Groupe de Galois et monodromie de certains problèmes géométriques *

Olivier Bernard & Rémy Tuyeras

17 Juin 2009

Résumé

La théorie de Galois et la théorie des revêtements présentent de multiples liens, au point que topologues et algébristes emploient souvent un vocabulaire emprunté à l'autre discipline. Ces liens vont nous permettre de comprendre certains aspects de problèmes géométriques classiques.

En particulier, si l'étude, par des méthodes classiques, des points d'intersection d'une courbe algébrique par des hyperplans a toujours échoué à montrer l'existence d'une structure sur ces points, structure qui serait invariante, des méthodes topologiques vont en fait nous permettre de montrer qu'il n'en existe aucune.

Pour ce faire, nous allons calculer un certain groupe de Galois, en utilisant un groupe issu de la topologie, le groupe de monodromie. Une grande partie de ce texte consistera à exhiber le lien entre ce groupe de monodromie et le groupe de Galois. Ensuite, nous calculerons effectivement ce groupe dans le cadre des intersections d'une courbe algébrique lisse projective avec des hyperplans.

* *(sous l'égide éclairée de François Charles)*

1 Rudiments sur les variétés complexes et algébriques

1.1 Variétés complexes sur $\mathbb{C}^n$

On supposera dans cet exposé que le lecteur est déjà familier avec les notions de base de la géométrie différentielle et donc qu'il sait en particulier ce qu'est une variété différentielle. Le but de cette sous-section est de présenter quelques notions de base de la géométrie complexe, dans laquelle on manipule cette fois-ci des variétés complexes. Celles-ci sont définies, comme les variétés différentielles, à l'aide de cartes mais dont les propriétés sont davantage liées à l'analyse complexe. Ainsi :

Définition 1.1 *Une* variété complexe *est une variété topologique munie d'un atlas maximal dont les cartes (homéomorphismes) $\varphi_i : X \supset U_i \to V_i \subset \mathbb{C}^n$ ont pour images des ouverts de $\mathbb{C}^n$, et tel que les changements de cartes*

$$\varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \to \varphi_i(U_i \cap U_j)$$

soient des biholomorphismes, c'est-à-dire des applications de plusieurs variables complexes holomorphes ainsi que leur inverse.

On rappelle toutefois ce que signifie l'holomorphie pour des applications à plusieurs variables :

Définition 1.2 *Une application $f : \mathbb{C}^n \to \mathbb{C}^p$ est* holomorphe *si elle l'est par rapport à chaque variable.*

Par exemple, on appelle *surfaces de Riemann* les variétés complexes de dimension 1. Un exemple de surface de Riemann est *la sphère de Riemann* définie par $\mathbb{S} = \mathbb{C} \cup \{\infty\}$ où ∞ est un symbole représentant un élément qui n'est pas dans $\mathbb{C}$. On munit alors $\mathbb{S}$ de la topologie suivante : les ouverts de $\mathbb{S}$ sont les ouverts de $\mathbb{C}$ ainsi que les ensembles de la forme $V \cup \{\infty\}$ où V est un ouvert de $\mathbb{C}$ dont le complémentaire est un compact de $\mathbb{C}$. La sphère de Riemann $\mathbb{S}$ est ensuite munie d'une structure de surface de Riemann définie par un atlas à deux cartes (U_1, φ_1) et (U_2, φ_2) que voici :

$$U_1 = \mathbb{C} \qquad \varphi_1 : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & z \end{array}$$

et

$$U_2 = \mathbb{C}^* \cup \{\infty\} \qquad \varphi_2 : \begin{array}{ccccc} \mathbb{C}^* \cup \{\infty\} & \longrightarrow & \mathbb{C} & & \\ z & \longmapsto & \frac{1}{z} & \text{si } z \neq \infty & \\ \infty & \longmapsto & 0 & \text{sinon} & \end{array}$$

L'existence des sous-variétés complexes est principalement dû au fait que l'on a aussi un théorème d'inversion locale pour les fonctions holomorphes. En effet :

Théorème 1.3 *Soit Ω un ouvert connexe de $\mathbb{C}$ et $f : \Omega \to \mathbb{C}$ une fonction holomorphe. Soit $z \in \Omega$ telle que $f'(z) \neq 0$. Alors il existe des voisinages U et V de z et $f(z)$ tels que f est une bijection holomorphe d'inverse holomorphe de U sur V. En particulier, si f est injective et f ne s'annule pas alors $f(\Omega)$ est ouvert et f^{-1} est holomorphe.*

Preuve : C'est une conséquence directe du théorème d'inversion locale : si f est holomorphe sur Ω, et si pour un certain $z_0 \in \Omega, f'(z_0) \neq 0$, alors en particulier f est continûment différentiable sur U et sa différentielle en z_0 est inversible. Par le théorème d'inversion locale f réalise donc un difféomorphisme entre un voisinage ouvert U de z_0 et un voisinage ouvert V de $f(z_0)$. Il reste à voir que f^{-1} est holomorphe sur V. Mais c'est clair par la formule $Df_a^{-1} = (Df_{f^{-1}(a)})^{-1}$ valable pour $a \in V$: comme f est holomorphe en $b = f^{-1}(a)$, sa différentielle en b est la multiplication par $f'(b)$ et donc son inverse est la multiplication par $1/f'(b)$. □

De là, le théorème des submersions et ses applications restent valables en géométrie complexe. De ce fait, on voit que l'ensemble des racines d'une fonction polynomiale sur les nombres complexes, qui est holomorphe, va former une sous-variété lisse au sens de la géométrie complexe. Mais cet ensemble forme aussi ce que l'on appelle une *variété algébrique* au sens de la géométrie algébrique. C'est pourquoi, par la suite, nous nous permettrons par exemple de parler de *variété algébrique lisse*. On définit ci-dessous ce qu'est formellement une variété algébrique dans un sens général.

1.2 Variétés algébriques affines

Comme on l'a fait jusqu'à maintenant, on se place sur l'espace affine $\mathbb{C}^n$, pour un $n \geq 1$ donné. Cet ensemble sera notre espace de points. On prend de même un espace de fonctions $A = \mathbb{C}[x_1, \ldots, x_n]$, qui est l'anneau polynomial en n variables. Comme on l'a déjà fait sous-entendre un peu plus haut, on va s'intéresser à l'ensemble des racines de polynômes. On définit alors pour une famille de polynômes F, l'*ensemble des zéros* de F par

$$Z(F) = \{P \in \mathbb{C}^n | f(P) = 0 \ \forall f \in F\}$$

Par nœthérianité de A, on peut toujours se ramener à une famille finie de polynômes. Ce type d'ensemble est appelé *ensemble algébrique*. Une chose importante à remarquer pour ce type d'espace est que l'on a une structure topologique naturelle :

Proposition 1.4 *L'union de deux ensembles algébriques est un ensemble algébrique. Toute intersection d'une famille d'ensembles algébriques est un ensemble algébrique. L'ensemble vide et l'ensemble des points de tout l'espace sont des ensembles algébriques.*

Preuve : Si $Y_1 = Z(T_1)$ et $Y_2 = Z(T_2)$, alors $Y_1 \cup Y_2 = Z(T_1 T_2)$, où $T_1 T_2$ désigne l'ensemble de tous les produits d'un élément de T_1 par un élément de T_2. En effet, si $P \in Y_1 \cup Y_2$ alors, soit $P \in Y_1$, soit $P \in Y_2$, donc P est un zéro de chaque polynôme appartenant à $T_1 T_2$. Inversement, si $P \in Z(T_1 T_2)$ et disons $P \notin Y_1$, alors il y a un $f \in T_1$ tel que$f(P) \neq 0$. Or pour tout $g \in T_2$, on a $(fg)(P) = 0$ ce qui implique que $g(P) = 0$ et donc que $P \in Y_2$. Si $Y_\alpha = Z(T_\alpha)$ est une famille d'ensembles algébriques, alors $\cap Y_\alpha = Z(\cup T_\alpha)$, donc $\cap Y_\alpha$ est aussi un ensemble algébrique. Enfin, on a pour l'ensemble vide l'égalité $\emptyset = Z(1)$, et pour tout l'espace $\mathbb{C}^n = Z(0)$. □

Définition 1.5 *On définit la* topologie de Zariski *sur $\mathbb{C}^n$ en considérant les sous-ensembles ouverts comme étant les complémentaires des ensembles algébriques.*

Preuve : C'est bien une topologie d'après la proposition, puisqu'alors, l'intersection de deux ouverts est un ouvert et l'union d'une famille d'ouverts est un ouvert. De plus, l'ensemble vide et tout l'espace sont aussi des ouverts. □

Nous en venons alors à la définition d'une variété algébrique :

Définition 1.6 *Une* variété algébrique affine *(ou simplement* variété affine*) est un sous-ensemble fermé de $\mathbb{C}^n$ (pour la topologie de Zariski). Un ouvert d'une variété affine sera appelé une* variété quasi-affine.

Une question que l'on pourrait alors se poser est de savoir si on peut toujours trouver un ouvert lisse (complexe) lorsqu'a priori on ne manipule avant tout que des variétés algébriques. La réponse est en fait affirmative, par le théorème suivant :

Proposition 1.7 *Il existe toujours dans une variété algébrique un ouvert dense lisse.*

On pourra donc toujours considérer sur une variété algébrique son *ouvert de lissité*.

1.3 Un mot à propos des fonctions et applications sur des variétés

On présente ici les divers types de fonctions que l'on va manipuler par la suite. Tout d'abord, on s'intéresse à des fonctions proches des polynômes.

Définition 1.8 *Une fonction $f : X \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ est dite* régulire *s'il existe un polynôme $P \in \mathbb{C}[T_1, \ldots, T_n]$ tel que pour tout $x \in X$, $f(x) = P(x)$. On note alors $\mathbb{C}[X]$ l'ensemble des fonctions régulières, qui est un anneau.*

De manière générale, on peut étendre la définition de régularité aux applications entres deux variétés.

Définition 1.9 *On dit qu'une application f de $X \subset \mathbb{C}^n$ dans $Y \subset \mathbb{C}^m$ est régulière s'il existe m fonctions $f_1, \ldots, f_m$ sur X tel que $f(x) = (f_1(x), \ldots, f_m(x))$ pour tout $x \in X$.*

Dans le cas où $\mathbb{C}[X]$ est intègre, on peut bien sûr définir son corps de fractions :

Définition 1.10 *Lorsque $\mathbb{C}[X]$ est intègre (ce qui se produit en particulier lorsque X est irréductible), alors le corps des fractions de l'anneau $\mathbb{C}[X]$ est appelé le* corps des fonctions rationnelles *sur X. Il est noté $\mathbb{C}(X)$.*

On peut préciser que le corps des fractions $\mathbb{C}(X)$ est l'ensemble des fonctions rationnelles de la forme $P(T_1, \ldots, T_n)/Q(T_1, \ldots, T_n)$ où $Q(T_1, \ldots, T_n)$ n'est pas identiquement nulle sur X, avec la relation d'égalité $P/Q = P_1/Q_1$ dans $\mathbb{C}(X)$ si $PQ_1 - P_1Q$ est identiquement nulle sur X.

Dans $\mathbb{P}^n(\mathbb{C})$, on a la même notion de régularité en considérant des polynômes homogènes.

Définition 1.11 *Une* fonction rationnelle *sur* $\mathbb{P}^n(\mathbb{C})$ *est de la forme* f/g *où* f *et* $g \neq 0$ *sont des fonctions polynomiales homogènes de même degré (sauf si* $f = 0$*). La condition sur le degré assure que la fonction est bien définie dans son domaine de définition,* $\mathbb{P}^n(\mathbb{C}) \setminus \{g = 0\}$.

Plus généralement, une fonction $f : V \to \mathbb{C}$ sur une variété quasi-projective $V \subset \mathbb{P}^n(\mathbb{C})$ sera appelée régulière si pour tout point, il existe un voisinage (pour la topologie de Zariski) où elle est la restriction d'une fonction régulière définie sur un sous-ensemble ouvert de $\mathbb{P}^n(\mathbb{C})$.

Plus généralement, on dira qu'une fonction f entre deux variétés X est Y est régulière, holomorphe ou méromorphe s'il existe deux atlas (U_i, φ_i) et (V_i, ψ_i) respectivement sur X et Y tels que $\psi \circ f \circ \varphi^{-1}$ soit régulière, holomorphe ou méromorphe.

1.4 Considérations topologiques

Nous avons vu au paragraphe précédent que l'on pouvait munir une variété algébrique de deux topologies distinctes, la topologie de Zariski induite par les fermés de Zariski de $\mathbb{C}^n$ et de $\mathbb{P}^n(\mathbb{C})$, et la topologie usuelle induite par les topologies usuelles de ces mêmes espaces. Nous essaierons autant que possible, quand le contexte n'est pas explicite, de préciser quelle topologie nous utilisons. Remarquons tout de même dès à présent que la topologie de Zariski est moins fine que la topologie usuelle, ce qui implique qu'un ensemble ouvert ou fermé pour la topologie de Zariski sera ouvert ou fermé également pour la topologie usuelle.

Nous commençons par la notion d'irréductibilité, et nous énoncerons ensuite quelques propriétés utiles :

Définition 1.12 *Soit* X *un espace topologique.* X *est* irréductible *s'il vérifie une des 4 propriétés équivalentes suivantes :*

1. *X ne peut s'écrire comme une union (quelconque) de deux fermés propres de X.*
2. *Deux ouverts non vides de X sont d'intersection non vide.*
3. *Tout ouvert non vide de X est dense dans X.*
4. *Tout fermé propre de X est d'intérieur vide.*

Remarque :

- Une variété algébrique, munie de la topologie de Zariski, étant un espace topologique, on pourra parler de variété algébrique *irréductible*. Nous considérerons le plus souvent des variétés algébriques irréductibles.
- Attention, la topologie usuelle étant séparée, une variété algébrique, vue avec la topologie usuelle induite par $\mathbb{C}^n$, ne sera jamais irréductible, par la propriété (2). On considérera donc toujours implicitement la topologie de Zariski pour parler de variétés algébriques irréductibles.

Preuve : La preuve est essentiellement laissée au lecteur.
(1) $\Leftrightarrow$ (2) et (3) $\Leftrightarrow$ (4). Obtenues par passage au complémentaire.
(2) $\Leftrightarrow$ (3). On utilise l'équivalence classique : A est dense dans $X \Leftrightarrow$ Tout ouvert non vide de X rencontre A. □

La propriété (1) donne directement qu'un espace topologique X irréductible est connexe. La proposition suivante est tout aussi immédiate :

Proposition 1.13 *Soit X irréductible. Tout sous-ensemble* ouvert *de X est irréductible.*

Proposition 1.14 *Soient X et Y deux espaces topologiques irréductibles. Alors l'espace $X \times Y$ muni de la topologie produit, est irréductible.*

Preuve : Une preuve est donnée dans [3, Chap. 1, §3, Th.3]. □

Nous admettons maintenant un résultat puissant de connexité, qui utilise le lemme de Chow de correspondance entre les variétés analytiques et les variétés algébriques dans l'espace projectif complexe :

Proposition 1.15 *Soit $X \subset \mathbb{P}^n(\mathbb{C})$. Si X est connexe pour la topologie de Zariski, X est aussi connexe pour la topologie usuelle.*

Preuve : Admis. □

Toujours dans l'espace projectif, on a également le résultat très utile suivant :

Proposition 1.16 *Soit X et Y deux variétés de $\mathbb{P}^n(\mathbb{C})$. Les applications de projection de $X \times Y$ dans X ou Y sont fermées.*

Preuve : Le lecteur se reportera fructueusement à [3, Chap. 1, §4, Th.3] pour une preuve détaillée. □

1.5 Notions de dimension

On sait que le théorème des submersions nous donne une caractérisation de la dimension d'une sous-variété. En fait, de manière plus générale, on peut présenter d'autres définitions de cette dimension, toutes aussi équivalentes les unes que les autres, dans le cas de variétés algébriques lisses. Par exemple, on peut considérer la définition suivante :

Définition 1.17 *Une variété algébrique V est de dimension n si la longueur maximale d'une chaîne descendante de sous-variétés irréductibles*

$$V \supset V_0 \supsetneq \cdots \supsetneq V_n \neq \emptyset$$

est $n+1$. La dimension de V sera notée dim V.

De même, il est facile de voir que cette définition peut aussi s'écrire sous la forme suivante :

Définition 1.18 *La* dimension *d'une variété quasi-projective irréductible X est le degré de transcendance du corps $\mathbb{C}(X)$ sur $\mathbb{C}$, où le degré de transcendance d'un corps L sur un corps K est le plus petit m tel que L soit une extension algébrique d'un corps $K(x_1, ..., x_m)$*

Ainsi, lorsque l'on parlera de dimension d'une variété, on pourra se référer à l'une comme à l'autre des définitions, car on aura pris garde de se placer sur des variétés lisses. Ayant maintenant introduit la notion de dimension, on peut définir ce qu'est une *courbe algébrique* :

Définition 1.19 *Une* courbe algébrique *est une variété projective ou quasi-projective dont les composantes connexes sont toutes de dimension 1.*

Par la suite, on étudiera le nombre de points d'intersection que l'on peut trouver entre une courbe et ce que l'on définit ci-dessous comme un *hyperplan* :

Définition 1.20 *Les variétés algébriques de la forme $\{f = 0\} \subset \mathbb{P}^n(\mathbb{C})$, où f est une fonction polynomiale non identiquement nulle, sont appelées des* hypersurfaces. *Lorsque f est linéaire, on parle d'*hyperplans.

Nous terminons cette sous-section par l'énoncé d'un résultat bien utile :

Proposition 1.21 *Soit X et Y des variétés algébriques. Si X est irréductible, Y est fermé dans X, et $\dim Y = \dim X$, alors $X = Y$.*

1.6 Revêtement

Le but de cette sous-section est de montrer brièvement que l'on peut se donner un ouvert d'une variété algébrique sur lequel on aura un revêtement. Ce résultat sera utile lorsque l'on travaillera sur le *groupe de monodromie* dont on donnera la définition un peu plus loin.

Définition 1.22 *Si un ensemble fermé X est irréductible, alors le corps de fractions de l'anneau $\mathbb{C}[X]$ est appellé le* corps des fonctions rationelles *sur X et est noté $\mathbb{C}(X)$.*

Dans les applications qui suivront, on manipulera des fonctions de type méromorphe sur des variétés analytiques, qui sont analogues aux fonctions rationnelles sur une variété algébrique. Pour définir correctement notre relèvement, on introduit une notion de degré qui nous permettra par la suite de définir le nombre de feuillets du revêtement.

Définition 1.23 *Soit X et Y deux variétés. Pour toute application $\pi : Y \to X$ on définit l'application étoilée $\pi^* : \mathbb{C}(X) \to \mathbb{C}(Y); f \mapsto f \circ \pi$.*

Définition 1.24 *Si X et Y sont des variétés irréductibles de même dimension, et si $\pi : Y \to X$ est une application régulière et surjective, on dit que π est* de degré *d si le degré de l'extension $\pi^*(\mathbb{C}(X)) \subset \mathbb{C}(Y)$ est égal à d.*

Tout d'abord, on a le théorème suivant qui nous garantit la finitude des fibres d'une application finie.

Théorème 1.25 *Si $\pi : Y \to X$ est une application finie de variétés lisses irréductibles, alors le cardinal de l'ensemble $\pi^{-1}(p), p \in X$ est inférieur ou égal à deg f.*

On peut alors montrer qu'au-dessus d'un ouvert de Zariski $V \subseteq X$ non vide, la fibre de π est constante et de cardinal d (cf [3, Chap. 2 §6, Th.7]). On peut également supposer que X et Y sont lisses, et appliquer le théorème de Sard, qui stipule que sous ces conditions, l'ensemble des valeurs régulières de π est dense.
Alors, pour tout $x \in X$, et pour tout $y \in \pi^{-1}(x)$, π est une submersion en y, donc $\mathrm{d}_y\pi$ est bijective. Par le théorème d'inversion locale (et par finitude de la fibre), il existe un voisinage ouvert W de x dans V, et pour tout $y \in \pi^{-1}(x)$, des voisinages ouverts deux à deux disjoints W_y de y tels que $\forall y, \pi_{|W_y} : W_y \longrightarrow W$ soient des C^∞-difféomorphismes.

On a alors, avec la topologie naturelle, un revêtement (non-ramifié) à d feuillets au-dessus de V, via π, au sens de la définition 2.5 qui est donnée dans la prochaine section.

2 Du Groupe Fondamental

On va maintenant introduire un invariant topologique, le groupe fondamental, qui sera fort utile par la suite.
Il s'agit d'un des foncteurs principaux de la topologie algébrique, qui crée une image algébrique d'un espace topologique à partir des lacets de cet espace.

2.1 Lacets et homotopies

Prenons un espace topologique X, et x_0 un point de X.
On commence par redonner deux définitions classiques :

Définition 2.1 *Un lacet de X basé en x_0 est une application* continue $\gamma : [0,1] \longrightarrow X$ *telle que* $\gamma(0) = \gamma(1) = x_0$.

On peut concaténer deux lacets de la manière suivante : soit deux lacets γ et δ basés en x_0. On note $\gamma \cdot \delta$ le lacet basé en x_0 obtenu en parcourant d'abord δ puis γ de telle sorte que :

$$\forall s \in [0,1], \quad \gamma \cdot \delta(s) = \begin{cases} \delta(2s) & \text{si} \quad 0 \leq s \leq 1/2 \\ \gamma(2s-1) & \text{si} \quad 1/2 \leq s \leq 1 \end{cases}$$

Il est facile de voir que l'application $\gamma \cdot \delta$ est bien définie et continue, puisque $\delta(1) = \gamma(0) = x_0$ et qu'elle est continue sur les fermés $[0, 1/2]$ et $[1/2, 1]$, donc sur leur réunion.

Une reparamétrisation du lacet γ est la composition $\gamma \circ \varphi$ de γ par toute application continue $\varphi : [0,1] \longrightarrow [0,1]$ telle que $\varphi(0) = 0$ et $\varphi(1) = 1$.

On cherche maintenant à déformer continûment les lacets de l'espace, ce qu'on formalise dans la définition suivante :

Définition 2.2 *Une* homotopie *(de lacets) est une famille de fonctions (continues)* $(\gamma_t)_{t\in[0,1]} : [0,1] \longrightarrow X$ *telle que :*

- $\forall t \in [0,1]$, γ_t *est un lacet de X basé en x_0 ;*
- *l'application* $H : \begin{cases} [0,1] \times [0,1] \longrightarrow X \\ (t\ ,\ s) \longmapsto \gamma_t(s) \end{cases}$ *est continue.*

Remarque :
- On notera par la suite $\gamma_0 \sim \gamma_1$ si γ_0 et γ_1 sont homotopes.
- On peut définir d'une manière tout à fait analogue une homotopie de chemins.
- Dans un sous-espace convexe d'un espace vectoriel topologique réel (ou complexe), deux chemins γ_0 et γ_1 d'extrémités fixées sont toujours homotopes, via $\gamma_t(s) = (1-t)\gamma_0(s) + t\gamma_1(s)$. En particulier, tout lacet y est homotope à un point (lacet trivial).

Proposition 2.3 *La relation d'homotopie de lacets basés en un point x_0 fixé est une relation d'équivalence. On note alors $[\gamma]$ la classe d'équivalence du lacet γ (ie sa classe* d'homotopie*).*

Preuve : Soient γ_0, γ_1 et γ_2 trois lacets de X basés en x_0. La symétrie et la réflexivité se vérifient aisément. γ est homotope à lui-même via l'homotopie constante $\gamma_t = \gamma$, et si $\gamma_0 \sim \gamma_1$ via γ_t, alors γ_1 est homotope à γ_0 par γ_{1-t}.
Reste donc à montrer la transitivité. Si $\gamma_0 \sim \gamma_1$ via f_t, et $\gamma_1 \sim \gamma_2$ via g_t, alors on définit l'application h_t qui vaut f_{2t} quand $0 \leq t \leq 1/2$ et g_{2t-1} quand $1/2 \leq t \leq 1$. h_t est bien définie, vu que $f_1 = g_0 = \gamma_1$, et la continuité de l'application associée $H(s,t) = h_t(s)$ vient de la continuité sur $[0,1/2] \times [0,1]$ et $[1/2,1] \times [0,1]$ par les applications F et G associées à f_t et g_t. h_t réalise donc une homotopie entre γ_0 et γ_2. □

On peut d'ores et déjà remarquer que toute reparamétrisation d'un lacet ne modifie pas sa classe d'homotopie. En effet, si $\varphi : [0,1] \longrightarrow [0,1]$ est une telle reparamétrisation, on considère la famille d'applications continues $(\varphi_t)_{t\in[0,1]}$ telle que $\forall s \in [0,1], \varphi_t(s) = (1-t)\varphi(s) + ts$. Ainsi, $\varphi_0 = \varphi$ et $\varphi_1 = id_{[0,1]}$, et il n'est alors pas difficile de voir que la famille d'applications $(\gamma \circ \varphi_t)_{t\in[0,1]}$ est une homotopie entre $\gamma \circ \varphi$ et γ.

De même, la concaténation des lacets respecte l'homotopie : si $\gamma_0 \sim \gamma_1$ et $\delta_0 \sim \delta_1$ via γ_t et δ_t, alors $\forall t \in [0,1]$, l'application $\gamma_t \cdot \delta_t$ est bien définie et fournit naturellement une homotopie $(\gamma_0 \cdot \delta_0) \sim (\gamma_1 \cdot \delta_1)$.

On en arrive maintenant au point qui nous intéressait au départ, le groupe fondamental.

2.2 Structure de groupe

Soit X un espace topologique, et x_0 un point de X.

On considère maintenant l'ensemble des classes d'homotopies des lacets de X basés en x_0, et on note cet ensemble $\pi_1(X, x_0)$. Nous pouvons casser un suspense important et affirmer d'emblée que c'est évidemment cet objet que l'on appellera le groupe fondamental de X au point x_0, une fois énoncée la proposition suivante :

Proposition 2.4 *L'ensemble $\pi_1(X, x_0)$ est un groupe pour la loi de composition interne $[\gamma][\delta] = [\gamma \cdot \delta]$.*

Preuve : Tout d'abord, la loi de composition est bien définie : la concaténation de deux lacets basés en x_0 est un lacet basé en x_0, et on a vu que la classe d'homotopie $\gamma \cdot \delta$ ne dépendait que des classes d'homotopies des lacets γ et δ par la remarque précédent ce paragraphe.
Pour montrer l'associativité, on considère β, γ et δ trois lacets de X basés en x_0, et on montre que $\beta \cdot (\gamma \cdot \delta) \sim (\beta \cdot \gamma) \cdot \delta$. Un retour à la définition de la concaténation des lacets montre que si $\varphi : [0,1] \longrightarrow [0,1]$ est l'application affine par morceaux telle que :

$$\varphi(s) = \begin{cases} 2s & \text{si} \quad s \in [0, 1/4] \\ s + 1/4 & \text{si} \quad s \in [1/4, 1/2] \\ (s+1)/2 & \text{si} \quad s \in [1/2, 1] \end{cases}, \text{ alors } \forall s \in [0,1],\ \beta \cdot (\gamma \cdot \delta)(s) = (\beta \cdot \gamma) \cdot \delta \circ \varphi(s).$$

Comme φ est une reparamétrisation, cela conclut par la remarque précédente.
Soit maintenant e le lacet constant (tel que $\forall s \in [0,1], e(s) = x_0$). On montre exactement de la même manière que $\gamma \cdot e \sim \gamma$ *(resp.* $e \cdot \gamma \sim \gamma$*)* en considérant comme reparamétrisation la fonction affine par morceaux qui vaut 0 sur $[0, 1/2]$ et 1 en 1 *(resp. 1 sur [1/2, 1] et 0 en 0)*. On a alors bien montré que pour tout lacet γ, $[\gamma][e] = [\gamma] = [e][\gamma]$, $[e]$ est l'élément neutre.
On prétend maintenant, pour tout lacet γ, que $\tilde{\gamma} : t \in [0,1] \longmapsto \gamma(1-t)$, le chemin "inverse" de γ, est de classe d'homotopie inverse de $[\gamma]$. En effet, soit γ_t et $\tilde{\gamma_t}$ les chemins définis comme suit :

$$\gamma_t(s) = \begin{cases} \gamma(s) & \text{si} \quad 0 \leq s \leq 1-t \\ \gamma(1-t) & \text{si} \quad 1-t \leq s \leq 1 \end{cases} \quad \text{et } \tilde{\gamma}_t(s) = \begin{cases} \gamma(1-t) & \text{si} \quad 0 \leq s \leq t \\ \gamma(1-s) & \text{si} \quad t \leq s \leq 1 \end{cases}$$

($\tilde{\gamma}_t$ est le chemin "inverse" de γ_t). Alors $h_t = \tilde{\gamma}_t \cdot \gamma_t$ est une homotopie de lacets, et puisque $h_0 = \tilde{\gamma} \cdot \gamma$ et $h_1 = e$, on a bien que $\tilde{\gamma} \cdot \gamma \sim e$. En échangeant les rôles de γ et de $\tilde{\gamma}$, on obtient $\gamma \cdot \tilde{\gamma} \sim e$, et ainsi $[\gamma][\tilde{\gamma}] = e = [\tilde{\gamma}][\gamma]$. □

Par la remarque 2.1, si X est un sous-espace convexe d'un espace vectoriel topologique réel (ou complexe), on a $\pi_1(X, x_0) = \{0\}$.

2.3 Relèvement des homotopies

On donne rapidement la définition d'un revêtement d'un espace topologique X, puis on exhibe une action du groupe fondamental de X en un point sur la fibre du revêtement au-dessus de ce point.

Définition 2.5 *Soit X un espace topologique. Un* revêtement *de X est un couple $(\tilde{X}, \pi)$ (où $\tilde{X}$ est un espace topologique et π une application continue de $\tilde{X}$ dans X) tel que : $\exists (U_i)_{i \in I}$ un recouvrement ouvert de X tel que $\forall i \in I, \pi^{-1}(U_i)$ est une union disjointe d'ouverts de $\tilde{X}$ tous homéomorphes à U_i via π.*

En d'autres termes, pour un tel recouvrement, on se donne pour chaque U_i un homéomorphisme : $\phi_i : U_i \times F \longrightarrow \pi^{-1}(U_i)$ tel que $\forall x \in U_i, \forall f \in F, \quad \pi \circ \phi_i(x, f) = x$, où F est un espace discret, c'est-à-dire que l'on demande que le diagramme suivant commute :

$$\begin{array}{ccc} U_i \times F & \xrightarrow{\phi_i} & \pi^{-1}(U_i) \\ & \searrow^{pr_1} & \downarrow \pi \\ & & U_i \end{array}$$

L'espace X est appelé *base de la fibration*, $\tilde{X}$ est *l'espace fibré* et l'application π est le *pied de la fibration*, de fibre F.

Remarque : Si on ne permet pas l'union disjointe vide, la définition demande que l'application π soit surjective. C'est le parti pris dans cet exposé. De plus, on se limitera au cas des revêtements connexes.

Une application directe de la définition du revêtement montre que le cardinal de la fibre est localement constant au-dessus de X. En particulier, si X est connexe, vu que la famille $(U_i)_{i\in I}$ est un recouvrement ouvert de X, le cardinal de la fibre est constant et indépendant du point x de X.

Recherchons dès lors comment les applications passent au revêtement. On voudrait donc savoir s'il est possible de *relever* une application $f : Y \longrightarrow X$ en une application $\tilde{f} : Y \longrightarrow \tilde{X}$ telle que le diagramme $\begin{array}{ccc} Y & \xrightarrow{f} & X \\ & \searrow^{\tilde{f}} & \uparrow{\scriptstyle \pi} \\ & & \tilde{X} \end{array}$ commute.

Pour les lacets et les homotopies, on a en fait le résultat très utile suivant :

Théorème 2.6 (Théorème de relèvement) *Soit $(\tilde{X}, \pi)$ un revêtement (connexe) de X.*

- *Pour tout chemin γ de X partant de x_0, et pour tout $\tilde{x}_i \in \pi^{-1}(x_0)$, il existe un unique relèvement en un chemin $\tilde{\gamma}_i : [0,1] \longrightarrow \tilde{X}$ issu de $\tilde{x}_i$;*
- *Pour toute homotopie γ_t de chemins de X partant de x_0, et pour tout $\tilde{x}_i \in \pi^{-1}(x_0)$, il existe un unique relèvement de γ_t en une homotopie $\tilde{\gamma}_t : [0,1] \longrightarrow \tilde{X}$ de chemins partant de $\tilde{x}_i$.*

Remarque : En particulier, tout relèvement en $\tilde{x}_i$ d'un lacet homotope au lacet trivial e en x_0 est homotope au chemin constant $\tilde{x}_i$.

Preuve : On pourra se reporter à [4, Prop. 1.30, p.60] pour une preuve de ce résultat. □

En d'autres termes, cela signifie que la classe d'homotopie du relèvement d'un chemin de X (ou d'un lacet) ne dépend que de sa classe d'homotopie dans l'espace de base.

On a donc, pour tout point x de X, une *action de groupe* à gauche de $\pi_1(X,x)$ sur la fibre $\pi^{-1}(x)$ au-dessus de x.
En effet, si γ est un lacet de X basé en x_0, son relèvement $\tilde{\gamma}_i$ en $\tilde{x}_i$ vérifie la propriété $\pi \circ \tilde{\gamma}_i = \gamma$, et ainsi $\pi \circ \tilde{\gamma}_i(1) = x_0$, ie $\tilde{\gamma}_i(1) \in \pi^{-1}(x_0)$. Alors, l'application :

$$\begin{array}{rccccc} (\cdot) : & \pi_1(X,x_0) & \times & \pi^{-1}(x_0) & \longrightarrow & \pi^{-1}(x_0) \\ & ([\gamma] & , & \tilde{x}_i) & \longmapsto & \tilde{\gamma}_i(1) \end{array}$$

est bien définie. De plus, on a, par la remarque, que $\forall \tilde{x}_i \in \pi^{-1}(x_0), \quad [e] \cdot \tilde{x}_i = \tilde{x}_i$ et on vérifie que $\forall [\gamma], [\gamma'] \in \pi_1(X,x_0), \quad [\gamma] \cdot ([\gamma'] \cdot \tilde{x}_i) = [\gamma \cdot \gamma'] \cdot \tilde{x}_i$.

Cette action de groupe induit alors un morphisme ψ de $\pi_1(X, x_0)$ dans le groupe des permutations des points de la fibre, et l'image de ψ est appelée le *groupe de monodromie* de la fibration π au-dessus de x_0, noté $\mathcal{M}$. On peut aussi voir $\mathcal{M}$ comme le groupe des automorphismes de la fibre.

On en arrive alors au point central de notre sujet.

3 Groupe de monodromie et groupe de Galois

3.1 Position du problème

Soit X et Y deux variétés algébriques lisses irréductibles de même dimension sur le corps $\mathbb{C}$. On note $\mathbb{C}(X)$ et $\mathbb{C}(Y)$ les corps de fonctions algébriques correspondants.

Soit $\pi : Y \longrightarrow X$ une application de degré $d \geq 1$. Alors, π^* est l'inclusion des corps de fonctions induite par π, définie par :

$$\begin{array}{rccc} \pi^* : & \mathbb{C}(X) & \longrightarrow & \mathbb{C}(Y) \\ & g & \longmapsto & g \circ \pi \end{array}$$

L'application π^* est clairement un morphisme de corps, donc injectif, et on identifiera par la suite $\mathbb{C}(X)$ à son image dans $\mathbb{C}(Y)$ via π^*.

Comme nous sommes en caractéristique nulle, l'extension de corps $\mathbb{C}(X) \subset \mathbb{C}(Y)$ est séparable, de degré d par définition de π, et le théorème de l'élément primitif nous assure l'existence d'une fonction algébrique $f \in \mathbb{C}(Y) \setminus \mathbb{C}(X)$ qui engendre $\mathbb{C}(Y)$ sur $\mathbb{C}(X)$. On a alors, pour P le polynôme minimal de f (irréductible) sur $\mathbb{C}(X)$:

$$\left\{ \begin{array}{l} \mathbb{C}(Y) = \mathbb{C}(X)[f] \\ P(f) = f^d + g_{d-1} f^{d-1} + \cdots + g_0 = 0, \qquad P \in \mathbb{C}(X)[u] \end{array} \right.$$

Comme expliqué dans la section 1.6, l'application π définit un revêtement à d feuillets, tel que défini par la définition 2.5, au-dessus de tout point d'un sous-ensemble dense de X. Nous sommes donc naturellement amenés à regarder ce qui se passe localement en un tel point p de X, que nous fixons.

On peut alors choisir un voisinage ouvert U de p dans X pour la topologie de Zariski, de telle sorte que la restriction $\tilde{\pi}$ de π à $V = \pi^{-1}(U)$ soit un revêtement non-ramifié à d feuillets, et on note $\Gamma = \pi^{-1}(p) = \{q_1, \ldots, q_d\}$ la fibre de π au-dessus de X au point p. On peut d'ores et déjà montrer l'importante proposition suivante :

Proposition 3.1 *Si f désigne l'élément primitif qui engendre $\mathbb{C}(Y)$ sur $\mathbb{C}(Y)$, alors f prend des valeurs distinctes en tout point $q_i \in \Gamma = \pi^{-1}(p)$.*

Preuve : Supposons qu'il existe deux points distincts de Γ où f prenne la même valeur. Pour fixer les idées, et sans perte de généralité, on suppose $f(q_1) = f(q_2)$. Pour tout élément $h \in \mathbb{C}(Y)$, il existe $a_0, \ldots, a_{d-1}$ dans $\mathbb{C}(X)$ tels que $h = a_{d-1} f^{d-1} + \ldots a_1 f + a_0$. Alors, pour tout $i \in [\![0, d-1]\!]$, on a $a_i(q_1) = a_i(p) = a_i(q_2)$ (ce sont des éléments de $\mathbb{C}(X)$), ce qui montre que pour tout $h \in \mathbb{C}(Y)$, $h(q_1) = h(q_2)$. Comme manifestement, il existe des fonctions algébriques de $\mathbb{C}(Y)$ qui prennent des valeurs distinctes en q_1 et q_2, on obtient une contradiction. □

Regardons maintenant ce qu'il advient lorsque l'on restreint les corps de fonctions algébriques à des voisinages de p et des points de la fibre. Pour bien comprendre ce mécanisme, on doit considérer une classe de fonctions plus grande.

Soit Δ le corps des germes de fonctions méromorphes au voisinage de p, et Δ_i celui au voisinage d'un point de la fibre q_i.

Proposition 3.2 *Pour tout point q_i de la fibre au-dessus de p, l'application π restreinte à tout petit voisinage de q_i induit un isomorphisme de Δ_i sur Δ.*

Preuve : Fixons q_i un point de la fibre Γ au-dessus de p, et considérons V_i un voisinage ouvert de q_i. Alors, par le théorème d'inversion locale appliqué à $\pi_{|V_i} : V_i \longrightarrow X$ (qui est lisse), il existe un voisinage ouvert $W_i \subset V_i$ de q_i et un voisinage ouvert W de p dans X telle que $\pi_{|W_i} : W_i \longrightarrow W$ soit un homéomorphisme (et même un $\mathcal{C}^\infty$-difféomorphisme). Soit maintenant u et v des éléments de Δ_i. Quitte à restreindre V_i, on peut supposer que u et v sont définies sur V_i. Alors l'application :

$$\begin{array}{rccc} \pi_i : & \Delta_i & \longrightarrow & \Delta \\ & u & \longmapsto & u \circ (\pi_{|W_{i,u}})^{-1} \end{array}$$

est bien définie (en prenant bien garde de restreindre suffisamment les voisinages). On vérifie sans problème que c'est un morphisme de corps pour les lois usuelles, donc injectif. Pour ce qui est de la surjectivité, si g est un élément de Δ, quitte encore une fois à considérer des voisinages plus petits, on peut supposer que g est défini sur W et que $\pi_{|W_i}$ réalise un homéomorphisme de W_i sur W. Comme composée d'une fonction méromorphe avec une fonction holomorphe, $g \circ \pi_{|W_i}$ est bien un élément de Δ_i, défini sur W_i, et

$$\pi_i(g \circ \pi_{|W_i}) = (g \circ \pi_{|W_i}) \circ (\pi_{|W_i})^{-1} = g.$$

□

3.2 Deux sous-groupes de $\mathfrak{S}_d$

Soit U un voisinage de p défini comme au paragraphe précédent.
Comme on l'a vu au dernier paragraphe de la section 2.3, le groupe fondamental $\pi_1(U, p)$ agit sur la fibre Γ et cette action induit un morphisme de groupe de $\pi_1(U, p)$ dans $\mathfrak{S}_d$, d'image le groupe de monodromie $\mathcal{M}$ de $\tilde{\pi}$ au-dessus de p.

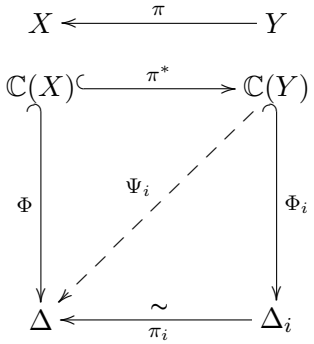
Remarque : On peut expliciter cet homomorphisme de la manière suivante :

$$\begin{array}{rccc} \varphi : & \pi_1(U,p) & \longrightarrow & \mathcal{M} \subset \mathfrak{S}_d \\ & [\gamma] & \longmapsto & \sigma \end{array}$$

où σ est la permutation telle que $\forall i \in [\![1, d]\!], \quad \tilde{\gamma}_i(1) = q_{\sigma(i)}$, pour $\tilde{\gamma}_i$ le relèvement d'un représentant quelconque de $[\gamma]$ en un chemin de Y issu de $q_i \in \Gamma$. On a déjà vu au paragraphe 2.3 en quoi cette application est bien définie.

On va maintenant, à partir des applications de restriction aux corps de germes de fonction méromorphes, exhiber différentes extensions de corps et construire ainsi un autre sous-groupe de $\mathfrak{S}_d$.

On a le diagramme (commutatif) suivant :



où on a appelé Φ (resp. Φ_1, ..., Φ_d) l'application de restriction de $\mathbb{C}(X)$ dans Δ (resp. de $\mathbb{C}(Y)$ dans Δ_1,..., Δ_d). On pose, pour alléger les notations, $\Psi_i = \pi_i \circ \Phi_i$. Ce sont tous des morphismes de corps, donc des isomorphismes sur leur image, et on note les sous-corps images comme suit :

$$\begin{array}{lcll} K & = & \Phi\left(\mathbb{C}(X)\right) & \subsetneq \ \Delta \\ \widetilde{K_i} & = & \Phi_i(\mathbb{C}(Y)) & \subsetneq \ \Delta_i \\ K_i & = & \Psi_i(\mathbb{C}(Y)) & \subsetneq \ \pi_i(\Delta_i) = \Delta \\ L & = & K_1 \cdot ... \cdot K_d & \subsetneq \ \Delta, \end{array}$$

où $K_1 \cdot ... \cdot K_d$ désigne le corps engendré sur K par les $K_i, i \in [\![1, d]\!]$.

Remarque :

- $\forall i \in [\![1, d]\!]$, on a la propriété de commutation $\Phi = \pi_i \circ \Phi_i \circ \pi^*$. En effet, si g est un élément de $\mathbb{C}(X)$, $\pi_i \circ (g \circ \pi)_{|W_i} = \pi_i(g \circ \pi_{|W_i}) = g_{|W} = \Phi(g)$, pour W et W_i des ouverts homéomorphes convenables, quitte à moduler leur taille comme on l'a déjà fait.
- En omettant (de fait) π^*, on obtient naturellement $\Phi = \pi_i \circ \Phi_i$ (*sur* $\mathbb{C}(X)$ *!*), et ce, pour tout i.

Proposition 3.3 *Chacune des extensions de corps $K \subset K_i$ est de degré d et engendrée sur K par l'élément $f_i = \Psi_i(f)$.*

Remarque : Par la proposition 3.1, f prend nécessairement des valeurs distinctes en tout point de la fibre au-dessus de p, ie les $f_i = \pi_i \circ \Phi_i(f)$ sont tous distincts (ils prennent fatalement des valeurs distinctes en p).

Preuve : Tout d'abord, chacun des K_i contient K, vu la propriété de commutation $\Phi = \pi_i \circ \Phi_i = \Psi_i$ sur $\mathbb{C}(X) \subset \mathbb{C}(Y)$.
D'autre part, si $P(u) = u^d + g_{d-1}u^{d-1} + \cdots + g_0 \in \mathbb{C}(X)[u]$ est le polynôme minimal de f, et que l'on note $\tilde{g}_n = \Phi(g_n)$ $(= \Psi_i(g_n))$, alors le polynôme obtenu par restriction

$\tilde{P} = \Psi_i(P) \in K[u]$ est toujours irréductible, et chaque $\tilde{f_i} = \Psi_i(f)$ vérifie l'équation polynomiale :

$$\tilde{P}(f_i) = \tilde{P}(\Psi_i(f)) = {f_i}^d + \tilde{g}_{d-1}{f_i}^{d-1} + \cdots + \tilde{g}_0 = \Psi_i(P(f)) = 0$$

Le polynôme $\tilde{P}$ est donc le polynôme minimal de f_i, pour tout i dans $[\![1, d]\!]$.
Par ailleurs, comme $\{1, f, \ldots, f^{d-1}\}$ est une base de $\mathbb{C}(Y)$ comme $\mathbb{C}(X)$-espace vectoriel, il est clair que tout élément de $K_i = \Psi_i(\mathbb{C}(Y))$ s'écrit comme combinaison linéaire sur K en les $\{1, f_i, \ldots, {f_i}^{d-1}\}$, c'est-à-dire que pour tout i, f_i engendre K_i sur K. □

On a alors exhibé les d racines distinctes du polynôme irréductible séparable $\tilde{P}$. On en déduit que le corps L est son corps de décomposition sur K. Ainsi l'extension de corps $K \subset L$ est galoisienne finie, et le groupe de Galois $\mathcal{G} = \mathrm{Gal}(L/K)$ de L sur K agit transitivement sur l'ensemble des racines de $\tilde{P}$. Cette action de groupe induit un homomorphisme injectif de $\mathcal{G}$ dans $\mathfrak{S}_d$.

Pour garder un maximum de clarté, on ne fera en fait pas l'identification entre $\mathcal{G}$ et son image dans $\mathfrak{S}_d$ par le morphisme d'action de groupe.

3.3 Lien entre groupe de Galois et groupe de monodromie

Le but de cette section est essentiellement de démontrer le théorème suivant :

Théorème 3.4 *Dans la situation décrite, le groupe de monodromie $\mathcal{M}$ et le groupe de Galois $\mathcal{G}$ sont canoniquement isomorphes.*

On commence par définir un morphisme de $\mathcal{M}$ dans $\mathcal{G} = \mathrm{Gal}(L/K)$.

On prend, avec les notations habituelles de cet exposé, γ un lacet de U basé en p et on note $\tilde{\gamma}_i$ l'unique relèvement de γ dans Y en un chemin issu de $q_i \in \Gamma$. Soit alors σ l'élément correspondant de $\mathcal{M}$ tel que $\forall i \in [\![1, d]\!], \quad \tilde{\gamma}_i(1) = q_{\sigma(i)}$.

Soit h un élément quelconque de $L = K_1 \cdot \ldots \cdot K_d$. L'idée générale est de prolonger analytiquement le germe h le long du lacet γ et de regarder le germe obtenu au terme de ce prolongement au voisinage de p. En fait, on va être capable de définir très naturellement un prolongement analytique le long d'un relèvement de γ dans Y, c'est-à-dire sur un petit voisinage ouvert autour de ce chemin dans Y.

Comme L est le corps engendré sur K par les sous-corps $K_1, \ldots, K_d$, h s'exprime comme un polynôme à d variables à coefficients dans K, calculé en les germes $h_i \in K_i$. Chacun des h_i est maintenant un polynôme à coefficients dans K, calculé en les f_i (on rappelle que pour tout i, $K_i = K(f_i)$). Finalement, h s'écrit $Q(f_1, \ldots, f_d)$, pour Q un polynôme sur K.

Pour chaque $f_i = \Psi_i(f) \in K_i$, on note $\tilde{f_i} = {\pi_i}^{-1}(f_i) = \Phi_i(f)$ le germe correspondant au voisinage de q_i.
Sur un petit ouvert (pour la topologie usuelle) dans Y autour de $\tilde{\gamma}_i$, f est bien définie et méromorphe, et a pour germe $\tilde{f_i}$ en q_i ; elle prolonge donc $\tilde{f_i}$ sur cet ouvert. Au voisinage

de $\tilde{\gamma}_i(1) = q_{\sigma(i)}$, le germe de f est $\tilde{f}_{\sigma(i)} = \Phi_{\sigma(i)}(f)$. En repassant dans L par l'isomorphisme $\pi_{\sigma(i)}$, on obtient l'élément $f_{\sigma(i)}$.

Remarque : La propriété de relèvement $\pi \circ \tilde{\gamma}_i = \gamma$ implique que, pour tout $t \in [0,1[$, on peut, de la même manière que l'on a défini les isomorphismes π_i entre les germes de fonction au voisinage de p et de q_i, définir par projection du germe de f en $\tilde{\gamma}(t)$ le germe du prolongement analytique de f_i en $\gamma(t)$. Ce prolongement est bien unique (pour chaque t) et prolonge f_i, par unicité du relèvement du lacet γ.
Attention cependant, il ne faut pas rêver (et c'est ce que l'on est en train de voir), ce prolongement sur un voisinage du chemin $\gamma(t)$ n'est plus défini dès que $\gamma_{|[0,t]}$ n'est plus injectif. En effet, on n'a aucune raison de retrouver le même germe au terme d'une boucle, et alors la fonction ainsi définie ne prolonge plus du tout le germe de départ.

On note alors ψ_σ l'application de L dans L qui à f_i associe $f_{\sigma(i)}$. Le lemme suivant montre que l'on a ainsi entièrement défini un automorphisme de L sur K.

Lemme 3.5

1. *$\psi_\sigma \in \mathcal{G} = Gal(L/K)$, et est entièrement déterminé par l'image des f_i.*
2. $\left\{ \begin{array}{ccccc} \psi : & \mathcal{M} & \hookrightarrow & Gal(L/K) \\ & \sigma & \longmapsto & \psi_\sigma \end{array} \right.$ *est un homomorphisme injectif de groupe.*

Preuve :

1. Comme tout élément de L s'écrit $Q(f_1, \ldots, f_d)$, pour Q un polynôme sur K, montrer que ψ est un automorphisme de L sur K donne gratuitement que ψ est défini sur L et est déterminé par l'image des f_i.
   - Soit $g \in K$, $\tilde{g} = \Phi^{-1}(g) \in \mathbb{C}(X)$. L'application $\tilde{g}$ est un prolongement le long de tout relèvement de γ dans Y, et par définition, $\forall i, j, \quad \Psi_i(\tilde{g}) = \Psi_j(\tilde{g}) = g$, c'est-à-dire que $\psi_\sigma(g) = g$.
     Donc ψ_σ fixe K.
   - Par unicité du prolongement analytique, on peut poser, pour tout i et j,

     $$\psi_\sigma(f_i + f_j) = \psi_\sigma(f_i) + \psi_\sigma(f_j) \quad \text{et} \quad \psi_\sigma(f_i f_j) = \psi_\sigma(f_i)\psi_\sigma(f_j)$$

     Ceci définit bien un prolongement analytique le long de γ, et ψ est tautologiquement un morphisme de corps.
   - Il n'est pas difficile de voir que ψ_σ est bijectif. Son inverse correspond au même processus effectué *en sens inverse*, associant $f_{\sigma^{-1}(j)}$ à f_j, pour tout j.

   D'où le résultat.
2. Il est clair que ψ est un morphisme de groupe. Il reste à montrer l'injectivité. Mais si $\psi = id_L$, alors pour tout i, f_i est envoyé sur $f_{\sigma(i)} = f_i$, et par la remarque qui suit la proposition 3.3, on a pour tout i, $\sigma(i) = i$, ie $\sigma = id_{\mathfrak{S}_d}$.

□

On peut alors identifier $\mathcal{M}$ à son image par ψ dans $\mathcal{G} = \mathrm{Gal}(L/K)$. Il reste à montrer l'inclusion réciproque. On va en fait montrer le lemme suivant.

Lemme 3.6 *Tout élément de L fixé par prolongement analytique le long de* tout *lacet γ de U basé en p est un élément de K.*

Montrons d'abord en quoi ceci implique le théorème 3.4.
On a $\mathcal{M} \subseteq \mathcal{G} = \mathrm{Aut}_K(L)$ est un sous-groupe fini, et par le lemme, $K = L^{\mathcal{M}}$. Alors, $\#\mathcal{M} = [L : K]$, et comme $K \subset L$ est une extension galoisienne finie, on en déduit que $\#\mathcal{M} = \#\mathrm{Gal}(L/K)$. Ainsi $\mathcal{M} = \mathrm{Gal}(L/K)$.

Preuve : Soit $g \in L$ fixé par prolongement analytique le long de *tout* lacet de U basé en p. On va montrer que l'hypothèse du lemme suffit pour construire un prolongement analytique de g en une fonction méromorphe G sur tout U. Ainsi, étant donné que g est un polynôme à coefficients dans K en les f_i, qui sont issues de fonctions méromorphes sur Y, g s'étend en une fonction méromorphe sur X de germe g en p, ie $g \in K$.
Soit $r \in U$ un point quelconque (distinct de p), et δ un chemin de p à r. En écrivant g comme un polynôme sur K en les f_i, on définit, comme expliqué dans la remarque ci-dessus, g_r le germe au voisinage de r obtenu par le polynôme sur K en les projections du germe du prolongement analytique de $\tilde{f}_i$ en $\tilde{\delta}_i(1)$ sur un voisinage ouvert de $\tilde{\delta}_i$.
Le point important est que ce germe est bien défini *de manière unique*, quel que soit le relèvement de δ choisi. En effet, pour tout autre chemin η allant de p à r dans U, $\delta \cdot \eta^{-1}$ est un lacet de U basé en p, et par hypothèse, le prolongement analytique le long de ce lacet est défini sur *tout* le lacet et donne toujours le germe g en p. Par unicité, le prolongement analytique le long de η donne donc le même germe g_r au voisinage de r.
On a ainsi prolongé $g \in L$ en une fonction méromorphe sur tout U, ce qui conclut. $\square$

4 Théorème de Position Générale

On considère maintenant une courbe algébrique $\mathcal{C}$ dans $\mathbb{P}^n(\mathbb{C})$, où n est un entier supérieur ou égal à 2, et on suppose que $\mathcal{C}$ est *irréductible* et *lisse*. $\mathcal{C}$ est le lieu des zéros d'une famille finie de polynômes homogènes $P_1, \ldots, P_m$, et est localement difféomorphe à $\mathbb{C}$.
Supposons de plus que $\mathcal{C}$ n'est contenue dans aucun hyperplan. En effet, dans le cas où il existe H tel que $\mathcal{C} \subset H$, on peut diminuer la dimension et travailler dans $\mathbb{P}^{n-1}(\mathbb{C})$.

On s'intéresse alors aux propriétés des intersections de cette courbe avec des hyperplans H de $\mathbb{P}^n(\mathbb{C})$.

Tout d'abord, remarquons que se donner un hyperplan de $\mathbb{P}^n(\mathbb{C})$ revient à se donner une équation linéaire homogène

$$\lambda : \quad \sum_{i=0}^{n} \lambda_i S_i = 0$$

Ainsi, on a une correspondance bijective entre les hyperplans de $\mathbb{P}^n(\mathbb{C})$ et les points $[\lambda_0 : ... : \lambda_n]$ de $\mathbb{P}^n(\mathbb{C})$. On notera $\check{\mathbb{P}}^n = (\mathbb{P}^n(\mathbb{C}))^*$ l'ensemble des hyperplans de $\mathbb{P}^n(\mathbb{C})$. L'affirmation précédente dit que $\check{\mathbb{P}}^n \simeq \mathbb{P}^n(\mathbb{C})$.

4.1 Degré d'une courbe et revêtement

Donnons la définition suivante :

Définition 4.1 *Soit un entier $d \geq 1$.*
Une courbe algébrique $\mathcal{C} \subset \mathbb{P}^n(\mathbb{C})$, $n \geq 2$ est dite de degré *d si tout hyperplan H transverse à $\mathcal{C}$ intersecte $\mathcal{C}$ en exactement d points.*

Remarque : Cette définition est cohérente : il est possible de montrer que dans $\mathbb{P}^n(\mathbb{C})$, le nombre de points d'intersections de $\mathcal{C}$ avec un hyperplan transverse est indépendant de l'hyperplan choisi ; ce résultat est faux dans $\mathbb{C}^n$. Le lecteur pourra se reporter à [3] pour une preuve de cette propriété.

Soit U l'ensemble des hyperplans transverses à $\mathcal{C}$.

Proposition 4.2 *U est un ouvert non vide de $\check{\mathbb{P}}^n$ pour la topologie de Zariski, ce qui en fait une sous-variété irréductible de $\mathbb{P}^n(\mathbb{C})$.*

Remarque : Par la proposition 1.7, U est lisse sur un ouvert de Zariski non vide. Nous identifierons par la suite U à cet ouvert de lissité.

Preuve : On va d'abord montrer, pour un point $x = [x_0 : \ldots : x_n] \in \mathcal{C}$ que l'ensemble :

$$F_x = \{H \in \check{\mathbb{P}}^n \text{ tq } H \text{ n'est pas transverse à } \mathcal{C} \text{ en } x\}$$

est fermé.

En un tel point x, l'espace tangent à $\mathcal{C}$ est une droite Δ_x, et demander que H ne soit pas transverse à $\mathcal{C}$ en x équivaut à demander que $T_x\mathcal{C} = \Delta_x \subset T_xH = H$. Alors, si H_x désigne l'ensemble des hyperplans contenant x, vu comme l'ensemble des formes linéaires qui s'annulent en x, on voit que $F_x = \{\lambda \in H_x \text{ tq } \lambda(\Delta_x) = 0\}$. La condition $\lambda(\Delta_x) = 0$ est clairement une condition fermée pour la topologie de Zariski. Donc, pour tout $x \in \mathcal{C}$, F_x est fermé.
Considérons maintenant l'ensemble $Z := \{(x, H) \text{ tq } x \in \mathcal{C}, H \in F_x\} \subseteq \mathcal{C} \times \check{\mathbb{P}}^n$. Z est fermé dans $\mathcal{C} \times \check{\mathbb{P}}^n$. On a alors la projection (trivialement continue) suivante :

$$pr_2 : Z \longrightarrow \check{\mathbb{P}}^n$$

Mais par fermeture des applications de projection entre deux variétés de l'espace projectif *(cf. la proposition 1.16)*, $pr_2(Z)$ est fermée dans $\check{\mathbb{P}}^n$. Or, $pr_2(Z) = \{H \in \check{\mathbb{P}}^n \text{ tq } \exists\ x \in \mathcal{C}, H \in F_x\} = U^c$. Donc U est ouvert.
Par ailleurs, la première projection $pr_1 : Z \longrightarrow \mathcal{C}$ est une application continue, et pour tout $x \in \mathcal{C}$, ${pr_1}^{-1}(\{x\}) = F_x \times \{x\} = \mathbb{P}^{n-2}(\mathbb{C})$, ie les fibres de pr_1 au-dessus de $\mathcal{C}$ sont toutes de dimension $n-2$. Ainsi, $\dim Z \leq (n-2)+1 = n-1$, ce qui implique que $\dim pr_2(Z) = \dim U^c \leq n-1$. Ceci montre que U est non vide et termine la preuve. □

On introduit alors l'ensemble :

$$I = \left\{ (p, H) \quad \text{tq} \quad \begin{array}{l} H \in U \\ p \in H \cap \mathcal{C} \end{array} \right\}$$

Proposition 4.3 *I est une sous-variété irréductible de $\mathcal{C} \times U$, de même dimension que U.*

Preuve : L'assertion « I est de même dimension que U » est immédiate.
Comme produit de deux variétés irréductibles, $\mathcal{C} \times U$ est une variété irréductible, et I est une sous-partie *fermée* de $\mathcal{C} \times U$. Supposons que I s'écrive comme union de 2 fermés F_1 et F_2. Soit pr_1 la projection de I dans $\mathcal{C}$. Alors,

$$\begin{aligned} \forall x \in \mathcal{C}, \quad {pr_1}^{-1}(\{x\}) &= \{H \in U \text{ tq } x \in H \cap \mathcal{C}\} \\ &= \{H \in U \text{ tq } x \in H\} \end{aligned}$$

Ce dernier ensemble, par la proposition 4.2, est ouvert dans $\{H \in \check{\mathbb{P}}^n \text{ tq } x \in H\} = \mathbb{P}^{n-1}$ qui est irréductible. Ainsi, pour tout $x \in \mathcal{C}$, la fibre de pr_1 au-dessus de x est irréductible. L'égalité :

$$\forall x \in \mathcal{C}, \quad {pr_1}^{-1}(\{x\}) = ({pr_1}^{-1}(\{x\}) \cap F_1) \cup ({pr_1}^{-1}(\{x\}) \cap F_2)$$

montre que ${pr_1}^{-1}(\{x\}) = ({pr_1}^{-1}(\{x\}) \cap F_1)$ ou $({pr_1}^{-1}(\{x\}) \cap F_2)$.
Comme l'ensemble $G_i = \{x \text{ tq } {pr_1}^{-1}(\{x\}) \subseteq F_i\} = pr_1(F_i)$ est fermé, et que clairement $\mathcal{C} = G_1 \cup G_2$, on a soit $G_1 = \mathcal{C}$, soit $G_2 = \mathcal{C}$. Supposons $G_1 = \mathcal{C}$ pour fixer les idées.

Cela prouve que $F_1 = I$. (En effet, s'il existe $(p, H) \in F_2 \setminus F_1$, on a la contradiction $F_1 \not\ni (p, H) \subset {pr_1}^{-1}(pr_1(p, H)) \subset F_1$.)
Donc, I est irréductible. $\square$

On a alors, en munissant tous ces ensembles de la topologie naturelle induite par $\mathbb{P}^n(\mathbb{C})$, le revêtement trivial à d feuillets :

$$\begin{array}{rccc} \pi : & I \subset \mathcal{C} \times U & \longrightarrow & U \\ & (p, H) & \longmapsto & H \end{array}$$

En effet, par définition du degré de $\mathcal{C}$, on a, pour tout H dans U, $\#\{p \in H \cap \mathcal{C}\} = d$, c'est-à-dire que :

$$\begin{array}{rcl} \forall H \in U, \quad \pi^{-1}(H) & = & \{(p_i, H), \qquad p_i \in (H \cap \mathcal{C}),\ i \in [\![1, d]\!]\} \\ & = & \{p_1, \ldots, p_d, \text{ où } p_i \in (H \cap \mathcal{C})\} \times H \end{array}$$

On se retrouve alors exactement dans la situation de la section 3. On se fixe donc un point de base $H_0 \in U$, et on note $\Gamma_0 = (\mathcal{C} \cap H_0, H_0) = \pi^{-1}(H_0)$ la fibre de π au-dessus de H_0.
On obtient ainsi un morphisme de groupes surjectif de $\pi_1(U, H_0)$ dans $\mathcal{M} = \mathrm{Aut}(\Gamma_0) \subseteq \mathfrak{S}_d$.

4.2 Détermination des automorphismes de la fibre

On cherche à déterminer le groupe de monodromie $\mathcal{M}$ de π au-dessus de Γ_0. Pour cela, on montre plusieurs propriétés de $\mathrm{Aut}(\Gamma_0)$, à partir desquelles on pourra joyeusement déduire que $\mathrm{Aut}(\Gamma_0) = \mathcal{M} = \mathfrak{S}_d$.
On introduit tout d'abord, $\forall k \in [\![1, d]\!]$,

$$I(k) = \left\{ (p_1, \ldots, p_k, H) \quad \text{tq} \quad \begin{array}{l} H \in U \\ \forall i,\ p_i \in \mathcal{C} \cap H \text{ et les } p_i \text{ sont 2 à 2 distincts} \end{array} \right\}$$

$I(k)$ est une sous-variété de $\mathcal{C}^k \times U$. Commençons par montrer le lemme suivant :

Lemme 4.4 *$\mathcal{M} = Aut(\Gamma_0)$ est doublement transitif $\iff$ $I(2)$ est connexe par arcs (pour la topologie usuelle).*

Remarque :

- En utilisant exactement les mêmes arguments, on montre que pour tout $k \in [\![1, d]\!]$, le fait que $I(k)$ soit connexe par arcs (pour la topologie usuelle) est équivalent au fait que $\mathcal{M}$ agisse k fois transitivement sur Γ_0.
- On a montré dans le théorème 3.4 que $\mathcal{M}$ était égal au groupe de Galois d'une certaine extension de corps. Cela montre en particulier que $\mathcal{M}$ agit transitivement sur la fibre de π au-dessus de H_0, et que I est connexe, ce qui n'est pas surprenant (I est irréductible).

Preuve : On procède par la méthode mondialement connue de la double implication.

1. Supposons que $I(2) \subset \mathcal{C} \times \mathcal{C} \times U$ soit connexe par arcs.

   Quitte à renuméroter, pour alléger les notations, on considère deux points de Γ_0, (p_1, p_2, H_0) et (p_3, p_4, H_0), non nécessairement distincts. $I(2)$ étant connexe par arcs,

   $$\exists\, \tilde{\gamma} : [0,1] \longrightarrow I(2) \text{ continue tq } \left\{ \begin{array}{lcl} \tilde{\gamma}(0) & = & (p_1, p_2, H_0) \\ \tilde{\gamma}(1) & = & (p_3, p_4, H_0) \end{array} \right.$$

   Alors, avec les notations évidentes, $pr_1 \circ \tilde{\gamma}$ est un chemin allant de (p_1, H_0) à (p_3, H_0). De même, $pr_2 \circ \tilde{\gamma}$ est un chemin allant de (p_2, H_0) à (p_4, H_0).

   De plus on a bien entendu que $\pi \circ pr_1 \circ \tilde{\gamma} = \pi \circ pr_2 \circ \tilde{\gamma}$, c'est un lacet γ de U, basé en H_0. La propriété de relèvement de γ (et son unicité) induit, comme cela a été vu, une permutation σ de $\mathrm{Aut}(\Gamma_0)$ qui envoie (p_1, H_0) sur (p_3, H_0) et (p_2, H_0) sur (p_4, H_0). Ceci montre que $\mathcal{M}$ agit doublement transitivement sur Γ_0.

2. Supposons maintenant que $\mathcal{M}$ soit doublement transitif.

   On reprend (toujours quitte à numéroter), les mêmes points de Γ_0 qu'au-dessus. Par double transitivité de $\mathcal{M}$,

   $$\exists\, \sigma \in \mathrm{Aut}(\Gamma_0) : \left\{ \begin{array}{lcl} (p_1, H_0) & \longmapsto & (p_3, H_0) \\ (p_2, H_0) & \longmapsto & (p_4, H_0) \end{array} \right.$$

   Par définition du groupe de monodromie, il existe un lacet γ de U basé en H_0 tel que les relèvements issus respectivement de (p_1, H_0) et (p_2, H_0) vérifient $\tilde{\gamma}_1(1) = (p_3, H_0)$ et $\tilde{\gamma}_2(1) = (p_4, H_0)$, avec les notations utilisées tout au long du mémoire. Alors :

   $$\begin{array}{rccc} \tilde{\gamma} : & [0,1] & \longrightarrow & I(2) \\ & t & \longmapsto & (pr_1 \circ \tilde{\gamma}_1(t) \quad , \quad pr_1 \circ \tilde{\gamma}_2(t) \quad , \quad H(t) = pr_2 \circ \tilde{\gamma}_i(t)) \end{array}$$

   est continue, par les propriétés de la topologie produit. Le même raisonnement étant en fait valable pour n'importe quel point de base dans U, on a bien que $I(2)$ est connexe (par arcs).

□

Proposition 4.5 *$\mathcal{M}$ est doublement transitif.*

Preuve : On pose :

$$\widetilde{I}(2) = \left\{ (p_1, p_2, H) \quad \text{tq} \quad \begin{array}{l} H \in \check{\mathbb{P}}^n \\ p_1 \neq p_2, \quad p_i \in H \cap \mathcal{C} \end{array} \right\}$$

Ceci est légèrement différent de $I(2)$, au sens où on l'on se permet d'intersecter $\mathcal{C}$ avec n'importe quel hyperplan de $\mathbb{P}^n(\mathbb{C})$, et non plus uniquement par des hyperplans transverses à $\mathcal{C}$ de U.

On va montrer que $\widetilde{I}(2)$ est irréductible. Ainsi, comme $I(2)$ est *ouvert* dans $\widetilde{I}(2)$, $I(2)$ est irréductible, donc connexe (pour la topologie de Zariski). Par la proposition 1.15, $I(2)$ est connexe pour la topologie usuelle (donc connexe par arcs en dimension finie), et par le lemme 4.4 que l'on vient de montrer, cela conclut.
Soit $\Delta = \{(p,q) \in \mathcal{C} \times \mathcal{C} \text{ tq } p = q\}$. Δ est fermée dans $\mathcal{C} \times \mathcal{C}$, donc $(\mathcal{C} \times \mathcal{C}) \setminus \Delta$ est irréductible. On a la projection canonique suivante :

$$\begin{array}{ccccc} \widetilde{I}(2) & \longrightarrow & (\mathcal{C} & \times & \mathcal{C}) \setminus \Delta \\ (p,q,H) & \longmapsto & (p & , & q) \end{array}$$

et

$$\begin{array}{rcl} \forall (p,q) \in (\mathcal{C} \times \mathcal{C}) \setminus \Delta, \quad \pi^{-1}(p,q) & = & \{H \in \check{\mathbb{P}}^n \text{ tq } p,q \in H\} \\ & \simeq & \mathbb{P}^{n-2}(\mathbb{C}) \end{array}$$

Alors, pour tout couple d'éléments distincts de $\mathcal{C}$, la fibre de cette projection est irréductible. Si $\widetilde{I}(2) = F_1 \cup F_2$, où F_1 et F_2 sont fermés, les mêmes arguments que dans la preuve de la proposition 4.3, montrent que chaque fibre est soit dans F_1 soit dans F_2, et par irréductibilité de $(\mathcal{C} \times \mathcal{C}) \setminus \Delta$, que F_1 ou F_2 est en fait $\widetilde{I}(2)$ tout entier. Ainsi, $\widetilde{I}(2)$ est irréductible. □

Remarque : On utilise dans cette preuve qu'un couple d'éléments distincts de $\mathcal{C} \times \mathcal{C}$ détermine exactement une droite de $\mathbb{P}^n(\mathbb{C})$. Les arguments développés ne fonctionneraient *plus* si l'on voulait considérer des ensembles $\widetilde{I}(k), k > 2$, les fibres n'étant plus de dimension constante.

Proposition 4.6 *$\mathcal{M}$ contient une transposition.*

Preuve : On pose $\mathcal{C}^* = \{H \in \check{\mathbb{P}}^n \text{ tq } \exists\, x \in \mathcal{C}, T_x\mathcal{C} \subset H\} = \check{\mathbb{P}}^n \setminus U$.
Comme le lieu des points d'inflexion de $\mathcal{C}$ est fermé dans $\mathcal{C}$, et que, par les mêmes arguments que ceux développés dans la preuve de la proposition 4.2, l'ensemble des hyperplans de $\mathcal{C}^*$ tangents en deux points distincts de $\mathcal{C}$ est fermé dans $\mathcal{C}^*$, on peut trouver $H_1 \in \mathcal{C}^*$ qui soit simplement tangent en un point p de $\mathcal{C}$, et transverse à $\mathcal{C}$ en tous les autres points d'intersection.
Par ailleurs, comme $\mathcal{C}^*$ est un fermé propre de $\check{\mathbb{P}}^n$, il existe un sous-espace de $\check{\mathbb{P}}^n$ de dimension au moins 1 qui intersecte transversalement $\mathcal{C}^*$ en H_1.
$\mathcal{C}$ est une variété différentielle lisse de dimension 1, on peut, localement en p, la plonger dans $\mathbb{C}^2$ de manière C^∞ par un difféomorphisme φ (sur son plan osculateur par exemple), de sorte que $\varphi(p) = 0$. Comme p n'est pas un point d'inflexion, dans un tel plan, l'équation de $\mathcal{C}$ est de la forme $y = \alpha x^2$, où $\alpha \neq 0$. (Et on supposera que $\alpha > 0$ sans perte de généralité.)
On considère alors une famille (H_t) d'hyperplans d'équation (via φ) $y = (t-1)$, où $t \in \mathbb{C}, |t-1| \leq \varepsilon$, tels que pour tout $t \neq 1$, $H_t \in U$. Remarquons que (H_t) intersecte

transversalement $\mathcal{C}^*$ en H_1. On a alors que $H_t \cap \varphi(\mathcal{C})$ est défini par le système d'équations :

$$\left\{ \begin{array}{rcl} y & = & \alpha x^2 \\ y & = & t-1 \end{array} \right. \tag{1}$$

Posons $t-1 = \varepsilon e^{i\theta}, \theta \in [0, 2\pi]$. Alors le système (1) se résout en :

$$\left\{ \begin{array}{rcl} y & = & \varepsilon e^{i\theta} \\ x & = & \pm \sqrt{\varepsilon/\alpha}\ e^{i\theta/2} \end{array} \right.$$

On voit alors que quand t tend vers 1, (ie ε tend vers 0), $H_t \cap \varphi(\mathcal{C})$ tend vers $0 = \varphi(p)$, et quand t tourne autour de 1, c'est-à-dire quand θ parcourt $[0, 2\pi]$, $(\sqrt{\varepsilon/\alpha}, 1+\varepsilon)$ est envoyé sur $(-\sqrt{\varepsilon/\alpha}, 1+\varepsilon)$, et vice-versa. En repassant dans $\mathbb{P}^n(\mathbb{C})$ par le difféomorphisme φ^{-1}, on voit qu'on a échangé deux points de la courbe au voisinage de p.
De plus, on a choisi H_1 tel que H_1 soit simplement tangent en *un seul* point de $\mathcal{C}$, et les $(H_t)_{t\in\mathbb{C}}, |t-1| \leq \varepsilon$ dans U pour tout $t \neq 1$. Ceci montre que quand t tourne une fois autour de 1, les autres points d'intersection restent inchangés.
Le groupe de monodromie ne dépendant pas du point de base choisi (en effet, U est irréductible, donc connexe, et le groupe fondamental d'un espace connexe ne dépend pas du choix du point de base), on a donc montré que $\mathcal{M}$ contient une transposition. □

Nous arrivons maintenant au bout de nos peines, étant donné que l'on a pratiquement démontré le théorème annoncé au début de la section :

Théorème 4.7 *Dans les conditions décrites ci-dessus,* $\mathrm{Aut}(\Gamma_0) = \mathcal{M} = \mathfrak{S}_d$.

Preuve : Par les propositions 4.5 et 4.6, $\mathcal{M} \subseteq \mathfrak{S}_d$ est doublement transitif et contient une transposition τ. Il ne manque en fait plus que quelques arguments d'algèbre élémentaire. Supposons pour fixer les idées que $\tau = (12)$. Alors, par double transitivité, pour tous $i \neq j \in [\![1, d]\!]$, il existe $\sigma \in \mathcal{M}$ tel que $\sigma(1) = i$ et $\sigma(2) = j$. Mézalors, $\sigma\tau\sigma^{-1}$ est encore un élément de $\mathcal{M}$, qui envoie i sur j, j sur i, et laisse tous les autres invariants, c'est-à-dire que $\sigma\tau\sigma^{-1} = (ij)$.
Donc $\mathcal{M}$ contient toutes les transpositions, c'est donc le groupe symétrique $\mathfrak{S}_d$ tout entier, qui est, comme tout un chacun le sait, engendré par les transpositions. □

Moralement, ce théorème signifie qu'il n'existe aucune structure sur les points d'intersection de $\mathcal{C}$ avec H (d'alignement par exemple) qui serait conservée quand H parcourt l'ensemble des hyperplans transverses. C'est un théorème négatif.

4.3 Indépendance linéaire

On considère toujours dans $\mathbb{P}^n(\mathbb{C}), n \geq 2$, H un hyperplan transverse à $\mathcal{C}$ ($\mathcal{C} \not\subset H$, qui intersecte $\mathcal{C}$ en exactement d points. On a le résultat suivant :

Théorème 4.8 *Soit $\mathcal{P}_n(H)$ un n-uplet de points deux à deux distincts de $H \cap \mathcal{C}$. Alors il existe un ouvert $\mathcal{O}$ non vide de U tel que pour tout $H \in \mathcal{O}$, les éléments de $\mathcal{P}_n(H)$ sont linéairement indépendants.*

Précisons un peu le sens de ce théorème. A chaque point de $\mathbb{P}^n(\mathbb{C})$ dans l'intersection de $\mathcal{C}$ avec $H \in \mathcal{O}$ correspond une droite (et une seule) de l'espace vectoriel complexe $\mathbb{C}^{n+1}$. Le théorème affirme que tout tel n-uplet de droites est libre.

Remarque : Il peut arriver que le degré de la courbe soit strictement inférieur à n. Dans ce cas, le théorème reste vrai, à condition de se limiter bien évidemment à des multi-uplets ayant moins de d éléments. Dans la suite, on suppose $n \leq d$.

Preuve : Considérons le sous-ensemble de $I(n)$:

$$J = \left\{ (p_1, ...p_n, H) \quad \text{tq} \quad \begin{array}{l} H \in U \\ \mathcal{P}_n = (p_1, \ldots, p_n) \text{ est un des } n\text{-uplets décrits ci-dessus} \\ \mathcal{P}_n \text{ est liée} \end{array} \right\}$$

J est fermé dans $I(n)$ pour la topologie de Zariski. En effet, les points de $I(n)$ appartenant à J vérifient $\mathrm{Rg}(p_1, \ldots, p_n) \leq n-1$. Une caractérisation du rang en fonction des mineurs d'ordre n donne une condition polynomiale pour que $\mathcal{P}_n$ soit liée. Plus précisément, si on note Δ_n l'ensemble des mineurs d'ordre n, J correspond au lieu des solutions du système de polynômes homogènes :

$$\forall \delta \in \Delta_n, \quad \det\left[\delta(p_1, \ldots, p_n)\right] = 0$$

J est strictement inclus dans $I(n)$, par l'hypothèse que $\mathcal{C}$ n'est contenue dans aucun hyperplan. Ainsi, J est une sous-variété propre de $I(n)$.
$\mathcal{M} = \mathfrak{S}_d$ implique que $\mathcal{M}$ agit n fois transitivement sur la fibre, c'est-à-dire que $I(n)$ est connexe par arcs pour la topologie usuelle, donc connexe pour la topologie de Zariski, par la proposition 1.15. Mais maintenant, si $I(n)$ s'écrit comme une union de deux fermés propres (donc distincts), soit ils sont disjoints et $I(n)$ n'est pas connexe, soit ils sont non-disjoints et $I(n)$ n'est plus lisse en un point de l'intersection. Donc $I(n)$ est irréductible. Par irréductibilité de $I(n)$ *(cf. proposition 1.21)*, $\dim J < \dim I(n) = \dim U$. Alors J se projette via π dans U, et :

$$\dim \pi(J) \leq \dim J < \dim U$$

Ceci prouve que $\pi(J)$, qui est fermée, est une sous-variété propre de U. Et $\mathcal{O} = U \setminus \pi(J)$, qui est non vide, convient. □

On a donc démontré le « Théorème de Position Générale » :

Théorème 4.9 *Soit $\mathcal{C} \subset \mathbb{P}^n(\mathbb{C}), n \geq 2$ une courbe algébrique irréductible lisse de degré d. Alors un hyperplan* générique *intersecte $\mathcal{C}$ en d points, et chaque n-uplet de ces d points est* libre.

Remarque : Le terme *générique* signifie que l'ensemble des hyperplans de $\check{\mathbb{P}}^n$ qui vérifient ces propriétés est un ouvert non vide de $\check{\mathbb{P}}^n$, pour la topologie de Zariski. On le rencontre très souvent en géométrie algébrique. Il est en quelque sorte l'équivalent du « presque-partout » que l'on côtoie en analyse.

Table des matières

1 Rudiments sur les variétés complexes et algébriques **2**
1.1 Variétés complexes sur $\mathbb{C}^n$ . . . 2
1.2 Variétés algébriques affines . . . 3
1.3 Un mot à propos des fonctions et applications sur des variétés . . . 4
1.4 Considérations topologiques . . . 5
1.5 Notions de dimension . . . 6
1.6 Revêtement . . . 7

2 Du Groupe Fondamental **9**
2.1 Lacets et homotopies . . . 9
2.2 Structure de groupe . . . 10
2.3 Relèvement des homotopies . . . 11

3 Groupe de monodromie et groupe de Galois **14**
3.1 Position du problème . . . 14
3.2 Deux sous-groupes de $\mathfrak{S}_d$ . . . 15
3.3 Lien entre groupe de Galois et groupe de monodromie . . . 17

4 Théorème de Position Générale **20**
4.1 Degré d'une courbe et revêtement . . . 20
4.2 Détermination des automorphismes de la fibre . . . 22
4.3 Indépendance linéaire . . . 26

Références

[1] J. Harris : *Galois groups of enumerative problems*, Duke Mathematical Journal **46** 1978, n.4, pp. 685-724.

[2] E. Arbarello, M. Cornalba, P.A. Griffiths, J. Harris : *Geometry of Algebraic Curves*, Vol. I, pp. 109-112, Grundlehren der mathematischen Wissenschaften, **267** Springer-Verlag, Berlin, 1985.

[3] I.R. Shafarevitch : *Basic Algebraic Geometry*, Grundlehren der mathematischen Wissenschaften, **213** Springer-Verlag, Berlin, 1974.

[4] A. Hatcher : *Algebraic Topology*, Cambridge University Press, 2002. (disponible sur la page de Allen Hatcher).

[5] F. Paulin : *Géométrie différentielle élémentaire*, Cours de première année de mastère, École Normale Supérieure, 2006. (disponible à l'adresse http ://www.fimfa.ens.fr/)