principaux** *et le groupe quotient $\mathcal{C}_F = \mathcal{D}_F/\mathbf{P}_F$ est le* **groupe des classes de diviseurs**. *On note $\simeq$ la relation d'équivalence sur $\mathcal{D}_F$ associé à $\mathcal{C}_F$.*
On note D_F^0 le groupe des diviseurs principaux de degré zéro et $Pic_{F/k}^0 = \mathcal{D}_F/\mathbf{P}_F$ le **groupe de Picard** *(d'après le théorème 5.8 $\mathbf{P}_F \subset D_F^0$)*

Remarque 5.1.1 *Ainsi, étant donné une courbe C définie sur k, on a défini le corps de fonctions F de C. A partir de ce corps de fonctions, on a défini un groupe $Pic_{C/k}^0$. On peut identifier les éléments de ce groupe aux points d'un courbe et parfois cette courbe coincide avec la courbe de départ. Précisement, le résultat motivant ce travail est le suivant : soit $k \subset L \subset \overline{k}$, on peut montrer que $Pic_{C/L}^0 = J_C(L)$ correspond aux L-points d'une variété projective lisse (irréductible) sur $\overline{k}$ muni d'une structure de groupe algébrique (J_C est dite variété abelienne). Donc à partir d'une courbe projective C, on a défini une variété abelienne J_C, i.e une autre courbe avec une loi de groupe. Si C est une courbe elliptique, on montre $J_C = C$ donc on a défini une structure de variété abelienne sur C. Ce résutlat s'obtient comme application du théorème de Riemann-Roch.*

Pour le moment, définissons un autre invariant sur les diviseurs $A \in D_F$, la dimension. L'objet du théorème de Riemann (et sa version affinée, le théorème de Rieman-Roch) est de relier les dimension et degré d'un diviseur.

Définition 5.3 *Soit $A \in \mathcal{D}_F$ un diviseur, on note*

$$\mathcal{L}(A) = \{x \in F, (x) \geq -A\} \cup \{0\}$$

ainsi $v_P(x) \geq -v_P(A)$, pour tout $P \in \mathbf{P}_F$.

Remarque 5.1.2 • *Si $A = \sum_{i=1}^r n_i P_i - \sum_{j=1}^s m_j Q$ avec $n_i > 0$ et $m_j > 0$, alors $\mathcal{L}(A)$ est l'ensemble des éléments de F ayant des zéros d'ordre au moins m_j en Q_j et ayant tous ses pôles en P_i, l'ordre en P_i étant au plus n_i.*

• $\mathcal{L}(A) \neq \{0\}$ *ssi il existe un diviseur* $A' \simeq A$, *avec* $A' \geq 0$ *(en effet* $A' = A + (x) \geq 0$ *avec* $x \in \mathcal{L}(A) - \{0\}$*).*
• *On a* $k \subset \mathcal{L}(0)$ *et* $x \in \mathcal{L}(0)$ *n'a ni pôle ni zéro donc n'est pass transcendant sur* k *donc* $x \in \tilde{k} = k$ *et* $\mathcal{L}(0) = k$.

Lemme 5.4 *Soit* $A \in \mathcal{D}_F$.
i. L'ensemble $\mathcal{L}(A)$ *est un* k*-espace vectoriel.*
ii. Si A' *est un diviseur équivalent à* A, *alors* $\mathcal{L}(A)$ *et* $\mathcal{L}(A')$ *sont isomorphes en tant que* k*-espaces vectoriels.*

Preuve : i. Soit $x, y \in \mathcal{L}(A)$, $\lambda, \mu \in k$. On a $\lambda x + \mu y \in \mathcal{L}(A)$ car

$$v_P(\lambda x + \mu y) \geq \min(v_P(\lambda x), v_P(\mu y)) \geq \min(v_P(x), v_P(y)) \geq -v_P(A).$$

ii. $A' \simeq A$ donc il existe $z \in F - \{0\}$, $A' = A + (z)$. Les applications k-linéaires

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}(A) & \to & F \\ x & \mapsto xz & \end{array} \right. \quad \varphi' : \left\{ \begin{array}{ccc} \mathcal{L}(A') & \to & F \\ x & \mapsto xz^{-1} & \end{array} \right.$$

sont à valeurs dans $\mathcal{L}(A')$, $\mathcal{L}(A)$ respectivement et sont inverses l'une de l'autre. Donc φ induit un isomorphisme de $\mathcal{L}(A)$ sur $\mathcal{L}(A')$. ∎

Lemme 5.5 *Soit* A, B *des diviseurs de* F/k *avec* $A \leq B$. *Alors* $\mathcal{L}(A) \subset \mathcal{L}(B)$ *et*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A.$$

Ainsi $\dim B - \deg B \geq \dim A - \deg A$.

Preuve : L'inclusion $\mathcal{L}(A) \subset \mathcal{L}(B)$ est claire.
Par récurrence, on peut supposer $B = A + P$ pour un $P \in \mathcal{P}_F$. Soit $t \in F$ tel que $v_P(t) = v_P(B) = v_P(A) + 1$ et $x \in \mathcal{L}(B)$. On a $v_P(x) \geq -v_P(B) = -v_P(t)$ donc $xt \in \mathcal{O}_P$. On a donc une application k-linéaire

$$\phi : \mathcal{L}(B) \to F_P, x \mapsto xt \mod P$$

de noyau $\mathcal{L}(A)$ qui induit une application injective de $\mathcal{L}(B)/\mathcal{L}(A)$ dans F_P. On a donc $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim(F_P) = \deg(P) = \deg(B) - \deg(A)$. ∎

Définition 5.6 *La* **dimension** *d'un diviseur A est définie par*

$$\dim(A) = \dim_k \mathcal{L}(A).$$

5.2 Genre d'un corps de fonctions, théorème de Riemann

Le genre de F/k est le maximum de $\deg A - \dim A + 1$ pour $A \in \mathcal{D}_F$. Pour voir qu'il est effectivement bien défini, nous devons donner quelques propriétés du degré et de la dimension d'un diviseur, d'abord pour les diviseurs principaux.

Définition 5.7 *Soit $x \in F - \{0\}$. Notons Z (resp. N) l'ensemble des zéros (resp. pôles) de x. On définit* **le diviseur de zéros** *de x par*

$$(x)_0 = \sum_{P \in Z} v_P(x) P$$

et le **diviseur des pôles** *de x*

$$(x)_\infty = -\sum_{P \in N} v_P(x) P$$

Remarque 5.2.1 *Le diviseur principal de x est donc $(x) = (x)_0 - (x)_\infty$.*

Théorème 5.8 *Pour tout $x \in F - k$, on a*

$$\deg((x)_0) = \deg((x)_\infty) = [F : k(x)]$$

En particulier $\deg(x) = 0$.

Preuve : Nous avons $(x)_0 = (x^{-1})_\infty$ donc il suffit de montrer que $\deg(x)_\infty = [F : k(x)] = n$ pour avoir $\deg((x)_0) = \deg((x^{-1})_\infty) = [F : k(x^{-1})] = [F : k(x)]$.
Par définition et d'après la proposition 4.4.1

$$\deg(x)_\infty = \sum_{P \in N} v_P(x^{-1}) \deg P \leq [F : k(x)]$$

Soit $(u_i)_{1 \leq i \leq n}$ une base de $F/k(x)$. Soit C un diviseur effectif ($C \geq 0$) de degré $c = \deg C$ avec $(u_i) \geq -C$ pour tout $1 \leq i \leq n$.

Pour $l \geq 0$, $1 \leq i \leq n$, $0 \leq j \leq l$, $x^j u_i \in \mathcal{L}(l(x)_\infty + C) \geq n(l+1)$. Or ces éléments sont linéairement indépendants sur k car les u_i sont linéairement indépendants sur $k(x)$. Donc $\dim_k \mathcal{L}(l(x)_\infty + C) \geq n(l+1)$.
D'après le lemme 5.5 appliqué aux diviseurs 0 et $l(x)_\infty + C$,

$$\forall n \in \mathbf{N}, n(l+1) \leq \dim(l(x)_\infty + C) \leq l \deg(x)_\infty + \deg C + 1$$

Donc $\forall l \in \mathbf{N}$, $l(\deg(x)_\infty - n) \geq n - c - 1$. Pour l assez grand, on obtient alors $\deg(x)_\infty - n \geq 0$. D'où $\deg(x)_\infty \geq n$. ∎

Corollaire 5.2.2 *i. Deux diviseurs équivalents ont même degré et même dimension.*
ii. Si A est un diviseur de degré $\deg(A) < 0$*, alors* $\dim A = 0$.
iii. Si A est un diviseur de degré 0, alors on a l'équivalence entre :
(a). A est principal
(b). $\dim A \geq 1$
(c). $\dim(A) = 1$.

Preuve : i. Si A' est équivalent à A alors, $\mathcal{L}(A)$ et $\mathcal{L}(A')$ sont isomorphes donc $\dim A = \dim A'$. De plus $\deg A = \sum_{P \in \mathcal{P}_F} v_P(A) \deg P = \deg A' + \deg(x)$ car $A = A' + (x)$ et $\deg(x) = \deg(x)_0 - \deg(x)_\infty = 0$.
ii. Si $\mathcal{L}(A) \neq \{0\}$, il existe un diviseur $A' = (x) + A$ ($x \in \mathcal{L}(A) - \{0\}$) équivalent à A tel que $A' \geq 0$ donc $\deg A' = \deg A \geq 0$ exclu.
iii. $a \Rightarrow b$ si $A = (x)$ alors $x^{-1} \in \mathcal{L}(A)$ (car $(x) + (x^{-1}) = (x) - (x) \geq 0$) donc $\dim A \geq 1$.
$b \Rightarrow c$ Si $\dim A \geq 1$, alors il existe $A' = A + (x)$ équivalent à A avec $A' \geq 0$. Or $\deg A = 0 = \deg A'$ donc $A' = 0$ donc $\dim A = \dim A' = \dim 0 = 1$.
$c \Rightarrow a$ Soit $z \in \mathcal{L}(A) - \{0\}$, ainsi $A + (z) \geq 0$. Or $\deg((z) + A) = \deg A = 0$ donc $(z) + A = 0$ donc $A = -(z) = (z^{-1})$ est principal. ∎

Définition 5.9 *Le* **genre** *de F/k est*

$$g = \max\{\deg A - \dim A + 1, A \in \mathcal{D}_F\}$$

Proposition 5.2.3 *Le genre est bien défini* $g \in \mathbf{N}$.

PREUVE : Pour $A = 0$ alors $\deg 0 - \dim 0 + 1 = 0$ (on a vu que $\dim 0 = 1$). Donc $g \geq 0$. Il suffit donc de montrer que g est fini. C'est le corollaire des deux lemmes 5.10 et 8.15.
∎

Lemme 5.10 *Soit* $x \in F - k$ *et* $B = (x)_\infty$. *Il existe* $\gamma \in \mathbf{Z}$ *tel que* $\deg(lB) - \dim(lB) \leq \gamma$, $\forall l > 0$.

PREUVE : Comme on l'a fait pour la démontration du théorème 5.8, il existe un diviseur $C \geq 0$ (qui dépend de x) tel que $\dim(lB + C) \geq (l+1)\deg B$, $\forall l \geq 0$. Or $\dim(lB + C) \leq \dim(lB) + \deg C$. Donc $\dim(lB) \geq (l+1)\deg B - \deg C = \deg(lB) + [F : k(x)] - \deg C$.
∎

Lemme 5.11 *Il existe une constante* $\gamma \in Z$ *tel que pour tout diviseur* $A \in \mathcal{D}_F$, *on a*

$$\deg A - \dim A \leq \gamma.$$

PREUVE : On note B, γ les éléments donnés par la preuve du lemme précédent. Soit $A \in \mathcal{D}_F$. Soit $A_1 \in D_F$ avec $A_1 \geq 0, A$. Alors $\dim(lB - A_1) \geq \dim(lB) - \deg A_1 \geq \deg(lB) - \gamma - \deg A_1 > 0$ pour l assez grand. Donc il existe $z \neq 0 \in \mathcal{L}(lB - A_1)$. Soit $D = A_1 - (z) \simeq A_1$. On a $D \leq A_1 - (A_1 - lB) = lB$.
Ainsi

$$\deg A - \dim A \leq \deg A_1 - \dim A_1 = \deg D - \dim D \leq \deg(lB) - \dim(lB) \leq \gamma.$$

∎

Théorème 5.12 *(Théorème de Riemann)*
Soit F/k un corps de fonctions de genre g.
i. Pour tout diviseur $A \in D_F$, $\dim A \geq \deg A + 1 - g$.
ii. Il existe $c \in \mathbf{Z}$ dépendant de F/k tel que

$$\deg A \geq c \Rightarrow \dim A = \deg A + 1 - g.$$

Preuve : ii. Par définition du genre, il existe $A_0 \in \mathcal{D}_F$ tel que $g = \deg A_0 - \dim A_0 + 1$. Montrons que la constante $c = \deg A_0 + g$ convient. Soit $A \in \mathcal{D}_F$ tel que $\deg A \geq c$, alors

$$\dim(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g \geq 1.$$

Donc il existe $z \in \mathcal{L}(A - A_0) - \{0\}$. Soit $A' = A + (z) \geq A_0$, on a

$$\deg A - \dim A = \deg A' - \deg A' \geq \deg A_0 - \dim A_0 = g - 1.$$

∎

6 Théorème de Riemann-Roch

L'objet du théorème de Riemann-Roch est une formule plus précise reliant le degré et la dimension d'un diviseur. Pour F/k un corps de fonctions, on va définir la notion de diviseur canonique et le théorème de Riemann-Roch s'énonce :

Théorème 6.1 *(Théorème de Riemann-Roch)*
Soit F/k un corps de fonctions de genre g. Soit W un diviseur canonique de F/k. Alors pour tout $A \in \mathcal{D}_F$,

$$\dim A = \deg A + 1 - g + \dim(W - A)$$

Remarque 6.0.4 • *Le diviseur canonique est de dimension g (prendre $A = 0$, $1 = \dim 0 = \deg 0 + 1 - g + \dim W$) et de degré 2g-2 (prendre $A = W$, $g = \dim W = \deg W + 1 - g + \dim 0$).*

Définition 6.2 *Soit $A \in \mathcal{D}_F$, on note $i(A) = \dim A - \deg A + g - 1$.*

Définition 6.3 *Une* **adèle** *de F/k est un élément $\alpha = (\alpha_P)_{P \in \mathcal{P}_F} \in \Pi_{P \in \mathcal{P}_F} F$ tel que $\alpha_P \in \mathcal{O}_P$ pour presque tout $P \in \mathbf{P}_F$.*
L'ensemble des adèles est une k-algèbre $\mathbf{A}_F$.
Pour $x \in F$, on peut définir l'adèle constant (x) (qui n'a qu'un nombre fini de pôles).
La valuation v_P de F/k s'étend à $\mathbf{A}_F$ via $v_P(\alpha) = v_P(\alpha_P)$.

Définition 6.4 *Pour $A \in \mathcal{D}_F$, on définit*

$$\mathbf{A}_F(A) = \{\alpha \in \mathbf{A}_F, v_P(\alpha) \geq -v_P(A), \forall P \in \mathbf{P}_F\}$$

On peut alors interpréter $i(A)$ comme la dimension de l'espace vectoriel suivant :

Théorème 6.5 *On a*

$$i(A) = \dim A - \deg A + g - 1 = \dim_k \mathbf{A}_F/(\mathbf{A}_F(A) + F)$$

Preuve : • Soit $A_1 \leq A_2 \in \mathcal{D}_F$. Alors $\mathbf{A}_F(A_1) \subset \mathbf{A}_F(A_2)$ et nous allons montrer que

$$\dim_k(\mathbf{A}_F(A_2)/\mathbf{A}_F(A_1)) = \deg A_2 - \deg A_1.$$

Par récurrence, il suffit de montrer la formule pour $A_2 = A_1 + P$ avec $P \in \mathcal{P}_F$ Soit $t \in F$ avec $v_P(t) = v_P(A_1) + 1$. Soit l'application k-linéaire

$$\varphi : \begin{cases} \mathbf{A}_F(A_2) & \to & \mathbf{F}_P = \mathcal{O}_P/P, \\ \alpha & \mapsto & (t\alpha_P) \mod P. \end{cases}$$

L'application φ est surjective et son noyau est $\mathbf{A}_F(A_1)$. Ainsi

$$\deg A_2 - \deg A_1 = \deg P = [F_P : k] = \dim_k(\mathbf{A}_F(A_2)/\mathbf{A}_F(A_1)).$$

• Soit $A_1 \leq A_2 \in \mathcal{D}_F$. Montrons que

$$\dim((A_F(A_2) + F)/(\mathbf{A}_F(A_1) + F)) = (\deg A_2 - \dim A_2) - (\deg A_1 - \dim A_1).$$

Le noyau de l'application

• Soit B un diviseur avec $\dim B = \deg B + 1 - g$. Montrons que

$$\mathbf{A}_F = \mathbf{A}_F(B) + F.$$

En effet si $B_1 \geq B$ alors

$$\dim B_1 \leq \deg B_1 + \dim B - \deg B = \deg B_1 + 1 - g$$

D'après le théorème de Riemann, $\dim B_1 \geq \deg B_1 + 1 - g$. Donc pour tout $B_1 \geq B$, on a $\dim B_1 = \deg B_1 + 1 - g$.

Soit $\alpha \in \mathbf{A}_F$. Il existe un diviseur $B_1 \geq B$ tel que $\alpha \in \mathbf{A}_F(B_1)$. D'après létape précédente, on a alors

$$\dim((A_F(B_1)+F)/(\mathbf{A}_F(B)+F) = (\deg B_1 - \dim B_1) - (\deg B - \dim B) = (g-1)-(g-1) = 0$$

Donc $\mathbf{A}_F(B) + F = \mathbf{A}_F(B_1) + F$. Or $\alpha \in \mathbf{A}_F(B_1)$ donc $\alpha \in \mathbf{A}_F(B) + F$. D'où $\mathbf{A}_F = \mathbf{A}_F(B) + F$.

• Soit $A \in \mathcal{D}_F$. D'après le théorème de Riemann, il existe $A_1 \geq A$, tel que $\dim A_1 = \deg A_1 + 1 - g$. Ainsi $\mathbf{A}_F = \mathbf{A}_F(A_1) + F$. L'étape 2 donne ainsi

$$\dim_k(\mathbf{A}_F/(\mathbf{A}_F(A)+F)) = \dim_k(\mathbf{A}_F(A_1)+F)/(\mathbf{A}_F(A)+F) = (\deg A_1 - \dim A_1) - (\deg A - \dim A) = (g-$$

■

Et maintenant le diviseur canonique pour interpréter le terme $\dim \mathbf{A}_F/(\mathbf{A}_F(A) + F)$.

Définition 6.6 *Une différentielle de Weil de F/k est une application k-linéaire $\omega : \mathbf{A}_F \to k$ telle qu'il existe $A \in \mathcal{D}_F$ tel que ω est nulle sur $\mathbf{A}_F(A) + F$. On note*

$$\Omega_F = \{\omega, \omega \text{ différentielle de Weil de } F/k\}$$

le module des différentielles de Weil de F/k. Pour $A \in \mathcal{D}_F$, on pose

$$\Omega_F(A) = \{\omega \in \Omega_F, \omega \text{ s'annule sur } \mathbf{A}_F(A) + F\}.$$

Remarque 6.0.5 • *Le module des différentielles $\Omega_{F/k}$ est un k-espace vectoriel ($\omega_1 + \omega_2$ s'annule sur $\mathbf{A}_F(A_3)$ avec $A_3 \leq A_2, A_1$ et $a\omega$ s'annule sur $\mathbf{A}_F(A) + F$ pour $a \in k$) et $\Omega_F(A)$ et un sous-espace vectoriel de Ω_F.*
• *Pour $A \in \mathcal{D}_F$, $i(A) = \dim \Omega_F(A)$. En effet, $\Omega_F(A)$ est isomorphe à l'espace des formes linéaires sur $\mathbf{A}_F/(\mathbf{A}_F(A) + F)$ qui est de dimension finie égale à $i(A)$.*

Proposition 6.0.6 *Le module des différentielle Ω_F a une structure de F-espace vectoriel via*

$$(x\omega)(\alpha) = \omega(x\alpha), \omega \in \Omega_F, x \in F, \alpha \in \mathbf{A}_F$$

Preuve : L'application $x\omega$ est une différentielle nulle sur $\mathbf{A}_F(A + (x)) + F$. ∎

Proposition 6.0.7 *Le module des différentielle Ω_F est de dimension 1 sur F.*

Preuve : Soit $\omega_1 \in \Omega_F - \{0\}$. Il s'agit de montrer que pour tout $\omega_2 \in \Omega_F$, il existe $z \in F$ tel que $\omega_2 = z\omega_1$. Pour cela, on peut supposer $\omega_2 \neq 0$. Soit A_1, A_2 avec $\omega_1 \in \Omega_F(A_1)$ et $\omega_2 \in \Omega_F(A_2)$. Pour $B \in \mathcal{D}_F$, on considère les applications k-linéaires injectives :

$$\varphi_i : \begin{cases} \mathcal{L}(A_i + B) & \to & \Omega_F(-B), \\ x & \mapsto x\omega_i & \end{cases} \quad i = 1, 2.$$

On va montrer qu'il existe un diviseur B tel que $\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}$. Cela démontre la proposition car alors on prend $x_1 \in \mathcal{L}(A_1 + B)$ et $x_2 \in \mathcal{L}(A_2 + B)$ avec $x_1\omega_1 = x_2\omega_2 \neq 0$. Alors $\omega_2 = (x_1 x_2^{-1})\omega_1$.
D'après le théorème de Riemann, si le degré de B est suffisamment grand alors

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g, i = 1, 2$$

Or

$$\dim \Omega_F(-B) = i(-B) = \dim(-B) - \deg(-B) + g - 1 = \deg B - 1 + g$$

On pose $U_i = \varphi_i(Ł(A_i + B)) \subset \Omega_F(-B)$. Ainsi,

$$\dim(U_1 \cap U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cup U_2) \geq \dim U_1 + \dim U_2 - \dim \Omega_F(-B)$$

$\geq \deg(A_1+B)+1-g+\deg(A_2+B)+1-g-(\deg B+g-1) \geq \deg B+(\deg A_1+\deg A_2+3(g-1))$
Le terme entre parenthèses est indépendant de B, donc $\dim(U_1 \cap U_2) > 0$ si $\deg B$ est assez grand. Donc $U_1 \cap U_2 \neq \{0\}$. ∎

On va pouvoir maintenant définir la notion de diviseur canonique de F/k.

Lemme 6.7 *Soit $\omega \in \Omega_F - \{0\}$. Soit*

$$M(\omega) = \{A \in \mathcal{D}_F, \omega \text{ s'annule sur } \mathbf{A}_F(A) + F\}.$$

Alors il existe un unique diviseur $W = (\omega) \in M(\omega)$ tel que $A \leq W$ pour tout $A \in M(\omega)$. Un diviseur $W \in D_F$ est dit canonique s'il existe $\omega \in \Omega_F - \{0\}$ tel que $W = (\omega)$.

Preuve : D'après le théoréme de Riemann, il existe une constant c ne dépendant que du corps de fonctions F/k tel que $i(A) = 0$ pour tout $A \in \mathcal{D}_F$ avec $\deg A \geq c$. Comme $\dim(\mathbf{A}_F/(\mathbf{A}_F(A)+F)) = i(A)$, pour tout $A \in M(\omega)$, $\deg A < c$. Donc il existe $W \in M(\omega)$ de degré maximal.
Raisonnons par l'absurde : supposons qu'il existe $A_0 \in M(\omega)$ avec $A \not\leq W$, i.e $v_Q(A) > v_Q(W)$ pour un $Q \in \mathcal{P}_F$. Nous allons montrer que $W+Q \in M(\omega)$ ce qui est contraire à la maximalité de W. Soit une adèle $\alpha = (\alpha_P)_{P \in \mathcal{P}_F} \in \mathbf{A}_F(W+Q)$. On peut écrire $\alpha = \alpha' + \alpha''$ avec

$$\alpha'_P = \begin{cases} \alpha_P \text{ si } P \neq Q, \\ 0 \text{ si } P = Q. \end{cases} \quad \alpha''_P = \begin{cases} 0 \text{ si } P \neq Q, \\ \alpha_Q \text{ si } P = Q. \end{cases}$$

Alors $\alpha' \in \mathbf{A}_F(W)$ et $\alpha'' \in \mathbf{A}_F(A_0)$. Donc $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Donc ω s'annule sur $\mathbf{A}_F(W+Q) + F$ donc $W + Q \in M(\omega)$ absurde ! L'unicité provient de $W \leq W'$ et $W' \leq W$. ∎

Lemme 6.8 *i. Si $x \in F - \{0\}$ et $0 \neq \omega \in \Omega_F$, alors $(x\omega) = (x) + (\omega)$.*
ii. Deux diviseurs canoniques de F/k sont équivalents.

Preuve : i. Si ω s'annule sur $\mathbf{A}_F(A) + F$, alors $x\omega$ s'annule sur $\mathbf{A}_F(A + (x)) + F$. Donc $(\omega) + (x) \leq (x\omega)$. De même $(x\omega) + (x^{-1}) \leq (\omega)$. Donc

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x)$$

ii. i + Ω_F est de dimension 1. ∎

Lemme 6.9 *Soit $A \in \mathcal{D}_F$ et $W = (\omega)$ un diviseur canonique de F/k. Alors*

$$i(A) = \dim(W - A)$$

Preuve : On va montrer que l'application

$$\mu : \begin{cases} \mathcal{L}(W - A) & \to & \Omega_F(A), \\ x & \mapsto & x\omega \end{cases}$$

est un isomorphisme de k-espace vectoriel. Comme $i(A) = \dim \Omega_F(A) = \dim(W - A)$, on aura alors démontrer le lemme.
Pour $x \in \mathcal{L}(W - A)$, on a

$$(x\omega) = (x) + (\omega) \geq -(W - A) + W = A$$

Or ω' s'annule sur $\mathbf{A}_F(A) + F$, ssi $\omega' = 0$ ou $(\omega') \geq A$. Donc $x\omega \in \Omega_F(A)$. Donc $\mu : \mathcal{L}(W - A) \to \Omega_F(A)$. Cette application est linéaire et injective. Montrons qu'elle est surjective. Soit $\omega_1 \in \Omega_F(A)$. Comme Ω_F est de dimension 1, $\omega_1 = x\omega$ pour un $x \in F$. Or

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A$$

donc $(x) \geq -(W - A)$ donc $x \in \mathcal{L}(W - A)$ et $\omega_1 = \mu(x)$. ∎

L'énoncé du lemme 6.9 se réinterprète comme le théorè de Riemann-Roch :

Théorème 6.10 *Soit F/k un corps de fonctions de genre g. Soit W un diviseur canonique de F/k. Alors pour tout $A \in \mathcal{D}_F$,*

$$\dim A = \deg A + 1 - g + \dim(W - A).$$

7 Compléments et Précisions sur les ensembles algébriques affines

7.1 Rappels et compléments sur les morphismes d'ensembles algébriques

Il est facile de voir si deux courbes C et C' affines sont isomorphes : elles sont isomorphes si et seulement si les k-algèbres $k[C]$ et $k[C']$ sont isomorphes.

Définition 7.1 *Soit $V \subset k^n$ et $W \subset k^m$ deux ensembles algébriques affines et $\varphi : V \to W$ une application que l'on peut écrire $\varphi = (\varphi_1, \dots, \varphi_m$ avec $\varphi : V \to k$. On dit que φ est un* **morphisme** *si les composantes de $\varphi_i \in k[V]$. On note $\mathrm{Reg}(V, W)$ l'ensemble des morphismes de V dans W.*

Exemples 7.1.1 • *Les éléments de $k[V]$, et en particulier les fonctions coordonnées, sont dse morphismes de V dans k.*
• *Les applications affines bijectives de k^n dans k^n sont des isomorphismes : elles correspondent aux polynômes de degr$\acute{1}$.*
• *Soit $V \subset k^n$. La projection $\varphi : V \to k^p, (x_1, \dots, x_n) \mapsto (x_1, \dots, x_p)$ est un morphisme.*
• *Soit $V = V(Y - X^2)$ une parabole. La projection $\varphi : V \to k, (x, y) \mapsto x$ est un isomorphisme de réciproque $x \mapsto (x, x^2)$.*
• *L'application $\varphi : k \to V(-X^3 + Y^2 - X^2), t \mapsto (t^2 - 1, t(t^2 - 1))$ (on coupe V avec la droite $Y = tX$) est un morphisme.*
• *L'application $\varphi : k \to V(Y^2 - X^3)$, $t \mapsto (t^2, t^3)$ est un morphisme bijectif mais n'est pas un isomorphisme (voir plus loin).*

Définition 7.2 *Soit $\varphi \in \mathrm{Reg}(V, W)$. Pour $f \in k[W]$. On définit le morphisme de k-algèbre : $\varphi^* : k[W] \to k[V]$, $\varphi^*(f) = f \circ \varphi$.*

Exemples 7.1.2 • $(g \circ f)^* = f^* \circ g^*$.
• *Soit $\varphi = (\varphi_1, \dots, \varphi_m) : V \to W$ un morphisme. Soit η_i la i-ème fonction coordonnés sur W, image de l'indéterminée Y_i dans $k[W]$. Alors $\varphi^*(\eta_i) = \varphi_i$. Plus généralement si les fonctions $\varphi_i = \overline{P}_i(X_1, \dots, X_n) \in k[V]$ alors*

$$\varphi^* : k[Y_1, \dots, Y_m]/I(W) \to k[X_1, \dots, X_n]/I(V), \;\; Y_i \mapsto \overline{P}_i(X_1, \dots, X_n).$$

• *Si $\varphi : V(F) \subset k^2 \to k, \varphi(x, y) = x$ alors $\varphi^* : k[X] \mapsto k[X, Y]/(F)$, $X \mapsto X$.*
• *Pour $\varphi : k \to V(Y^2 - X^3)$, $t \mapsto (t^2, t^3)$, $\varphi^* : k[X, Y]/(Y^2 - X^3) \to k[T]$, $\varphi(\bar{X}) = T^2$ et $\varphi(\bar{Y}) = T^3$.*

Proposition 7.1.3 *L'application $\gamma : \mathrm{Reg}(V, W) \to \mathrm{Hom}_{k-alg}(k[W], k[V])$ est bijective.*

PREUVE : On suppose $V \subset k^n$ et $W \subset k^m$ et on note η_i les fonctions coordonnées sur W.
Injectivité : Si $\varphi^* = \psi^*$ alors $\varphi_i = \varphi^*(\eta_i) = \psi^*(\eta_i) = \psi_i$ donc $\varphi = \psi$.
Surjectivité : Soit $\theta : k[W] \to k[V]$ un morphisme de k-algèbres. Soit $\varphi_i = \theta(\eta_i) \in k[V]$. Cela définit $\varphi : V \to k^m$. Il s'agit de montrer que φ est à valeurs dans W et ainsi $\varphi^* = \theta$. Soit $F(Y_1, \dots, Y_m) \in I(W)$ et $x \in V$. Ainsi $F(\varphi(x)) = F(\theta(\eta_1), \dots \theta(\eta_m))(x)$. Or θ est un morphisme de k-algèbre donc $F(\theta(\eta_1), \dots \theta(\eta_m))) = \theta(F(\eta_1, \dots, \eta_m))$. Or $F(\eta_1, \dots, \eta_m)$ est l'image de $F(Y_1, \dots, Y_m) \in I(W)$ dans $k[W]$, donc est nul. ∎

Corollaire 7.3 *Soit $\varphi : V \to W$ un morphisme. Alors φ est un isomorphisme si et seulement si φ^* en est un. Par conséquent V et W sont isomorphes si et seulement si $k[V]$et $k[W]$ le sont.*

Exemple 7.1.4 *L'application $\varphi : k \to V(Y^2 - X^3)$, $t \mapsto (t^2, t^3)$ est un morphisme bijectif mais n'est pas un isomorphisme : sinon on aurait un isomorphisme de $k[T^2, T^3]$ dans $k[T]$.*

7.2 Crière de lissité

Définition 7.4 *Soit V un ensemble algébrique et $x \in V$. On appelle* **vecteur tangent** *à V en x, une application k-linéaire $v : k[V] \to k$ telle que pour tout $f, g \in k[V]$, $v(fg) = f(x)v(g) + g(x)v(f)$ (dérivation). L'ensemble des vecteurs tangents à V en x est noté $T_x(V)$ et est appelé* **espace tangent** *à V en x. C'est un k-espace vectoriel.*

Proposition 7.2.1 *Pour $x \in V$, on note $\chi_x : k[V] \to k$, $f \mapsto f(x)$. Soit $k[\varepsilon] = k[X]/(X^2)$ et $p : k[\varepsilon] \to k$ la projection qui envoie ε sur 0. La donnée de $v \in T_x(V)$ est équivalente à la donnée d'un morphisme de k-algèbre (dit déformation) $t^* : k[V] \to k[\varepsilon])$ avec $pt^* = \chi_x$.*

PREUVE : Si $pt^* = \chi_x$ alors $t^*(f) = f(x) + \varepsilon v_t(f)$ avec $v_t(f) \in k$. L'application v_t est linéaire (car t^* est un homomorphisme) et $v_t \in T_x(V)$ (car $\varepsilon^2 = 0$).
Réciproquement, si $v \in T_x(V)$, alors $t^* = \chi_x + \varepsilon v$ est un k-homomorphisme. ∎

Exemples 7.2.2 • *Pour $V = k^n$ et $a = (a_1, \dots, a_n) \in V$. L'espace tangent est formé des applications k-linéaires $v : k[X_1, \dots, X_n] \to k$ qui vérifie la formule de dérivation. Elles sont donc déterminées par les images de X_i donc par un vecteur $(b_1, \dots, b_n) \in k^n$. Ainsi $T_{V,a} = k^n$.*

• *Soit $V \subset \mathbf{A}_n$ une variété algébrique affine, d'idéal $I(V) = (F_1, \dots, F_r)$. Soit $a = (a_1, \dots, a_n) \in V$. Nous allons déterminer l'espace tangent à V en a. Il s'agit de définir $v : k[X_1, \dots, X_n]/(F_1, \dots, F_r) \to k$. Pour cela, il faut se donner les images $b = (b_i)$ des X_i par v et ces images doivent satisfaire $t^*(F_j) = F_j(a + \varepsilon b) = 0$. C'est à dire, (vu que $\varepsilon^2 = 0$ et d'après Taylor) :*

$$\sum_{i=1}^{n} b_i \frac{\partial F_j}{\partial X_i}(a_1, \dots, a_n) = 0$$

Ainsi si J est la matrice jacobienne des F_j, alors $T_a(V) = \ker J$ est de dimension finie.

Proposition 7.2.3 *Soit A un anneau local noethérien, $\mathbf{m}$ son idéal maximal, $k = A/\mathbf{m}$. Le quotient $\mathbf{m}/\mathbf{m}^2$ est un k-espace vectoriel.*

Preuve : Pour $\lambda \in A$ et $x \in \mathbf{m}$, on pose $\bar{\lambda}\bar{x} = \overline{\lambda x}$. ∎

Proposition 7.2.4 *Soit V un ensemble algébrique affine, $x \in V$ et $\mathbf{m}_x = \{f \in k[V], f(x) = 0\}$, idéal maximal de $k[V]$. On a un isomorphisme de k-espace vectoriel $T_x(V) \simeq (\mathbf{m}_x/\mathbf{m}_x^2)^*$, où $*$ désigne le dual au sens des espaces vectoriels.*

Preuve : Soit $v \in T_x(V)$, $v : k[V] \to k$. La restriction de v à $\mathbf{m}_x$ est une application linéaire nulle sur $\mathbf{m}_x^2$ car pour tous $f, g \in \mathbf{m}_x$, $v(fg) = f(x)v(g) + g(x)v(f)$ et comme $f, g \in \mathbf{m}_x$, $f(x) = g(x) = 0$. Donc on a une application $\bar{v} : \mathbf{m}_x/\mathbf{m}_x^2 \to k$, soit $\bar{v} \in (\mathbf{m}_x/\mathbf{m}_x^2)^*$. Réciproquement, soit $\theta \in (\mathbf{m}_x/\mathbf{m}_x^2)^*$, on retrouve v par la formule $v(f) = \theta(\overline{f - f(x)})$. ∎

Corollaire 7.5 *Soit V une variété algébrique affine, $x \in V$, $\mathcal{O}_{V,x} = k[V]_{\mathbf{m}_x} = \{f/g, f, g \in k[V], g(x) \neq 0\}$ l'anneau local de V en x et $\mathbf{m}_{V,x}$ son idéal maximal. On a un isomorphisme $T_x(V) \simeq (\mathbf{m}_{V,x}/\mathbf{m}_{V,x}^2)^*$. En particulier l'espace tangent ne dépend que de l'anneau local de V en x.*

Preuve : L'idéal maximal $\mathbf{m}_{V,x} = \mathbf{m}_x\mathcal{O}_{V,x}$. L'homomorphisme naturel $\mathbf{m}_x \to \mathbf{m}_x\mathcal{O}_{V,x}$ $y \mapsto y/1$ se factorise en $\theta : \mathbf{m}_x/\mathbf{m}_x^2 \mapsto (\mathbf{m}_x\mathcal{O}_{V,x})/(\mathbf{m}_x\mathcal{O}_{V,x})^2$. Il s'agit de voir que θ est un isomorphisme de k-espaces vectoriels.
θ est injectif : Soit $y \in \mathbf{m}_x$ tel que $y/1 \in (\mathbf{m}_x\mathcal{O}_{V,x})^2$. Cela signifie qu'il existe $s \notin \mathbf{m}_x$ tel que $sy \in \mathbf{m}_x^2$. Mais si $s \notin \mathbf{m}_x$, comme $k[V]/\mathbf{m}_x$ est un corps, il existe $t \in k[V]$ avec $st = 1 - a$, $a \in \mathbf{m}_x$. Donc $y = sty + ay \in \mathbf{m}_x^2$.
θ est surjectif : Soit $y/s \in \mathbf{m}_x\mathcal{O}_{V,x}$ avec $y \in \mathbf{m}_x$ et $s \notin \mathbf{m}_x$. Alors $y/s = \theta(ty)$ car $y/s - ty = tya/(1-a) \in (\mathbf{m}_x\mathcal{O}_{V,x})^2$. ∎

On en déduit également

Corollaire 7.6 *Soit $V \subset k^n$ une variété algébrique affine irréductible de dimension d et $x \in V$. Soit $I(V) = (F_1, \ldots, F_r)$ son idéal de relation et J la matrice jacobienne de $F_1, \ldots, F_r$. La définition de V est lisse en x si et seulement si $rangJ = n - d$, ne dépend pas du choix des générateurs F_i de $I(V)$.*

Preuve : Cela découle immédiatement de $T_x(V) = \ker J$. ∎

8 Différentielles et différentielles de Weil

8.1 Dérivations et différentielles

Généralisons et précisons la définition des dérivations que nous avons vue dans le paragraphe précédent.

Définition 8.1 *Soit F/k un corps de fonctions. Soit M un module sur F. Une application $\delta : F \to M$ est une* **dérivation** *de F/k si δ est k-linéaire et si on a*

$$\delta(uv) = u\delta(v) + v\delta(u), \quad u, v \in F.$$

Remarque 8.1.1 *Le module des différentielles est le coupe (Δ_F, d), où Δ_F est un F-module, $d : \Delta_F \to F$ une dérivation vérifiant la propriété universelle suivante : pour toute dérivation $\delta : F \to M$, il existe une unique application F-linéaire $\mu : \Delta_F \to M$ telle que $\delta = \mu \circ d$. Dans ce paragraphe, nous allons décrire une construction de (Δ_F, d).*

Les propriétés suivantes sont immédiates :

Proposition 8.1.2 *Soit $\delta : F \to M$ une dérivation de F/k dans M. Alors*
i. $\delta(a) = 0$, $a \in k$,
ii. $\delta(z^n) = nz^{n-1}\delta(z)$, $z \in F$, $n \geq 0$,
iii. si char $k = p > 0$, $\delta(z^p) = 0$, $z \in F$,
iv. $\delta(x/y) = (y\delta(x) - x\delta(y))/y^2$.

Définition 8.2 *Un élément $x \in F$ est dit* **élément séparant** *de F/k si $F/k(x)$ est une extension algébrique séparable.*

Remarque 8.1.3 *En caractétique zéro, comme $k = \tilde{k}$ (et que toutes les extensions sont séparables), les éléments non séparants de F/k sont les éléments de k.*
En caractéristique $p > 0$, les éléments non séparants de F/k sont les éléments de k et les $y \in F$ tel que $y = u^p$ avec $u \in F$ (car ils induisent des extensions qui ne sont pas séparables).

On déduit de la Proposition 8.1.2, le lemme suivant :

Lemme 8.3 *Soit x un élément séparant de F/k et deux dérivations $\delta_1, \delta_2 : F \to M$ de F/k avec $\delta_1(x) = \delta_2(x)$. Alors $\delta_1 = \delta_2$.*

Preuve : Soit $f(x) = \sum a_i x^i \in k[x]$. Alors $\delta_j(f(x)) = (\sum i a_i x^{i-1})\delta_j(x)$, $j = 1, 2$ donc $\delta_1(f(x)) = \delta_2(f(x))$.
Soit $z = f(x)/g(x) \in F$. Alors

$$\delta_1(x) = \frac{g(x)\delta_1(f(x)) - f(x)\delta_1(g(x))}{g(x)^2} = \delta_2(z).$$

Donc les restrictions de δ_1 et δ_2 à $k(x)$ coincident.
Soit $y \in F$ de polynôme minimal $h(T) = \sum u_i T^i \in k(x)[T]$. En appliquant δ_j à $h(y) = 0$, nous obtenons

$$0 = \delta_j\Big(\sum u_i y^i\Big) = \sum(u_i\delta_j(y^i) + y^i\delta_j(u_i)) = \Big(\sum i u_i y^{i-1}\Big)\delta_j(y) + \sum y^i\delta_j(u_i).$$

Comme y est séparable sur $k(x)$ la dérivée $h'(y) = \sum i a_i y^{i-1} \neq 0$. Donc $\delta_j(y) = \frac{-1}{h'(y)} \sum y^i \delta_j(u_i)$.
Comme $u_i \in k(x)$ alors $\delta_1(u_i) = \delta_2(u_i)$ donc $\delta_1(y) = \delta_2(y)$. ∎

La proposition suivante va permettre de définir les dérivations par rapport à un élément séparant $x \in F$.

Proposition 8.1.4 *i. Soit E/F une extension finie séparable et $\delta_0 : F \to N$ une dérivation de F/k dans un corps N avec $E \subset N$. Alors δ_0 s'étend en une unique dérivation $\delta : E \to N$.*
ii. Si x est un élément séparant de F/k et $F \subset N$ est un corps alors il existe une unique dérivation $\delta : F \to N$ de F/k telle que $\delta(x) = 1$.

Preuve : i. L'unicité découle du lemme 8.3. Pour montrer l'existence, on introduit deux applications dérivations de $F[T]$ dans $N[T]$:

$$s(T) = \sum s_i T^i \mapsto s'(T) = \sum i s_i T^{i-1}, \quad s(T) = \sum s_i T^i \mapsto s^0(T) = \sum \delta_0(s_i) T^i.$$

Soit $u \in E$ avec $E = F(u)$. On note $f(T)$ le polynôme minimal de u sur F, $n = \deg f = [E : F]$ et $E \simeq F[T]/(f(T))$. Pour $y \in E$, il existe un unique $h(T) \in F[T]$ avec $\deg h < n$ et $y = h(u)$. On peut alors définir

$$\delta : E \to N, \;\; \delta(y) = h^0(u) - \frac{f^0(u)}{f'(u)} h'(u).$$

On vérifie alors que δ est une dérivation de E qui étend δ_0.
ii. L'unicité découle du lemme 8.3. Pour l'existence, on pose

$$\delta_0\Big(\frac{f(x)}{g(x)}\Big) = \frac{g(x)f'(x) - f(x)g(x)}{g(x)^2}$$

et on vérifie que δ_0 est un dérivation de $k(x)/k$ avec $\delta_0(x) = 1$. ∎

Définition 8.4 *i. Soit x un élément séparant de F/k. L'unique dérivation $\delta_x : F \to F$ de F/k telle que $\delta_x(x) = 1$ est dite* **dérivation par rapport à** x.
ii. Soit $\mathrm{Der}_F := \{\eta : F \to F | \eta$ est une dérivation de $F/k\}$. Pour $\eta_1, \eta_2 \in \mathrm{Der}_F$ et $z, u \in F$, on définit

$$(\eta_1 + \eta_2)(z) = \eta_1(z) + \eta_2(z), \quad (u\eta_1)(z) = u\eta_1(z);$$

Der_F *est ainsi un F-module dit* **module des dérivations** *de F/k.*

Lemme 8.5 *Soit $x \in F/k$ un élément séparant de F/k. Alors*
i. Pour toute dérivation $\eta \in \mathrm{Der}_F$, on a $\eta = \eta(x)\delta_x$. Ainsi Der_F est un F-module de dimension 1.
ii. Si y est un autre élément séparant de F/k alors

$$\delta_y = \delta_y(x)\delta_x$$

iii. Pour $t \in F$, on a

$$\delta_x(t) \neq 0 \Leftrightarrow t \text{ est un élément séparant.}$$

Preuve : i. Corollaire du lemme 8.3.
ii. Cas particulier de i.
iii. Si t est un élément séparant, $1 = \delta_t(t) = \delta_t(x)\delta_x(t)$ (d'après ii). Donc $\delta_x(t) \neq 0$.
Réciproquement supposons que t ne soit pas un élément séparant. Si car$k = 0$, alors $t \in k$ et $\delta_x(t) = 0$ car toute dérivation de F/k s'annule sur k. Si car$k = p > 0$, alors $t = u^p$ pour $u \in F$ et $\delta_x(t) = \delta_x(u^p) = 0$. ∎

Nous pouvons à présent définir le module des différentielles :

Définition 8.6 *i. Sur l'ensemble* $Z = \{(u,x) \in F \times F | x$ *est un élément séparant*$\}$*, on définit la relation d'équivalence* $\simeq$ *par*

$$(u,x) \simeq (v,y) \Leftrightarrow v = u\delta_y(x).$$

ii. La classe d'équivalence de $(u,x) \in Z$ *est notée* udx *et est appelée* **différentielle** *de* F/k*. La classe d'équivalence de* $(1,x)$ *est notée* dx*. Ainsi*

$$udx = vdy \Leftrightarrow v = u\delta_y(x)$$

iii. Soit $\Delta_F = \{udx | u \in F, x \in F$ *élément séparant*$\}$ *l'ensemble des différentielles de* F/k*. Pour* $udx = (u\delta_z(x))dz$ *et* $vdy = (v\delta_z(y))dz$*, on note*

$$udx + vdy = (u\delta_z(x) + v\delta_z(y))dz,$$

et cette définition est indépendante du choix de z *(lemme 8.5 ii.). De plus* Δ_F *est muni d'une structure de* F*-module via*

$$w(udx) = (wu)dx \in \Delta_F, w \in F, udx \in \Delta_F.$$

iv. Pour un élément non séparant $t \in F$ *on définit* $dt = 0$ *et ainsi, on définit*

$$d : \begin{cases} F & \to & \Delta_F, \\ t & \mapsto & dt. \end{cases}$$

Le couple (Δ_F, d) *est dit* **module des différentielle de** F/k*.*

Résumons les principales propriétés du module des différentielles :

Proposition 8.1.5 *i. Soit* z *un élément séparant. Alors* $dz \neq 0$ *et toute différentielle* $\omega \in \Delta_F$ *s'écrit de façon unique sous la forme* $\omega = udz$ *avec* $u \in \mathbf{F}$*. Ainsi* Δ_F *est un* F*-module de dimension 1.*
ii. L'application $d : F \to \Delta_F$ *définie ci-dessus est une dérivation de* F/k*, i.e*

$$d(ax) = adx, d(x+y) = dx + dy, \;\; d(xy) = xdy + ydx, \;\; a, y \in F, a \in k.$$

iii. Pour $t \in F$, $dt \neq 0 \Leftrightarrow t$ est un élément séparant.
iv. Soit $\delta : F \to M$ une dérivation de F/k dans un F-module M. Alors il existe une unique application F-linéaire $\mu : \Delta_F \to M$ telle que $\delta = \mu \circ d$. (Propriété universelle du module des différentielles).

PREUVE : i. $0 = 0dz \in \Delta_F$ et $(0, z) \not\simeq (1, z)$, donc $dz \neq 0$.
Soit $\omega = vdy \in \Delta_F$. Pour $u = v\delta_x(y)$, on a $udz = vdy = \omega$. L'unicité d'un tel u est clair et Δ_z est un F-espace vectoriel de dimension 1.
ii. Soit z un élément séparant de F/k. Alors pour tout $t \in F$, on a $dt = \delta_x(t)dz$ (même si t n'est pas séparant car alors =0) et on vérifie que d est une déraivation (en utilisant que δ_x en est une).
iii. Par définition de d.
iv. Soit $\delta : F \to M$ une dérivation. D'après i. on peut définir l'application F linéaire :

$$\mu : \Delta_F \to M, \ \ \omega = udz \mapsto u\delta(z).$$

Pour montrer que $\delta = \mu \circ d$, il suffit de prouver que $\delta(z) = (\mu \circ d)(z)$. Et c'est clair par définition de μ.
Pour l'unicité, si ν en est une autre, alors

$$\nu(udz) = u\nu(dz) = u(\nu \circ d)(z) = u\delta(z) = \mu(udz),$$

donc $\nu = \mu$. ∎

Définition 8.7 *Soit P une place de F/k d'uniformisante t. Alors pour tout $z \in F$, on peut écrire z sous la forme*

$$z = \sum_{i=n}^{\infty} a_i t^i, \ \ n \in \mathbf{Z}, a_i \in k$$

et on définit le résidue de z par rapport à P et t par

$$\mathrm{res}_{P,t}(z) = a_{-1}.$$

8.2 Compléments sur les différentielles de Weil

Rappel : $\mathbf{A}_F$ est l'espace des adèles de F/k : ces éléments sont les adèles $\alpha = (\alpha_P)_{P\in\mathcal{P}_F}$ où les P-composantes $\alpha_P \in F$ de α sont presque toutes de valuation $v_P(\alpha) = v_P(\alpha_P) \geq 0$. Le corps F est un sous-espace de $\mathbf{A}_F$ via le plongement diagonal $F \to \mathbf{A}_F$. Si A est un diviseur de F/k, on a défini

$$\mathbf{A}_F(A) = \{\alpha \in \mathbf{A}_F | v_P(\alpha) \geq v_P(A)\}.$$

Une différentielle de Weil est une application k-linéaire $\omega : \mathbf{A}_F \to k$ qui s'annule sur un $\mathbf{A}_F(A) + F$. Les différentielles de Weil forment un F-module Ω_F de dimension 1 sur F. Pour $0 \neq \omega \in \Omega_F$, il existe un unique diviseur, dit diviseur canonique de F/k et noté $W = (\omega) \in \mathcal{D}_F$, tel que ω s'annule sur $\mathbf{A}_F(W)$ mais pas sur $\mathbf{A}_F(B)$ si $B \geq W$.
Pour $P \in \mathcal{P}_F$, on a un autre plongement

$$\iota_P : F \to \mathbf{A}_F, \quad \iota(z)_Q = \begin{cases} z & \text{si} \quad Q = P, \\ 0 & \text{si} \quad Q \neq P. \end{cases}$$

Définition 8.8 *La* **composante locale de la différentielle de Weil ω à la place P** *est l'application $\omega_P : F \to k$, $\omega_P(z) = \omega(\iota_P(z))$. C'est une application k-linéaire.*

Proposition 8.2.1 *Soit $\omega \in \Omega_F$ et $\alpha = (\alpha_P) \in \mathbf{A}_F$. Alors $\omega_P(\alpha_P) = 0$ presque partout et $\omega(\alpha) = \sum_{P\in\mathcal{P}_F} \omega_P(\alpha_P)$.*

Preuve : Soit $\omega \neq 0$ et $W = (\omega)$ le diviseur de ω. Il existe un ensemble fini $S \subset \mathcal{P}_F$ tel que

$$v_P(W) = 0, v_P(\alpha_P) \geq 0, P \notin S$$

Soit $\beta = (\beta_P) \in \mathbf{A}_F$ défini par

$$\beta_P = \begin{cases} \alpha_P & \text{si} \quad P \notin S, \\ 0 & \text{si} \quad P \in S. \end{cases}$$

Alors $\beta \in \mathbf{A}_F(W)$ et $\alpha = \beta + \sum_{P\in S} \iota_P(\alpha_P)$ donc $\omega(\beta) = 0$ et

$$\omega(\alpha) = \sum_{P\in S} \omega_P(\alpha_P)$$

Pour $P \notin S$, $\iota_P(\alpha_P) \in \mathbf{A}_F(W)$ donc $\omega_P(\alpha_P) = 0$. ∎

Nous montrons à présent qu'une différentielle de Weil est déterminée par ces composantes locales.

Proposition 8.2.2 *i. Soit $0 \neq \omega \in \Omega_F$ et $P \in \mathcal{P}_F$. Alors*

$$v_P(\omega) = \max\{r \in \mathbf{Z}, \omega_P(x) = 0 \forall x \in F \text{ avec } v_P(x) \geq -r\}.$$

En particulier $\omega_P \neq 0$.
ii. Si $\omega, \omega' \in \Omega_F$ et $\omega_P = \omega'_P$ pour un $P \in \mathcal{P}_F$ alors $\omega = \omega'$.

Preuve : i. Soit $s = v_P(\omega) = v_P(W)$ pour $W = (\omega)$. Soit $x \in F$ avec $v_P(x) \geq -s$, alors $\iota_P(x) \in \mathbf{A}_F(W)$. Donc $\omega_P(x) = \omega(\iota_P(x)) = 0$.
Si $\omega_P(x) = 0$ pour tout $x \in F$ tel que $v_P(x) \geq -s-1$. Soit $\alpha = (\alpha_Q) \in \mathbf{A}_F(W+P)$. Alors

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

avec $\alpha - \iota_P(\alpha_P) \in \mathbf{A}_F(W)$ et $v_P(\alpha_P) \geq -s-1$, donc

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0.$$

Donc ω s'annule sur $\mathbf{A}_F(W+P)$ absurde !
ii. Si $\omega_P = \omega'_P$ alors $(\omega - \omega')_P = 0$ donc d'après i. $\omega - \omega' = 0$. ∎

On peut alors montrer l'existence d'une différentielle de Weil spécifique $\eta \in \Omega_{k(x)}$ qui est déterminée de façon unique par les propriétés suivantes : Notons P_∞ le pôle de x dans $k(x)$ et η_{P_∞} est la composante locale de η en P_∞.

Proposition 8.2.3 *Soit le corps de fonctions $k(x)/k$ (de genre 0). Alors*
i. Le diviseur $-2P_\infty$ est canonique.
ii. Il existe une unique différentielle de Weil $\eta \in \Omega_{k(x)}$ avec $(\eta) = -2P_\infty$ et $\eta_{P_\infty}(x^{-1}) = -1$.

Preuve : i. $\deg(-2P_\infty) = -2 = 2g-2$ et $\dim(-2P_\infty) = 0 = g$ donc

$$g \leq \dim(-2P_\infty) = \deg(-2P_\infty) + 1 - g + \dim(W - (-2P_\infty)) = g - 1 + \dim(W - (-2P_\infty))$$

Donc $\dim(W - (-2P_\infty)) \geq 1$. Or $\deg(W - (-2P_\infty)) = 0$ donc W et $(-2P_\infty)$ sont équivalents. ii. Soit une différentielle de Weil ω de diviseur $(\omega) = -2P_\infty$. Alors ω s'annule sur $\mathbf{A}_{k(x)}(-2P_\infty)$ mais ne s'annule pas sur $\mathbf{A}_{k(x)}(-P_\infty)$ tout entier. Or

$$\dim \mathbf{A}_{k(x)}(-P_\infty)/\mathbf{A}_{k(x)}(-2P_\infty) = \deg(-P_\infty) - \deg(-2P_\infty) = 1$$

et $\iota_{P_\infty}(x^{-1}) \in \mathbf{A}_{k(x)}(-P_\infty) - \mathbf{A}_{k(x)}(-2P_\infty)$, on a que

$$\omega_{P_\infty}(x^{-1}) = \omega(\iota_{P_\infty}(x^{-1})) = c \neq 0$$

On pose $\eta = -c^{-1}\omega$ et ainsi $(\eta) = -2P_\infty$ et $\eta_{P_\infty}(x^{-1}) = -1$.
Pour l'unicité si η^* a les mêmes propriétés, $\eta - \eta^*$ s'annule sur $\mathbf{A}_{k(x)}(-P_\infty)$ donc $\eta = \eta^*$.
∎

Définition 8.9 *Soit F'/F une extension finie séparable de corps de fonctions sur k. Une place $P' \in \mathcal{P}_{F'}$ est dite au-dessus de $P \in \mathcal{P}_F$ (et on note P'/P) si $P \subset P'$. Ainsi il existe $e \geq 1$ tel que $v_{P'}(x) = ev_P(x)$, pour tout $x \in F$. L'entier $e = e(P'/P)$ est dit* **indice de ramification** *de P' sur P. On dit que P'/P est ramifiée si $e(P'/P) > 1$ et non ramifiée et $e(P'/P) = 1$.*

Définition 8.10 *Si F'/F est une extension finie séparable de corps de fonctions sur k et $\omega \in \Omega_F$, on peut définir la cotrace $\omega' = CotrF'/F(\omega) \in \Omega_{F'}$ où ω' est caractérisée par la propriété :*

$$\omega_P(\mathrm{tr}_{F'/F}(y)) = \sum_{P'/P} \omega'_{P'}(y)$$

pour tout $P \in \mathcal{P}_F$ et $y \in F'$.

Remarque 8.11 *Si $x \in F$ est séparant, nous admettons qu'il n'y a qu'un nombre fini de places ramifiées de $F/k(x)$.*

8.3 Comparaison différentielles et différentielles de Weil

Définition 8.12 *Soit F/k un corps de fonctions. On définit la fonction*

$$\delta : \begin{cases} F & \to & \Omega_F \\ x & \mapsto & \delta(x) \end{cases}$$

de la façon suivante : si $x \in F - k$ est un élément séparant de F/k alors

$$\delta(x) = \ CoTr_{F/k(x)}(\eta)$$

sinon $\delta(x) = 0$. On appelle $\delta(x)$, la différentielle de Weil de F/k associée à x.

Remarque 8.13 *Si $\delta(x) \neq 0$, alors x est un élément séparant de F/k et pour tout $\omega \in \Omega_F$, ll existe $z \in F$ tel que $\omega = z\delta(x)$.*

Maintenant le théorème d'isomorphisme entre les différentielles et les différentielles de Weil.

Théorème 8.14 *Soit F/k un corps de fonctions sur un corps algébriquement clos k et $x \in F$ un élément séparant. Alors*
i. L'application $\delta : F \to \Omega_F$ définie si-dessus est une dérivation de F/k.
ii. Pour tout $y \in F$, on a $\delta(y) = \frac{dy}{dx}\delta(x)$.
iii. L'application

$$\mu : \begin{cases} \Delta_F & \to & \Omega_F, \\ zdx & \mapsto & z\delta(x). \end{cases}$$

est un isomorphisme du module des différentielles Δ_F sur Ω_F. Cet isomorphisme est compatible aux dérivations $d : F \to \Delta_F$ et $\delta : F \to \Omega_F$, i.e $\mu \circ d = \delta$.

Pour le démontrer nous avons besoin du lemme technique suivant (admis):

Lemme 8.15 *Soit F un corps de fonctions sur k algébriquement clos. Soit $x \in F$ un élément séparant de F/k et $P_0 \in \mathcal{P}_{k(x)}$ telle que*
i. P_0 n'est pas ramifiée dans $F/k(x)$,
ii. P_0 n'est pas le pôle de x dans $k(x)$. Alors la différentielle de Weil $\delta(x)$ associée à x vérifie

$$\delta(x)_P(u) = \mathrm{res}_P(udx), u \in F, P \in \mathcal{P}_F \text{ telle que } P|P_O.$$

Preuve : (démontration du théorème).
ii. Si $y \in F$ n'est pas un élément séparant, $\delta(y) = 0$ et $\frac{dy}{dx} = 0$ (voir proposition 8.1.5). Donc $\delta(y) = \frac{dy}{dx}\delta(x)$.
Supposons à présent que $y \in F$ est un élément séparant. Comme $\delta(x) \neq 0$ et Ω_F est un F-module de dimension 1, $\delta(y) = z\delta(x)$ pour un $z \in F$. Il n'y a qu'un nombre fini de places ramifiées sur $k(x)$ ou sur $k(y)$. Par conséquent il existe une place $P \in \mathcal{P}_F$ qui n'est pas ramifiée sur $k(x)$ (resp. $k(y)$) et qui n'est pas un pole de x (resp. y). Alors pour tout $u \in F$,

$$\delta(y)_P(u) = (z\delta(x))_P(u) = \delta(x)_P(zu)$$

D'après le lemme 8.15 (pour $F/k(y)$ et $F/k(x)$),

$$\delta(y)_P(u) = \mathrm{res}_P(udy) = \mathrm{res}_P\left(u\frac{dy}{dx}dx\right) = \delta(x)_P\left(u\frac{dy}{dx}\right)$$

Donc

$$\delta(x)_P(u(z - \frac{dy}{dx})) = 0, \forall u \in F$$

Donc $z = \frac{dy}{dx}$ car une différentielle de Weil est déterminée par un facteur local.
i. D'après ii et la proposition 8.1.5, pour tous $y_1, y_2 \in F$, et $a \in k$,

$$\delta(y_1 + y_2) = \frac{d(y_1 + y_2)}{dx}\delta(x) = \left(\frac{dy_1}{dx} + \frac{dy_2}{dx}\right)\delta(x) = \delta(y_1) + \delta(y_2)$$

$$\delta(ay_1) = \frac{d(ay_1)}{dx}\delta(x) = a\frac{dy_1}{dx}\delta(x) = a\delta(y_1)$$

$$\delta(y_1y_2) = \frac{d(y_1y_2)}{dx}\delta(x) = \left(y_1\frac{dy_2}{dx} + y_2\frac{dy_1}{dx}\right)\delta(x) = y_1\delta(y_2) + y_2\delta(y_1).$$

iii. D'après la proposition 8.1.5, il existe une unique application F-linéaire $\mu : \Delta \to \Omega_F$ telle que, pour tout $y \in F$,

$$\delta(y) = (\mu \circ d)(y) = \mu(dy).$$

Comme μ est F-linéaire, $\mu(zdx) = z\mu(dx) = z\delta(x)$. Comme dx engendre Δ_F et $\delta(x)$ engendre Ω_F (comme F-module), μ est bijective. ∎