THÉORIE DE GALOIS

Cours accélérée de DEA

Alain Kraus

Université de Paris VI

Octobre 1998

Théorie de Galois des extensions de corps

Tous les corps que l'on considérera dans la suite seront supposés commutatifs.

I. Extensions de corps

Tout d'abord une définition :

Définition 1.1. *Soit K un corps. Une extension de K est la donnée d'un couple (L, j), où L est un corps et où $j : K \to L$ est un homomorphisme de corps de K dans L.*

Un homomorphisme de corps $j : K \to L$ est nécessairement injectif. On identifiera souvent K et son image $j(K)$ dans L, de sorte que, à isomorphisme près, K peut être considéré comme un sous-corps de L. Il n'y a pas en général d'inconvénient à faire cette identification. Dans une situation cependant cette identification est à proscrire : celle où $K = L$ et où j est un automorphisme de K. Si L contient K, (L, i) est une extension de K au moyen de l'injection canonique i (donnée par l'inclusion). On omettra souvent l'homomorphisme j pour désigner une extension (L, j) de K. Si L est une extension de K, le corps L est naturellement muni d'une structure d'espace vectoriel sur le corps K.

I.1. Éléments algébriques, Éléments transcendants

Soient K et L deux corps tels que L contienne K. Soit α un élément de L. Le plus petit sous-anneau de L contenant K et α est l'ensemble $K[\alpha]$ des expressions polynomiales en α. Son corps des fractions, que l'on notera $K(\alpha)$, est le plus petit sous-corps de L contenant K et α. On dit que $K(\alpha)$ est une extension simple de K.

Soit X une indéterminée. Considérons l'homomorphisme d'anneaux

$$\varphi_\alpha : K[X] \to K[\alpha]$$

défini par les égalités $\varphi_\alpha(a) = a$ si a est dans K, et par $\varphi_\alpha(X) = \alpha$. Il est surjectif. Soit I son noyau. C'est un idéal de $K[X]$. Deux cas peuvent se présenter suivant que I est nul ou non :

Définition 1.2. *On dit que α est transcendant sur K si $I = (0)$, et que α est algébrique sur K si I est non nul.*

1) Si α est transcendant sur K, il n'existe pas de polynôme P non nul de $K[X]$ tel que $P(\alpha) = 0$. L'homomorphisme φ est dans ce cas un isomorphisme de l'anneau $K[X]$ sur $K[\alpha]$.

2) Supposons que α soit algébrique sur K. Dans ce cas, φ_α passée au quotient réalise un isomorphisme de $K[X]/I$ sur $K[\alpha]$. On déduit de là que I est un idéal premier, et puisqu'il est non nul, il est en fait maximal. Cela montre en particulier que $K[\alpha]$ est un corps. On a donc l'égalité $K[\alpha] = K(\alpha)$. Par ailleurs, il existe un unique polynôme unitaire P qui engendre I. Puisque I est premier, P est un polynôme irréductible.

Définition 1.3. *On dit que P est le polynôme minimal de α sur K. Le degré de α est le degré de P.*

On peut résumer ce qui précède par le résultat suivant :

Proposition 1.1. *Les assertions suivantes sont équivalentes :*
(i) l'élément α est algébrique sur K ;
(ii) on a $K[\alpha] = K(\alpha)$;
(iii) le K-espace vectoriel $K(\alpha)$ est de dimension finie.
Si α est algébrique sur K le K-espace vectoriel $K(\alpha)$ est de dimension n égal au degré de α. La famille $(\alpha^i)_{0\leq i\leq n-1}$ est alors une base de $K(\alpha)$ sur K.

Démonstration : Montrons l'équivalence des conditions (i) et (ii). Si α est algébrique sur K, on a vu que $K[\alpha] = K(\alpha)$. Inversement si l'on a $K[\alpha] = K(\alpha)$, $K[\alpha]$ est un corps et nécessairement α est algébrique. Montrons maintenant que (ii) $\Rightarrow$ (iii). Soit x un élément de $K[\alpha]$. Soient P le polynôme minimal de α et n le degré de P. On a $x = f(\alpha)$, où f est un élément de $K[X]$. On effectue alors la division euclidienne de f par P : on a $f = QP + R$, où le degré de R est $\leq n-1$. On a ainsi $x = R(\alpha)$, ce qui prouve que $(\alpha^i)_{0\leq i\leq n-1}$ est un système générateur du K-espace vectoriel $K(\alpha)$. D'où l'implication. Supposons la condition (iii) réalisée. Si n est la dimension du K-espace vectoriel $K(\alpha)$, la famille $(\alpha^i)_{0\leq i\leq n}$ est alors liée, ce qui entraîne le fait que α soit algébrique.

Enfin si α est algébrique de degré n, le système $(\alpha^i)_{0\leq i\leq n-1}$ est libre car un polynôme non nul de degré $\leq n-1$ ne peut appartenir à l'idéal noyau de l'homomorphisme φ_α. D'où la proposition.

Exemples

1) Soit d un entier relatif sans facteur carré. Le corps $K = \mathbb{Q}[X]/(X^2 - d)$ est une extension de degré 2 de $\mathbb{Q}$. On dit que K est une extension quadratique de $\mathbb{Q}$.
2) Soit X une indéterminée, $L = \mathbb{Q}(X)$ et $K = \mathbb{Q}(X^3)$. Alors L est une extension algébrique de K de degré 3. Le polynôme minimal, en l'indéterminée Y, de X sur K est $Y^3 - X^3$.
3) On peut démontrer que les nombres e et π sont transcendants sur $\mathbb{Q}$.
4) le polynôme X^2+1 est irréductible sur $\mathbb{R}$. Le corps $\mathbb{R}[X]/(X^2+1)$ est une extension de degré 2 de $\mathbb{R}$. C'est (par définition) le corps $\mathbb{C}$ des nombres complexes.

Exercices. 1) Soit α un nombre complexe racine du polynôme $X^3 - X + 1$. Posons $K = \mathbb{Q}(\alpha)$ (K est le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et α). Soit $a = 1 + 2\alpha - 3\alpha^2$. Le corps K est une extension de $\mathbb{Q}$ de degré 3. Déterminer les coordonnées de l'inverse de a dans la base $(1, \alpha, \alpha^2)$ de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. Le nombre 2 est-il un carré dans $\mathbb{Q}(\alpha)$?

2) Montrer que l'élément $\sqrt{2} + \sqrt{3}$ dans $\mathbb{C}$ est algébrique. Quel est son degré ?

3) Soit α une racine dans $\mathbb{C}$ du polynôme $X^3 - 2$. Posons $K = \mathbb{Q}(\alpha)$. Montrer que le polynôme $X^2 + \alpha X + \alpha^2$ est irréductible sur $\mathbb{Q}(\alpha)$.

4) Soient p un nombre premier et $\mathbb{F}_p$ le corps à p éléments. Montrer que si 4 divise $p-3$, $\mathbb{F}_p[X]/(X^2+1)$ est une extension de degré 2 de $\mathbb{F}_p$.

I.2. Extensions finies

Considérons deux corps L et K tels que L soit une extension de K : on dispose d'un homomorphisme de corps $j : K \to L$.

Définition 1.4. *On dit que L est une extension finie de K, si L en tant que K-espace vectoriel est de dimension finie. On note souvent $[L : K]$ cette dimension.*

On identifiera désormais K et son image $j(K)$ dans L.

Proposition 1.2. *Si L est une extension finie de K et si K est une extension finie de H alors L est une extension finie de H et l'on a $[L : H] = [L : K][K : H]$.*

Démonstration : C'est un exercice facile d'algèbre linéaire.

Corollaire 1.1. *Supposons que L soit une extension de K de degré n. Alors tout élément de L est algébrique sur K et son degré sur K est un diviseur de n.*

Démonstration : Soit α un élément de L. Les $n+1$ éléments 1, α, ...α^n de L sont K-linéairement dépendants. Donc α est un zéro d'un polynôme non nul à coefficients dans K et α est algébrique sur K. On déduit de là que le sous-corps $K(\alpha)$ de L engendré par K est α est une extension finie de K (proposition 1.1). La proposition 1.2 entraîne alors le résultat.

Exercices. 1) Soient L une extension d'un corps K et α un élément de L algébrique de degré impair sur K. Montrer que l'on a $K(\alpha) = K(\alpha^2)$.

2) Soient L une extension finie de degré n d'un corps K et F un polynôme de degré m de $K[X]$, irréductible sur K. Montrer que si m et n sont premiers entre eux, F est irréductible sur L.

3) Soit p un nombre premier impair. Montrer que le sous-corps de $\mathbb{C}$ engendré sur $\mathbb{Q}$ par $\cos(2\pi/p)$ est une extension finie de $\mathbb{Q}$ dont on déterminera le degré sur $\mathbb{Q}$ (on pourra d'abord traiter le cas où $p = 5$).

Définition 1.5. *Soient $(\alpha_i)_{1\leq i\leq n}$ des éléments de L. On notera $K(\alpha_1, ..., \alpha_n)$ le sous-corps de L engendré sur K par les α_i. On dira que L est obtenu par adjonction à K des éléments (α_i).*

Proposition 1.3. *Supposons que L soit une extension finie d'un corps K. Il existe un nombre fini d'éléments $(\alpha_i)_{1\leq i\leq n}$ de L, tels que l'on ait l'égalité $L = K(\alpha_1, ..., \alpha_n)$.*

Démonstration : Il suffit de prendre pour $(\alpha_i)_{1\leq i\leq n}$ une base de L sur K, où n est la dimension de L sur K.

I.3. Extensions algébriques

Considérons deux corps L et K tels que L soit une extension de K : on dispose d'un homomorphisme de corps $j : K \to L$.

Définition 1.6. *Soient K et L deux corps tels que L soit une extension de K. On dit que L est une extension algébrique de K si tous les éléments de L sont algébriques sur $j(K)$.*

Exemple. Toute extension finie d'un corps K est une extension algébrique de K.

On identifiera K et son image $j(K)$ dans L.

Proposition 1.4. *Si L est une extension algébrique de K et si K est une extension algébrique de H, alors L est une extension algébrique de H.*

Démonstration : Soit α un élément de L. Soit

$$g(X) = \sum_{0 \leq i \leq n} l_i X^i$$

le polynôme minimal de α sur K. Considérons le corps

$$M = H(l_0, ..., l_n)$$

obtenu par adjonction à H des coefficients l_i de g (qui sont dans K). Le corps M est une extension finie de H, et $M(\alpha)$ est une extension finie de M (car α est algébrique sur M). Cela montre que $M(\alpha)$ est une extension finie de H et donc que α est algébrique sur H. D'où le résultat.

Proposition-Définition 1.5. *Soit F l'ensemble des éléments de L qui sont algébriques sur K. Cet ensemble est un corps qui s'appelle la fermeture algébrique de K dans L. C'est la plus grande extension algébrique de K contenue dans L.*

Démonstration : Si α et β sont dans F, $K(\alpha, \beta)$ est une extension finie de K, et en particulier $\alpha + \beta$, $\alpha\beta$ et $1/\beta$ si β est non nul, sont algébriques sur K.

Définition 1.7. *On dit qu'un corps L est algébriquement clos s'il n'existe pas d'extension algébrique autre que L qui contienne L.*

Proposition 1.6. *Soit L un corps. Les assertions suivantes sont équivalentes :*
(i) Le corps L est algébriquement clos ;
(ii) tout polynôme de degré ≥ 1 de $L[X]$ possède au moins une racine dans L :
(iii) tout polynôme irréductible de $L[X]$ est de degré 1 ;

(iv) tout polynôme de degré ≥ 1 de $L[X]$ se décompose dans $L[X]$ en un produit de polynômes de degré 1.

Démonstration. Exercice.

Par exemple un corps fini n'est jamais algébriquement clos. En effet, soient K un corps fini et $(a_i)_{1\leq i\leq n}$ les éléments de K. Alors le polynôme

$$f(X) = \prod_{1\leq i\leq n} (X - a_i) \ + 1$$

ne possède pas de racine dans K.

I.4. Corps de décomposition d'un polynôme

Considérons un corps K et f un polynôme à coefficients dans K de degré $n \geq 1$.

Soit (K_1, K_2, j) un triplet formé de deux corps K_1 et K_2 et d'un homomorphisme j de K_1 dans K_2. L'homomorphisme j se prolonge de façon naturelle en un homomomorphisme d'anneaux

$$j^* : K_1[X] \to K_2[X],$$

qui est défini par

$$j^*\left(\sum a_k X^k\right) = \sum j(a_k) X^k.$$

Si f est un polynôme dans $K_1[X]$, $j^*(f)$ est donc en fait un polynôme dans $j(K_1)[X]$. Par exemple, si f est irréductible dans $K_1[X]$, alors $j^*(f)$ est aussi irréductible dans $j(K_1)[X]$.

Définissons maintenant ce que l'on appelle un corps de décomposition de f.

Définition 1.8. *Un corps de décomposition de f est la donnée d'une extension (L, j) de K telle que les deux conditions suivantes soient réalisées :*

a) Il existe une famille d'éléments $(\alpha_i)_{1\leq i\leq n}$ de L et c dans K, tels que l'on ait

$$j^*(f) = j(c) \prod_{1\leq i\leq n} (X - \alpha_i).$$

b) On a $L = j(K)(\alpha_1, ..., \alpha_n)$.

Remarque. Sauf précisions supplémentaires, étant donnés un corps K' et (K'', h) une de ses extensions, on identifiera K' et son image $h(K')$ dans son extension K''.

Par exemple si $K = \mathbb{Q}$ on peut prendre comme corps de décomposition de f le sous-corps de $\mathbb{C}$, ou le sous-corps de la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$, engendré par les racines de f.

Nous allons montrer le résultat suivant :

Théorème 1.1. *Il existe un corps de décomposition pour f. Si L et L' sont deux corps de décomposition de f, il existe un isomorphisme de L sur L' égal à l'identité sur K.*

Démonstration : 1) Existence : soit g un facteur irréductible de f. On pose

$$K_1 = K[X]/(g).$$

Soit α_1 l'image de X dans K_1. On a $K_1 = K(\alpha_1)$ et $g(\alpha_1) = 0$ (cela montre en particulier qu'il existe une extension de K dans laquelle g possède une racine). Le polynôme $X - \alpha_1$ divise g, et donc f, dans $K_1[X]$. Il existe donc f_1 dans $K_1[X]$, de degré strictement plus petit que celui de f, tel que l'on ait

$$f(X) = (X - \alpha_1) f_1(X).$$

En raisonnant par récurrence sur le degré de f, on peut supposer qu'il existe un corps de décomposition K_2 pour f_1 sur K_1. Il existe donc des éléments α_i de K_2, et c dans K, tels que l'on ait

$$f_1(X) = c \prod_{2 \leq i \leq n} (X - \alpha_i),$$

avec l'égalité $K_2 = K_1(\alpha_2, ..., \alpha_n)$. Cela entraîne que K_2 est un corps de décomposition du polynôme f.

2) Unicité : On va montrer le résultat suivant :

Proposition 1.7. *Soient (K_1, K_2, j) un triplet formé de deux corps K_1 et K_2 et d'un isomorphisme j de K_1 sur K_2. Soient g un polynôme à coefficients dans K_1 de degré ≥ 1 et Σ_1 un corps de décomposition de g sur K_1. Soit Σ_2 un corps de décomposition de $j^*(g)$ sur K_2. Alors il existe un isomorphisme de Σ_1 sur Σ_2 qui prolonge l'homomorphisme j.*

Démonstration : On procède par récurrence sur l'entier $n = [\Sigma_1 : K_1]$. L'énoncé est vrai si $n = 1$. Supposons donc $n > 1$. Dans ce cas les racines de g ne sont pas toutes dans K_1, de sorte que g possède un facteur irréductible h de degré $d > 1$. Soit α une racine de h dans Σ_1. Le polynôme $j^*(h)$ dans $K_2[X]$ est aussi irréductible de degré d et $\beta = j(\alpha)$ est racine de $j^*(h)$. Il existe un isomorphisme φ de $K_1(\alpha)$ sur $K_2(\beta)$ qui prolonge j, qui est défini par

$$\varphi\Big(\sum_{0 \leq k \leq t-1} a_k \alpha^k\Big) = \sum_{0 \leq k \leq t-1} j(a_k) \beta^k.$$

En effet, φ est bien défini : supposons que l'on ait

$$\sum_{0 \leq k \leq t-1} a_k \alpha^k = \sum_{0 \leq k \leq t-1} b_k \alpha^k.$$

Alors h divise le polynôme $\sum(a_k - b_k)X^k$, car h est irréductible, ce qui implique l'égalité $\sum j(a_k - b_k)\beta^k = 0$. Il est alors immédiat de vérifier que φ est un isomorphisme de $K_1(\alpha)$ sur $K_2(\beta)$ qui prolonge j. Par ailleurs, Σ_1 et Σ_2 sont des corps de décomposition respectivement de g et $j(g)$ sur $K_1(\alpha)$ et $K_2(\beta)$. Mais on a $[\Sigma_1 : K_1(\alpha)] = n/d$ qui est $\leq n-1$. D'après l'hypothèse de récurrence, on peut donc prolonger φ en un isomorphisme ψ de Σ_1 sur Σ_2. En particulier, ψ prolonge j, ce qui démontre la proposition.

L'unicité dans le théorème 1.1 se déduit alors du résultat précedent avec $K_1 = K_2 = K$ et en prenant pour j l'identité de K.

Au cours de la démontration de la proposition 1.7, on a en fait prouvé le résultat suivant :

Proposition 1.8. *Soient K un corps et f un polynôme irréductible à coefficients dans K. Soient L un corps de décomposition de f, α et β deux racines de f dans L. Alors il existe un automorphisme de L qui envoie α sur β et qui vaut l'identité sur K.*

Démonstration : L'application $\varphi : K(\alpha) \to K(\beta)$ définie par

$$\varphi\left(\sum_{0\leq k\leq t} a_k\alpha^k\right) = \sum_{0\leq k\leq t} a_k\beta^k,$$

est un isomorphisme de $K(\alpha)$ sur $K(\beta)$ égal à l'identité sur K (cf. dém. de la prop. 1.7). Soit i l'inclusion de $K(\beta)$ dans Ω. Il existe un homomorphisme de corps $\psi : L \to \Omega$ qui prolonge $i \circ \varphi$ (cf. *loc. cit.*) : en particulier, on a $\psi(\alpha) = \beta$ et ψ fixe les éléments de K. Si α_i est une racine de f dans Ω, $\psi(\alpha_i)$ est aussi une racine de f. On a ainsi $\psi(L) = L$, ce qui prouve le résultat.

I.5. Clôture algébrique d'un corps

Définition 1.9. *Soit K un corps. Une clôture algébrique de K est une extension algébrique L de K qui soit un corps algébriquement clos.*

Exemple. 1) La fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}$.

2) Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

On a le résultat suivant :

Théorème 1.2. *Tout corps K possède une clôture algébrique. Si L et L' sont deux clôtures algébriques de K il existe un isomorphisme de L sur L' égal à l'identité sur K.*

Démonstration : On va démontrer ce théorème, ou tout au moins en donner les idées principales, dans le cas plus facile où K est dénombrable. Dans ce cas l'anneau $K[X]$

est aussi dénombrable, ce qui permet de numéroter ses éléments : soit $(f_n)_{n\geq 1}$ une suite formée des éléments de $K[X]$.

1) Existence : pour construire une clôture algébrique de K , on procède comme suit : on construit un corps de décomposition K_1 pour f_1 sur K, puis un corps de décomposition K_2 pour f_2 sur K_1, puis un corps de décomposition de f_3 sur K_2, etc....Posons alors $L = \cup K_n$. L'ensemble L ainsi obtenu est une clôture algébrique de K : on définit d'abord dans L les opérations suivantes : si x et y sont dans L, x et y sont dans un K_n pour un n assez grand. Le calcul de $x + y$, xy et xy^{-1} (si y est non nul) ne dépend pas de n, car modulo les identifications faites, K_n est un sous-corps de K_m si n est plus petit que m. Ces opérations définissent ainsi une structure de corps sur L. Le corps L est une extension algébrique de K : cela résulte de la propriété de transitivité des extensions algébriques. Le corps L est algébriquement clos. En effet, soient M une extension algébrique de L et α un élément de M. L'extension $L(\alpha)/L$ est finie et α est algébrique sur K (transitivité). Ainsi α est racine d'un polynôme à coefficients dans K et donc α appartient à L. D'où $M = L$ et notre assertion.

2) Unicité : prouvons d'abord le lemme suivant :

Lemme 1.1. *Soit Ω un corps algébriquement clos. Soient K un corps et $j : K \to L$ une extension algébrique de K. Soit $\sigma : K \to \Omega$ un homomorphisme de corps. Alors σ se prolonge en un homomorphisme de L dans Ω.*

Démonstration : a) Identifions K et $j(K)$. Supposons que l'extension L soit de degré fini sur K. On procède par récurrence sur le degré de L sur K. Soit α un élément de L qui ne soit pas dans K. Soit f son polynôme minimal. Soit α' une racine de $\sigma^*(f)$ dans Ω (qui est le polynôme déduit de f par l'action de σ sur ses coefficients). Il y a un homomorphisme φ de $K(\alpha)$ dans Ω égal à σ sur K et appliquant α sur α' (le vérifier). Puisque le degré de L sur $K(\alpha)$ est strictement plus petit que le degré de L sur K (car α n'est pas dans K), l'hypothèse de récurrence permet de prolonger φ en un homomorphisme de L dans Ω. D'où le résultat dans ce cas.

b) Démontrons maintenant le cas général, avec l'hypothèse simplificatrice que L soit réunion dénombrable de sous-corps L_n de degré fini sur K. Dans ce cas on peut supposer que L_n est contenu dans L_{n+1}. Chaque prolongement de σ à L_n (qui existe d'après l'alinéa a)), se prolonge à L_{n+1} par le même argument. On déduit de cette façon, de proche en proche, un prolongement de σ à L. D'où l'assertion dans ce cas.

L'unicité résulte du lemme ci-dessus : soient (L, σ) et (L', σ') deux clôtures algébriques de K. D'après le lemme σ' se prolonge en un homomorphisme de corps $\varphi : L \to L'$. Ainsi $\varphi(L)$ est un corps algébriquement clos contenu dans L', qui est aussi un corps algébriquement clos. On a donc $\varphi(L) = L'$ et φ est un isomorphisme de L sur L'. D'où l'unicité.

Remarque. Soit $\bar{\mathbb{Q}}$ la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Alors $\bar{\mathbb{Q}}$ est une clôture

algébrique de $\mathbb{Q}$. En effet le corps $\bar{\mathbb{Q}}$ est algébriquement clos : soit P un polynôme irréductible à coefficients dans $\bar{\mathbb{Q}}$. Les coefficients de P appartiennent à une extension finie K de $\mathbb{Q}$. Les racines de P dans $\mathbb{C}$ sont algébriques sur K et donc aussi sur $\mathbb{Q}$. Elles sont donc dans $\bar{\mathbb{Q}}$, ce qui prouve que le degré de P est 1. D'où l'assertion.

II. Extensions séparables, théorème de l'élément primitif

Considérons désormais un corps algébriquement clos Ω et K un sous-corps de Ω. Ces deux corps sont donc fixés pour toute la suite. Par ailleurs, lorsque l'on évoquera une extension de K, il s'agira d'un corps qui contient K et qui est contenu dans Ω. Cette situation n'est pas restrictive car tout corps peut être plongé dans un corps algébriquement clos (th. 1.2).

II.1. Plongements dans Ω

Soit L un sous-corps de Ω contenant K et de degré fini sur K. Étant donné un plongement σ de K dans Ω, on a vu qu'il existe un plongement de L dans Ω qui coïncide sur K avec σ (lemme 1.1). La question qui se pose est alors la suivante :

Question. *Combien y-a-t-il de tels plongements ?*

Une réponse partielle est donnée par le théorème suivant :

Théorème 2.1. *Soit L un sous-corps de Ω contenant K et de degré fini n sur K. Alors il y a au plus n plongements de L dans Ω égaux à l'identité sur K.*

Démonstration : Considérons Ω et L comme espaces vectoriels sur K. Soit V l'ensemble des applications K-linéaires de L dans Ω. Cet ensemble est muni, de façon naturelle, d'une structure d'espace vectoriel sur Ω. C'est ainsi un espace vectoriel de dimension finie n sur Ω : en effet, soit (a_i) une K-base de L. L'application $\varphi : V \to \Omega^n$ définie par $\varphi(u) = (u(a_i))$ est Ω-linéaire et est une bijection de V sur Ω^n. Pour démontrer le théorème, il suffit ainsi de prouver le théorème suivant dû à Dedekind :

Théorème 2.2. *Soient N un entier, et $(\sigma_i)_{1\leq i\leq N}$ N plongements de L dans Ω égaux à l'identité sur K et deux à deux distincts (ce sont donc en particulier N éléments de V). Alors ceux-ci sont linéairement indépendants sur Ω.*

Démonstration : On procède par l'absurde : supposons que le système $(\sigma_i)_{1\leq i\leq N}$ soit lié. Soit r son rang : on a $r < N$. Modulo une permutation des σ_i, on peut supposer que le système $(\sigma_i)_{1\leq i\leq r}$, est libre. Il existe donc des constantes $(\lambda_i)_{1\leq i\leq r}$ uniques dans Ω, telles que l'on ait l'égalité

$$\sigma_{r+1} = \sum_{1\leq i\leq r} \lambda_i \sigma_i. \tag{1}$$

Considérons alors un élément y de L non nul. On déduit de l'égalité (1) que l'on a pour tout x dans L

$$\sigma_{r+1}(x) = \sum_{1 \leq i \leq r} \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} \sigma_i(x).$$

D'après l'unicité des λ_i, on a donc pour tout i entre 1 et r l'égalité

$$\lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} = \lambda_i.$$

Il existe nécessairement au moins un indice i tel que λ_i soit non nul. On déduit de là que l'on a $\sigma_i(y) = \sigma_{r+1}(y)$. Cela montre que σ_{r+1} est l'un des σ_i, ce qui contredit le fait que les σ_i soient deux à deux distincts. D'où le résultat.

Corollaire 2.1. *Soit L un sous-corps de Ω contenant K et de degré fini n sur K. Soit $\sigma : K \to \Omega$ un plongement de K dans Ω. Alors il y a au plus n plongements de L dans Ω qui prolongent σ sur K.*

Démonstration : D'après le lemme 1.1, σ se prolonge en un homomorphisme de L dans Ω. En remplaçant les corps K et L par leurs images dans Ω, on se ramène alors à la situation du théorème 2.1.

II.2. Cas d'une extension simple

Soit f un polynôme irréductible à coefficients dans K. Soit α une racine de f dans Ω. Étant donné un plongement $\sigma : K \to \Omega$, rappelons que l'on note $\sigma^*(f)$ le polynôme déduit de f par action de σ sur ses coefficients. On a le résultat suivant :

Proposition 2.1. *Soit $\sigma : K \to \Omega$ un plongement de K dans Ω. Le nombre de plongements de $K(\alpha)$ dans Ω, qui prolongent σ sur K, est le nombre de racines distinctes du polynôme $\sigma^*(f)$ dans Ω. C'est donc aussi le nombre de racines distinctes de f dans Ω.*

Démonstration : Soit n le nombre de racines distinctes de $\sigma^*(f)$ dans Ω. Soit β une racine de $\sigma^*(f)$. On définit une application τ de $K(\alpha)$ dans Ω par l'égalité

$$\tau\left(\sum a_k \alpha^k\right) = \sum \sigma(a_k)\beta^k.$$

D'abord cette égalité définit bien une application : par définition τ est égale à σ sur K et envoie α sur β. C'est un homomorphisme (par définition). On obtient ainsi n plongements de $K(\alpha)$ dans Ω égaux à σ sur K. Par ailleurs, un plongement de $K(\alpha)$ dans Ω, égal à σ sur K, envoie nécessairement α sur une racine de $\sigma^*(f)$. Donc n est le nombre plongements de $K(\alpha)$ dans Ω, qui prolongent σ sur K. Or n est le nombre de racines distinctes de f dans Ω. En effet, soit $L = K(\alpha_1, ..., \alpha_t)$ le corps de décomposition de f dans Ω. On peut prolonger σ en un plongement φ de L dans Ω. On a $\sigma^*(f) = \varphi^*(f)$. Par ailleurs

si $f(X) = \prod_i (X - \alpha_i)^{e_i}$, on a $\varphi^*(f)(X) = \prod_i \big(X - \varphi(\alpha_i)\big)^{e_i}$. D'où notre assertion et la proposition.

Remarque. Il y en a "en général" autant que le degré de f, sauf si f possède des racines multiples ; d'où la notion de séparabilité que l'on va étudier maintenant.

II.3. Extension séparables

Définition 2.1. *Soit f un polynôme de degré n à coefficients dans K. On dit que f est séparable sur K s'il possède n racines distinctes dans Ω, et inséparable dans le cas contraire.*

Exemples. 1) Le polynôme $X^3 - 2$ est séparable sur $\mathbb{Q}$ (on peut prendre $\Omega = \mathbb{C}$).

2) Soit p un nombre premier. Soit X une indéterminée, L le corps des fractions rationnelles $\mathbb{F}_p(X)$ et Ω un corps algébriquement clos contenant L. Soit $K = \mathbb{F}_p(X^p)$; c'est un sous-corps de L. Dans l'anneau des polynômes $K[Y]$, le polynôme $Y^p - X^p$ est irréductible. On déduit de là que X est un élément algébrique sur K de degré p, et que son polynôme minimal sur K est $Y^p - X^p$. Le corps de décomposition de ce polynôme dans Ω est L et X est sa seule racine (on est en caractéristique p). Ainsi $Y^p - X^p$ est inséparable sur K.

Proposition 2.2. *Soit f un polynôme à coefficients dans K. Alors f est séparable sur K si et seulement si f et sa dérivée formelle f' sont des polynômes premiers entre eux.*

Démonstration : Soit n le degré de f. Si f est séparable sur K, f possède n racines α_i distinctes dans L, et on constate immédiatement qu'aucun des α_i ne peut être racine de f'. Inversement, supposons par exemple que f soit inséparable : il existe $k \geq 2$ et α dans L tels que l'on ait $f(X) = (X - \alpha)^k g(X)$. On constate alors que α est racine de f', ce qui montre que f et f' ne sont pas premiers entre eux. D'où le résultat.

Corollaire 2.2. *Un polynôme irréductible à coefficients dans K est séparable si et seulement si sa dérivée formelle n'est pas nulle.*

Démonstration : D'après la proposition 2.2, la condition est clairement nécessaire. Inversement soit f un polynôme irréductible inséparable. Alors f et f' ont un zéro commun α (prop. 2.2). Puisque f est irréductible, f est le polynôme minimal de α. Ainsi f divise f'. Or le degré de f' est strictement plus petit que le degré de f, donc f' est nul. D'où le résultat.

Exemples. 1) Si K est de caractéristique 0, tout polynôme irréductible sur K est séparable : en effet, la condition $f' = 0$ entraîne que f doit être constant. Ce résultat est faux en caractéristique p (cf. l'exemple 2) ci-dessus).

2) Soit T une indéterminée. Montrer que le polynôme $X^5 - T$ est irréductible et inséparable sur le corps $\mathbb{F}_5(T)$.

Corollaire 2.3. *Supposons que K soit de caractéristique p. Soit f un polynôme irréductible sur K. Alors f est inséparable si et seulement si il existe g dans $K[X]$ tel que l'on ait $f(X) = g(X^p)$.*

Démonstration : Si f est de la forme $g(X^p)$, f est inséparable d'après le corollaire 2.1 (car alors f' est nul). Inversement, soit $f = \sum_{i=0}^{n} a_i X^i$ un polynôme irréductible sur K. On a $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$. La condition $f' = 0$ entraîne alors $ia_i = 0$. Si a_i n'est pas nul, i doit donc être divisible par p. D'où le résultat.

Définition 2.2. *Soit α un élément de Ω algébrique sur K. On dit que α est séparable sur K, s'il est racine d'un polyôme séparable sur K ; cela revient à demander que le polynôme minimal de α sur K soit séparable sur K. Une extension L de K est dite séparable si tout les éléments de L sont séparables sur K.*

Proposition 2.3. *Soient L une extension de K et H une extension de L. Si H est séparable sur K, alors H est séparable sur L et L est séparable sur K.*

Démonstration : Soit α un élément de H. Le polynôme minimal de α sur K est un multiple du polynôme minimal de α sur L. Cela montre que H est séparable sur L. Le fait que L soit séparable sur K est immédiat.

Définition 2.3. *Soit K un corps. On dit que K est un corps parfait si toutes les extensions algébriques de K sont séparables.*

Un corps K de caractéristique 0 est parfait (exemple 1) ci-dessus). Les corps parfaits de caractéristique p non nulle se caractérisent de la façon suivante :

Proposition 2.4. *Soit K un corps de caractéristique p non nulle. Alors K est parfait si et seulement si l'on a $K^p = K$ (i.e. tout élément de K possède une racine p-ième dans K).*

Démonstration : 1) Supposons que l'on ait $K^p = K$. Soit f un polynôme irréductible de $K[X]$. Si f n'est pas séparable, il existe $g(X) = \sum a_i X^i$ un polynôme de $K[X]$ tel que $f(X) = g(X^p)$. D'après l'hypothèse faite sur K, il existe des éléments b_i de K tels que $b_i^p = a_i$. On a alors $f(X) = \sum b_i^p X^{ip} = \left(\sum b_i X^i\right)^p$, ce qui contredit le fait que f soit irréductible. D'où le fait que K soit parfait.

2) Inversement, supposons que l'on ait $K^p \neq K$. Soit a un élément de K qui n'appartienne pas à K^p. On considère le polynôme $f(X) = X^p - a$. Il possède une unique racine α dans une clôture algébrique $\bar{K}$ de K. Cela entraîne que f est irréductible : en effet, soit h un polynôme irréductible à coefficients dans K qui divise f. Dans $\bar{K}$, α est la seule racine de h ; par suite, on a $h(X) = g(X^p)$ pour un certain g dans $K[X]$, ce qui contredit le fait que le degré de h soit $< p$. Ainsi α n'est pas séparable sur K et il existe des extensions de K qui ne sont pas séparables. D'où le résultat.

Corollaire 2.4. *Tout corps fini est parfait.*

Démonstration : Soit K un corps fini de caractéristique p. L'application $\varphi : K \to K$ définie par $\varphi(x) = x^p$ est un homomorphisme de corps. Il est donc injectif. Puisque K est fini, il est aussi surjectif, et l'on a $K^p = K$. D'où le corollaire.

Le corps $\mathbb{F}_p(X)$ des fractions rationnelles à coefficients dans le corps fini $\mathbb{F}_p$ est un exemple de corps qui ne soit pas parfait.

II.4. Théorème fondamental

Nous allons maintenant démontrer le résultat suivant :

Théorème 2.3. *Soit L une extension finie de K de degré n. Les conditions suivantes sont équivalentes :*

(i) L'extension L est séparable sur K ;
(ii) l'extension L est engendrée sur K par des éléments séparables ;
(iii) il y a exactement n plongements distincts de L dans Ω égaux à l'identité sur K ;
(iv) on a $L = K(\alpha)$, où α est un élément séparable sur K.

Démonstration : 1) L'implication (i) $\Rightarrow$ (ii) est évidente, car tout élément de L est séparable sur K.

2) Montrons l'implication (ii) $\Rightarrow$ (iii). Supposons que l'on ait $L = K(\alpha_1, ..., \alpha_n)$, où les α_i sont des éléments séparables sur K. Considérons le corps $L_i = K(\alpha_1, ..., \alpha_i)$. Pour tout i entre 2 et n on a $L_i = L_{i-1}(\alpha_i)$. L'élément α_i est séparable sur L_{i-1} (prop. 2.3) de sorte que le polynôme minimal de α_i sur L_{i-1} possède exactement le degré $[L_i : L_{i-1}]$ de L_i sur L_{i-1} racines dans Ω. Par suite tout plongement de L_{i-1} dans Ω se prolonge de $[L_i : L_{i-1}]$ façons à L_i (prop. 2.1). Il y a donc

$$\prod_{1 \leq i \leq n} [L_i : L_{i-1}] = [L : K] = n$$

plongements de L dans Ω égaux à l'identité sur K. D'où l'implication.

3) Montrons l'implication (iii) $\Rightarrow$ (iv). Considérons les n plongements $(\sigma_i)_{1 \leq i \leq n}$ de L dans Ω égaux à l'identité sur K. Supposons qu'il existe un élément α de L tel que les éléments $\sigma_i(\alpha)$ soient distincts deux à deux. Le polynôme minimal de α sur K possede alors (au moins) n racines distinctes et le degré de $K(\alpha)$ sur K est donc au moins n. On a ainsi nécessairement $[K(\alpha) : K] = n$, ce qui conduit à l'égalité $L = K(\alpha)$. Tout revient donc à trouver un tel élément α de L. On considère pour cela les deux cas suivants :

premier cas : le corps K est fini. Dans ce cas L est un corps fini et le groupe multiplicatif L^* est cyclique. On peut alors choisir pour α un générateur de ce groupe (qui est un élément séparable sur K d'après le corollaire 2.4).

Deuxième cas : le corps K est infini. Pour tout i et j distincts, compris entre 1 et n, considérons le sous-ensemble $H_{i,j}$ de L formé des éléments x tels que $\sigma_i(x) = \sigma_j(x)$. Ce

sont des sous-K-espaces vectoriels de L. Si i est distinct de j, on a $\sigma_i \neq \sigma_j$, de sorte que $H_{i,j}$ est distinct de L. Tout revient alors à montrer que la réunion des $H_{i,j}$ est distinct de L, car alors n'importe quel élément α dans le complémentaire de la réunion des $H_{i,j}$ conviendra. Cela résulte du lemme suivant :

Lemme 2.1. *Soit V un espace vectoriel de dimension finie sur un corps k infini. Soit (V_i) une famille finie de sous-espaces vectoriels de V tous distincts de V. Alors la réunion des V_i est aussi distincte de V.*

Démonstration : Pour tout i il existe au moins une forme linéaire non nulle f_i qui s'annule sur V_i, car V_i est par hypothèse distinct de V. Il suffit alors de montrer que la fonction polynômiale F définie sur V par

$$F(x) = \prod_{1 \leq i \leq n} f_i(x),$$

est non nulle sur V. Puisque k est infini, cela revient à montrer que le polynôme correspondant, que l'on note encore F, est non nul dans l'anneau des polynômes en n variables $k[X_1, ..., X_n]$. Si F est nul, $k[X_1, ..., X_n]$ étant un anneau intègre, cela implique que l'un des polynômes f_i soit nul, ce qui conduit à une contradiction. D'où le résultat.

4) Il reste à démontrer l'implication (iv) $\Rightarrow$ (i) : supposons que l'on ait $L = K(\alpha)$, où α est un élément séparable sur K. Il y a n plongements distincts de L dans Ω égaux à l'identité sur K (qui correspondent aux racines du polynôme minimal de α sur K). Considérons alors un élément β de L. Notons $m = [K(\beta) : K]$ et r le nombre de plongements de $K(\beta)$ dans Ω égal à l'identité sur K. On a $r \leq m$. Un tel plongement se prolonge à son tour d'au plus $[L : K(\beta)]$ façon possibles à L (cor. 2.1). Si l'on avait $r < m$, on aurait donc moins de n plongements possibles de L dans Ω égaux à l'identité sur K. D'où $r = m$ et β est racine simple de son polynôme minimal sur K. D'où l'implication.

Cela termine la démonstration du théorème.

Corollaire 2.5. *Supposons que K soit de caractéristique 0. Soit L une extension finie de K dans Ω. Il existe α dans K tel que l'on ait $L = K(\alpha)$ et il y a exactement $[L : K]$ plongements de L dans Ω qui sont égaux à l'identité sur K.*

III. Théorie de Galois

On considère désormais un corps K et une clôture algébrique Ω de K fixés.

III.1. Extensions normales, extensions galoisiennes

Définition 3.1. *Soit L une extension de K contenue dans Ω.*

a) On dit que L est une extension normale de K si pour tout plongement σ de L dans Ω, égal à l'identité sur K, on a $\sigma(L) = L$.

b) On dit que L est une extension galoisienne de K si L est une extension normale et séparable sur K.

Définition 3.2. *Soit L une extension de K contenue dans Ω. On appelle groupe de Galois de L sur K, et on note souvent $\mathrm{Gal}(L/K)$, le groupe des automorphismes du corps L qui laissent fixe K. C'est un sous-groupe du groupe des automorphismes de L.*

Exemples. Le groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$ est d'ordre 2 : son élément non trivial est la conjugaison complexe.

Exercice. Montrer que le groupe $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{R})$ est réduit à l'identité.

Proposition 3.1. *Soit L une extension finie de K contenue dans Ω. On a toujours*

$$| \mathrm{Gal}(L/K) | \leq [L : K]. \tag{1}$$

On a $| \mathrm{Gal}(L/K) | = [L : K]$ si et seulement si L est une extension galoisienne de K.

Démonstration : L'inégalité (1) résulte du théorème 2.1. Posons $n = [L : K]$. Supposons que L soit une extension galoisienne de K. Elle est donc par définition normale, et le groupe $\mathrm{Gal}(L/K)$ est donc l'ensemble des plongements de L dans Ω, égaux à l'identité sur K. Puisque L est séparable sur K, il y a n tels plongements (th. 2.3). D'où l'égalité ci-dessus. Inversement, supposons que l'on ait $| \mathrm{Gal}(L/K) | = n$. Dans ce cas il y a en particulier au moins n plongements de L dans Ω qui sont égaux à l'identité sur K. Comme il y en a au plus n (th. 2.1), il y en a donc n, et ils conservent tous L. Cela montre que L est galoisienne sur K (cf. th. 2.3 et définitions ci-dessus).

Proposition 3.2 : critère de normalité. *Soit L une extension finie de K contenue dans Ω. Pour que L soit normale sur K il faut et il suffit que tout polynôme irréductible de $K[X]$ ayant une racine dans L possède toutes ses racines dans L.*

Démonstration : Supposons L normale sur K. Soit f un polynôme irréductible à coefficients dans K. Supposons que f possède une racine α dans L. Soit β une racine quelconque de f dans Ω. Soit τ un plongement de $K(\alpha)$ dans Ω, égal à l'identité sur K, tel que $\tau(\alpha) = \beta$. On peut prolonger τ en un plongement σ de L dans Ω. Puisque L est normale sur K, on a $\sigma(L) = L$. Or on a $\sigma(\alpha) = \tau(\alpha)$, donc β appartient à L, et toutes les racines de f sont dans L. Inversement, soit $\sigma : L \to \Omega$ un plongement de L dans Ω égal à l'identité sur K. Soit α un élément de L. On considère le polynôme minimal f de α sur K. Posons $\beta = \sigma(\alpha)$. On $f(\beta) = 0$, et comme f a une racine dans L, toutes les racines de f sont dans L par hypothèse, ce qui entraîne que β est aussi dans L. Ainsi $\sigma(L)$ est contenu dans L. Par suite on a $\sigma(L) = L$, car $\sigma(L)$ et L sont des espaces vectoriels sur K de même dimension. D'où le résultat.

Exemple. Soit f un polynôme irréductible dans $K[X]$. Le corps de décomposition L de f dans Ω est une extension normale de K : en effet, soient $(\alpha_i)_{1\leq i\leq n}$ les racines de f dans Ω. On a $L = K(\alpha_1, ..., \alpha_n)$. Par ailleurs, un K-plongement de L dans Ω permute les racines α_i entre elles, donc envoie L dans L. D'où l'assertion.

Lemme 3.1. *Soient L une extension galoisienne de K et α un élément de L. Si pour tout σ dans le groupe de Galois* $\mathrm{Gal}(L/K)$*, l'on a $\sigma(\alpha) = \alpha$, alors α appartient à K.*

Démonstration : Supposons que α ne soit pas dans K. L'élément α est, par hypothèse, séparable sur K. Donc son polynôme minimal a au moins une racine β distincte de α. Mais il y a un σ dans $\mathrm{Gal}(L/K)$ que envoie α sur β, ce qui conduit à une contradiction. D'où le lemme.

III.2. Groupe de Galois d'un polynôme

On suppose dans ce paragraphe que toutes les extensions algébriques de K sont séparables, autrement dit que K est un corps parfait. On a démontré que tel est par exemple le cas si K est de caractéristique 0, ou si K est un corps fini (corollaire 2.4).

Définition 3.3. *Soit f un polynôme de $K[X]$. Soit L le corps de décomposition de f dans Ω. On appelle groupe de Galois du polynôme f, le groupe de Galois de L sur K. On le note parfois* $\mathrm{Gal}(f)$.

Lemme 3.2. *Soit f un polynôme de $K[X]$. Soit n le nombre de racines distinctes de f dans Ω (ou dans son corps de décomposition). Soit $(\alpha_i)_{1\leq i\leq n}$ ces n racines (on a donc choisi implicitement une numérotation des racines de f). L'application* $\mathrm{Gal}(f) \to \mathbb{S}_n$ *qui à σ associe la permutation déduite de σ par son action sur les α_i est un homomorphisme injectif de groupes. Ainsi, une fois choisie une numérotation des racines,* $\mathrm{Gal}(f)$ *s'identifie à un sous-groupe de $\mathbb{S}_n$. Un changement de numérotation transforme* $\mathrm{Gal}(f)$ *en un sous-groupe conjugué dans $\mathbb{S}_n$.*

Démonstration : C'est immédiat puisqu'un élément de $\mathrm{Gal}(f)$ est entierement déterminé par son action sur les α_i.

En particulier, si f est un polynôme irréductible de $K[X]$de degré n, une fois choisie une numérotation des racines, $\mathrm{Gal}(f)$ s'identifie à un sous-groupe de $\mathbb{S}_n$.

Exemple. Groupe de Galois d'un polynôme de degré 3 sur $\mathbb{Q}$.

Soit $f(X) = X^3 + pX + q$ un polynôme irréductible de degré 3 à coefficients dans $\mathbb{Q}$. On va déterminer le groupe $\mathrm{Gal}(f)$. Soient α_1, α_2 et α_3 les trois racines de f dans $\mathbb{C}$. On sait que $\mathrm{Gal}(f)$ s'identifie à un sous-groupe de $\mathbb{S}_3$, qui ne peut être que $\mathbb{A}_3$ ou $\mathbb{S}_3$. En fait $\mathrm{Gal}(f)$ est isomorphe à $\mathbb{A}_3$ si et seulement si le corps de décomposition L de f est de degré 3 sur $\mathbb{Q}$. On va démontrer l'énoncé suivant :

Lemme 3.3. *On a* $[L : \mathbb{Q}] = 3$ *si* $-4p^3 - 27q^2$ *est un carré dans* $\mathbb{Q}$ *et* $[K : \mathbb{Q}] = 6$ *sinon.*

Démonstration : Posons $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. Soit σ un élément de $\mathrm{Gal}(f)$. On a $\sigma(\delta) = \epsilon(\sigma)\delta$, où $\epsilon(\sigma)$ est la signature de σ (on a identifié $\mathrm{Gal}(f)$ à un sous-groupe de $\mathbb{S}_3$). On constate que $\mathrm{Gal}(f) = \mathbb{A}_3$ si et seulement si pour tout σ dans $\mathrm{Gal}(f)$, on a $\sigma(\delta) = \delta$, autrement dit, si et seulement si δ est dans $\mathbb{Q}$ (lemme 3.1). Or on vérifie que l'on a l'égalité $\delta^2 = -4p^3 - 27q^2$ (exercice). D'où le résultat.

En fait on peut généraliser l'énoncé précedent. Définissons pour cela la notion de discriminant d'un polynôme unitaire f de $K[X]$:

Définition 3.4. *Soit* f *un polynôme unitaire de* $K[X]$ *de degré* n. *Soient* $(\alpha_i)_{1 \leq i \leq n}$ *les racines de* f *dans* Ω. *On appelle discriminant de* f *l'élément algébrique, noté parfois* $D(f)$,

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Il résulte directement de cette définition qu'un polynôme de $K[X]$ est séparable si et seulement si son discriminant n'est pas nul.

Lemme 3.4. *L'élément* $D(f)$ *est dans* K.

Démonstration : Soient σ un élément de $\mathrm{Gal}(f)$ et $\epsilon(\sigma)$ sa signature. On a l'égalité

$$\sigma\Big(\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)\Big) = \epsilon(\sigma) \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j). \tag{1}$$

Le lemme en résulte (lemme 3.1).

Un polynôme f unitaire de degré n étant donné, il est en fait facile de calculer son discriminant $D(f)$. On peut montrer que l'on a

$$D(f) = (-1)^{n(n-1)/2} Res(f, f'),$$

où $Res(f, f')$ est le résultant de f et f' (cf. les références bibliographiques).

Corollaire 3.1. *Soit* f *un polynôme unitaire de* $K[X]$ *ayant* n *racines distinctes dans* Ω. *Identifions* $\mathrm{Gal}(f)$ *à un sous-groupe de* $\mathbb{S}_n$. *Alors,* $\mathrm{Gal}(f)$ *est contenu dans* $\mathbb{A}_n$ *si et seulement si le discriminant de* f *est un carré dans* K.

Démonstration : Cela résulte directement de la formule (1).

Exemples de détermination de groupes de Galois

On admettra le résultat suivant :

Proposition 3.3. *Soit p un nombre premier. Soit f un polynôme unitaire séparable de degré n dans $\mathbb{Z}[X]$. Soit $\bar{f}$ le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ déduit de f par réduction via l'homomorphisme $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. On suppose que $\bar{f}$ est séparable. Soit*

$$\bar{f} = \prod_{1 \leq i \leq t} \bar{f}_i,$$

la décomposition de $\bar{f}$ en produit de polynômes irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$. Pour tout i entre 1 et t, soit n_i le degré de $\bar{f}_i$. Alors, $\mathrm{Gal}(f)$ *étant identifié à un sous-groupe de $\mathbb{S}_n$, il existe t cycles $(\sigma_i)_{1 \leq i \leq t}$ de $\mathbb{S}_n$ à supports disjoints, tels que, σ_i soit d'ordre n_i, et que le produit $\prod_{i=1}^{t} \sigma_i$ appartienne à* $\mathrm{Gal}(f)$.

Application. Le groupe de Galois sur $\mathbb{Q}$ du polynôme $f(X) = X^4 + 8X + 12$ est isomorphe à $\mathbb{A}_4$. En effet, son discriminant étant $2^{12}.3^4$, on déduit du corollaire 3.1, que $\mathrm{Gal}(f)$ est contenu dans $\mathbb{A}_4$. Par ailleurs, le polynôme f réduit modulo 5, se décompose en $(X^3 - X^2 + X + 2)(X + 1)$. Puisque $X^3 - X^2 + X + 2$ est irréductible dans $\mathbb{Z}/5\mathbb{Z}$, $\mathrm{Gal}(f)$ contient un élément d'ordre 3 (prop. 3.3). Il contient aussi un élément d'ordre 2 (car f étant irréductible de degré 4, l'ordre de $\mathrm{Gal}(f)$ est pair). Donc 6 divise l'ordre de $\mathrm{Gal}(f)$. Mais $\mathbb{A}_4$ ne possède pas de sous-groupe d'ordre 6. Donc $\mathrm{Gal}(f) = \mathbb{A}_4$.

Proposition 3.4. *Soit p un nombre premier. Soit f un polynôme irréductible de $\mathbb{Q}[X]$ de degré p. Soit L le corps de décomposition de f dans $\mathbb{C}$. On suppose que f possède exactement deux zéros non réels. Alors le groupe de Galois* $\mathrm{Gal}(L/\mathbb{Q})$ *(ou le groupe de Galois de f) est isomorphe à $\mathbb{S}_p$.*

Démonstration : On peut supposer que p est ≥ 3, car l'énoncé est vrai si $p = 2$. Soit α une racine de f. Puisque $\mathbb{Q}(\alpha)$ est contenu dans L, et que le degré de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ est p, le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ possède un élément d'ordre p. Par ailleurs la conjugaison complexe induit un élément de $\mathrm{Gal}(L/\mathbb{Q})$ car f étant à coefficients dans $\mathbb{Q}$, si z est racine de f, sont conjugué $\bar{z}$ aussi. Puisque f a exactement deux racines non réelles, la conjugaison complexe laisse fixe les $p - 2$ racines réelles de f et échange les deux racines imaginaires. On déduit de là que l'image de $\mathrm{Gal}(L/\mathbb{Q})$ dans $\mathbb{S}_p$ contient une transposition. Puisqu'elle contient un cycle d'ordre p, l'image de $\mathrm{Gal}(L/\mathbb{Q})$ dans $\mathbb{S}_p$ est donc $\mathbb{S}_p$ tout entier. D'où le résultat.

Cet énoncé fournit des exemples d'équations de degré $p \geq 5$ non résoluble par radicaux (cf. les références bibliographiques).

Exemple. Le groupe de Galois sur $\mathbb{Q}$ du polynôme $f(X) = X^5 - 4X^3 - 2$ est isomorphe à $\mathbb{S}_5$. D'abord il est irréductible car c'est un polynôme d'Eiseinstein. Le groupe $\mathrm{Gal}(f)$ contient donc un élément d'ordre 5. Par ailleurs, f possède trois racines réelles et deux racines imaginaires. Or la conjugaison complexe est un élément de $\mathrm{Gal}(f)$. On déduit de

là qu'il existe une transposition dans $\mathrm{Gal}(f)$. Par suite $\mathrm{Gal}(f)$ possède un cycle d'ordre 5 et une transposition. Cela entraîne que $\mathrm{Gal}(f) = \mathbb{S}_5$.

Exercices. 1) Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ le sous-corps de $\mathbb{C}$ engendré par une racine carrée de 2 et une racine carrée de 3. Montrer que K est une extension galoisienne de $\mathbb{Q}$ dont le groupe de Galois est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Dresser la liste des extensions intermédiaires entre $\mathbb{Q}$ et K. Trouver un élément primitif de K sur $\mathbb{Q}$.

2) Soit p un nombre premier. Soit $\Phi_p(X)$ le polynôme (cyclotomique) défini par

$$\Phi_p(X) = \sum_{0 \leq i \leq p-1} X^i.$$

a) Montrer que Φ_p est irréductible dans $\mathbb{Q}[X]$.
b) Soit ζ une racine de Φ_p. Montrer que $\mathbb{Q}(\zeta)$ est une extension galoisienne de $\mathbb{Q}$ de degré $p-1$. On explicitera un isomorphisme de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sur le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.
c) Montrer que le groupe de Galois de Φ_p est cyclique d'ordre $p-1$.

3) Soit f le polynôme de $\mathbb{Q}[X]$ défini par

$$f = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1.$$

a) Montrer que f est irréductible dans $\mathbb{Q}[X]$.
b) $(*)$ Soit α une racine de f. Montrer que $\mathbb{Q}(\alpha)$ est une extension galoisienne de $\mathbb{Q}$ de degré 5 (en particulier le groupe de Galois de f est isomorphe à $\mathbb{Z}/5\mathbb{Z}$).
c) $(*)$ Soit ζ une racine primitive 11-ième de l'unité. Montrer que $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{Q}(\zeta)$: c'est en fait *le* sous-corps de degré 5 de $\mathbb{Q}(\zeta)$.

Pour la question b), on vérifiera en fait que si α est une racine de f, alors $\alpha^3 - 3\alpha$, $\alpha^4 - 4\alpha^2 + 2$, $-\alpha^4 - \alpha^3 + 3\alpha^2 + 2\alpha - 1$, et $\alpha^2 - 2$ sont aussi racines de f. En particulier toutes les racines de f appartiennent à $\mathbb{Q}(\alpha)$, ce qui montre que l'extension $\mathbb{Q}(\alpha)$ de $\mathbb{Q}$ est galoisienne.

Pour la question c), on vérifiera que si ζ une racine primitive 11-ième de l'unité, alors $\alpha = \zeta^3 + \zeta^8$ est une racine de f, ce qui entraîne l'assertion.

Dans l'exercice précédent, le groupe de Galois de $K = \mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ est abélien. On dit que K est une extension abélienne finie de $\mathbb{Q}$. On a constaté que K est un sous-corps d'une extension cyclotomique. Ce fait est général : toute extension *abélienne* finie de $\mathbb{Q}$ est contenue dans un corps cyclotomique $\mathbb{Q}(\zeta)$, où ζ est une racine n-ième de l'unité, pour un certain n. C'est le résultat principal de ce qu'on appelle la théorie du corps de classes pour $\mathbb{Q}$. On a d'ailleurs des résultats analogues si l'on remplace le corps de base $\mathbb{Q}$ par n'importe laquelle de ses extensions finies. C'est alors la théorie du corps de classes.

4) (∗) Montrer que le corps de décomposition K du polynôme

$$X^7 + X^6 - 12X^5 - 7X^4 + 28X^3 + 14X^2 - 9X + 1$$

est une extension abélienne de degré 7 de $\mathbb{Q}$. Trouver un corps cyclotomique qui contienne le corps K.

Les exercices 3) et 4) peuvent en fait être traités en utilisant l'annexe sur les périodes de l'équation cyclotomique.

5) Déterminer le groupe de Galois sur $\mathbb{Q}$ du polynôme $f(X) = X^4 - 3$. Expliciter un élément primitif du corps de décomposition de f.

III.3. Correspondance de Galois

Commençons par énoncer le théorème fondamental de la théorie de Galois (dans le cas des extensions finies) :

Théorème 3.1. *Soit L une extension galoisienne (de degré fini) d'un corps K. Posons $G = \mathrm{Gal}(L/K)$ le groupe de Galois de L sur K. Pour tout sous-groupe H de G, on note L^H l'ensemble des éléments x de L tels que l'on ait $\sigma(x) = x$, pour tout σ dans H.*

a) L'ensemble L^H est un sous-corps de L contenant K (c'est le corps fixe de H). Le corps L est une extension galoisienne de L^H, et l'on a $\mathrm{Gal}(L/L^H) = H$.

b) L'application $H \mapsto L^H$ est une bijection entre l'ensemble des sous-groupes de G et l'ensemble des sous-corps de L contenant K.

c) Soit H un sous-groupe de G. L'extension L^H de K est galoisienne si et seulement si H est un sous-groupe distingué de G. L'application de restriction réalise alors un isomorphisme de groupes de G/H sur $\mathrm{Gal}(L^H/K)$.

Démonstration du théorème

On va d'abord démontrer le résultat suivant :

Lemme 3.5 (Artin). *Soient L un corps et G un groupe fini d'automorphismes de L. Soit $K = L^G$ l'ensemble des invariants de L par G. Alors K est un sous-corps de L et L est une extension galoisienne de K. On a de plus $\mathrm{Gal}(L/K) = G$.*

Démonstration : Le fait que K soit un sous-corps de L est immédiat. Considérons alors un élément α de L. Soit G_α le stabilisateur de α dans G. Si σ est un élément de G, l'élément $\sigma(\alpha)$ ne dépend que de la classe à gauche σG_α de σ modulo G_α. On peut ainsi former le polynôme

$$f_\alpha(X) = \prod_{\sigma \in G/G_\alpha} \big(X - \sigma(\alpha)\big).$$

On remarque que α est racine simple de f_α. Par ailleurs, f_α est à coefficients dans K : cela résulte du fait que les coefficients de f_α sont des polynômes symétriques en les racines $\sigma(\alpha)$ à coefficients dans $\mathbb{Z}$, et que les opérations de G permutent les $\sigma(\alpha)$ sans changer les coefficients de ces polynômes. Ainsi α est racine simple d'un polynôme à coefficients dans K. Par suite l'extension L de K est algébrique et séparable. Montrons que le degré de L sur K est fini. En effet, on vient de constater que tout α dans L est racine d'une équation à coefficients dans K de degré $\leq \mid G \mid = n$. Pour tout α dans L, on a donc

$$[K(\alpha) : K] \leq n.$$

Par ailleurs, tout sous-corps de L' de L et de degré fini sur K est de la forme $K(\alpha)$, car L' est séparable sur K. Pour toute extension finie L' de K contenue dans L, on a donc $[L' : K] \leq n$. Mais cela implique l'inégalité

$$[L : K] \leq n, \tag{2}$$

sinon il devrait exister une extension finie de K contenue dans L engendrée par $n+1$ éléments de L linéairement indépendants sur K, ce qui n'est pas. Montrons que L est une extension normale de K. On considère pour cela un polynôme f de $K[X]$ irréductible sur K qui possède une racine α dans L. Par conséquent, f divise le polynôme f_α défini ci-dessus, donc est décomposé dans L, autrement dit f a toutes ses racines dans L. D'où le fait que L soit normale sur K (prop. 3.2) et que L soit galoisienne sur K. Il reste à montrer que G est le groupe de Galois de cette extension. D'après l'inégalité (2) et la prop. 3.1, le groupe de Galois $\mathrm{Gal}(L/K)$ possède au plus n éléments. Comme il contient évidemment les n éléments de G, on a nécessairement $G = \mathrm{Gal}(L/K)$. Cela termine la démonstration du lemme.

Démontrons maintenant le théorème 3.1.

(1) D'abord on a $L^G = K$ (lemme 3.1).

(2) Soit F un sous-corps de L contenant K. Alors L est une extension galoisienne de F, et le groupe de Galois $\mathrm{Gal}(L/F)$ est l'ensemble des éléments de $\mathrm{Gal}(L/K)$ qui se réduisent à l'identité sur F.

En effet, L est une extension séparable de F (prop. 2.3). De plus un F-plongement de L dans Ω est un K-plongement de L dans Ω, donc applique L sur L. Ainsi L est normale sur F. Par ailleurs, les F-automorphismes de L sont les K-automorphismes de L qui, par définition, se réduisent à l'identité sur F. D'où l'assertion.

(3) Soit F un sous-corps de L contenant K. Soit H le sous-groupe de G formé des éléments égaux à l'identité sur F. Alors on a $F = L^H$: cela résulte du lemme 3.1 et de l'assertion (2), car $H = \mathrm{Gal}(L/F)$.

(4) Soit H un sous-groupe de G. Alors L^H est un sous-corps de L qui contient K, et L est une extension galoisienne de L^H. De plus on $\mathrm{Gal}(L/L^H) = H$: cela résulte du lemme 3.5. Cela constitue l'assertion a) du théorème.

Démontrons l'assertion b) du théorème. D'abord l'assertion (3) fournit une application de l'ensemble des sous-corps de L contenant K dans l'ensemble des sous-groupes de G : celle donnée par

$$F \mapsto \mathrm{Gal}(L/F).$$

Par ailleurs, l'assertion (4) fournit une application en sens inverse : celle qui est donnée par

$$H \mapsto L^H.$$

Ces applications sont réciproques l'une de l'autre : en effet, on a

$$L^{\mathrm{Gal}(L/F)} = F \quad \text{(assertion (3))} \quad \text{et} \quad \mathrm{Gal}(L/L^H) = H \quad \text{(assertion (4))}.$$

D'où l'assertion b) du théorème.

(5) Soit F un sous-corps de L contenant K, tel que l'extension F de K soit galoisienne. Soit H le groupe de Galois $\mathrm{Gal}(L/F)$. Alors H est distingué dans G. De plus l'application de restriction $Res : G \to \mathrm{Gal}(F/K)$, qui à σ dans G associe sa restriction à F, est surjective de noyau H.

On remarque d'abord que l'application Res est bien définie, car F est normale sur K (la restriction d'un élément de G à F définit bien un automorphisme de F). C'est un homomorphisme de groupes. Considérons un élément τ de $\mathrm{Gal}(F/K)$. Cet élément τ se prolonge à L, et le prolongement obtenu fixe K, donc est dans G. Cela montre que Res est surjective. Le fait que son noyau soit H résulte de l'assertion (2) ci-dessus. En particulier H est distingué dans G. Cela démontre l'assertion (5).

(6) Soit H un sous-groupe distingué de G. Soit $F = L^H$. Alors F est une extension galoisienne de K. On dispose d'une application de restriction $Res : G \to \mathrm{Gal}(F/K)$, qui à σ dans G associe sa restriction à F ; elle est surjective de noyau H.

Montrons que l'on a $\sigma(F) = F$ pour tout σ dans G. Soient x un élément de F et τ un élément de H. Il s'agit de vérifier que l'on a $\tau(\sigma(x)) = \sigma(x)$, i.e. que l'on a $\sigma^{-1}\tau\sigma(x) = x$, ce qui est clair car H est par hypothèse distingué dans G. On déduit de là que chaque élément σ de G induit, par restriction, un K-automorphisme σ_F de F. L'application $\sigma \mapsto \sigma_F$ est donc un homomorphisme de G sur *un* groupe G_F d'automorphismes de F. Montrons que l'on a en fait $G_F = \mathrm{Gal}(F/K)$. D'après le lemme 3.5, il suffit de vérifier que K est exactement le sous-ensemble de F laissé fixe par G_F. Considérons donc un élément x de F, tel que l'on ait pour tout σ, $\sigma_F(x) = x$. Alors pour tout σ dans G, on $\sigma(x) = x$. D'après l'assertion (1), x appartient donc à K. D'où notre assertion et le fait que l'on dispose d'un homomorphisme de restriction $Res : G \to \mathrm{Gal}(F/K)$ qui est

surjectif (cf. dém. de l'assertion(5)). Son noyau est le groupe de Galois de L sur F, qui n'est autre que H (assertion (4)). D'où l'assertion (6).

Les assertions (5) et (6) fournissent l'assertion c) du théorème et terminent sa démonstration.

Les énoncés (importants) qui suivent sont laissés à titre d'exercices :

On considère toujours une extension galoisienne finie L/K de groupe de Galois G.

1) Soient F et F' deux sous-corps intermédiaires de l'extension L/K. Soient H et H' les deux sous-groupes de G correspondant à F et F' par la correspondance de Galois. Alors le sous-groupe $H \cap H'$ correspond au composé FF' des corps F et F'.

2) Soit F une extension finie (quelconque) de K contenue dans Ω (Ω étant une clôture algébrique que l'on a fixée au départ : cf. p. 13). Alors LF est une extension galoisienne de F et L est une extension galoisienne de $L \cap F$. Soit H le groupe de Galois de LF sur F. L'application de restriction $H \to \mathrm{Gal}(L/L \cap F)$ réalise un isomorphisme de groupes de H sur $\mathrm{Gal}(L/L \cap F)$.

3) Soit F une extension finie (quelconque) de K contenue dans Ω. Alors le degré de LF sur F divise le degré de L sur K. Cette assertion est fausse si L n'est pas une extension galoisienne de K.

4) Soit L' une extension galoisienne finie de K contenue dans Ω. Soit G' le groupe de Galois de L' sur K. Alors le composé LL' est une extension galoisienne de K. Soit $\mathcal{G}$ le groupe de Galois de LL' sur K. L'application de restriction $\mathcal{G} \to G \times G'$ est injective. Si $L \cap L'$ est égal à K, cette application est un isomorphisme de groupes de $\mathcal{G}$ sur $G \times G'$.

Annexe sur les périodes de l'équation cyclotomique

On considère un nombre premier ≥ 5. On note L le sous-corps de $\mathbb{C}$ obtenu en adjoignant à $\mathbb{Q}$ une racine primitive p-ième de l'unité : on a $L = \mathbb{Q}\big(\exp(2\pi i/p)\big)$. Le degré de L sur $\mathbb{Q}$ est $n = p-1$. On se propose ici de résoudre le problème suivant : on considère une décomposition de n sous la forme

$$n = ef, \tag{1}$$

où e et f sont deux entiers > 1. D'après le théorème de correspondance de Galois, le corps L possède un unique sous-corps K de degré e sur $\mathbb{Q}$. On va déterminer un polynôme irréductible à coefficients dans $\mathbb{Q}$ qui définit l'extension K.

On introduit pour cela les notations suivantes :

(i) $\zeta = \exp(2\pi i/p)$;
(ii) g une racine primitive modulo p : g est un entier compris entre 2 et $p-1$ et la classe de g modulo p engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^*$;
(iii) $G = \mathrm{Gal}(L/\mathbb{Q})$; le groupe G est cyclique d'ordre n ;
(iv) σ un générateur de G : on a

$$\sigma(\zeta) = \zeta^g. \tag{2}$$

(v) H le sous-groupe de G engendré par σ^e ; le groupe H est l'unique sous-groupe d'ordre f de G, dont le corps des invariants correspondant est K.
(vi) si j est un entier relatif, on note

$$\zeta_j = \sigma^j(\zeta). \tag{3}$$

On a ainsi

$$\zeta_j = \zeta^{g^j}. \tag{4}$$

Pour tout i et j dans $\mathbb{Z}$, on a donc l'égalité

$$\sigma^i(\zeta_j) = \zeta_{i+j}. \tag{5}$$

Les éléments ζ_0, ζ_1,..., ζ_{n-1} sont à l'ordre près, ζ, ζ^2, ..., ζ^n. Le système $(\zeta_j)_{0\leq j\leq n-1}$ est en particulier une base de L sur $\mathbb{Q}$.

Étant donné un entier relatif h, considérons maintenant l'élément η_h défini par l'égalité

$$\eta_h = Tr_{L/K}(\zeta_h). \tag{6}$$

Par définition de la trace d'un élément de L sur K, on a en fait

$$\eta_h = \sum_{0\leq t\leq f-1} \sigma^{te}(\zeta_h).$$

On a donc d'après les notations ci-dessus

$$\eta_h = \sum_{0\leq t\leq f-1} \zeta_{h+te}. \tag{7}$$

Les éléments η_h sont appelés *périodes de l'équation cyclotomique* associées à e et p. Ces nombres algébriques vérifient les propriétés suivantes :

1) Les η_h sont des éléments de K (cela résulte de la définition et du lemme 3.1) ;

2) le système $(\eta_i)_{0\leq i\leq e-1}$ est une base de K sur $\mathbb{Q}$ (cf. formule (7)) ;
2) pour tout h et i dans $\mathbb{Z}$, on a l'égalité (cf. formule(5))

$$\sigma^i(\eta_h) = \eta_{h+i}. \tag{8}$$

En particulier, η_h ne dépend que de la classe de h modulo e.

On déduit de là le résultat suivant :

Proposition. *On a $K = \mathbb{Q}(\eta_0)$. Le polynôme minimal P de η_0 sur $\mathbb{Q}$ est donné par*

$$P(X) = \prod_{0\leq h\leq e-1} (X - \eta_h).$$

Démonstration : D'abord le corps $\mathbb{Q}(\eta_0)$ est contenu dans K. Le degré de η_0 sur $\mathbb{Q}$ est donc au plus e. Par ailleurs, pour tout h dans $\mathbb{Z}$, on a d'après (8)

$$\eta_h = \sigma^h(\eta_0).$$

Ainsi, η_0 possède au moins e conjugués sur $\mathbb{Q}$. Le degré de η_0 sur $\mathbb{Q}$ est donc e. Cela entraîne que P est le polynôme minimal de η_0 sur $\mathbb{Q}$ et que $K = \mathbb{Q}(\eta_0)$. D'où le résultat.

Afin d'expliciter le polynôme P, il suffit donc de connaître la table de multiplication de K dans la base $(\eta_i)_{0\leq i\leq e-1}$. Autrement dit il s'agit de savoir calculer les produits $\eta_h\eta_k$. On considère pour cela, pour tout r dans $\mathbb{Z}$, les éléments de K

$$\eta^{(r)} = Tr_{L/K}(\zeta^r).$$

On vérifie directement l'énoncé suivant :

Lemme. *(Gauss) Soient r et s deux entiers relatifs. On a l'égalité*

$$\eta^{(r)}\eta^{(s)} = \sum_{0\leq l\leq f-1} \eta^{(r+sg^{le})}. \tag{9}$$

Cet énoncé fournit la table de multiplication cherchée. En effet soit r un entier relatif.

a) Si r est multiple de p, on a par définition $\eta^{(r)} = \eta^{(0)} = [L : K] = f$. Or la somme des éléments η_h, pour h compris entre 0 et $e-1$, vaut -1. On a donc

$$\eta^{(0)} = -f \sum_{0\leq h\leq e-1} \eta_h. \tag{10}$$

b) Supposons que r ne soit pas multiple de p. Soit h le plus petit entier naturel compris entre 0 et $n-1$ tel que l'on ait

$$r \equiv g^h \text{ mod. } p.$$

On a alors l'égalité (cf. formule (6))

$$\eta^{(r)} = \eta_h. \tag{11}$$

Les formules (9), (10) et (11) permettent alors d'écrire la table de multiplication cherchée.

Exemple numérique. Prenons $p = 7$. Déterminons le polynôme irréductible définissant le sous-corps de $\mathbb{Q}(\exp(2\pi i/7))$ de degré 3 sur $\mathbb{Q}$. On a donc $e = 3$, $f = 2$. On vérifie que $g = 3$. On a par ailleurs

$$\eta^{(0)} = 2, \quad \eta^{(1)} = \eta_0, \quad \eta^{(2)} = \eta_2, \quad \eta^{(3)} = \eta_1, \quad \eta^{(4)} = \eta_4 = \eta_1,$$

$$\eta^{(5)} = \eta_5 = \eta_2, \quad \eta^{(6)} = \eta_3 = \eta_0.$$

On déduit de là que

$$\eta_0\eta_1\eta_2 = 1 \quad \text{et} \quad \eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2 = -2.$$

Par suite le polynôme P cherché est donné par l'égalité

$$P(X) = X^3 + X^2 - 2X - 1.$$

Introduction au problème de la théorie de Galois inverse

Il s'agit du problème suivant :

Problème. *Soit G un groupe fini. Existe-t-il une extension galoisienne finie K de $\mathbb{Q}$ telle le groupe de Galois de K sur $\mathbb{Q}$ soit isomorphe à G ?*

Ce problème n'est toujours pas résolu. Il y a cependant de nombreux groupes G pour lesquels on sait répondre positivement à cette question. Tel est par exemple le cas si G est *résoluble* ; ce résultat a été prouvé par Shafarevich en 1954. En particulier, un groupe fini d'ordre une puissance d'un nombre premier est groupe de Galois sur $\mathbb{Q}$. Feit et Thompson ont démontré en 1962 qu'un groupe fini d'ordre impair est résoluble. On a ainsi le résultat suivant :

Théorème. *Soit G un groupe fini d'ordre impair. Alors G est groupe de Galois sur $\mathbb{Q}$.*

On pourra consulter les références [13], [14] pour connaître plus précisément les résultats démontrés sur ce problème, ainsi que les techniques d'attaques qui sont actuellement utilisées.

L'objectif ici est seulement de donner quelques exemples classiques de groupes G se réalisant comme groupe de Galois sur $\mathbb{Q}$. Remarquons que si un groupe G répond positivement au problème, il en est de même de tous ses quotients.

I. Le cas abélien

Le premier exemple est donné par les groupes abéliens.

Théorème 1.1. *Soit G un groupe abélien. Alors G est groupe de Galois sur $\mathbb{Q}$.*

Démonstration : On montre d'abord qu'il existe un entier $N \geq 1$ tel que G soit isomorphe à un quotient de $(\mathbb{Z}/N\mathbb{Z})^*$. Puisque G est abélien, G est isomorphe à un produit de groupes cycliques :

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}.$$

On cherche alors une famille de nombres premiers $(p_i)_{1\leq i\leq r}$ telle que, pour tout i compris entre 1 et r, $\mathbb{Z}/n_i\mathbb{Z}$ soit un quotient de $\mathbb{Z}/(p_i-1)\mathbb{Z}$. Il suffit pour cela de chercher des nombres premiers p_i de sorte que l'on ait $p_i \equiv 1$ mod. n_i. Or il existe une infinité de tels nombres premiers (théorème de Dirichlet). On déduit de là un homomorphisme surjectif de groupes

$$\prod_{i=1}^{r} \mathbb{Z}/(p_i-1)\mathbb{Z} \to G,$$

du produit des $\mathbb{Z}/(p_i - 1)\mathbb{Z}$ sur G. Posons alors

$$N = \prod_{i=1}^{r} p_i.$$

L'entier N convient. En effet, les groupes $\mathbb{Z}/(p_i - 1)\mathbb{Z}$ et $(\mathbb{Z}/p_i\mathbb{Z})^*$ sont isomorphes, et l'on a un isomorphisme canonique (lemme chinois)

$$(\mathbb{Z}/N\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^*,$$

d'où notre assertion. Par ailleurs, si ζ est une racine primitive N-ième de l'unité, l'application

$$\varphi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}),$$

définie par l'égalité

$$\varphi(u)(\zeta) = \zeta^u,$$

est un isomorphisme de groupes. Le résultat provient alors du théorème de la correspondance de Galois : d'après ce qui précède il existe un homomorphisme de groupes surjectif ψ de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sur G. Soient H le noyau de ψ et K le sous-corps de $\mathbb{Q}(\zeta)$ laissé fixe par H. Le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe à G ; d'où le théorème.

II. Le groupe symétrique $\mathbb{S}_n$

La lecture de ce paragraphe nécessite quelques connaissances de théorie algébrique des nombres, notamment la notion de ramification dans les extensions finies de $\mathbb{Q}$ (cf. par exemple [10]). Le théorème suivant a été démontré par Selmer (cf. [11]) :

Théorème 2.1. *Soit n un entier ≥ 2. Le polynôme $X^n - X - 1$ dans $\mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$ et son groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathbb{S}_n$.*

Démonstration : On posera $P = X^n - X - 1$.

1) Montrons que P est irréductible sur $\mathbb{Q}$. D'abord P n'a pas de racine dans $\mathbb{Q}$: si tel était le cas, 1 ou -1 serait racine de P, ce qui n'est pas. On peut supposer désormais que l'on a $n \geq 4$. Par ailleurs les racines de P dans $\mathbb{C}$ sont simples. En effet, une racine multiple z de P devrait vérifier l'égalité $nz^{n-1} = 1$, ce qui entraîne $n(z + 1) = z$, et z devrait être dans $\mathbb{Q}$.

Étant donné un facteur unitaire de P à coefficients entiers de degré $d \geq 2$, on note $R(Q)$ l'ensemble des racines de Q. On pose

$$S(Q) = \sum_{z \in R(Q)} \left(z - \frac{1}{z} \right).$$

Si $(\sigma_i)_{1\leq i\leq d}$ sont les fonctions symétriques élémentaires des racines de Q, on a l'égalité

$$S(Q) = \sigma_1 - \frac{\sigma_{d-1}}{\sigma_d}. \tag{1}$$

Les σ_i sont des entiers, et l'on a $\sigma_d = \pm Q(0) = \pm 1$. En particulier $S(Q)$ est un entier relatif. On a de plus

$$S(P) = 1. \tag{2}$$

(On a dans ce cas $\sigma_1 = 0$ et $\sigma_{d-1} = -\sigma_d$).

Supposons alors que P soit réductible sur $\mathbb{Q}$. On a $P = QT$, où Q et T sont deux polynômes unitaires de degré ≥ 2 à coefficients dans $\mathbb{Z}$ ($\mathbb{Z}$ est intégralement clos). On a

$$S(P) = S(Q) + S(T).$$

Afin d'obtenir une contradiction il suffit, d'après (2), de prouver que l'on a

$$S(Q) \geq 1. \tag{3}$$

Considérons pour cela une racine z de P. Il existe deux nombres réels θ et r tel que l'on ait $z = r\exp(i\theta)$. On a $r^n = \mid z+1 \mid$, ce qui implique l'égalité

$$r^{2n} = r^2 + 1 + 2r\cos\theta. \tag{4}$$

On remarque d'abord que l'on a

$$r \neq 1. \tag{5}$$

En effet, si r était égal à 1, z serait d'après l'égalité (4) une racine cubique de l'unité, ce qui n'est pas. Montrons alors que l'on a l'inégalité

$$2\ \Re\left(z - \frac{1}{z}\right) > \frac{1}{r^2} - 1. \tag{6}$$

On a

$$2\ \Re\left(z - \frac{1}{z}\right) = 2\cos\theta\ \left(r - \frac{1}{r}\right),$$

et l'on déduit de l'égalité (4)

$$2\ \Re\left(z - \frac{1}{z}\right) = \frac{(r^2-1)(r^{2n} - r^2 - 1)}{r^2}.$$

Puisque l'on a $(r^2-1)(r^{2n}-r^2) > 0$ (considérer les cas où $r > 1$ et $r < 1$), on obtient ainsi l'inégalité (6).

On considère alors les racines $(z_i)_{1\leq i\leq d}$ de Q. Posons $r_i = \mid z_i \mid$. On a

$$1 = \mid Q(0) \mid = \prod_{i=1}^{d} r_i.$$

En particulier on a

$$\prod_{i=1}^{d} \frac{1}{r_i^2} = 1.$$

L'inégalité entre moyennes arithmétique et géométrique entraîne alors

$$\frac{1}{d}\left(\sum_{i=1}^{d} \frac{1}{r_i^2}\right) \geq 1.$$

On déduit alors de l'inégalité (6),

$$2S(Q) = \sum_{i=1}^{d} 2\ \Re\left(z_i - \frac{1}{z_i}\right) > \sum_{i=1}^{d}\left(\frac{1}{r_i^2} - 1\right) \geq 0.$$

(La première égalité ayant lieu car $S(Q)$ est entier et sa partie imaginaire est nulle). On obtient ainsi l'assertion (3), ce qui prouve l'irréductibilité de P.

2) Montrons maintenant que le groupe de Galois de P est isomorphe à $\mathbb{S}_n$. Soient $(x_i)_{1\leq i\leq n}$ les n racines de P dans $\mathbb{C}$. On pose $L = \mathbb{Q}(x_1, .., x_n)$ le corps obtenu en adjoignant à $\mathbb{Q}$ les x_i. On désigne par A l'anneau d'entiers de L (la fermeture intégrale de $\mathbb{Z}$ dans L) et G le groupe de Galois de L sur $\mathbb{Q}$. Le fait que P soit irréductible signifie que G opère transitivement sur l'ensemble $R = \{x_1, ..., x_n\}$. La démonstration comporte plusieurs lemmes :

Lemme 2.1. *Le groupe G est engendré par ses sous-groupes d'inertie $I_\wp$ lorsque $\wp$ parcourt les idéaux maximaux de A.*

Démonstration : Ce lemme est en fait valable en remplacant P par n'importe quel polynôme iréductible sur $\mathbb{Q}$. On considère le sous-groupe H de G engendré par ses sous-groupes d'inertie $I_\wp$ lorsque $\wp$ parcourt les idéaux maximaux de A. C'est un sous-groupe distingué de G. En effet, si p est un nombre premier, les $I_\wp$ lorsque $\wp$ parcourt les idéaux premiers de A au-dessus de p, forment une classe de conjugaison de sous-groupes de G. Soit K le sous-corps de L laissé fixe par H. Tout revient à montrer que l'on a $K = \mathbb{Q}$. Pour cela il suffit de montrer que si p est un nombre premier, p est non ramifié dans K (car il n'existe pas de corps de nombres, autre que $\mathbb{Q}$, partout non ramifié sur $\mathbb{Q}$: c'est le théorème d'Hermite-Minkowski, cf. [10], p. 71). On considère donc un nombre premier p et un idéal premier $\wp$ de A au-dessus de p. Posons $\mathcal{P} = \wp \cap K$. L'extension $K/\mathbb{Q}$

est galoisienne, et l'image de $I_\wp$ par le morphisme de restriction $G \to \mathrm{Gal}(K/\mathbb{Q})$ est le sous-groupe d'inertie en $\mathcal{P}$ de $\mathrm{Gal}(K/\mathbb{Q})$. Or par définition H contient $I_\wp$, et l'image de H est triviale dans $\mathrm{Gal}(K/\mathbb{Q})$. Cela prouve que p est non ramifié dans K. D'où le lemme.

Lemme 2.2. *Soient p un nombre premier et $\wp$ un idéal premier de A au-dessus de p. Alors l'ordre du sous-groupe d'inertie $I_\wp$ de G est ≤ 2. Si $I_\wp$ n'est pas trivial, il est engendré par une transposition.*

Démonstration : Étant donné un élément x de A, on note $\bar{x}$ son image dans le corps résiduel $A/\wp$, et $\bar{P}$ le polynôme déduit de P par réduction de ses coefficients modulo p. On a

$$\bar{P} = \prod_{i=1}^{n}(X - \bar{x}_i) = X^n - X - 1 \in \big(A/\wp\big)[X].$$

De l'égalité $\bar{P}' = nX^{n-1} - 1$, on déduit que

$$X\bar{P}' - n\bar{P} = (n-1)X + n.$$

Il en résulte que le PGCD de $\bar{P}$ et $\bar{P}'$ est un polynôme de degré ≤ 1 (p ne peut diviser n et $n-1$). Ainsi $\bar{P}$ possède n racines distinctes dans le corps fini $A/\wp$, ou bien $\bar{P}$ a une unique racine double et $n-2$ racines simples dans $A/\wp$.

Supposons que $I_\wp$ ne soit pas trivial. Soit s un élément de $I_\wp$ autre que l'élément neutre e. Il existe i entre 1 et n tel que l'on ait $s(x_i) = x_j$ avec $i \neq j$. Puisque s est dans $I_\wp$, on a

$$\overline{x_i} = \overline{s(x_i)} = \overline{x_j},$$

donc $\overline{x_i}$ est une racine multiple de $\bar{P}$. Puisque $\bar{P}$ ne peut posséder qu'une seule racine multiple, on déduit de là que si k est un entier compris entre 1 et n, distinct de i et j, on a nécessairement $s(x_k) = x_k$. Par conséquent, considéré comme un élément du groupe symétrique de R, s est la transposition (x_i, x_j), et s est en particulier d'ordre 2. Cela entraîne que l'on a $I_\wp = \{e, s\}$ (car $\bar{P}$ a une unique racine double). D'où le lemme.

Corollaire 2.1. *Le groupe G, considéré comme sous-groupe du groupe symétrique de R, est engendré par des transpositions.*

Démonstration : C'est une conséquence immédiate des lemmes précédents

Rappelons que P étant irréductible sur $\mathbb{Q}$, le groupe G opère transitivement sur R. Tout revient alors à démontrer l'énoncé suivant :

Lemme 2.3. *Soient n un entier ≥ 1 et G un sous-groupe transitif de $\mathbb{S}_n$ engendré par des transpositions. Alors on a $G = \mathbb{S}_n$.*

Démonstration : Soit (a, b) une transposition. Il suffit de prouver que (a, b) appartient à G. Soit T l'ensemble des transpositions qui appartiennent à G. Puisque G est transitif,

il existe un élément g de G tel que l'on ait $g(a) = b$. Il existe un entier $p \geq 1$ et une famille d'éléments $(t_i)_{1 \leq i \leq p}$ de T tel que l'on ait

$$g = \prod_{i=1}^{p} t_i.$$

Parmi tous les choix possibles de g et des éléments t_i, on suppose que l'entier p est *minimal*. On peut supposer que l'on a $p \geq 2$. On remarque d'abord que b appartient au support de t_1. En effet, posons $u = t_2 ... t_p(a)$; on a $t_1 g(a) = t_1(b) = u$ et si $u = b$ cela contredit la minimalité de p. Soit alors j un entier entre 2 et p. Pour tout i entre 1 et $p-1$, posons $t'_i = t_j t_i t_j^{-1}$. On a l'égalité

$$g = t_j \Big(\prod_{i=1}^{j-1} t'_i \Big) \Big(\prod_{i=j+1}^{p} t_i \Big).$$

Le raisonnement précédent montre que b appartient au support de t_j. En particulier b est dans le support de t_p. De même a appartient au support de t_p, sinon $t_1 ... t_{p-1}$ envoie a sur b, ce qui contredit encore la minimalité de p. Puisque t_p est une transposition on a donc $t_p = (a, b)$, et ainsi (a, b) est dans G. D'où le résultat.

Terminons ce paragraphe par le résultat suivant :

Proposition 2.1. *Soit $K = \mathbb{Q}(\alpha)$ où α est une racine de P. Alors $\mathbb{Q}$ et K sont les seules extensions de $\mathbb{Q}$ contenues dans K.*

Démonstration : Identifions le groupe de Galois de P à un sous-groupe de $\mathbb{S}_n$. Soit G le groupe de Galois de L sur K. C'est un sous-groupe d'indice n de $\mathbb{S}_n$. Il est donc isomorphe à $\mathbb{S}_{n-1}$ (car c'est le fixateur de α). Considérons alors une extension H de $\mathbb{Q}$ contenue dans K distincte de K. Le groupe $\mathrm{Gal}(L/H)$ contient strictement G. Cela entraîne $G = \mathbb{S}_n$ (le vérifier) et donc $H = \mathbb{Q}$. D'où le résultat.

III. Le groupe $\mathbb{GL}_2(\mathbb{F}_p)$ (p premier)

On a l'énoncé suivant :

Théorème 3.1. *Pour tout nombre premier p le groupe $\mathbb{GL}_2(\mathbb{F}_p)$ se réalise comme groupe de Galois sur $\mathbb{Q}$.*

Cet énoncé peut se déduire de la théorie des courbes elliptiques sur $\mathbb{Q}$. Étant donnée une courbe elliptique E sur $\mathbb{Q}$, i.e. une courbe projective lisse définie sur $\mathbb{Q}$, de genre 1, possédant un point rationnel sur $\mathbb{Q}$, on peut parler, pour tout nombre premier p, de son groupe des points de p-division. C'est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$, sur lequel opère le groupe de Galois de $\bar{\mathbb{Q}}$ sur $\mathbb{Q}$. On obtient ainsi un homomorphisme

$$\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{GL}_2(\mathbb{F}_p),$$

dont le corps laissé fixe par le noyau de ρ_p est une extension finie de $\mathbb{Q}$: c'est le corps des points de p-division de E. Jean-Pierre Serre a prouvé en 1972, "qu'en général", ρ_p est surjectif (cf. [12]). Par exemple, si l'on prend pour E la courbe elliptique (de conducteur 37) d'équation

$$y^2 + y = x^3 - x,$$

l'homomorphisme ρ_p correspondant est surjectif pour tout nombre premier p. Cela entraîne en particulier le théorème.

Un exemple de polynôme irréductible sur $\mathbb{Q}$ dont le groupe de Galois soit isomorphe à $\mathbb{GL}_2(\mathbb{F}_3)$ (qui est d'ordre 48) est

$$f = X^8 + 72X^6 - 1998X^4 - 332667.$$

Il existe un point P d'ordre 3 de E tel que, si α est une racine de f, l'on ait $\mathbb{Q}(\alpha) = \mathbb{Q}(P)$.

IV. Un produit semi-direct $\mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/(p-1)\mathbb{Z}$ (p premier)

Soit p un nombre premier. Choisissons un générateur a de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Notons φ l'homomorphisme de groupes de $\mathbb{Z}/(p-1)\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, le groupe des automorphismes de $\mathbb{Z}/p\mathbb{Z}$, défini par

$$\varphi\big(n + (p-1)\mathbb{Z}\big) = \big\{t \mapsto a^n t\big\}.$$

Considérons le produit semi-direct $\mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/(p-1)\mathbb{Z}$: c'est un groupe d'ordre $p(p-1)$ non abélien, qui est ensemblistement le produit cartésien $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$, et dont la loi de composition interne est donnée par

$$\big((a,b),(c,d)\big) \mapsto \big(a + \varphi(b)(c), b + d\big).$$

L'élément neutre est $(0,0)$ et l'inverse de (a,b) est $\big(\varphi(-b)(-a), -b\big)$. On va montrer l'énoncé suivant (cf. [4], p. 147 si $p = 5$) :

Proposition 4.1. *Le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^p - 2$ est isomorphe au produit semi-direct $\mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/(p-1)\mathbb{Z}$.*

On montre d'abord le lemme suivant :

Lemme 4.1. *Soient G un groupe, d'élément neutre e, N un sous-groupe distingué de G et H un sous-groupe de G. Notons $\psi : H \to Aut(N)$ l'homomorphisme qui à h associe $\{n \mapsto hnh^{-1}\}$. Supposons que l'on ait les égalités*

$$G = NH \quad et \quad H \cap N = \{e\}.$$

Alors le produit semi-direct $N \times_\psi H$ est isomorphe à G via l'application

$$(n, h) \mapsto nh.$$

Démonstration : Notons f cette application. On a

$$f\big((n,h).(n',h')\big) = f(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h' = f(n,h)f(n',h'),$$

ce qui prouve que f est un morphisme de groupes. Les hypothèses faites sur N et H entraînent par ailleurs que f est une bijection. D'où le lemme.

Remarque

Soit G un groupe, d'élément neutre e, et N un sous-groupe *distingué* de G : on a la suite exacte de groupes

$$\{e\} \to N \xrightarrow{i} G \xrightarrow{p} G/N \to \{e\},$$

où i est l'inclusion et p la surjection canonique. Supposons que cette suite exacte soit *scindée*, autrement dit que p possède une section, c'est-à-dire encore qu'il existe un homomorphisme de groupes $s : G/N \to G$ tel que $p \circ s$ soit l'application identique de G/N. Soit $H = s(G/N)$. Alors s réalise un isomorphisme de G/N sur le sous-groupe H de G, et l'on vérifie que l'on a les égalités

$$G = NH \quad \text{et} \quad H \cap N = \{e\}.$$

(Si g est dans G, en posant $h = s(gN)$, on a $g = h(h^{-1}g)$ et $h^{-1}g$ appartient à N).

Démonstration de la proposition

Soient ζ une racine primitive p-ième de l'unité et α une racine p-ième de 2. On notera $f = X^p - 2$. Il est irréductible sur $\mathbb{Q}$ (c'est un polynôme d'Eisenstein). Le corps de décomposition de f est $K = \mathbb{Q}(\zeta, \alpha)$: en effet, K est une extension galoisienne de $\mathbb{Q}$ et c'est la plus petite extension de $\mathbb{Q}$ qui contient toutes les racines de f. Notons G le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$. Puisque $\mathbb{Q}(\zeta)$ est une extension galoisienne de $\mathbb{Q}$, le groupe de Galois $N = \mathrm{Gal}\big(K/\mathbb{Q}(\zeta)\big)$ est un sous-groupe distingué de G. Posons $H = \mathrm{Gal}\big(K/\mathbb{Q}(\alpha)\big)$. On a les égalités $G = HN$ et $H \cap N = \{e\}$: il suffit pour le vérifier de remarquer que G est d'ordre $p(p-1)$, que N et H sont respectivement d'ordre p et $p-1$, et que les groupes NH/N et $H/H \cap N$ sont isomorphes. Il résulte du lemme 4.1 que G est isomorphe au produit semi-direct $N \times_\psi H$, où ψ désigne l'opération de H sur N par automorphismes intérieurs. Il reste à vérifier que ce produit semi-direct est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/(p-1)\mathbb{Z}$. Le groupe N est engendré par l'élément σ, où σ est déterminé par les égalités

$$\sigma(\zeta) = \zeta \quad \text{et} \quad \sigma(\alpha) = \zeta\alpha.$$

Notons encore a le représentant de a compris entre 1 et p. Le groupe H est engendré par l'élément τ défini par

$$\tau(\zeta) = \zeta^a \quad \text{et} \quad \tau(\alpha) = \alpha.$$

La flêche $\Gamma : N \times_\psi H \to \mathbb{Z}/p\mathbb{Z} \times_\varphi \mathbb{Z}/(p-1)\mathbb{Z}$ définie par $\Gamma(\sigma^i, \tau^j) = \big(i + p\mathbb{Z}, j + (p-1)\mathbb{Z}\big)$ est alors un isomorphisme de groupes. En effet, on vérifie que l'on a

$$\psi(\tau)(\sigma) = \tau\sigma\tau^{-1} = \sigma^a.$$

En particulier, pour tout j et l, l'on a l'égalité

$$\psi(\tau^j)(\sigma^l) = \sigma^{a^j l}.$$

On déduit de là que Γ est un homomorphisme de groupes. Par ailleurs, Γ est clairement bijectif. D'où la proposition.

V. Le groupe alterné $\mathbb{A}_5 \simeq \mathbb{SL}_2(\mathbb{F}_4)$

Montrons le lemme suivant :

Lemme 5.1. *Soit f un polynôme irréductible unitaire de $\mathbb{Z}[X]$ de degré 5. Supposons que les deux conditions suivantes soient réalisées :*

a) Le discriminant $D(f)$ de f est un carré dans $\mathbb{Z}$;

b) il existe un nombre premier l, qui ne divise pas $D(f)$, tel que le polynôme de $\mathbb{F}_l[X]$ déduit de f par réduction modulo l posssède exactement deux racines dans $\mathbb{F}_l$.

Alors le groupe de Galois de f est isomorphe à $\mathbb{A}_5$.

Démonstration : Supposons les conditions a) et b) réalisées : identifions $\mathrm{Gal}(f)$ à un sous-groupe de $\mathbb{S}_5$. Il résulte de la condition a) que $\mathrm{Gal}(f)$ est contenu dans $\mathbb{A}_5$. Puisque l ne divise pas $D(f)$, le polynôme f mod. l est séparable, et en utilisant la proposition 3.3, on constate que 3 divise l'ordre de $\mathrm{Gal}(f)$. Par ailleurs, f étant irréductible de degré 5, $\mathrm{Gal}(f)$ a un ordre divisible par 5. Ainsi 15 divise $|\ \mathrm{Gal}(f)\ |$. Or un groupe d'ordre 15 est cyclique et $\mathbb{A}_5$ ne contient pas d'élément d'ordre 15. On déduit de là que $|\ \mathrm{Gal}(f)\ | = 30$ ou 60. Mais $\mathbb{A}_5$ étant un groupe simple et un sous-groupe d'indice 2 étant distingué, cela entraîne que $|\ \mathrm{Gal}(f)\ | = 60$ i.e. que $\mathrm{Gal}(f) = \mathbb{A}_5$. D'où le lemme.

Remarque

Pour vérifier que les groupes $\mathbb{A}_5$ et $\mathbb{SL}_2(\mathbb{F}_4)$ sont isomorphes, on peut remarquer que $\mathbb{SL}_2(\mathbb{F}_4)$ opère à droite non trivialement sur la droite projective sur $\mathbb{F}_4$, i.e. sur l'ensemble des droites du $\mathbb{F}_4$-espace vectoriel $\mathbb{F}_4 \times \mathbb{F}_4$, qui est un ensemble à cinq éléments. On obtient ainsi un homomorphisme de groupes $\mathbb{SL}_2(\mathbb{F}_4) \to \mathbb{S}_5$. Notre assertion résulte alors du fait que $\mathbb{SL}_2(\mathbb{F}_4)$ est un groupe simple de même ordre que $\mathbb{A}_5$. On a en fait le lemme suivant :

Lemme 5.2. *Un groupe simple qui opère non trivialement sur un ensemble à n éléments est isomorphe à un sous-groupe du groupe alterné $\mathbb{A}_n$.*

Application

(Mestre) Soit $f = X^5 - 10X^3 + 2X^2 + 19X - 6$. Le dicriminant de f est $(2^3.887)^2$. On a

$$f \text{ mod. } 3 = X(X-1)(X^3 + X^2 - 1) \in \mathbb{F}_3[X].$$

D'après le lemme 5.1 on a $\mathrm{Gal}(f) = \mathbb{A}_5$.

Montrer que si l'on prend $f = X^5 - 23X^3 + 55X^2 - 33X - 1$, on a encore $\mathrm{Gal}(f) = \mathbb{A}_5$.

VI. Les groupes d'ordre 8

Commencons par déterminer, à isomorphisme près, tous les groupes d'ordre 8 (cf. par exemple [4], p. 22). D'abord il résulte du théorème de structure des modules de type fini sur $\mathbb{Z}$, que les groupes abéliens d'ordre 8 sont

$$(\mathbb{Z}/2\mathbb{Z})^3, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/8\mathbb{Z}.$$

Considérons alors un groupe G d'ordre 8. Soit r le maximum des ordres des éléments de G. D'après le théorème de Lagrange, on a $r \in \{2, 4, 8\}$. Si $r = 8$, G est cyclique d'ordre 8. Si $r = 2$ le groupe G est abélien isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. Supposons donc désormais que l'on a $r = 4$ et que G n'est pas commutatif. Soit a un élément de G d'ordre 4 (a existe par hypothèse). Soit N le sous-groupe de G engendré par a. Puisque N est d'indice 2, il est distingué dans G. On dispose ainsi de la suite exacte :

$$\{e\} \to N \xrightarrow{i} G \xrightarrow{p} G/N \to \{e\},$$

où i est l'inclusion et p la surjection canonique. On distingue alors deux cas suivant que cette suite exacte est scindée ou non.

1) Supposons que cette suite exacte soit scindée. Cela signifie par définition que p possède une section s. Posons $H = s(G/N)$. Le groupe G est alors isomorphe au produit semi-direct $N \times_\varphi H$ où $\varphi : H \to \mathrm{Aut}(N)$ est l'homomorphisme qui correspond à l'opération de H sur N par conjugaison (lemme 4.1 et la remarque qui le suit). Dans ce cas G est donc engendré par deux éléments a et b vérifiant les égalités $a^4 = b^2 = e$ et $bab^{-1} = a^{-1}$ (l'ordre de a est celui bab^{-1}). Cela montre que G est diedral (c'est le groupe généralement noté D_4).

En fait le groupe $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ est d'ordre 2 : ses deux éléments sont l'application identique et l'homomorphisme ψ défini par l'égalité $\psi(1) = -1$. Ce qui précède montre que, plus concrétement, G est isomorphe au produit semi-direct $\mathbb{Z}/4\mathbb{Z} \times_\varphi \mathbb{Z}/2\mathbb{Z}$, où φ l'homomorphisme de $\mathbb{Z}/2\mathbb{Z}$ dans le groupe des automorphismes $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ tel que $\varphi(0)$ soit l'application identique de $\mathbb{Z}/4\mathbb{Z}$ et que $\varphi(1) = \psi$.

2) Supposons que cette suite exacte ne soit pas scindée. Cela signifie que les éléments de G qui n'appartiennent pas à N sont d'ordre 4. Soit b un élément de G qui ne soit pas dans N.On a alors

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Considérons alors le centre Z de G. Il est d'ordre 2 : en effet, le centre d'un 2-groupe n'est pas trivial et si G/Z était d'ordre 2, il serait cyclique, et G serait alors abélien. Puisque a^2 est le seul élément de G d'ordre 2, on a donc $Z = \{e, a^2\}$. L'élément b^2 est d'ordre 2 et l'on a donc $b^2 = a^2$. Par définition, G est le groupe quarternionien $\mathbb{H}_8$ d'ordre 8.

Remarquons que les groupes D_4 et $\mathbb{H}_8$ ne sont pas isomorphes : le groupe $\mathbb{H}_8$ possède un unique sous-groupe d'ordre 2, à savoir son centre, ce qui n'est pas le cas pour D_4. En fait les trois sous-groupes d'ordre 4 de $\mathbb{H}_8$ sont cycliques, et D_4 possède trois sous-groupes d'ordre 4 dont un seul est cyclique.

Conclusion. Il y a (à isomorphisme près) cinq groupes d'ordre 8. Ceux qui ne sont pas abéliens sont le groupe diédral D_4 et le groupe des quaternions $\mathbb{H}_8$.

On va montrer le résultat suivant (cf. [4], p. 160) :

Proposition 6.1. *1) Le groupe de Galois sur $\mathbb{Q}$ de $X^8 - 72X^6 + 180X^4 - 144X^2 + 36$ est isomorphe à $\mathbb{H}_8$.*
2) Le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^4 - 2$ est isomorphe à D_4.

Démonstration : 1) Posons $g = X^8 - 72X^6 + 180X^4 - 144X^2 + 36$. D'abord g est irréductible sur $\mathbb{Q}$ (le vérifier). Soit α une racine de g dans $\mathbb{C}$. Posons

$$\beta = \frac{1}{2}\alpha^7 - \frac{215}{6}\alpha^5 + 78\alpha^3 - 42\alpha, \quad \gamma = \frac{-9}{8}\alpha^7 + \frac{961}{12}\alpha^5 - \frac{549}{4}\alpha^3 + \frac{101}{2}\alpha,$$

$$\delta = \frac{-5}{8}\alpha^7 + \frac{133}{3}\alpha^5 - \frac{261}{4}\alpha^3 + 23\alpha.$$

On vérifie alors (à l'aide d'un logiciel de calcul) que les racines de g sont

$$\{\pm\alpha, \pm\beta, \pm\gamma, \pm\delta\}.$$

Cela montre que l'extension $\mathbb{Q}(\alpha)$ de $\mathbb{Q}$ est galoisienne (puisque toutes les racines de g sont dans $\mathbb{Q}(\alpha)$) de degré 8. C'est le corps de décomposition de g.

Soient σ et τ les éléments de $\mathrm{Gal}(g)$ définis par les égalités

$$\sigma(\alpha) = \beta \quad \text{et} \quad \tau(\alpha) = \gamma.$$

On vérifie que l'on a

$$\sigma \circ \tau(\alpha) = -\delta \quad \text{et} \quad \tau \circ \sigma(\alpha) = \delta.$$

Cela prouve que G n'est pas abélien. On vérifie ensuite que l'on a $\sigma^4 = \tau^4 = e$. Cela suffit pour conclure que $\mathrm{Gal}(g)$ est isomorphe à $\mathbb{H}_8$, car le groupe D_4 possède un unique sous-groupe cyclique d'ordre 4. On vérifie que l'on a en fait

$$\mathrm{Gal}(g) = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}.$$

En effet, ces éléments sont tous distincts et sont dans $\mathrm{Gal}(g)$.

D'après le théorème de correspondance de Galois il existe donc un unique sous-corps K de $\mathbb{Q}(\alpha)$ de degré 4 sur $\mathbb{Q}$. Il s'agit du corps $K = \mathbb{Q}(\theta)$, où θ est racine du polynôme $X^4 + 68X^3 - 30X^2 - 4X + 1$ (dont une racine est $1 - \alpha^2$). Les trois sous-corps de $\mathbb{Q}(\alpha)$ de degré 2 sur $\mathbb{Q}$, qui correspondent aux trois sous-groupes cycliques d'ordre 4 de $\mathrm{Gal}(g)$, sont $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{6})$. On a $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2) Posons $f = X^4 - 2$. C'est un polynôme d'Eiseinstein donc est irréductible sur $\mathbb{Q}$. Soient K le corps de décomposition de f et θ une racine de f. On a $K = \mathbb{Q}(\theta, i)$ où $i^2 = -1$. On vérifie que l'on a $K = \mathbb{Q}(\alpha)$, où α est une racine du polynôme $X^8 + 4X^6 + 2X^4 + 28X^2 + 1$. Il suffit alors d'imiter la démonstration de l'assertion 1) pour obtenir le résultat.

Terminons ce paragraphe par les exercices suivants :

1) Posons $f = X^8 + X^7 - 7X^6 - 6X^5 + 15X^4 + 10X^3 - 10X^2 - 4X + 1$. Montrer que le groupe de Galois de f est cyclique d'ordre 8. Si α est une racine de f, le corps $\mathbb{Q}(\alpha)$ est en fait le sous-corps totalement réel de $\mathbb{Q}\big(\exp(\frac{2\pi i}{17})\big)$.

2) Trouver un polynôme défini sur $\mathbb{Q}$ dont le groupe de Galois sur $\mathbb{Q}$ soit isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3) Trouver le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^8 - 40X^6 + 352X^4 - 960X^2 + 576$.

4) Soient K_1 et K_2 les extensions K de $\mathbb{Q}$ définie par

$$K_1 = \mathbb{Q}\left(\sqrt{\sqrt{2} + \sqrt{3}}\right) \quad \text{et} \quad K_2 = \mathbb{Q}\left(\sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}\right).$$

Montrer que K_2 est une extension galoisienne de $\mathbb{Q}$, mais pas K_1. Montrer que le groupe de Galois $\mathrm{Gal}(K_2/\mathbb{Q})$ est isomorphe à $\mathbb{H}_8$.

VII. Le groupe $\mathbb{PSL}_2(\mathbb{F}_7)$

Le groupe $\mathbb{PSL}_2(\mathbb{F}_7) = \mathbb{SL}_2(\mathbb{F}_7)/\{\pm 1\}$ est un groupe simple d'ordre $168 = 2^3.3.7$. Il y a une seule classe d'isomorphisme de groupes simples d'ordre 168.

Théorème 7.1. *Le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^7 - 7X + 3$ est isomorphe au groupe $\mathbb{PSL}_2(\mathbb{F}_7)$.*

On posera $f = X^7 - 7X + 3$. Soit $G(f)$ le groupe de Galois sur $\mathbb{Q}$ de f. On identifie $G(f)$ à un sous-groupe de $\mathbb{S}_7$. Ce polynôme est irréductible sur $\mathbb{Q}$ (le vérifier).

Pour démontrer ce théorème il convient déjà de connaître les classes de conjugaison de sous-groupes transitifs de $\mathbb{S}_7$. Il y a en fait sept classes de conjugaison de sous-groupes de $\mathbb{S}_7$ qui sont transitifs : des représentants de ces classes sont $\mathbb{S}_7$, $\mathbb{A}_7$, un groupe isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$, et quatre groupes métacycliques M_n définis de la façon suivante : posons

$$C_1 = \{1\}, \quad C_2 = \{1, 6\}, \quad C_3 = \{1, 2, 4\}, \quad C_6 = \{1, 2, 3, 4, 5, 6\}.$$

Soient b un entier tel que $1 \leq b \leq 7$ et a un élément de C_n ; pour tout entier i tel que $1 \leq i \leq 7$, on note $\sigma_{a,b}(i)$ le représentant de $ai + b$ mod. 7 compris entre 1 et 7 : on obtient ainsi une permutation $\sigma_{a,b}$ de $\mathbb{S}_7$. Le groupe M_n est alors le sous-groupe de $\mathbb{S}_7$ formé des éléments $\sigma_{a,b}$ lorsque a parcourt C_n et b les entiers entre 1 et 7. C'est un groupe d'ordre $7n$ (en fait M_n est isomorphe au sous-groupe du groupe affine sur $\mathbb{F}_7$ formé des transformations affines $t \mapsto at + b$, où b parcourt $\mathbb{F}_7$, et où a parcourt les éléments du sous-groupe cyclique d'ordre n de $(\mathbb{Z}/7\mathbb{Z})^*$). Si M_n est d'ordre impair (i.e. d'ordre 7 ou 21), il est contenu dans $\mathbb{A}_7$.

Pour vérifier que $\mathbb{PSL}_2(\mathbb{F}_7)$ est isomorphe à un sous-groupe de $\mathbb{S}_7$, en fait de $\mathbb{A}_7$, on construit une opération non triviale de $\mathbb{PSL}_2(\mathbb{F}_7)$ sur un ensemble à sept éléments (cela n'est pas immédiat). On obtient ainsi un homomorphisme de groupes φ de $\mathbb{PSL}_2(\mathbb{F}_7)$ dans $\mathbb{S}_7$. Le noyau de φ n'est pas $\mathbb{PSL}_2(\mathbb{F}_7)$ car l'opération n'est pas triviale. Puisque $\mathbb{PSL}_2(\mathbb{F}_7)$ est simple, φ est injectif. En fait son image est contenue dans $\mathbb{A}_7$. En effet, en composant φ avec le morphisme signature, on obtient un homomorphisme $\mathbb{PSL}_2(\mathbb{F}_7) \to \mathbb{S}_7/\mathbb{A}_7$ dont le noyau est $\varphi^{-1}(\mathbb{A}_7)$. Si l'image de φ n'était pas contenue dans $\mathbb{A}_7$, l'image réciproque $\varphi^{-1}(\mathbb{A}_7)$ serait un sous-groupe d'indice 2 de $\mathbb{PSL}_2(\mathbb{F}_7)$, ce qui n'est pas car $\mathbb{PSL}_2(\mathbb{F}_7)$ est simple.

1) Le discriminant de f est $3^8.7^8$. Puisque c'est un carré, le groupe de Galois de f est contenu dans $\mathbb{A}_7$.

2) Le polynôme f étant irréductible de degré 7, l'ordre de $G(f)$ est donc divisible par 7.

3) Le polynôme f possède trois racines réelles et quatre racines complexes non réelles. On déduit de là que la conjugaison complexe, restreinte au corps de décomposition de f et identifiée à un élément de $\mathbb{S}_7$, est un produit de deux transpositions à supports disjoints. En particulier, l'ordre de $G(f)$ est pair.

Lemme 7.1. *Le groupe $G(f)$ est isomorphe à $\mathbb{A}_7$ ou à $\mathbb{PSL}_2(\mathbb{F}_7)$.*

Démonstration : Puisque $G(f)$ est contenu dans $\mathbb{A}_7$, il s'agit de vérifier que $G(f)$ n'est pas isomorphe à un groupe M_n. Supposons que $G(f)$ soit isomorphe à l'un des M_n. D'après la remarque 3), on a $n = 2$ ou $n = 6$. L'élément $\sigma_{3,7}$ est le 6-cycle (132645), qui n'appartient pas à $\mathbb{A}_7$; les groupes $G(f)$ et M_6 ne sont donc pas conjugués, et par suite ils ne sont pas isomorphes (par exemple les ordres des représentants des classes de

conjugaison de sous-groupes transitifs de $\mathbb{S}_7$ sont tous distincts). Par ailleurs, on a l'égalité $\sigma_{6,7} = (16)(25)(34)$, qui n'est pas dans $\mathbb{A}_7$. Ainsi $G(f)$ et M_2 ne sont pas isomorphes. D'où le lemme.

Remarque. La démonstration du lemme précédent montre qu'un sous-groupe transitif de $\mathbb{S}_7$ qui est contenu dans $\mathbb{A}_7$, et distinct de $\mathbb{A}_7$, est isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$ ou à l'un des deux groupes M_1 ou M_3. Si de plus il est d'ordre pair, il est isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$.

Nous allons maintenant déterminer des conditions nécessaires pour que $G(f)$ et $\mathbb{A}_7$ soient isomorphes.

Conditions pour qu'un groupe de Galois soit isomorphe à $\mathbb{A}_n$

La référence concernant ce paragraphe est [3]. Considérons un entier $n \geq 2$ et un entier r vérifiant les inégalités $0 < r < n$. Soient f un polynôme irréductible unitaire de degré n à coefficients dans $\mathbb{Z}$ et $(a_i)_{1 \leq i \leq n}$ la famille des racines de f dans $\mathbb{C}$. On pose $m = C_n^r$ et $K = \mathbb{Q}(a_1, ..., a_n)$.

Lemme 7.2. *Soit S l'ensemble des m éléments de K formé des sommes de r éléments a_i distincts. Soit $\mathbb{Q}(S)$ l'extension de $\mathbb{Q}$ obtenue par adjonction des éléments de S. On a $K = \mathbb{Q}(S)$.*

Démonstration : Le résultat est évident si $r = 1$. Supposons donc $r \geq 2$. Soit i un entier tel que $1 \leq i \leq n$. Soient S_i le sous-ensemble de S formé des éléments où a_i apparaît dans la somme des r termes et c_i la somme des éléments qui sont dans S_i. On a

$$c_i = C_{n-1}^{r-1}\ a_i + C_{n-2}^{r-2} \sum_{k \neq i} a_k.$$

On a ainsi

$$c_i = C_{n-2}^{r-1}\ a_i + C_{n-2}^{r-2} \sum_{1 \leq k \leq n} a_k.$$

Cette formule montre que a_i appartient à $\mathbb{Q}(S)$ et donc que K est contenu dans $\mathbb{Q}(S)$. Inversement il est clair que $\mathbb{Q}(S)$ est contenu dans K. D'où le lemme.

Proposition 7.1. *Soit f_m le polynôme unitaire (à coefficients dans $\mathbb{C}$) dont les racines sont les éléments de S : c'est un polynôme à coefficients dans $\mathbb{Z}$. Supposons que le groupe de Galois de f soit isomorphe à $\mathbb{A}_n$. Alors f_m est irréductible sur $\mathbb{Q}$.*

Démonstration : Le polynôme f_m est à coefficients dans $\mathbb{Z}$: en effet, les a_i sont des entiers algébriques et un élément de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ laisse stable S. D'après le lemme précédent et l'hypothèse faite sur f, le groupe de Galois de f_m est isomorphe à $\mathbb{A}_n$. Supposons $r \leq n-2$. Puisque le groupe $\mathbb{A}_n$ est $n-2$-transitif sur $X = \{1, 2, ..., n\}$, le groupe de Galois de f_m agit transitivement sur les racines de f_m. Cela entraîne que f_m

est irréductible sur $\mathbb{Q}$. Supposons maintenant $r = n - 1$. Dans ce cas, en utilisant le fait que $\mathbb{A}_n$ est transitif, on constate que $\mathbb{A}_n$ agit transitivement sur l'ensemble des parties *non ordonnées* à $n-1$ éléments de X. Ainsi $\mathbb{A}_n$ agit encore transitivement sur les racines de f_m. D'où la proposition.

On déduit de là le résultat suivant :

Corollaire 7.1. *Supposons que f soit le polynôme $X^7 + aX + b \in \mathbb{Z}[X]$, où a et b sont deux entiers relatifs, et que les conditions suivantes soient réalisées :*
1) le dicriminant de f est un carré dans $\mathbb{Z}$;
2) le polynôme f possède exactement trois racines réelles ;
3) le polynôme f_{35} est réductible sur $\mathbb{Q}$.
Alors le groupe de Galois de f est isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$.

Démonstration : Il suffit d'utiliser les résultats précédents avec $r = 3$ (on a alors $m = 35$).

Fin de la démonstration du théorème 7.1

On constate que le polynôme f_{35} dans $\mathbb{Z}[X]$ est donné par

$$f_{35}(X) = X^{35} - 280X^{29} + 906X^{28} - 79086X^{23} - 56826X^{22} + 34452X^{21}$$

$$+1739696X^{17} + 408366X^{16} + 1139292X^{15} + 978750X^{14} - 12357947X^{11}$$

$$+1393266X^{10} - 9345672X^9 + 4975614X^8 - 592029X^7 + 29042496X^5$$

$$-12446784X^4 - 2222640X^3 + 1227744X^2 + 36288X - 31104.$$

Ce polynôme est réductible sur $\mathbb{Q}$: il est divisible par $X^7 + 14X^4 - 42X^2 - 21X + 9$. D'après le corollaire 7.1, le groupe de Galois de f est donc isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$. D'où le théorème.

Exercices. 1) Avec les notations du corollaire, supposons que (a, b) soit l'un des deux couples $(-154, 99)$ (cf. [3]) ou bien $(-448, 384)$. Montrer que le groupe de Galois de f est encore isomorphe à $\mathbb{PSL}_2(\mathbb{F}_7)$.
2) Montrer que le groupe de Galois de $X^7 - 56X + 48$ est isomorphe à $\mathbb{A}_7$.
3) Montrer que le groupe de Galois de $X^7 - 2$ est isomorphe à M_6 (d'ordre 42).

VIII . Le groupe alterné $\mathbb{A}_n$

Hilbert a démontré que, pour tout entier n$\geq$ 2, $\mathbb{A}_n$ est groupe de Galois sur $\mathbb{Q}$. Il serait interessant d'expliciter, pour tout entier $n \geq 2$, un polynôme irréductible sur $\mathbb{Q}$ dont le groupe de Galois soit isomorphe au groupe $\mathbb{A}_n$ (comme pour le groupe $\mathbb{S}_n$).

Signalons dans cette direction que Schur a démontré que si n est divisible par 4, le polynôme exponentiel tronqué,

$$\sum_{k=0}^{n} \frac{X^k}{k!},$$

a pour groupe de Galois $\mathbb{A}_n$.

Considérons un entier $n \geq 4$ *pair*. Soit f le polynôme à coefficients dans $\mathbb{Q}(T)$, en l'indéterminée X, donné par

$$h_n(X,T) = (n-1)X^n - nX^{n-1} + 1 + (-1)^{\frac{n}{2}}(n-1)T^2.$$

On peut démontrer que f est irréductible sur $\mathbb{Q}(T)$ et que son groupe de Galois sur $\mathbb{Q}(T)$ est isomorphe à $\mathbb{A}_n$. Il existe une infinité de $t \in \mathbb{Q}$, qui dépend de n, tels que l'équation $h_n(X,t) = 0$ soit irréductible sur $\mathbb{Q}$ et de groupe de Galois $\mathbb{A}_n$. Signalons les deux questions suivantes :

Question 1. *Pour tout nombre rationnel $t \in \mathbb{Q}$ non nul, le polynôme $h_6(X,t)$ est-il irréductible sur $\mathbb{Q}$ de groupe de Galois $\mathbb{A}_6$?*

Soit t un nombre rationnel non nul. Après un changement de variables, on se ramène à l'étude du polynôme

$$f_t = X^6 - 6X^5 + 3125(1 - 5t^2).$$

Question 2. *Pour tout entier n pair, peut-on prendre $t = 1$? Autrement dit, pour tout entier n pair, le polynôme $h_n(X,1)$ est-il irréductible sur $\mathbb{Q}$ de groupe de Galois $\mathbb{A}_n$?*

a) Si n est multiple de 4, on se ramène après un changement de variables à l'étude du polynôme

$$f_n = X^n - n^{n-1}X + n^{n-1}(n-1).$$

b) Si n n'est pas multiple de 4, on se ramène à l'étude du polynôme

$$g_n = X^n - n(2-n)^{n-2}X + (2-n)^{n-1}(n-1).$$

Avant de faire quelques remarques sur ces questions démontrons plusieurs résultats sur les sous-groupes transitifs de $\mathbb{S}_n$.

Quelques remarques sur les sous-groupes transitifs de $\mathbb{S}_n$

Considérons un entier $n \geq 2$. On note $X = \{1, ..., n\}$.

Lemme 8.1. *1) Soient k un entier ≥ 2 et G un sous-groupe transitif de $\mathbb{S}_n$. Alors G agit k fois transitivement sur X si et seulement si, pour tout a de X, le fixateur de a agit $k-1$ fois transitivement sur $X - \{a\}$.*

2) Soient k un entier ≥ 3 et G un sous-groupe 2-transitif de $\mathbb{S}_n$. Alors G agit k fois transitivement sur X si et seulement si, pour tout couple de points distincts a et b de X, le fixateur de a et b agit $k-2$ fois transitivement sur $X - \{a, b\}$.

Démonstration : 1) Supposons que G agisse k-fois transitivement sur X. Soient a un point de X et $(x_1, ..., x_{k-1})$, $(y_1, ..., y_{k-1})$ deux $k-1$-uplets de $X - \{a\}$. Il existe $g \in G$ tel que l'on ait $g(a) = a$ et $g(x_i) = y_i$, ce qui signifie que le fixateur de a agit $k-1$ fois transitivement sur $X - \{a\}$. Inversement, soient $(x_1, ..., x_k)$ et $(y_1, ..., y_k)$, deux k-uplets d'éléments de X. Soit par ailleurs a un élément de X. Puisque G est transitif, il existe α et β dans G tels que l'on ait $\alpha(x_1) = a$ et $\beta(y_1) = a$. Pour tout i compris entre 2 et k, posons $x'_i = \alpha(x_i)$ et $y'_i = \beta(y_i)$. Par hypothèse, il existe un élément g du fixateur de a tel que l'on ait $g(a, x'_2, ..., x'_k) = (a, y'_2, ..., y'_k)$. On vérifie que l'on a alors l'égalité $\beta^{-1} g \alpha(x_1, ..., x_k) = (y_1, ..., y_k)$. D'où le lemme.

2) La démonstration est analogue à celle de l'assertion 1) (le vérifier).

Lemme 8.2. *1) Soit G un sous-groupe transitif de $\mathbb{S}_n$. Il existe un point a de X tel que le fixateur de a soit transitif sur $X - \{a\}$ si et seulement si, pour tout point b de X, le fixateur de b est transitif sur $X - \{b\}$.*
2) Soit G un sous-groupe 2-transitif de $\mathbb{S}_n$. Il existe deux points distincts a et b de X tel que le fixateur de a et b soit transitif sur $X - \{a, b\}$ si et seulement si, pour tout couple de points distincts c et d de X, le fixateur de c et d est transitif sur $X - \{c, d\}$.

Démonstration : 1) Soit a un point de X tel que le fixateur de a soit transitif sur $X - \{a\}$. Soit b un point de X. Il existe g dans G tel que l'on ait $g(a) = b$. Soient c et d deux éléments de $X - \{b\}$. Puisque g transforme $X - \{a\}$ en $X - \{b\}$, les éléments $g^{-1}(c)$ et $g^{-1}(d)$ sont dans $X - \{a\}$. Il existe par hypothèse h dans le fixateur de a tel que l'on ait $h(g^{-1}(c)) = g^{-1}(d)$. D'où l'égalité $ghg^{-1}(c) = d$. Or ghg^{-1} est dans le fixateur de b. D'où l'assertion 1).

2) La démonstration est la même. Soient a et b deux points de X tels que le fixateur de a et b soit transitif sur $X - \{a, b\}$. Soient c et d deux points de X. Il existe g dans G tel que l'on ait $g(a) = c$ et $g(b) = d$ (car G est 2-transitif). Soient α et β deux éléments de $X - \{c, d\}$. Puisque g transforme $X - \{a, b\}$ en $X - \{c, d\}$, les éléments $g^{-1}(\alpha)$ et $g^{-1}(\beta)$ sont dans $X - \{a, b\}$. Il existe par hypothèse h dans le fixateur de a et b tel que l'on ait $h(g^{-1}(\alpha)) = g^{-1}(\beta)$. D'où l'égalité $ghg^{-1}(\alpha) = \beta$. Or ghg^{-1} est dans le fixateur de c et d. D'où le lemme.

Lemme 8.3. *Soit G un sous-groupe transitif de $\mathbb{S}_n$ contenant un $n-1$-cycle. Alors G est doublement transitif. Si de plus G contient une transposition, on a $G = \mathbb{S}_n$.*

Démonstration : Puisque G contient un $n-1$-cycle il existe un point élément a de X tel que le stabilisateur de a agisse transitivement sur $X - \{a\}$. Par hypothèse G est transitif, donc pour tout b dans X le stabilisateur de b agit aussi transitivement sur

$X - \{b\}$ (lemme 8.2). Cela entraîne le fait que G est 2-transitif (lemme 8.1). Par ailleurs il existe a et b dans X tel que la transposition (a, b) soit dans G. Soit (c, d) une autre transposition de $\mathbb{S}_n$. Il existe σ dans G tel que l'on ait $\sigma(a) = c$ et $\sigma(b) = d$. D'où $\sigma(a, b)\sigma^{-1} = (c, d)$ et (c, d) appartient à G. D'où le lemme.

Lemme 8.4. *Soit G un sous-groupe transitif de $\mathbb{A}_6$. Supposons que G contienne un 3-cycle et un 5-cycle. Alors on a $G = \mathbb{A}_6$.*

Démonstration : Puisque G est transitif et contient un 5-cycle, G est 2-transitif (lemme 8.3). Par ailleurs, G contient un 3-cycle (a, b, c). Soient alors d et e deux points distincts de $X = \{1, ..., 6\}$, et distincts de a, b et c. Notons G_d (resp. $G_{d,e}$) le fixateur de d (resp. le fixateur des deux points d et e). Puisque G est 2-transitif, G_d est transitif sur $X - \{d\}$, et l'on a

$$\mid G \mid = 6 \mid G_d \mid = 6.5 \mid G_{d,e} \mid .$$

Or $G_{d,e}$ contient le trois cycle (a, b, c) donc son ordre est divisible par 3. Ainsi l'ordre de G est divisible par 90 et l'indice de G dans $\mathbb{A}_6$ est inférieur où égal à 4. Cela entraîne le fait que $G = \mathbb{A}_6$. En effet, pour tout entier $n \geq 5$, un sous-groupe de $\mathbb{A}_n$ d'indice strictement plus petit que n est $\mathbb{A}_n$ tout entier (le vérifier). D'où le lemme.

Lemme 8.5. *Soit G un sous-groupe de $\mathbb{A}_n$. Alors si G est 3-transitif et contient un 3-cycle, on a $G = \mathbb{A}_n$.*

Démonstration : Il résulte de l'hypothèse faite que tous les 3-cycles sont dans G. Or $\mathbb{A}_n$ est engendré par les 3-cycles. D'où le lemme.

Quelques remarques sur les questions 1 et 2

On choisit désormais implicitement un plongement du groupe de Galois G du polynôme considéré dans $\mathbb{S}_n$.

1) Supposons $n = 6$. On a

$$g_6 = X^6 - 1536X - 5120.$$

Le discriminant de g_6 est $2^{54}.3^6.5^6$, donc G est contenu dans $\mathbb{A}_6$. Vérifions que g_6 est irréductible, autrement dit que G est transitif sur l'ensemble des racines de g_6. En réduisant g_6 modulo 7, on constate que $G = \mathrm{Gal}(g_6)$ possède un 5-cycle. Donc si G n'est pas transitif, il existe deux orbites de X sous l'action de G, dont une est réduite à un élément, en particulier il existe un point fixe de X sous l'action de G. Or la réduction de g_6 modulo 17 montre l'existence d'un produit de deux 3-cycles à supports disjoints dans G, et en particulier il n'existe pas de point fixe de X sous l'action de G (pour démontrer que X n'a pas de point fixe, on peut aussi évoquer le fait que g_6 n'a pas de

racine rationnelle : en effet une telle racine serait dans $\mathbb{Z}$ et devrait diviser 5120). Il existe ainsi une seul orbite, ce qui signifie que G est transitif. Par ailleurs, en réduisant g_6 modulo 47, on constate que G possède un 3-cycle. Cela prouve que $G = \mathbb{A}_6$ (lemme 8.4).

2) Supposons $n = 10$. On a

$$g_{10} = X^{10} - 167772160\ X - 1207959552.$$

Le discriminant de g_{10} est $2^{250}.3^{20}.5^{10}$ donc G est contenu dans $\mathbb{A}_{10}$.

En réduisant g_{10} modulo 7, on constate que $\mathrm{Gal}(g_{10})$ possède un 9-cycle. Donc si G n'est pas transitif, il existe deux orbites de X sous l'action de G, et il existe donc un point fixe de X sous l'action de G. Mais en réduisant g_{10} modulo 17, on constate que G possède un produit à supports disjoints d'un 2-cycle et d'un 6-cycle, et il ne peut alors y avoir de point fixe. Donc G est transitif, i.e. g_{10} est irréductible. On déduit aussi de là que G est 2-transitif (lemme 8.3).

Montrons en fait que G est 3-transitif. En réduisant g_{10} modulo 17, on constate qu'il existe un élément σ dans G dont la décomposition en produit de cycles à support disjoints est de la forme $(a, b, c, d, e, f)(g, h)$. Cet élément fixe deux points i et j, autrement dit σ est dans le fixateur $G_{i,j}$ des deux points i et j. On considère alors l'action du groupe $G_{i,j}$ sur l'ensemble $X - \{i, j\}$. Montrons que cette action est transitive, ce qui prouvera notre assertion (cf. lemmes 8.1 et 8.2). Supposons que ce ne soit pas le cas. Il y a alors deux orbites, une de cardinal 6 et une autre de cardinal 2 (il ne peut y avoir de point fixe). Puisque G est 2-transitif, pour tout point α et β de X, l'action de $G_{\alpha,\beta}$ sur $X - \{\alpha, \beta\}$ possède la même propriété (les fixateurs de deux couples de points sont conjugués). Or en réduisant g_{10} modulo 67, on constate qu'il doit exister une orbite de cardinal 5 et une autre de cardinal 3, ce qui conduit à une contradiction. D'où le fait que G soit 3-transitif.

Par ailleurs en réduisant g_{10} modulo 13, on constate qu'il existe un élément α dans G dont la décomposition en produit de cycles à supports disjoints est de la forme $(a, b)(c, d, e)(f, g, h, i)$. L'élément α^4 est un 3-cycle qui est dans G. D'où le fait que $G = \mathbb{A}_{10}$ (lemme 8.5).

3) On peut en fait démontrer, par des arguments analogues, que g_n est irréductible et de groupe de Galois $\mathbb{A}_n$ pour tout les entiers n non multiples de 4 et plus petit que 50.

Exercice. Montrer que g_{102} est irréductible de groupe de Galois $\mathbb{A}_{102}$.

4) En ce qui concerne la question 2, on peut démontrer que si t est un entier non nul compris entre -100 et 100, le polynôme g_t est irréductible de groupe de Galois $\mathbb{A}_6$.

Homotopie et Groupe fondamental

Soit X un espace topologique. On va associer à X une catégorie $\pi_1(X)$ dans laquelle tous les morphismes seront des isomorphismes. On appelle souvent $\pi_1(X)$ le groupoïde fondamental de X. En particulier, on va associer à chaque point x de X un groupe, noté $\pi_1(X, x)$, appelé groupe fondamental, ou groupe de Poincaré, de X en x. Ces groupes jouent un role crucial dans ce que l'on appelle la théorie de Galois des revêtements.

I. Homotopie des chemins

Commençons par définir la notion de chemin d'un espace topologique. On notera I l'intervalle $[0, 1]$.

Définition 1.1. *On appelle chemin de X une application continue α de l'intervalle I dans X. Les points $\alpha(0)$ et $\alpha(1)$ sont l'origine et l'extrémité du chemin. Si $\alpha(0) = \alpha(1) = a$, on dit que α est un lacet au point a.*

Soient x et y deux points de X. Définissons maintenant la relation d'équivalence d'homotopie, avec origine fixe et extrémité fixe, dans l'ensemble des chemins de X d'origine x et d'extrémité y.

Définition 1.2. *Soient x et y deux points de X. Soient α et β deux chemins de X ayant même origine x et même extrémité y. On dit que α est homotope à β (avec origine et extrémité fixes), s'il existe une application continue*

$$H : I \times I \to X$$

telle que pour tout s et t dans I l'on ait :

(i) $H(t, 0) = \alpha(t)$ *et* $H(t, 1) = \beta(t)$ *;*
(ii) $H(0, s) = x$ *et* $H(1, s) = y$.

On dit alors que H est une homotopie de α à β.

Remarque. Si pour tout s dans I l'on pose

$$\gamma_s(t) = H(t, s) \quad \text{pour} \quad t \in I,$$

on obtient une famille de chemins de X d'origine x et d'extrémité y, qui peut être vue comme une déformation continue de α à β, lorsque s parcourt I. La condition (i) signifie que, pour tout t dans I l'on a

$$\gamma_0(t) = \alpha(t) \quad \text{et} \quad \gamma_1(t) = \beta(t).$$

La condition (ii) exprime le fait que les extrémités $\alpha(0) = \beta(0) = x$ et $\alpha(1) = \beta(1) = y$ restent fixes au cours de la déformation : on a $\gamma_s(0) = x$ et $\gamma_s(1) = y$ pour tout s dans I.

Lemme 1.1. *La relation d'homotopie est une relation d'équivalence dans l'ensemble des chemins de X d'origine x et d'extrémité y.*

Démonstration : a) Cette relation est reflexive : Étant donné un chemin α de X, α est homotope à α via l'application $H : I \times I \to X$ définie, pour tout s et t dans I, par l'égalité

$$H(t, s) = \alpha(t).$$

b) Cette relation est symétrique : Soient α et β deux chemins de X. Soit H une homotopie de α à β. Alors l'application $G : I \times I \to X$ définie, pour tout s et t dans I, par l'égalité

$$G(t, s) = H(t, 1 - s),$$

est une homotopie de β à α.

c) Cette relation est transitive : Soient α, β et γ trois chemins de X. Soient F une homotopie de α à β et G une homotopie de β à γ. L'application $H : I \times I \to X$ définie, pour tout t et s dans I, par les égalités

$$H(t, s) = \begin{cases} F(t, 2s) & \text{si } 0 \leq s \leq 1/2 \\ G(t, 2s - 1) & \text{si } 1/2 \leq s \leq 1, \end{cases}$$

est une homotopie de α à γ ; en effet, on remarque d'abord que cette fonction est bien définie, car $F(t, 1) = G(t, 0) = \beta(t)$; par ailleurs, la restriction de H à chacun des sous-ensembles fermés $I \times [0, 1/2]$ et à $I \times [1/2, 1]$ est continue, donc H est aussi continue. Enfin on vérifie que l'on a $H(t, 0) = \alpha(t)$, $H(t, 1) = \gamma(t)$, $H(0, s) = x$ et $H(1, s) = y$. D'où le lemme.

Notation. *Si α est un chemin de X, on notera $[\alpha]$ sa classe d'équivalence d'homotopie.*

II. Composition des chemins

Commencons par définir, quand cela est possible, le composé de deux chemins de X.

Définition 2.1. *Soient $\alpha : I \to X$ et $\beta : I \to X$ deux chemins de X. Si l'extrémité $\alpha(1)$ coïncide avec l'origine $\beta(0)$, on peut définir un nouveau chemin, appelé le composé de α et β. Il s'agit du chemin $\gamma : I \to X$ défini, pour tout t de I, par les égalités*

$$\gamma(t) = \begin{cases} \alpha(2t) & \textit{si } 0 \leq t \leq 1/2 \\ \beta(2t - 1) & \textit{si } 1/2 \leq t \leq 1. \end{cases}$$

On notera $\gamma = \alpha \perp \beta$

Proposition 2.1. *a) La loi de composition des chemins est compatible avec la relation d'homotopie.*

b) La loi de composition qu'elle induit dans les classes de chemins est associative.

Démonstration : a) Considérons quatre chemins de X, f_0, f_1 ,g_0 et g_1 tels que f_0 et f_1 (resp. g_0 et g_1) soient homotopes. Soient F une homotopie de f_0 à f_1 et G une homotopie de g_0 à g_1. Il est immédiat de vérifier que l'application $H : I \times I \to X$ définie par

$$H(t,s) = \begin{cases} F(2t,s) & \text{si } 0 \leq t \leq 1/2 \\ G(2t-1,s) & \text{si } 1/2 \leq t \leq 1, \end{cases}$$

est une homotopie de $f_0 \perp g_0$ à $f_1 \perp g_1$.

b) Prouvons d'abord le lemme suivant :

Lemme 2.1. *Soient $k : I \to X$ un chemin de X et $\alpha : I \to I$ une application continue telle que $\alpha(0) = 0$ et $\alpha(1) = 1$. Alors les chemins k et $k \circ \alpha$ sont homotopes.*

Démonstration : On vérifie que l'application $H : I \times I \to X$ définie par

$$H(t,s) = k\big(s\ \alpha(t) + (1-s)t\big),$$

est une homotopie de k à $k \circ \alpha$.

Considérons alors $f : I \to X$, $g : I \to X$ et $h : I \to X$ trois chemins de X tels que $f(1) = g(0)$ et $g(1) = h(0)$. Il s'agit de prouver que les chemins $k_0 = (f \perp g) \perp h$ et $k_1 = f \perp (g \perp h)$ sont homotopes. On vérifie pour cela que l'on a

$$k_1 = k_0 \circ \alpha,$$

où $\alpha : I \to I$ est l'application continue définie comme suit : c'est l'unique application linéaire affine dans chacun des intervalles $[0, 1/2]$, $[1/2, 3/4]$, $[3/4, 1]$, telle que

$$\alpha(0) = 0, \quad \alpha(1/2) = 1/4, \quad \alpha(3/4) = 1/2, \quad \alpha(1) = 1.$$

Le lemme ci-dessus entraîne alors le résultat.

Les résultats précédents permettent de poser la définition suivante :

Définition 2.2. *Soient f un chemin de X d'origine x et d'extrémité y, et g un autre chemin d'origine y et d'extrémité z. Soit $\varphi = [f]$ la classe de f et $\psi = [g]$ la classe de g. On dira que x (resp. y) est l'origine (resp. l'extrémité) de la classe φ. Supposons que l'on ait $\varphi(1) = \psi(0)$. La classe du chemin composé $f \perp g$ est alors bien définie. La composée des classes φ et ψ est par définition la classe du chemin composé $f \perp g$. On notera dans cet ordre $\varphi.\psi$ la composée des classes φ et ψ. Si ϵ est une classe de chemin telle que $\psi(1) = \epsilon(0)$, on a les égalités*

$$(\varphi.\psi).\epsilon = \varphi.(\psi.\epsilon).$$

On notera alors simplement $\varphi.\psi.\epsilon$ la composée de ces trois classes.

Lemme 2.2. *Soit ϵ la classe d'un chemin constant $e : I \to X$: par définition il existe a dans X tel que l'on ait $e(t) = a$ pour tout t de I. Soient φ et ψ deux classes de chemins de X telles que $\varphi(1) = a$ et $\psi(0) = a$. Soient f (resp. g) un représentant de φ (resp. de ψ). On a alors*

$$\varphi.\epsilon = \varphi \quad et \quad \epsilon.\psi = \psi.$$

Démonstration : Vérifions par exemple que l'on a $\epsilon.\psi = \psi$. Il s'agit de vérifier que les chemins $e \perp g$ et g sont homotopes. D'après le lemme précédent, il suffit pour cela de remarquer que l'on a $e \perp g = g \circ \alpha$, où α est l'application continue de I dans I définie par

$$\alpha(t) = \begin{cases} 0 & \text{si } 0 \leq t \leq 1/2 \\ 2t - 1 & \text{si } 1/2 \leq t \leq 1. \end{cases}$$

L'égalité $\varphi.\epsilon = \varphi$ se démontre d'une manière analogue. D'où le résultat.

III. Le groupoïde fondamental de X

On va associer à X une *catégorie*, notée $\pi_1(X)$, que l'on appelle le groupoïde fondamental de l'espace X.

La catégorie $\pi_1(X)$

Il s'agit tout d'abord de définir les *objets* et les *morphismes* entre deux objets de cette catégorie. Par définition, les objets de $\pi_1(X)$ sont les points de X. On notera $\pi_1(X; x, y)$ l'ensemble des morphismes de x dans y. On le définit comme suit :

Définition 3.1. *Un élément de $\pi_1(X; x, y)$ est une classe d'homotopie de chemins d'origine x et d'extrémité y.*

Il s'agit ensuite de se donner pour tout x, y et z dans X une loi de composition

$$\pi_1(X; x, y) \times \pi_1(X; y, z) \to \pi_1(X; x, z).$$

On prend par définition l'application qui à (φ, ψ) dans $\pi_1(X; x, y) \times \pi_1(X; y, z)$ associe la classe composée $\varphi.\psi$.

Ces définitions satisfont aux axiomes d'une catégorie. En effet, la loi de composition des morphismes est associative d'après la proposition. Par ailleurs, si x est un point de X, i.e. un objet de $\pi_1(X)$, la classe du lacet constant en x est un élément neutre de $\pi_1(X; x, x)$. On notera désormais ϵ_x cet élément neutre. D'où le fait que $\pi_1(X)$ soit une catégorie.

Notation. *Étant un point x de X, on notera $\pi_1(X, x)$ l'ensemble $\pi_1(X; x, x)$. C'est l'ensemble des classes de lacets de X d'origine x.*

Théorème 3.1. *Dans la catégorie $\pi_1(X)$, tous les morphismes sont des isomorphismes. En particulier, pour tout point x de X, la loi de composition définie ci-dessus munit $\pi_1(X,x)$ d'une structure de groupe, dont l'élément neutre est la classe du lacet constant en x. L'inverse de la classe d'un lacet c est la classe du lacet qui à t dans I associe $c(1-t)$.*

Démonstration : Soit $f : I \to X$ un chemin de X d'origine x et d'extrémité y. Soit φ la classe de f dans $\pi_1(X; x, y)$. Il s'agit de démontrer l'existence d'un inverse de φ, c'est-à-dire d'un élément ψ de $\pi_1(X; y, x)$ tel que $\varphi.\psi = \epsilon_x$ et $\psi.\varphi = \epsilon_y$. Considérons pour cela le chemin $g : I \to X$ défini par l'égalité

$$g(t) = f(1-t)$$

(g est le chemin f parcouru en sens inverse). On va prouver que la classe de g est inverse de φ, autrement dit que le chemin $f \perp g$, qui est un lacet de X en x, est homotope au lacet constant en x. Il suffit de vérifier que l'application $H : I \times I \to X$ définie par

$$H(t,s) = \begin{cases} f(2ts) & \text{si } \ 0 \leq t \leq 1/2 \\ f(2s - 2ts) & \text{si } 1/2 \leq t \leq 1, \end{cases}$$

est une homotopie du lacet constant en x à $f \perp g$, ce qui résulte des définitions. Cela prouve que f est un isomorphisme. D'où le théorème.

Notation. *Étant donné φ un élément de $\pi_1(X,x)$, on notera φ^{-1} l'inverse de φ.*

Définition 3.2. *Le groupe $\pi_1(X,x)$ s'appelle le groupe fondamental de X en x.*

Proposition 3.1. *Soient x et y deux points de X qui appartiennent à une même composante connexe par arcs de X. Alors les groupes $\pi_1(X,x)$ et $\pi_1(X,y)$ sont isomorphes : on choisit un élément α de $\pi_1(X; x, y)$ et l'application $\pi_1(X,x) \to \pi_1(X,y)$ définie par*

$$\lambda \mapsto \alpha^{-1}.\lambda.\alpha,$$

est un isomorphisme de groupes de $\pi_1(X,x)$ sur $\pi_1(X,y)$. En particulier, si X est connexe par arcs, tous les groupes fondamentaux relatifs aux différents points de X sont isomorphes.

Démonstration : Cette application est un homomorphisme de groupes : soient λ et μ deux éléments de $\pi_1(X,x)$. D'après les résultats précédents on a l'égalité

$$\alpha^{-1}.(\lambda.\mu.)\alpha = (\alpha^{-1}.\lambda.\alpha).(\alpha^{-1}.\mu.\alpha),$$

ce qui prouve notre assertion. Cet homomorphisme est bijectif : l'homomorphisme de $\pi_1(X,y)$ dans $\pi_1(X,x)$ défini par $\lambda' \mapsto \alpha.\lambda'.\alpha^{-1}$, est réciproque du précédent. D'où le résultat.

Remarques. 1) L'ensemble $\pi_1(X; x, y)$ peut être vide. En fait cet ensemble est non vide si et seulement si x et y appartiennent à une même composante connexe par arcs de l'espace X.

2) L'isomorphisme de $\pi_1(X, x)$ sur $\pi_1(X, y)$ dépend de la classe de chemin α que l'on a choisie pour le définir. Pour que deux éléments α et β de $\pi_1(X; x, y)$ définissent le même isomorphisme de $\pi_1(X, x)$ sur $\pi_1(X, y)$ il faut et il suffit que, pour tout λ de $\pi_1(X, x)$, l'on ait l'égalité

$$(\beta.\alpha^{-1}).\lambda.(\alpha.\beta^{-1}) = \lambda.$$

On déduit de là le résultat suivant :

Proposition 3.2. *Soient x et y deux points de X qui appartiennent à une même composante connexe par arcs de X. Pour que l'isomorphisme de $\pi_1(X, x)$ sur $\pi_1(X, y)$ défini par un élément α de $\pi_1(X; x, y)$ soit indépendant du choix de α, il faut et il suffit que tout automorphisme intérieur du groupe $\pi_1(X, x)$ soit l'identité, c'est-à-dire que $\pi_1(X, x)$ soit commutatif.*

Démonstration : En effet, d'après la remarque 2), la condition demandée dans l'énoncé se traduit par le fait que l'on ait $\gamma.\lambda.\gamma^{-1} = \lambda$ pour tout λ et γ dans $\pi_1(X, x)$.

IV. Détermination du groupe fondamental de $\mathbb{S}^1$

Soit $\mathbb{S}^1$ le cercle unité de $\mathbb{R}^2$. On note $\exp : \mathbb{R} \to \mathbb{S}^1$ l'application définie par l'égalité $\exp(t) = \exp(2\pi i t)$. Passée au quotient elle induit un homéomorphisme de $\mathbb{R}/\mathbb{Z}$ sur $\mathbb{S}^1$.

Lemme 4.1. *Le cercle $\mathbb{S}^1$ est connexe par arcs.*

Démonstration : Soient x_0 et x_1 deux points de $\mathbb{S}^1$. On choisit t_0 et t_1 deux nombres réels tels que l'on ait $\exp(2\pi i t_0) = x_0$ et $\exp(2\pi i t_1) = x_0$. Soit $f : I \to \mathbb{R}$ l'application linéaire affine définie par les égalités $f(0) = t_0$ et $f(1) = t_1$: on a $f(t) = (t_1 - t_0)t + t_0$. L'application $\exp \circ f : I \to \mathbb{S}^1$ est alors un chemin de $\mathbb{S}^1$ d'origine x_0 et d'extrémité x_1. D'où le résultat.

Lemme 4.2. *Soient x et y deux nombres réels. L'ensemble $\pi_1(\mathbb{R}; x, y)$ est de cardinal* 1.

Démonstration : Considérons deux chemins f et g de $\mathbb{R}$ d'origine x et d'extrémité y : on a $f(0) = g(0) = x$ et $f(1) = g(1) = y$. L'application

$$H : I \times I \to \mathbb{R},$$

qui au couple (t, s) associe $(1 - s)f(t) + sg(t)$ est continue et définit une homotopie de f à g : on a en effet, $H(t, 0) = f(t)$, $H(t, 1) = g(t)$, $H(0, s) = x$ et $H(1, s) = y$. D'où le lemme.

Considérons alors un entier relatif n. L'ensemble $\pi_1(\mathbb{R}; 0, n)$ ayant un seul élément, cet élément est nécessairement la classe du chemin $f : I \to \mathbb{R}$ défini par $f(t) = nt$. L'application $\exp \circ f : I \to \mathbb{S}^1$ est alors un lacet de $\mathbb{S}^1$ d'origine 1.

Lemme 4.3. *Si l'on remplace f par un chemin homotope g (ayant donc comme origine 0 et extrémité n), les chemins $\exp \circ f$ et $\exp \circ g$ sont homotopes.*

Démonstration : En effet, si $G : I \times I \to \mathbb{R}$ est une homotopie de f à g, on vérifie que l'application $\exp \circ G : I \times I \to \mathbb{S}^1$ définit une homotopie de $\exp \circ f$ à $\exp \circ g$.

Proposition 4.1. *L'application $\Phi : \mathbb{Z} \to \pi_1(\mathbb{S}^1, 1)$ définie par*

$$n \mapsto [\exp \circ f],$$

réalise un isomorphisme de groupes de $\mathbb{Z}$ sur $\pi_1(\mathbb{S}^1, 1)$.

Démonstration : 1) Montrons d'abord que Φ est un homomorphisme de groupes. Soient n_1 et n_2 deux entiers relatifs. On considère les chemins γ_1, γ_2 et γ de $\mathbb{R}$ définis par les égalités

$$\gamma_1(t) = n_1 t, \quad \gamma_2(t) = n_2 t + n_1 \quad \text{et} \quad \gamma(t) = (n_1 + n_2)t.$$

On peut composer les chemins γ_1 et γ_2 de sorte que $\gamma_1 \perp \gamma_2$ soit un chemin de $\mathbb{R}$ d'origine 0 et d'extrémité $n_1 + n_2$. Puisque $\pi_1(\mathbb{R}; 0, n)$ a un seul élément, le chemin composé $\gamma_1 \perp \gamma_2$ est homotope au chemin γ, autrement dit l'on a

$$[\gamma_1 \perp \gamma_2] = [\gamma]. \tag{1}$$

On déduit de (1) l'égalité dans $\pi_1(\mathbb{S}^1; 0, n_1 + n_2)$

$$[\exp \circ (\gamma_1 \perp \gamma_2)] = [\exp \circ \gamma]. \tag{2}$$

Or on vérifie que l'on a (par définition)

$$\exp \circ \gamma_1 \perp \exp \circ \gamma_2 = \exp \circ (\gamma_1 \perp \gamma_2). \tag{3}$$

D'après les égalités (2) et (3) on a donc $[\exp \circ \gamma] = [\exp \circ \gamma_1].[\exp \circ \gamma_2]$. Or par définition de Φ, on a $[\exp \circ \gamma] = \Phi(n_1 + n_2)$ et $[\exp \circ \gamma_1] = \Phi(n_1)$. Par ailleurs, on vérifie aussi immédiatement que l'on a $[\exp \circ \gamma_2] = \Phi(n_2)$, ce qui prouve notre assertion.

2) Le fait que Φ soit une bijection de $\mathbb{Z}$ sur $\pi_1(\mathbb{S}^1, 1)$ provient du résultat suivant qui sera démontré ultérieurement dans le cadre de la théorie des revêtements d'un espace topologique.

Proposition 4.2. *a) Pour tout lacet $g : I \to \mathbb{S}^1$ tel que $g(0) = g(1) = 1$, il existe un (unique) chemin $f : I \to \mathbb{R}$ tel que l'on ait $f(0) = 0$ et $\exp \circ f = g$.*

b) Si f_0 et f_1 sont deux chemins $I \to \mathbb{R}$ tels que $f_0(0) = f_1(0) = 0$, et si $g_0 = \exp \circ f_0$ et $g_1 = \exp \circ f_1$ sont des lacets homotopes, alors les chemins f_0 et f_1 ont même extrémité : on a $f_0(1) = f_1(1)$.

La surjectivité de Φ résulte en fait de l'assertion a) et l'injectivité de l'assertion b).

On déduit du résultat précédent que $\mathbb{S}^1$ n'est pas simplement connexe. Par ailleurs, $\mathbb{S}^1$ étant connexe par arcs, et $\pi_1(\mathbb{S}^1, 1)$ étant abélien, les groupes fondamentaux de $\mathbb{S}^1$ relatifs à deux de ses points sont canoniquement isomorphes. On peut montrer en revanche que pour tout $n \geq 2$, la sphère unité $\mathbb{S}^n$ dans $\mathbb{R}^{n+1}$ est simplement connexe (bien qu'elle ne soit pas contractile).

Théorie des revêtements d'un espace topologique

I. Revêtements triviaux

Soient X et B deux espaces topologiques et $p : X \to B$ une application continue. Étant donné un point b de B, l'espace $p^{-1}(b)$ s'appelle la fibre de X au-dessus de b.

Définition 1.1. *On dit que $p : X \to B$ est un revêtement trivial s'il existe un espace topologique discret F tel que l'on ait $X = B \times F$ et que $p : B \times F \to B$ soit l'application de projection.*

Supposons qu'il en soit ainsi. Pour chaque élément f de F on dispose alors du sous-espace $X_f = B \times \{f\}$ de $X \times F$, qui est un ouvert et un fermé de $B \times F$. Ainsi $B \times F$ est réunion des sous-espaces ouverts disjoints X_f. La restriction de p à X_f induit un homéomorphisme de X_f sur B. Les espaces X_f s'appellent les *feuillets* du revêtement trivial.

Définition 1.2. *On appelle B-automorphisme d'un revêtement trivial $p : B \times F \to B$ tout homéomorphisme $f : B \times F \to B \times F$ tels que l'on ait $p \circ f = p$.*

Lorsque B est *connexe*, le résultat suivant décrit tous les automorphismes d'un revêtement trivial $B \times F \to B$.

Proposition 1.2. *Supposons B connexe. Pour tout B-automorphisme f d'un revêtement trivial $p : B \times F \to B$, il existe une permutation τ de l'ensemble F telle que l'on ait*

$$f(x, y) = \big(x, \tau(y)\big) \quad \textit{pour tout } (x, y) \textit{ de } B \times F.$$

En particulier un B-automorphisme permute les feuillets du revêtement trivial.

Démonstration : Elle résulte du lemme suivant :

Lemme 1.1. *Sans hypothèse particulière sur B, les B-automorphismes d'un revêtement trivial $B \times F \to B$ sont de la forme*

$$(x, y) \mapsto \big(x, \sigma(x, y)\big),$$

où $\sigma : B \times F \to F$ est une application continue telle que, pour tout x dans B, l'application $\sigma_x : F \to F$ définie par

$$\sigma_x(y) = \sigma(x, y),$$

soit une bijection de F sur F.

Démonstration : Soit f un B-automorphisme d'un revêtement trivial $B \times F \to B$. Puisque l'on a $p \circ f = p$, il existe nécessairement une application $\sigma : B \times F \to F$ telle que

l'on ait, pour tout (x, y) de $B \times F$, $f(x, y) = \big(x, \sigma(x, y)\big)$. Puisque f est continue (par hypothèse), l'application σ aussi (on compose avec la deuxième projection). Par ailleurs, pour tout x dans B, σ_x est une bijection de F sur F, car f est une bijection de $B \times F$ sur $B \times F$. Inversement, une application $f : B \times F \to B \times F$ satisfaisant aux conditions de l'énoncé du lemme, est un B-automorphisme du revêtement trivial $B \times F \to B$: il est clair qu'une telle application commute à la première projection. Montrons que f est un homéomorphisme de $B \times F$ sur $B \times F$. Soient u et v deux éléments de F et $A_{u,v}$ le sous-ensemble de B formé des éléments b tels que l'on ait $\sigma(b, v) = u$. L'ensemble $A_{u,v}$ est un ouvert de B (considérer l'application de B dans F qui à z associe $\sigma(z, v)$). Par ailleurs $B \times F$ est la réunion disjointe des ensembles $A_{u,v} \times \{v\}$, ainsi que la réunion disjointe des ensembles $A_{u,v} \times \{u\}$, lorsque u et v parcourent F. Or pour tout b dans $A_{u,v}$, on a $f(b, v) = (b, u)$, de sorte que f induit un homéomorphisme de $A_{u,v} \times \{v\}$ sur $A_{u,v} \times \{u\}$. D'où le lemme.

On déduit alors la proposition de la façon suivante : pour tout y dans F, l'application $B \to F$ définie par $x \mapsto \sigma_x(y)$ est localement constante, car F est discret. Si B est connexe, elle est constante. Il existe donc une permutation τ de F tel que l'on ait $\tau = \sigma_x$ pour tout x de B. D'où la proposition.

Définition 1.3. *On dit que $p : X \to B$ est un revêtement trivialisable de base B s'il est B-isomorphe à un revêtement trivial $B \times F \to B$, autrement dit, s'il existe un espace discret F et un homéomorphisme $f : B \times F \to X$, de $B \times F$ sur X, tel que $p \circ f : B \times F \to B$ soit l'application de première projection. Un tel homéomorphisme f s'appelle une trivialisation du revêtement p.*

On notera que si B est *connexe*, on peut définir les *feuillets* d'un revêtement trivialisable $p : X \to B$. En effet, si $f : B \times F \to X$ est une trivialisation de p, ce sont les images par f des feuillets de $B \times F$, qui ne sont autres si B est connexe, que les composantes connexes de X.

II. Revêtements

Soient X et B deux espaces topologiques et $p : X \to B$ une application continue.

Définition 2.1. *Soit A un sous-espace de B. On dit que A est trivialisant pour p si l'application $p : p^{-1}(A) \to A$, qui est la restriction de p à $p^{-1}(A)$, est un revêtement trivialisable.*

On notera que dans cette définition rien n'interdit l'éventualité où $p^{-1}(A)$ est vide : si $p^{-1}(A)$ est vide, A est trivialisant pour p.

Lemme 2.1. *Soit A un sous-espace de B. Alors, A est trivialisant pour p si et seulement si $p^{-1}(A)$ est réunion d'une famille de sous-ensembles V_α, ouverts dans $p^{-1}(A)$, deux à*

deux disjoints, tels que la restriction de p à chaque V_α soit un homéomorphisme de V_α sur l'espace A.

Démonstration : 1) Supposons que A soit trivialisant pour p. Soient F un espace discret et $f : A \times F \to p^{-1}(A)$ une trivialisation de $p : p^{-1}(A) \to A$. Étant donné α un élément de F, posons $V_\alpha = f\big(A \times \{\alpha\}\big)$. Puisque $A \times \{\alpha\}$ est un ouvert de $A \times F$, les V_α sont des ensembles ouverts de $p^{-1}(A)$, et il est clair qu'ils sont deux à deux disjoints. Par ailleurs, la première projection induisant un homéomorphisme de $A \times \{\alpha\}$ sur A, p induit aussi un homéomorphisme de V_α sur A.

2) Inversement, soit F l'ensemble des indices α indexant la famille des ensembles V_α. On munit F de la topologie discrète. Considérons alors l'application

$$f : A \times F \to p^{-1}(A),$$

définie par $f(x, \alpha) = y$, où y est l'unique élément de V_α tel que $p(y) = x$. Montrons que f est une trivialisation de p. D'abord la condition de commutativité $p \circ f = p_1$ (où p_1 est la première projection) est réalisée. Par ailleurs la restriction de f à chacun des sous-ensembles ouverts $A \times \{\alpha\}$ est un homéomorphisme de $A \times \{\alpha\}$ sur V_α. Cela entraîne notre assertion. D'où le lemme.

Remarque. Si A est un sous-espace de B trivialisant pour p, tout sous-espace A' de A est aussi trivialisant pour p : en effet, si $f : A \times F \to p^{-1}(A)$ est une trivialisation de $p : p^{-1}(A) \to A$, la restriction de f à $A' \times F$ induit une trivialisation de $p : p^{-1}(A') \to A'$.

Définition 2.2. *On dit que $p : X \to B$ est un revêtement de base B si tout point de B possède un voisinage U trivialisant pour p. Quitte à remplacer U par son intérieur, on peut supposer que U est ouvert. Ainsi $p : X \to B$ est un revêtement de base B si et seulement si l'on peut recouvrir B par des ouverts trivialisants.*

Soit U un ouvert trivialisant d'un revêtement $p : X \to B$. D'après le lemme 2.1, il existe donc des ouverts V_α de X, deux à deux disjoints, dont la réunion est $p^{-1}(U)$, tels que p induise un homéomorphisme de V_α sur U. Supposons de plus que U soit *connexe*. Alors, commme on l'a déjà constaté, les ensembles V_α sont nécessairement les composantes connexes de $p^{-1}(U)$. Ce sont les feuillets du revêtement p au-dessus de l'ouvert U.

Remarque. Un revêtement $p : X \to B$ est un homéomorphisme local : cela résulte directement de la définition. On notera qu'un homéomorphisme local n'est pas toujours un revêtement : par exemple, soient D le disque unité ouvert de $\mathbb{C}$ et $p : D \to \mathbb{C}$ l'injection canonique. Cette application est un homéomorphisme local mais n'est pas un revêtement : un nombre complexe de module 1 ne possède pas de voisinage ouvert trivialisant pour p.

Proposition 2.1. *Soit $p : X \to B$ un revêtement. Alors p est une application ouverte.*

Démonstration : Soit x un élément de X; Posons $y = p(x)$. Soit V un voisinage de x dans X. Il s'agit de voir que $p(V)$ est un voisinage de y dans B. Soit U un ouvert trivialisant de B contenant y. Posons $V' = p^{-1}(U) \cap V$. Alors V' est un voisinage de x et V' est contenu dans $p^{-1}(U)$. On peut donc supposer au départ que V est contenu dans l'image réciproque d'un ouvert trivialisant. On se ramène ainsi au cas où p est un revêtement trivialisable, puis trivial. L'assertion est alors claire dans ce cas.

Proposition 2.2. *Soit $p : X \to B$ un revêtement dont la base B est connexe. Alors toutes les fibres sont des espaces discrets homéomorphes entre eux.*

Démonstration : D'abord puisque l'on peut recouvrir B par des ouverts trivialisants, toutes les fibres de p sont des espaces discrets. Montrons maintenant que ces espaces sont homéomorphes entre eux. On considère pour cela un espace discret F. Soit B' le sous-ensemble de B formé des éléments b de B tels que la fibre $p^{-1}(b)$ soit homéomorphe à F. Puisque B est connexe, il suffit de montrer que B' est ouvert et fermé dans B. Soit b un élément de B'. On considère un ouvert trivialisant U de B contenant b : il résulte des définitions que U est contenu dans B', ce qui prouve que B' est ouvert. Montrons que B' est fermé. Soit b un point dans l'adhérence de B'. Soit U un ouvert trivialisant contenant b. Alors (par définition) U rencontre B'. Or les fibres de tous les points de U sont homéomorphes. Donc U est contenu dans B', et en particulier b appartient à B'. D'où le résultat.

Corollaire 2.2. *Si B est connexe et si X est non vide, p est surjective.*

Démonstration : Cela résulte du fait que le cardinal des fibres des points de B est constant (car B est connexe) et comme X est non vide, il y a au moins une fibre non vide.

Exemples de revêtements

1) Soit k un entier ≥ 1 et $p_k : \mathbb{C}^* \to \mathbb{C}^*$ l'application définie par $p_k(z) = z^k$; vérifions que p_k est un revêtement. Soit b un élément de $\mathbb{C}^*$. Considérons un élément a de $\mathbb{C}^*$ tel que $p_k(a) = b$. Choisissons un nombre $\epsilon > 0$ tel que, pour toute racine k-ième de l'unité ζ autre que 1, l'on ait l'inégalité

$$\epsilon < \frac{\mid a \mid\mid \zeta - 1 \mid}{2}.$$

Soit alors V_0 la boule ouverte de centre a et de rayon ϵ. Si ζ est une racine k-ième de l'unité, la boule ouverte de centre ζa et de rayon ϵ est l'ensemble des ζz, où z parcourt V_0. Posons, pour α compris entre 0 et $k-1$, $V_\alpha = \exp(2\pi i\alpha/k)V_0$. D'après le choix de ϵ, les ensembles V_α sont des ouverts disjoints deux à deux. Par ailleurs si l'on pose $p_k(V_0) = U$,

p_k est un homéomorphisme de V_0 sur U (p_k est holomorphe), et $p_k^{-1}(U)$ est la réunion des V_α. Cela montre que U est un ouvert trivialisant pour p_k contenant b. D'où notre assertion.

2) Soit k un entier ≥ 1. L'application $p_k : \mathbb{C}^* \to \mathbb{C}$ définie par $p_k(z) = z^k$ n'est pas un revêtement (cf. le corollaire 2.2).

3) L'application exp : $\mathbb{C} \to \mathbb{C}^*$, qui à z associe e^z, est un revêtement. En effet, soit b un élément de $\mathbb{C}^*$. L'application exp est surjective : il existe a dans $\mathbb{C}$ tel que $\exp(a) = b$. Par ailleurs, il existe un voisinage ouvert V_0 de a tel que exp induise un homéomorphisme de V_0 sur $\exp(V_0)$: il suffit de prendre pour V_0 une boule ouverte de centre a et de rayon $< \pi$; étant injective sur V_0, et holomorphe, l'application exp réalise alors un homéomorphisme de V_0 sur son image U. Étant donné n dans $\mathbb{Z}$, posons $V_n = V_0 + 2\pi in$. Tous les V_n sont disjoints, et pour la même raison que ci-dessus, exp est un homéomorphisme de V_n sur U. Par ailleurs, $\exp^{-1}(U)$ est la réunion des V_n. D'où le résultat.

4) L'application exp : $\mathbb{R} \to \mathbb{S}^1$, qui à t associe $\exp(2\pi it)$, est un revêtement. En effet, soit b un élément de $\mathbb{S}^1$. Il suffit de montrer que $\mathbb{S}^1 - \{b\}$ est un ouvert trivialisant pour exp (cela montrera que $\mathbb{S}^1$ peut être recouvert par des ouverts trivialisants pour exp). L'image réciproque de b par exp est formée des translatés entiers d'un réel a. L'image réciproque de $\mathbb{S}^1 - \{b\}$ est donc une réunion disjointes d'intervalles ouverts de longueur 1, l'application exp induisant sur chacun d'entre eux un homéomorphisme sur $\mathbb{S}^1 - \{b\}$. D'où le résultat.

Le résultat suivant fournit de nombreux exemples de revêtements :

Proposition 2.3. *Soient X et B deux espaces topologiques. On suppose que X est séparé. Soit $p : X \to B$ un homéomorphisme local, tel que pour tout élément b de B la fibre $p^{-1}(b)$ soit finie de cardinal constant indépendant de b. Alors p est un revêtement.*

Démonstration : Soit b un élément de B. Pour tout x dans $p^{-1}(b)$, il existe un voisinage ouvert V_x de x tel que p soit un homéomorphisme de V_x sur $p(V_x) = U_x$ (car p est un homéomorphisme local). Puisque X est séparé, on peut supposer que les ensembles V_x sont disjoints. Par ailleurs, puisque la fibre en b est finie, l'intersection des U_x lorsque x parcourt $p^{-1}(b)$, est un ouvert U de B, qui contient b. On peut ainsi supposer (quitte à diminuer les V_x) que pour tout x dans $p^{-1}(b)$, p induit un homéomorphisme de V_x sur U. Or les fibres de tous les points de U ayant même cardinal, l'image réciproque par p de U est la réunion des V_x. Cela montre que U est un ouvert trivialisant pour p qui contient b. D'où la proposition.

Exercice : Posons $X = \mathbb{C} - \{0, \pm i, \pm i\sqrt{2}\}$ et $B = \mathbb{C} - \{0, 1\}$. Montrer que l'application $p : X \to B$ définie par $p(z) = (z^2 + 1)^2$ est un revêtement.

Le paragraphe suivant fournit une nouvelle source d'exemples de revêtements.

III. Opération d'un groupe discret sur un espace topologique

Soient X un espace topologique et G un groupe discret qui opère à gauche sur X. Cela signifie que l'on s'est donné une application *continue*

$$\rho : G \times X \to X,$$

telle que pour tout g et g' dans G l'on ait

$$\begin{cases} \rho(e, x) = x \\ \rho(g, \rho(g', x)) = \rho(gg', x)), \end{cases}$$

où e est l'élément neutre de G. On note

$$\rho(g) : X \to X$$

l'application définie par $\rho(g)(x) = \rho(g, x)$. C'est un homéomorphisme de X sur X. On notera aussi gx l'image de x par $\rho(g)$.

Soit X/G l'espace quotient, muni de la topologie quotient. On note

$$\pi : X \to X/G$$

la surjection canonique. Par définition O est ouvert dans X/G si et seulement si $\pi^{-1}(O)$ est un ouvert de X. L'ensemble des ouverts de X qui sont stables par G s'identifie, via π, à l'ensemble des ouverts de X/G : en effet, soit U un ouvert de X stable par G. Vérifions que $\pi(U)$ est un ouvert de X/G. Cela revient à vérifier que $\pi^{-1}(\pi(U))$ est un ouvert de X. On démontre en fait que l'on a $\pi^{-1}(\pi(U)) = U$: soit x un élément de $\pi^{-1}(\pi(U))$. Par définition $\pi(x)$ est dans $\pi(U)$. Il existe donc $g \in G$ et $y \in U$ tels que l'on ait $x = gy$. Puisque U est stable par G, cela implique que x est dans U. D'où notre assertion (l'inclusion inverse est évidente). Inversement, soit O un ouvert de X/G. Il s'agit de voir que $\pi^{-1}(O)$ est stable par G, ce qui résulte de l'égalité $\pi(gx) = \pi(x)$, pour tout $x \in X$ et tout $g \in G$ (par définition). Notons enfin que si U est un ouvert de X, on a l'égalité

$$\pi^{-1}(\pi(U)) = \cup_{g \in G}\ gU, \tag{1}$$

ce qui montre en particulier que π est une application *ouverte*.

Définition 3.1. *On dit que G opère proprement sans point fixe si tout point x de X possède un voisinage ouvert U tel que les ouverts $\rho(g)(U)$ forment une famille d'ouverts disjoints lorsque g parcourt G.*

Tel est le cas pour le groupe $\mathbb{Z}$ qui opère sur $\mathbb{R}$ par translations entières. Plus généralement :

Lemme 3.1. *Soient X un groupe topologique et G un sous-groupe discret de X. Le groupe G opère sur X par translations à gauche. Avec cette opèration, G opère proprement sans point fixe sur X.*

Démonstration : Il suffit de vérifier qu'il existe un voisinage ouvert U de l'élément neutre e de G tel que les ouverts gU soient disjoints lorsque g parcourt G. Il suffit de démontrer l'existence d'un voisinage U de e tel que $U \cap gU = \emptyset$ pour tout $g \in G$ autre que e. Cela revient encore à prouver l'assertion suivante : il existe un voisinage ouvert U de e tel que, étant donnés deux éléments x et y de U, si yx^{-1} appartient à G, alors $x = y$. Puisque $\{e\}$ est ouvert, car G est discret, il existe par définition de la topologie induite de X sur G, un voisinage V de e dans X tel que l'on ait $V \cap G = \{e\}$. Par ailleurs, l'application $X \times X \to X$ définie par $(x, y) \mapsto yx^{-1}$ est continue au point (e, e), donc il existe un voisinage U de e dans X tel que l'image de $U \times U$ par cette application soit contenue dans V. D'où le lemme.

Proposition 3.1. *Supposons que G opère proprement sans point fixe sur X. Alors la surjection canonique $\pi : X \to X/G$ est un revêtement.*

Démonstration : Il s'agit de voir que l'on peut recouvrir X/G par des ouverts trivialisants. Soit y un élément de X/G. Il existe $x \in X$ tel que $\pi(x) = y$. Soit U un ouvert de X contenant x, tel que les ouverts $\rho(g)(U) = gU$ forment une famille d'ouverts disjoints lorsque g parcourt G (U existe par hypothèse). Puisque π est ouverte, $\pi(U)$ est un ouvert de X/G. On montre en fait que $\pi(U)$ est un ouvert trivialisant de X/G contenant y. Par hypothèse les ouverts gU lorsque g parcourt G sont disjoints, et pour tout $g \in G$ l'application π induit un homéomorphisme de gU sur $\pi(U)$: cela revient à vérifier que $\pi : U \to \pi(U)$ est un homéomorphisme. D'abord $\pi : U \to \pi(U)$ est injective d'après l'hypothèse faite sur l'opération de G sur X. Notre assertion provient alors du fait que π est ouverte. D'où le résultat d'après l'égalité (1).

Corollaire 3.1. *Soient X un groupe topologique, G un sous-groupe discret de X et X/G l'ensemble des classes à droites de X modulo G. L'application $\pi : X \to X/G$ est un revêtement. On a un énoncé analogue pour l'ensemble des classes à gauches.*

Démonstration : Étant donné un point $x \in X$, $\pi(x)$ est par définition la classe d'équivalence de x pour l'opération de G sur X par translations à gauche (ou bien par translations à droite). D'où l'assertion.

IV. Sections continues d'un revêtement

Définition 4.1. *Soit $p : X \to B$ une application continue. On appelle section continue de p toute application continue $s : B \to X$ tel que $p \circ s = id_B$. Soit U un ouvert de B. Une section locale au-dessus de U est une application continue $s : U \to X$ telle que $p \circ s = id_U$.*

Une section continue (globale) associe donc à chaque $b \in B$ un point $s(b)$ de la fibre $p^{-1}(b)$, et ceci de manière continue.

Lemme 4.1. *Soit $p : X \to B$ un revêtement. Soit U un ouvert trivialisant de p. Soient F un espace discret et $\varphi : U \times F \to p^{-1}(U)$ une trivialisation au-dessus de U. Les sections continues au-dessus de l'ouvert U correspondent bijectivement (de façon dépendante de φ) aux applications continues de U dans la fibre discrète F.*

Démonstration : Soit s une section continue au-dessus de U. Soit φ un homéomorphisme de $U \times F$ sur $p^{-1}(U)$. L'application $\varphi^{-1} \circ s : U \to U \times F$ est continue et est de la forme $b \mapsto (b, \sigma(b))$, où $\sigma : U \to F$ est une application continue (si p_1 est la première projection, on a $p_1 \circ \varphi^{-1} \circ s(b) = b$ car $s(b)$ est un point de la fibre $p^{-1}(b)$). Inversement, si f est une application continue de U fans F, l'application $x \mapsto (x, f(x)) \mapsto \varphi(x, f(x))$ est une section au-dessus de U. D'où le lemme.

On déduit ainsi de la démonstration du lemme que toute section continue $s : U \to X$ est de la forme $x \mapsto \varphi(x, f(x))$, où $f : U \to F$ est une application continue.

Corollaire 4.1. *Soit U un ouvert trivialisant de p. Toute section continue $s : U \to X$ est un homéomorphisme de U sur $s(U)$ (en particulier $s(U)$ est ouvert et fermé dans $p^{-1}(U)$). Si s_1 et s_2 sont deux sections continues $U \to X$, l'ensemble des points de U où s_1 et s_2 coïncident est un ouvert et un fermé de U.*

Démonstration : On déduit du lemme qu'une section au-dessus de U est une application ouverte. Puisque s est une injection de U dans $s(U)$, $s : U \to X$ est un homéomorphisme de U sur $s(U)$. Soient f_1 et f_2 les deux applications continues $U \to F$ qui correspondent respectivement à s_1 et s_2. L'ensemble des éléments x de U où s_1 et s_2 coïncident est l'ensemble des x de U tels que $f_1(x) = f_2(x)$ (dém. du lemme 4.1). C'est donc l'image réciproque de la diagonale de $F \times F$ par l'application continue $U \to F \times F$ qui à x associe $(f_1(x), f_2(x))$. Le corollaire résulte alors du fait que $F \times F$ est un ensemble discret.

On déduit des résulats précédents le résultat suivant :

Proposition 4.1. *Soit $p : X \to B$ un revêtement. Soit $s : B \to X$ une section continue de p. Alors s est un homéomorphisme de B sur $s(B)$; en particulier $s(B)$ est ouvert et fermé dans X. Si s_1 et s_2 sont deux sections continues $B \to X$, l'ensemble des points de B où s_1 et s_2 coïncident est un ouvert et un fermé de B.*

Démonstration : Le fait que s soit homéomorphisme de B sur $s(B)$ résulte de ce que l'on peut recouvrir B par des ouverts trivialisants. Le fait que l'ensemble des points de B où s_1 et s_2 coïncident soit ouvert et fermé résulte aussi du même argument (pour voir que cet ensemble est fermé on utilise le fait que si U est un ouvert trivialisant, l'ensemble des $b \in U$ tels que $s_1(b) \neq s_2(b)$ est un ouvert de U). D'où le résultat.

Corollaire 4.2. *Soit $p : X \to B$ un revêtement de base B connexe. Deux sections continues $B \to X$ qui prennent la même valeur en un point de B sont identiques.*

Démonstration : C'est immédiat d'après la proposition 4.1.

Proposition 4.2. *Soit $p : X \to B$ un revêtement tel que X soit connexe (et B non vide). Il n'y a pas de section continue $B \to X$ sauf si p est un homéomorphisme.*

Démonstration : Soit $s : B \to X$ une section continue de p. Puisque X est connexe, on a $s(B) = X$ (proposition 4.1) et s est un homéomorphisme de B sur X, et p est nécessairement l'homéomorphisme réciproque. D'où l'assertion.

V. Image réciproque d'un revêtement

Considérons X, B, B' trois espaces topologiques et $p : X \to B$ un revêtement. On se donne par ailleurs une application continue $g : B' \to B$. On note X' le sous-espace de $B' \times X$ formé des éléments (b', x) tels que l'on ait $g(b') = p(x)$.

Définition 5.1. *On appelle image réciproque de p par l'application g, le couple (X', p'), où $p' : X' \to B'$ est l'application de première projection (sur B').*

Si $f : X' \to X$ est l'application de deuxième projection (sur X), on a ainsi $p \circ f = g \circ p'$.

Définition 5.2. *On appelle relèvement de l'application $g : B' \to B$ au revêtement p toute application continue $h : B' \to X$ telle que l'on ait $p \circ h = g$.*

Proposition 5.1. *Les relèvements $h : B' \to X$ de g sont en correspondance bijective avec les sections continues de $p' : X' \to B'$ image réciproque de p par g. Plus précisément, l'application qui à un relèvement continu h de g associe l'application $s : B' \to X'$ définie par $s(b') = (b', h(b'))$, est une bijection de l'ensemble des relèvements continus de g dans l'ensemble des sections continues de p'.*

Démonstration : Soit h un relèvement de g. L'application $B' \to B' \times X$ qui à b' associe $\big(b', h(b')\big)$ prend en fait ses valeurs dans l'espace X'. De plus c'est une section continue de p'. On définit de la sorte une application de l'ensemble des relèvements de g dans l'ensemble des sections continues de p'. Cette application est bijective : en effet, elle est clairement injective. Par ailleurs soit s une section continue de $p' : B' \to X'$. Puisque $p' \circ s$ est l'application identique de B', il existe une application $h : B' \to X$, nécessairement continue, telle que l'on ait $s(b') = \big(b', h(b')\big)$ pour tout b' de B'. En particulier h est un relèvement de g. D'où le résultat.

Théorème 5.1. *L'image réciproque (X', p') de p par l'application g est un revêtement.*

Démonstration : Il s'agit de montrer que l'on peut recouvrir B' par des ouverts trivialisants. soit b' un élément de B'. Posons $b = g(b')$. Soit U un ouvert de B contenant

b et trivialisant pour p. On va en fait montrer que $U' = g^{-1}(U)$ est un ouvert trivialisant pour B' qui contient b'. Par définition $p'^{-1}(U')$ est l'ensemble des couples (b', x) de $B' \times X$ tels que $g(b') = p(x)$ soit dans U. Considérons alors un espace discret F et

$$\varphi : U \times F \to p^{-1}(U)$$

une trivialisation de p au-dessus de U. On va en déduire une trivialisation

$$\varphi' : U' \times F \to p'^{-1}(U')$$

de la façon suivante : étant donné (b', y) un élément de $U' \times F$, on pose

$$\varphi'(b', y) = \big(b', \varphi(g(b'), y)\big).$$

Il est immédiat de vérifier que φ' est bien définie. Par ailleurs les deux projections de φ' sur sont continues, donc φ' est aussi continue. Soit alors

$$\psi' : p'^{-1}(U') \to U' \times F,$$

l'application définie, pour tout (b', x) de $p'^{-1}(U')$, par l'égalité

$$\psi'(b', x) = (b', y),$$

où y est l'unique élément de F tel que $\varphi(g(b'), y) = x$. En remarquant que y est l'image par la deuxième projection de $\varphi^{-1}(x)$, on constate que ψ' est continue. On vérifie par ailleurs que les applications ψ' et φ' sont inverses l'une de l'autre. Cela montre que φ' est un homéomorphisme, ce qui entraîne notre assertion.

VI. Relèvement des chemins de la base d'un revêtement

VI.1. Revêtements de base $[0,1]$ ou $[0,1] \times [0,1]$

Posons $I = [0,1]$. On montre ici le théorème suivant :

Théorème 6.1. *Tout revêtement de base I ou $I \times I$ est trivialisable.*

Démonstration : Elle utilise les deux lemmes suivants :

Lemme 6.1. *Soit $p : X \to B$ un revêtement. Soient B' et B'' deux fermés de B tels que $B' \cup B'' = B$ et que $B' \cap B'' = C$ soit un ensemble connexe non vide. Si p est trivialisable au-dessus de B' et au-dessus de B'', il est trivialisable au-dessus de B.*

Démonstration : Soient $\varphi' : B' \times F' \to p^{-1}(B')$ et $\varphi'' : B' \times F'' \to p^{-1}(B'')$ des trivialisations de p au-dessus de B' et B''. L'application

$$\psi = \varphi'^{-1} \circ \varphi'' : C \times F'' \to C \times F'$$

est un automorphisme de revêtements triviaux de base C. Puisque C n'est pas vide, cela entraîne en particulier que F' et F'' sont homéomorphes, et l'on peut donc supposer $F = F'' = F$ (si $a \in C$ la restriction de ψ à $\{a\} \times F'$ est un homéomorphisme de $\{a\} \times F'$ sur $\{a\} \times F''$). Ainsi

$$\psi : C \times F \to C \times F$$

est un automorphisme du revêtement trivial $C \times F \to C$. Puisque C est connexe, il existe donc une permutation σ de F tel que l'on ait

$$\psi(x, y) = (x, \sigma(y)) \quad \text{pour tout} \quad (x, y) \in C \times F.$$

Notons σ' l'application précédente définie sur $B' \times F$. Il est immédiat de vérifier que $\varphi' \circ \sigma' : B' \times F \to p^{-1}(B')$ est aussi une trivialisation de p au-dessus de B'. Par ailleurs, d'après ce qui précède, on a dans $C \times F$ l'égalité $\varphi'' = \varphi' \circ \sigma'$ (car $\psi = \sigma' \mid_{C \times F}$). On déduit de là que les applications φ'' et $\varphi' \circ \sigma'$ définies respectivement sur $B'' \times F$ et $B' \times F$ coïncident sur l'intersection $C \times F$. Notons alors φ l'application $B \times F \to p^{-1}(B)$ qui coïncide avec φ'' et $\varphi' \circ \sigma'$ respectivement sur $B'' \times F$ et $B' \times F$. Cette application φ est continue et est une trivialisation de p. D'où le résultat.

Lemme 6.2. *Soient X un espace métrique compact et $(U_j)_{j \in J}$ un recouvrement par ouverts de X. Il existe un nombre réel $\lambda > 0$ tel que toute boule fermée de rayon strictement plus petit que λ soit contenue dans l'un des ouverts U_j.*

Démonstration : Supposons que pour tout entier $n \geq 1$, il existe une boule fermée B_n de rayon $1/n$ qui ne soit pas contenue dans l'un des U_j. Soit x_n le centre de B_n. On peut extraire de (x_n) une suite convergente $(x_{\rho(n)})$: soit x la limite de cette suite extraite. Soit U_j un ouvert de X contenant x. Il existe un entier M tel que la boule fermée de centre x et de rayon $1/M$ soit contenue dans U_j. Par ailleurs il existe un entier $n_0 \geq 2M$ tel que pour tout $n \geq n_0$, la distance de x à $x_{\rho(n)}$ soit $< 1/2M$. Il en résulte que la boule fermée $B_{\rho(n)}$ est contenue dans U_j (inégalité du triangle), ce qui conduit à une contradiction. D'où le lemme.

Démonstration du théorème 6.1 : 1) Montrons que tout revêtement p de base I est trivialisable. D'après le lemme 6.2, il existe un entier $n \geq 1$ tel que, pour tout i entre 0 et $n-1$, le revêtement p soit trivialisable au-dessus de l'intervallle $[i/n, (i+1)/n]$ (on utilise ici le fait que, par hypothèse on peut recouvrir I par des ouverts trivialisants U_j, puis le lemme 6.2). D'après le lemme 6.1, l'intersection des intervalles $[i/n, (i+1)/n]$ et $[(i+1)/n, (i+2)/n]$ (qui est $(i+1)/n$) étant connexe, p est trivialisable au-dessus de la réunion de ces deux intervalles (et ce pour tout i entre 0 et $n-1$). On construit ainsi de proche en proche une trivialisation de p au-dessus de I. D'où l'assertion.

2) Montrons que tout revêtement de base $I \times I$ est trivialisable. Le principe de démonstration est le même. Il existe un entier $n \geq 1$ tel que, pour tout i et j compris entre

0 et $n-1$, p soit trivialisable au-dessus des pavés $S_{i,j} = [i/n, (i+1)/n] \times [j/n, (j+1)/n]$. Les lemmes 6.1 et 6.2 permettent de même de construire une trivialisation de p au-dessus de p. D'où l'assertion.

Cela termine la preuve du théorème.

VI.2. Théorèmes de relèvement des chemins pour les revêtements

On va démontrer maintenant les deux théorèmes fondamentaux ci-dessous :

Théorème 6.2. *Soit $p : X \to B$ un revêtement. Soient $g : I \to B$ un chemin de B et x un point de X qui est dans la fibre de $g(0)$: on a $p(x) = g(0)$. Alors il existe un unique relèvement continu $h : I \to X$ de g, tel que $h(0) = x$.*

Démonstration : 1) Montrons d'abord l'existence d'un tel relèvement. Soit $p' : X' \to I$ le revêtement image réciproque de p par g (rappelons que X' est le sous-ensemble de $I \times X$ formé des éléments (t, y) tels que $p(y) = g(t)$). Le revêtement p' est trivialisable, donc il existe une section continue s passant par le point $(0, x)$ (car pour un revêtement trivial $A \times F \to A$, il existe toujours une section continue passant par un point (a, f) : par exemple celle qui à z associe (z, f)). Si $p_2 : X' \to X$ est la deuxième projection, l'application composée $p_2 \circ s$ est alors un relèvement cherché.

2) Montrons l'unicité d'un tel relèvement. Soient h et h' deux relèvements continus de g tels que $h(0) = h'(0) = x$. Alors h et h' définissent deux sections $s : I \to X'$ et $s' : I \to X'$ où $s(t) = \big(t, h(t)\big)$ et où $s'(t) = \big(t, h'(t)\big)$. On a $s(0) = s'(0) = (0, x)$. Puisque p' est un *revêtement* et que I est *connexe*, on a donc $s = s'$ (cor. 4.2). Cela entraîne $h = h'$. D'où le résultat.

Théorème 6.3. *Soit $p : X \to B$ un revêtement et soient $g_0 : I \to B$ et $g_1 : I \to B$ deux chemins de B homotopes (avec origine et extrémité fixes) : on a $g_0(0) = g_1(0)$ et $g_0(1) = g_1(1)$. Soit x un point de la fibre $p^{-1}\big(g_0(0)\big)$. Soient h_0 et h_1 les relèvements de g_0 et g_1 tels que $h_0(0) = h_1(0) = x$. Alors les chemins h_0 et h_1 ont même extrémité : on a $h_0(1) = h_1(1)$; de plus h_0 et h_1 sont homotopes (avec origine et extrémité fixes).*

Démonstration : Soit $G : I \times I \to B$ une homotopie de g_0 à g_1 : on a donc pout tout (s, t) dans $I \times I$:

$$G(t, 0) = g_0(t), \quad G(t, 1) = g_1(t), \quad G(0, s) = g_0(0), \quad G(1, s) = g_0(1).$$

Soit $p' : X' \to I \times I$ le revêtement image réciproque de p par G. Puisque p' est trivialisable, il existe une section continue $I \times I \to X'$ passant par le point $\big((0, 0), x\big)$. Cette section définit un relèvement $H : I \times I \to X$ de l'application G tel que $H(0, 0) = x$. Par ailleurs, l'application $t \mapsto H(t, 0)$ est un relèvement de g_0 qui prend la valeur x en 0. On a donc pour tout t dans I, $h_0(t) = H(t, 0)$; de même on vérifie que $h_1(t) = H(t, 1)$ $(*)$: en effet, on a l'égalité $p \circ H(t, 1) = g_1(t)$. Par ailleurs, on a pour tout s de I, $p \circ H(0, s) = g_0(0)$

; or on a $x = H(0,0)$ et $p(x) = g_0(0)$. Donc $H(0,s) = x$ pour tout s de I, de sorte que $H(0,1) = h_1(0)$. D'où l'égalité $(*)$. De même $s \mapsto H(1,s)$ est un relèvement du chemin constant $s \mapsto g_0(1)$; il est donc aussi constant : c'est $s \mapsto h_1(1)$, car pour tout s, on a $H(1,s) = h_1(1)$. Or on a $H(1,0) = h_0(1)$ et $H(1,1) = h_1(1)$. Cela entraîne l'égalité $h_0(1) = h_1(1)$. On déduit de là en particulier que H est une homotopie (avec origine et extrémité fixes) de h_0 à h_1. D'où le théorème.

VI.3. Conséquence sur les homomorphismes des groupes fondamentaux déduits des revêtements

Nous allons maintenant déduire des résultats précedents le théorème suivant :

Théorème 6.4. *Soient X et B deux espaces topologiques et $p : X \to B$ un revêtement. Soit x_0 un point de X. Alors l'homomorphisme naturel $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1\big(B, p(x_0)\big)$ est injectif.* ∎

On va en fait démontrer un résultat plus général. Considérons donc $p : X \to B$ un revêtement (sans hypothèse topologique sur X et B). Soient y_0 et y deux points de B. Choisissons un point x_0 dans la fibre $p^{-1}(y_0)$. Pour tout x dans $p^{-1}(y)$, l'application

$$\pi_1(p; x_0, x) : \pi_1(X; x_0, x) \to \pi_1(B; y_0, y)$$

est injective. En effet, soient γ_0 et γ_1 deux chemins de X d'origine x_0 et d'extrémité x ; par définition, γ_0 et γ_1 sont des relèvements de $p \circ \gamma_0$ et $p \circ \gamma_1$ tels que $p \circ \gamma_0(0) = p \circ \gamma_1(0) = y_0$ et $p \circ \gamma_0(1) = p \circ \gamma_1(1) = y$. Il résulte alors du théorème 6.3 que si $p \circ \gamma_0$ et $p \circ \gamma_1$ sont homotopes, il en est de même de γ_0 et γ_1. Par ailleurs, on dispose de l'application

$$\Phi : \bigcup_{x \in p^{-1}(y)} \pi_1(X; x_0, x) \to \pi_1(B; y_0, y).$$

Vérifions que Φ est une bijection. Montrons que Φ est injective. D'abord sa restriction à chaque sous-ensemble $\pi_1(X; x_0, x)$ l'est d'après ce que l'on vient de voir. Par ailleurs, soient x et x' deux éléments distincts de la fibre $p^{-1}(y)$. Il s'agit de voir qu'un élément de $\pi_1(X; x_0, x)$ et un élément de $\pi_1(X; x_0, x')$ n'ont pas la même image dans $\pi_1(B; y_0, y)$: cela résulte du fait que le relèvement de deux chemins homotopes ont la même extrémité dès qu'ils ont la même origine (théorème 6.3). Enfin le théorème 6.2 entraîne immédiatement le fait que Φ est surjective.

Le théorème se déduit alors du résultat précédent en faisant $y = y_0$: l'application

$$\Phi : \bigcup_{x \in p^{-1}(y_0)} \pi_1(X; x_0, x) \to \pi_1(B; y_0)$$

est une bijection. En particulier, l'homomorphisme $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, y_0)$ est injectif. D'où le théorème.

On déduit de là le résultat suivant :

Proposition 6.1. *Supposons que X et B soient connexes par arcs. Soit $p : X \to B$ un revêtement. S'il existe un point x_0 de X tel que l'homomorphisme*

$$\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1\big(B, p(x_0)\big),$$

soit surjectif (donc bijectif), alors $p : X \to B$ est un homéomorphisme.

Démonstration : D'après ce qui précède, pour que l'homomorphisme $\pi_1(p, x_0)$ soit bijectif, il faut et il suffit que pour tout x dans la fibre $p^{-1}(y_0)$ autre que x_0 (on a $p(x_0) = y_0$), l'ensemble $\pi_1(X; x_0, x)$ soit vide. Puisque X est connexe par arcs, cela entraîne que la fibre $p^{-1}(y_0)$ est réduite à un point. Si de plus B est connexe, toutes les fibres de p sont donc réduites à un point. Tout ouvert trivialisant U pour p est donc homéomorphe à $p^{-1}U$ via l'application réciproque de p. En particulier p^{-1} est une application continue et p est un homéomorphisme. D'où le résultat.

Corollaire 6.2. *Supposons que X soit connexe par arcs et que B soit simplement connexe. Si $p : X \to B$ est un revêtement, alors p est un homéomorphisme.*

Démonstration : Puisque B est simplement connexe, le groupe $\pi_1(B, y)$ est réduit à l'élément neutre. Le corollaire est alors une conséquence directe de la proposition.

VII. Cas où la base est localement connexe

Proposition 7.1. *Soit $p : X \to B$ un revêtement dont la base B est localement connexe. Soit Y une composante connexe de X. Alors $q = p\,|_Y : Y \to B$ est un revêtement de B.*

Démonstration : Il s'agit de montrer que l'on peut recouvrir B par des ouverts trivialisants pour q. Soit $b \in B$. Puisque B est localement connexe, il existe un ouvert connexe U trivialisant pour p. Montrons que U est en fait trivialisant pour q. On considère pour cela les composantes connexes V_i de $p^{-1}(U)$. Les V_i sont des ouverts de X, donc aussi par définition de $p^{-1}(U)$, et ils recouvrent $p^{-1}(U)$. Si un V_i rencontre Y, la réunion $V_i \cup Y$ est connexe, et c'est donc Y. Par suite V_i est contenu dans Y. Ainsi $q^{-1}(U)$, qui est $p^{-1}(U) \cap Y$, est la réunion des V_i qui sont contenus dans Y, et q est un homéomorphisme de chacun d'eux sur U car tel est le cas pour p. Cela montre que U est trivialisant pour q. D'où le résultat.

Proposition 7.2. *Soient $p : X \to B$ et $q : Y \to B$ deux revêtements dont la base B est localement connexe. Soit $f : X \to Y$ un B-morphisme, c'est-à-dire une application continue telle que $q \circ f = p$. Alors f est un revêtement.*

Démonstration : Étant donné un point b de B il existe un ouvert connexe U de B qui est trivialisant à la fois pour p et q. En effet, soient U_1 et U_2 deux ouverts trivialisants respectivement pour p et q qui contiennent b. Tout voisinage ouvert U_3 de B contenu dans $U_1 \cap U_2$ est trivialisant pour p et q. Puisque B est localement connexe il existe un voisinage ouvert connexe U de b contenu dans U_3 et il est trivialisant pour p et q. D'où l'assertion.

Il s'agit alors de montrer que Y est recouvert par des ouverts trivialisants. Considérons pour cela un point y de Y. Soient $b = q(y) \in B$ et U un voisinage ouvert connexe trivialisant pour p et q. Soit V la composante connexe de $q^{-1}(U)$ qui contient y. On va montrer que V est un ouvert trivialisant pour f.

Soit W une composante connexe de $p^{-1}(U)$. Puisque U est connexe, p est un homéomorphisme de W sur U, et de même q est un homéomorphisme de V sur U ; ainsi V est en particulier ouvert. On est en fait dans l'un des deux cas suivants :

a) on a $f(W) \cap V = \emptyset$;

b) l'application f est un homéomorphisme de W sur V.

Supposons en effet que $f(W)$ rencontre V. La réunion $f(W) \cup V$ est alors connexe et elle est contenue dans $q^{-1}(U)$. On a donc $f(W) \cup V = V$ (car V est une composante connexe). Ainsi $f(W)$ est contenu dans V. Cela entraîne alors l'assertion b), car W est homéomorphe à U via p et V est homéomorphe à U via q.

On déduit de là en particulier que si $f(W) \cap V$ n'est pas vide, W est contenu dans $f^{-1}(V)$. Par ailleurs il existe nécessairement une composante connexe de $p^{-1}(U)$ telle que $f(W) \cap V$ ne soit pas vide, car en fait f est surjective (car p l'est). Ainsi $f^{-1}(V)$ est réunion de certaines composantes connexes W_i de $p^{-1}(U)$ (en fait celles dont l'image par f possèdent une intersection non vide avec V), et pour chacune de ces W_i, f est un homéomorphisme de W_i sur V. Cela montre que V est un ouvert trivialisant pour f. D'où le résultat $(*)$.

$(*)$ En fait, si $f^{-1}(V)$ est vide, V est un ouvert trivialisant de f. On peut donc supposer que $f^{-1}(V)$ n'est pas vide.

VIII. Problème du relèvement, théorème fondamental

On désignera parfois par LCA le fait pour un espace d'être localement connexe par arcs, et par CA le fait d'être connexe par arcs. Rappelons le résultat suivant :

Lemme 8.1. *Tout espace localement connexe par arcs (LCA) et connexe est connexe par arcs (CA).*

On considère la catégorie des espaces topologiques pointés. Un morphisme

$$f : (Y, y_0) \to (X, x_0)$$

est une application continue $f : Y \to X$ telle que $f(y_0) = x_0$. Une application $p : (Y, y_0) \to (X, x_0)$ est un revêtement pointé si de plus $p : Y \to X$ est un revêtement.

Fixons désormais un revêtement pointé $p : (X, x_0) \to (B, b_0)$ et une application continue $g : (Y, y_0) \to (B, b_0)$. On étudie ici le problème de l'existence d'un relèvement de l'application g : un tel relèvement, s'il existe, est par définition une application continue $h : (Y, y_0) \to (X, x_0)$ telle que $p \circ h = g$.

Lemme 8.2. *Supposons Y connexe. Il existe au plus un tel relèvement.*

Démonstration : Soit $q : Z \to Y$ le revêtement image réciproque du revêtement $p : X \to B$ par l'application g. On a vu que les relèvements continus $h : (Y, y_0) \to (X, x_0)$ sont en correspondance bijective avec les sections continues $s : Y \to Z$ de q, telles que $s(y_0) = (y_0, x_0)$ (prop. 5.1). Or puisque Y est connexe, il existe au plus une telle section (cor. 4.2). D'où le résultat.

Théorème fondamental 8.1. *Dans la situation précédente, supposons de plus Y connexe et LCA. Dans ce cas un relèvement $h : (Y, y_0) \to (X, x_0)$ existe si et seulement si l'image de l'homomorphisme de groupes*

$$\pi_1(g) : \pi_1(Y, y_0) \to \pi_1(B, b_0)$$

est contenue dans l'image de l'homomorphisme

$$\pi_1(p) : \pi_1(X, x_0) \to \pi_1(B, b_0).$$

Si h existe, alors h est unique.

Démonstration : 1) Montrons d'abord que si h existe, alors Im $\pi_1(g)$ est contenu dans Im $\pi_1(p)$. Cela résulte en fait de l'égalité $p \circ h = g$: en effet, on a alors $\pi_1(g) = \pi_1(p) \circ \pi_1(h)$.

2) Inversement supposons que l'on ait Im $\pi_1(g) \subseteq$ Im $\pi_1(p)$. Montrons alors l'existence de h. On considère pour cela le revêtement $q : Z \to Y$ image réciproque de p par g. Posons $z_0 = (y_0, x_0)$. Il s'agit de trouver une section continue $s : (Y, y_0) \to (Z, z_0)$ de q.

Considérons un lacet $\varphi : I \to Y$ de base le point y_0 : on a $\varphi(0) = \varphi(1) = y_0$. Montrons que φ se relève en un lacet λ de Z au point z_0. Soit $[\varphi]$ l'image de φ dans $\pi_1(Y, y_0)$. Par définition on a $\pi_1(g)[\varphi] = [g \circ \varphi]$. D'après l'hypothèse faite, il existe un lacet α de X au point x_0 tel que l'on ait

$$[g \circ \varphi] = [p \circ \alpha]. \tag{1}$$

Soit $\psi : I \to X$ le relèvement de $g \circ \varphi$ tel que $\psi(0) = x_0$. Par définition α est un relèvement de $p \circ \alpha$. D'après l'égalité (1), ψ et α ont la même extrémité (th. 6.3), de sorte que ψ est un lacet de X de base x_0. On a ainsi

$$g \circ \varphi = p \circ \psi, \tag{2}$$

où $\psi : I \to X$ est un lacet de X au point x_0. Considérons alors l'application $I \to Y \times X$ définie par $t \mapsto (\varphi(t), \psi(t))$. D'après l'égalité (2), elle prend ses valeurs dans Z. Elle définit donc un lacet $\lambda : I \to Z$ au point z_0, tel que $q \circ \lambda = \varphi$. D'où notre assertion.

On déduit de là que l'homomorphisme

$$\pi_1(q) : \pi_1(Z, z_0) \to \pi_1(Y, y_0)$$

est surjectif. Il est donc bijectif (th. 6.4). Considérons alors la composante connexe Z_0 de Z qui contient z_0. Soit

$$q_0 : (Z_0, z_0) \to (Y, y_0)$$

la restriction de q à Z_0. Puisque que Y est LC (localement connexe), car Y est par hypothèse LCA, q_0 est un revêtement (prop. 7.1). Puisque Y est LCA et que q_0 est un revêtement, Z_0 est donc aussi LCA. On déduit de là que Z_0 est connexe par arcs. Ainsi Z_0 est la composante connexe par arcs de Z qui contient z_0 (cette composante connexe par arcs est nécessairement contenue dans Z_0). L'inclusion canonique $Z_0 \to Z$ induit donc un isomorphisme de $\pi_1(Z_0, z_0)$ sur $\pi_1(Z, z_0)$ (cf. le lemme 8.3 ci-dessous). Par suite l'homomorphisme

$$\pi_1(q_0) : \pi_1(Z_0, z_0) \to \pi_1(Y, y_0)$$

est un isomorphisme. L'application $q_0 : Z_0 \to Y$ est donc un homéomorphisme, car Z_0 et Y sont CA (prop. 6.1). Il suffit alors de composer l'homéomorphisme réciproque $(Y, y_0) \to (Z_0, z_0)$ avec l'inclusion $(Z_0, z_0) \to (Z, z_0)$ pour obtenir la section cherchée. D'où le théorème.

Démontrons le lemme suivant que l'on a utilisé dans la preuve du théorème :

Lemme 8.3. *Soient X un espace topologique, x un point de X et C la composante connexe par arcs de x dans X. Soit $i : C \to X$ l'inclusion canonique. L'homomorphisme de groupes $\pi_1(i) : \pi_1(C, x) \to \pi_1(X, x)$ est un isomorphisme.*

Démonstration : Soit $\gamma : I \to X$ un lacet de X de base x. Puisque I est connexe par arcs et que γ est continue, $\gamma(I)$ est aussi connexe par arcs et il contient x. Ainsi $\gamma(I)$ est contenu dans C. Cela montre en particulier que $\pi_1(i)$ est surjectif. Reste à montrer qu'il est injectif. On utilise pour cela le fait que $I \times I$ est connexe par arcs, et donc qu'une homotopie $I \times I \to X$ a une image connexe par arcs ; elle est donc contenue dans C si x est dans l'image.

Th éorie de Galois des rev êtements

I. La catégorie des revêtements connexes pointés ; notion de revêtement universel

On fixe désormais dans ce paragraphe un espace topologique B connexe et LCA (i.e. localement connexe par arcs), et un point b_0 de B. On définit la catégorie des revêtements connexes pointés de base (B, b_0) comme suit : les objets de cette catégorie sont des revêtements pointés

$$p : (X, x_0) \to (B, b_0)$$

tels que X soit connexe (d'après l'hypothèse faite sur B, X est aussi LCA, et comme il est connexe, il est aussi connexe par arcs). Un morphisme de cette catégorie

$$(Y, y_0, q) \to (X, x_0, p)$$

est une application continue $f : (Y, y_0) \to (X, x_0)$ tel que $p \circ f = q$. Étant donnés deux tels objets, il existe au plus un tel morphisme f. Pour que f existe il faut et il suffit que la condition suivante soit réalisée (th. 8.2) :

$$\text{Im } \pi_1(q) \subseteq \text{Im } \pi_1(p). \tag{1}$$

De plus, si f existe, c'est en fait un revêtement $(Y, y_0) \to (X, x_0)$ (prop. 7.2).

la question qui se pose est alors la suivante :

Question. *Cette catégorie admet-elle un objet intial ? Autrement dit, existe-t-il un revêtement connexe $q : (Y, y_0) \to (B, b_0)$ qui satisfasse à la condition (1) quelque soit le revêtement connexe $p : (X, x_0) \to (B, b_0)$?*

Une condition suffisante pour qu'il en soit ainsi est que Y soit simplement connexe (car alors Im $\pi_1(q)$ est réduit à l'élément neutre de $\pi_1(B, b_0)$. D'où le résultat suivant :

Théorème 1.1. *Supposons que (B, b_0) possède un revêtement pointé $q : (Y, y_0) \to (B, b_0)$ tel que Y soit simplement connexe. Alors ce revêtement est objet initial dans la catégorie des revêtements connexes pointés de base (B, b_0).*

Définition 1.1. *Un tel revêtement s'appelle revêtement universel de l'espace (B, b_0).*

Supposons qu'il en soit ainsi, autrement dit que (B, b_0) possède un revêtement universel $q : (Y, y_0) \to (B, b_0)$. Soit $p : (X, x_0) \to (B, b_0)$ un revêtement connexe pointé. Alors il existe un revêtement $f : (Y, y_0) \to (X, x_0)$ tel que $p \circ f = q$. C'est un quotient du revêtement universel.

On démontrera plus loin une condition nécessaire et suffisante pour qu'un espace B connexe et LCA, possède un revêtement simplement connexe, autrement dit un revêtement universel.

II. Groupe des automorphismes d'un revêtement connexe

On définit ici le groupe de Galois d'un revêtement $p : X \to B$ dans le cas où X et B sont connexes et LCA. Rappelons qu'un espace topologique connexe et LCA est connexe par arcs.

Définition 2.1. *Soient X et B deux espaces topologiques connexes et LCA et $p : X \to B$ un revêtement. On appelle B-automorphisme de p un homéomorphisme $f : X \to X$ tel que $p \circ f = p$. Ces automorphismes forment un groupe $G(p)$. C'est le groupe de Galois du revêtement.*

Étant donné un point $b_0 \in B$, le groupe $G(p)$ opère sur la fibre $p^{-1}(b_0)$.

Choisissons désormais un point $x_0 \in X$. Posons $b_0 = p(x_0) \in B$. Notons par ailleurs $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, b_0)$ l'homomorphisme naturel déduit de p.

Proposition 2.1. *Soit x_1 un point de $p^{-1}(b_0)$. Il existe au plus un élément $f \in G(p)$ tel que $f(x_0) = x_1$. Un tel élément f existe si et seulement si l'on a l'égalité*

$$Im\ \pi_1(p, x_0) = Im\ \pi_1(p, x_1).$$

Démonstration : D'après le théorème fondamental 8.1, il existe au plus un revêtement pointé $(X, x_0) \to (X, x_1)$ de base (B, b_0). Par ailleurs, le fait que si f existe l'on ait nécessairement Im $\pi_1(p, x_0) =$ Im $\pi_1(p, x_1)$ provient du même théorème 8.1. Supposons inversement que l'on ait l'égalité Im $\pi_1(p, x_0) =$ Im $\pi_1(p, x_1)$.Toujours d'après le théorème fondamental, il existe deux morphismes $f : (X, x_0) \to (X, x_1)$ et $g : (X, x_1) \to (X, x_0)$ tels que l'on ait les égalités $p \circ f = p$ et $p \circ g = p$. On a alors $p \circ f \circ g = p$ et $p \circ g \circ f = p$. D'après la propriété de l'unicité du relèvement, on a $f \circ g = Id$ et $g \circ f = Id$, ce qui prouve que $f : (X, x_0) \to (X, x_1)$ est un isomorphisme de revêtement pointés de base (B, b_0), autrement dit que f appartient à $G(p)$. D'où le résultat.

Corollaire 2.1. *Le groupe de Galois $G(p)$ opère sans point fixe sur X (ou sur les fibres du revêtement p).*

Démonstration : Si f est distincte de l'identité, f ne peut avoir de points fixe d'après la proposition. D'où l'assertion.

Corollaire 2.2. *Pour que le groupe de Galois opère transitivement dans la fibre $p^{-1}(b_0)$ il faut et il suffit que l'image de l'homomorphisme*

$$\pi_1(p, x) : \pi_1(X, x) \to \pi_1(B, b_0)$$

soit indépendante du point x de la fibre $p^{-1}(b_0)$.

Démonstration : C'est immédiat d'après la proposition 2.1.

Lemme 2.1. *Le groupe $G(p)$ opère transitivement dans la fibre $p^{-1}(b_0)$ si et seulement si, pour tout b dans B, il opère transitivement dans la fibre $p^{-1}(b)$ (autrement dit $G(p)$ opère transitivement sur une fibre si et seulement si il opère transitivement sur chacune des fibres de p).*

Démonstration : On démontre que l'ensemble B' des points $b \in B$ tels que $G(p)$ opère transitivement dans la fibre $p^{-1}(b)$ est ouvert et fermé dans B. Si l'on suppose que $G(p)$ opère transitivement dans la fibre $p^{-1}(b_0)$, l'ensemble en question est non vide. Puisque B est connexe, c'est donc B tout entier. Considérons donc un élément b de B'. Soit U un ouvert connexe trivialisant de B contenant b (un tel U existe car B est localement connexe car LCA). On va montrer que $G(p)$ opère transitivement sur les fibres des points de U. Par définition il existe un espace discret F et un homéomorphisme φ de $U \times F$ sur $p^{-1}(U)$ tel que l'on ait $p \circ \varphi = p_1$, où p_1 est la première projection. Considérons un élément x de U et deux éléments α et β de $p^{-1}(x)$. Il existe t_0 et t_1 dans F tels que l'on ait $(x, t_0) = \varphi^{-1}(\alpha)$ et $(x, t_1) = \varphi^{-1}(\beta)$. Posons alors $y_0 = \varphi((b, t_0))$ et $y_1 = \varphi((b, t_1))$. Soit f un élément de $G(p)$ tel que $f(y_0) = y_1$ (f existe car b appartient à B'). On vérifie alors que l'on a $f(\alpha) = \beta$: en effet, puisque U est connexe, et que $\varphi^{-1} \circ f \circ \varphi$ est un automorphisme du revêtement trivial $U \times F \to U$, il existe une permutation σ de F telle que l'on ait $\varphi^{-1} \circ f \circ \varphi((z, t)) = (z, \sigma(t))$, pour tout $z \in U$ et tout $t \in F$. Or on a $\varphi^{-1} \circ f \circ \varphi((b, t_0)) = (b, t_1)$. On déduit de là l'égalité $\varphi^{-1} \circ f \circ \varphi((x, t_0)) = (x, t_1)$, i.e. $f(\alpha) = \beta$. Cela montre notre assertion et en particulier que B' est ouvert. Par ailleurs, soient b un élément dans $B - B'$, et U un ouvert connexe trivialisant de p contenant b. D'après ce qui précède, pout tout $x \in U$ le groupe $G(p)$ ne peut opérer transitivement sur la fibre $p^{-1}(x)$ (sinon $G(p)$ devrait opérer transitivement sur $p^{-1}(b)$). Cela montre que B' est fermé. D'où le lemme.

Définition 2.2. *On dit que le revêtement $p : X \to B$ est galoisien si $G(p)$ opère transitivement sur chaque fibre de p.*

III. Lien entre les images de $\pi_1(p, x_0)$ et de $\pi_1(p, x_1)$ dans $\pi_1(B, b_0)$ pour x_0 et x_1 dans une même fibre de p

On se place dans la situation suivante : on considère notre revêtement $p : X \to B$, un point b_0 de B et deux points x_0 et x_1 dans la fibre $p^{-1}(b_0)$. On dispose des homomorphismes $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, b_0)$ et $\pi_1(p, x_1) : \pi_1(X, x_1) \to \pi_1(B, b_0)$.

Lemme 3.1. *Les deux sous-groupes de $\pi_1(B, b_0)$, Im $\pi_1(p, x_0)$ et Im $\pi_1(p, x_1)$, sont conjugués dans $\pi_1(B, b_0)$.*

Démonstration : On choisit un chemin c de X joignant x_0 à x_1 (un tel chemin existe car X est CA) ; le choix de c définit un isomorphisme φ de $\pi_1(X, x_0)$ sur $\pi_1(X, x_1)$ via

la flêche $[\gamma] \to [c^{-1}\gamma c]$. Soit $\alpha = [p \circ c]$ l'image de la classe d'homotopie $[c]$ de c dans $\pi_1(B, b_0)$. Montrons que l'on a

$$\alpha^{-1}\text{Im } \pi_1(p, x_0)\alpha = \text{Im } \pi_1(p, x_1).$$

Pour tout élément γ de $\pi_1(X, x_0)$, on a l'égalité

$$\alpha^{-1}[p \circ \gamma]\alpha = [p \circ c^{-1} \perp p \circ \gamma \perp p \circ c].$$

Or on a $[p \circ c^{-1} \perp p \circ \gamma \perp p \circ c] = [p \circ c^{-1} \perp (p \circ \gamma \perp c)] = [p \circ (c^{-1} \perp \gamma \perp c)]$. On déduit de là l'égalité

$$\alpha^{-1}[p \circ \gamma]\alpha = \pi_1(p, x_1)\big([c^{-1}][\gamma][c]\big).$$

Étant donné un élément λ de Im $\pi_1(p, x_0)$, $\alpha^{-1}\lambda\alpha$ appartient donc à l'image de $\pi_1(p, x_1)$. On construit ainsi un homomorphisme de groupes Im $\pi_1(p, x_0) \to$ Im $\pi_1(p, x_1)$ définit par $\lambda \mapsto \alpha^{-1}\lambda\alpha$. C'est un homomorphisme de groupes dont l'isomorphisme réciproque est celui donné par la flêche $\mu \mapsto \alpha\mu\alpha^{-1}$. D'où le résultat.

On déduit alors le résultat suivant :

Proposition 3.1. *Pour que le revêtement $p : X \to B$ soit galoisien, il faut et il suffit que pour tout $x_0 \in X$ l'image de l'homomorphisme $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, p(x_0))$ soit un sous-groupe distingué de $\pi_1(B, p(x_0))$. Cela revient à demander qu'il existe un élément $x_0 \in X$ tel que l'image de l'homomorphisme $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, p(x_0))$ soit un sous-groupe distingué de $\pi_1(B, p(x_0))$.*

Démonstration : a) Supposons $p : X \to B$ galoisien. Soit x_0 un point de X. Considérons un élément $\alpha = [f]$ de $\pi_1(B, p(x_0))$. Soit g le relèvement de f tel que $g(0) = x_0$. Posons $g(1) = x_1$. D'après la démonstration du lemme précédent, on a l'égalité

$$\alpha^{-1} \text{ Im } \pi_1(p, x_0) \ \alpha = \text{Im } \pi_1(p, x_1).$$

Or p étant galoisien, on a Im $\pi_1(p, x_1) =$ Im $\pi_1(p, x_0)$. D'où le fait que Im $\pi_1(p, x_0)$ soit un sous-groupe distingué dans $\pi_1(B, p(x_0))$.

b) Supposons maintenant qu'il existe un élément x_0 de X tel que l'image de l'homomorphisme $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, p(x_0))$ soit un sous-groupe distingué de $\pi_1(B, p(x_0))$. Montrons que p est galoisien. Vérifions pour cela que l'image de l'homomorphisme

$$\pi_1(p, x) : \pi_1(X, x) \to \pi_1(B, p(x_0))$$

ne dépend pas d'un point x choisi dans la fibre de p en $p(x_0)$ (cor. 2.2). Considérons donc un point x_1 de la fibre $p^{-1}(p(x_0))$. D'après le lemme 3.1, il existe α dans $\pi_1(B, p(x_0))$ tel que l'on ait α^{-1} Im $\pi_1(p, x_0)$ $\alpha =$ Im $\pi_1(p, x_1)$. Cela entraîne Im $\pi_1(p, x_1) =$ Im $\pi_1(p, x_0)$. D'où notre assertion et la proposition.

Corollaire 3.1. *Le revêtement universel de B, s'il existe, est galoisien.*

Démonstration. C'est immédiat d'après la proposition 3.1.

IV. Opération du groupe fondamental $\pi_1(B, b_0)$ dans la fibre d'un revêtement de base B

Proposition 4.1. *Soit $p : X \to B$ un revêtement (sans hypothèse topologique particulière sur X et B). Soit b_0 un point de B. Alors $\pi_1(B, b_0)$ opère à droite sur la fibre $p^{-1}(b_0)$.*

Démonstration : On va définir une application

$$p^{-1}(b_0) \times \pi_1(B, b_0) \to p^{-1}(b_0)$$

$(x, \alpha) \mapsto x.\alpha$ de la façon suivante : soient $x \in p^{-1}(b_0)$ et $\alpha \in \pi_1(B, b_0)$. On choisit un lacet f de B qui représente α. On relève f en un chemin g de X d'origine x (th. 6.2). Soit x' l'extrémité de g. on pose alors

$$x' = x.\alpha.$$

Cette application est bien définie, car x' ne dépend pas du choix de f (th. 6.3). Vérifions qu'il s'agit bien d'une opération. Il faut donc vérifier que, pour tout $x \in p^{-1}(b_0)$ et tout α et β dans $\pi_1(B, b_0)$, l'on a (si e est l'élément neutre de $\pi_1(B, b_0)$)

$$x.e = x \quad \text{et} \quad (x.\alpha).\beta = x.(\alpha.\beta).$$

a) Prouvons la première égalité. Il suffit pour cela de remarquer que le lacet constant de X en x relève le lacet constant de B en b_0 (qui est un représentant de $e \in \pi_1(B, b_0)$).

b) Prouvons la deuxième égalité. Soient α et β deux éléments de $\pi_1(B, b_0)$ et x un point de $p^{-1}(b_0)$. Soient f_α et f_β deux représentants de α et β. Soient g_α le relèvement de f_α d'origine x, et h_β et relèvement de f_β d'origine $g_\alpha(1) \in X$. En utilisant directement la définition de la composition de deux chemins (quand cela est possible), on constate que l'on a l'égalité

$$p \circ (g_\alpha \perp h_\beta) = f_\alpha \perp f_\beta, \tag{1}$$

autrement dit $g_\alpha \perp h_\beta$ est le relèvement de $f_\alpha \perp f_\beta$ d'origine x. Par définition, on a

$$(g_\alpha \perp h_\beta)(1) = x.(\alpha.\beta) \quad \text{et} \quad h_\beta(1) = g_\alpha(1).\beta = (x.\alpha).\beta.$$

Or on a aussi par définition $h_\beta(1) = (g_\alpha \perp h_\beta)(1)$. Cela montre notre égalité. D'où la proposition.

V. Suite exacte d'un revêtement galoisien $p : X \to B$ lorsque X et B sont connexes et LCA

Soit $p : X \to B$ un revêtement galoisien, X et B étant connexes et LCA. Soit $G(p)$ le groupe de Galois de p. Choisissons désormais un point b_0 de B et un point x_0 de la fibre $p^{-1}(b_0)$. On associe à ces données une application (qui dépend de b_0 et de x_0)

$$\rho : \pi_1(B, b_0) \to G(p)$$

de la façon suivante : soit α un élément de $\pi_1(B, b_0)$. On considère $x_0.\alpha$ qui est un élément de la fibre $p^{-1}(b_0)$. Puisque p est galoisien, il existe un unique élément de $G(p)$ qui envoie x_0 sur $x_0.\alpha$ ($G(p)$ agit transitivement dans la fibre $p^{-1}(b_0)$) . C'est par définition $\rho(\alpha)$. Ainsi $\rho(\alpha)$ est défini par la condition

$$\rho(\alpha)(x_0) = x_0.\alpha \quad \text{pour tout} \quad \alpha \in \pi_1(B, b_0).$$

Proposition 5.1. *L'application ρ est un homomorphisme de groupes surjectif. Le noyau de ρ est l'image de l'homomorphisme $\pi_1(p) = \pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, b_0)$. On a ainsi une suite exacte de groupes*

$$1 \longrightarrow \pi_1(X, x_0) \stackrel{\pi_1(p)}{\longrightarrow} \pi_1(B, b_0) \stackrel{\rho}{\longrightarrow} G(p) \longrightarrow 1.$$

Démonstration : a) Soient α et β deux éléments de $\pi_1(B, b_0)$. Il s'agit de montrer l'égalité $\rho(\alpha.\beta) = \rho(\alpha) \circ \rho(\beta)$. Il suffit pour cela de montrer qu'ils prennent la même valeur en un point x_0 de X. Cela revient à démontrer que l'on a l'égalité

$$(x_0.\alpha).\beta = (x_0.\beta).\alpha.$$

Posons $\sigma = \rho(\alpha)$. L'égalité précédente s'écrit aussi

$$\sigma(x_0).\beta = \sigma(x_0.\beta).$$

Soit alors f un représentant de β. Soit g le relèvement de f d'origine x_0 dans X. On a $p \circ \sigma \circ g = f$. L'égalité $g(1) = x_0.\beta$ (par définition) entraîne $\sigma \circ g(1) = \sigma(x_0.\beta)$. Par ailleurs on a aussi par définition $\sigma(x_0).\beta = \sigma \circ g(1)$. Cela prouve que ρ est un homomorphisme.

b) Montrons qu'il est surjectif. Soit f un élément de $G(p)$. Posons $x_1 = f(x_0)$. Soit γ un chemin de X d'origine x_0 et d'extrémité x_1. Posons $\alpha = [p \circ \gamma]$. Par définition, on a $x_0.\alpha = x_1$ et $\rho(\alpha)(x_0) = x_1$. D'où $\rho(\alpha) = f$ et notre assertion.

c) Soit α un élément de $\pi_1(B, b_0)$ tel que $\rho(\alpha)$ soit l'identité de X. On a alors $x_0.\alpha = x_0$. Considérons f un représentant de α et g le relèvement de f d'origine x_0 dans X. Par définition g est un lacet de X en x_0, et $[g]$ est un élément de $\pi_1(X, x_0)$ dont l'image dans $\pi_1(B, b_0)$ est α. Inversement soit $[p \circ h]$ un élément de l'image de $\pi_1(p, x_0)$

dans $\pi_1(B, b_0)$. On alors $\rho([p \circ h])(x_0) = h(1) = x_0$, ce qui prouve que $\rho([p \circ h])$ est l'identité de X. D'où la proposition.

Corollaire 5.1. *Supposons que X soit simplement connexe, autrement dit que $p : X \to B$ soit le revêtement universel de B. Alors $\rho : \pi_1(B, b_0) \to G(p)$ est un isomorphisme de groupes.*

Terminons ce paragraphe par une remarque. On suppose toujours X et B connexes et LCA. On considère un revêtement $p : X \to B$ non nécessairement galoisien. Soient x_0 un point de X et $b_0 = p(x_0)$.

Proposition 5.2. *Soit H l'image de l'homomorphisme $\pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, b_0)$. Les ensembles $\pi_1(B, b_0)/H$ des classes à droite de $\pi_1(B, b_0)$ modulo H, et $p^{-1}(b_0)$, sont en bijection via la flêche $\varphi : H.\alpha \mapsto x_0.\alpha$.*

Démonstration : Puisque X est connexe par arcs, $\pi_1(B, b_0)$ opère transitivement sur la fibre $p^{-1}(b_0)$. En effet, Soit x_1 un élément de $p^{-1}(b_0)$. Il existe un chemin γ de X d'origine x_0 et d'extrémité x_1. Posons $\alpha = [p \circ \gamma]$. On a alors par définition $x_1 = x_0.\alpha$; d'où notre assertion. Ainsi l'orbite de x_0 est la fibre $p^{-1}(b_0)$ tout entière. Regardons maintenant le stabilisateur de x_0 : c'est l'ensemble des α de $\pi_1(B, b_0)$ tel que $x_0.\alpha = x_0$. C'est en fait l'image de $\pi_1(X, x_0)$ dans $\pi_1(B, b_0)$ (cf. démonstration de l'assertion c) de la prop. 5.1). D'où le résultat.

Corollaire 5.2. *Supposons que $p : X \to B$ soit un revêtement à deux feuillets (X et B sont ici connexes et LCA). Alors p est galoisien.*

Démonstration : Soit x_0 un point de X. Posons $b_0 = p(x_0)$. Alors p est galoisien si et seulement si l'image de $\pi_1(p, x_0)$ dans $\pi_1(B, b_0)$ est distinguée dans $\pi_1(B, b_0)$. Or tel est bien le cas car cette image est d'indice 2 dans $\pi_1(B, b_0)$ (prop. 5.2).

VI. Suite exacte d'un revêtement non nécessairement galoisien $p : X \to B$ lorsque X et B sont connexes et LCA

Soit $p : X \to B$ un revêtement qui n'est plus nécessairement galoisien X et B étant connexes et LCA. Soit $G(p)$ le groupe de Galois de p. Choisissons désormais un point b_0 de B et un point x_0 de la fibre $p^{-1}(b_0)$. Soit N le normalisateur de l'image de $\pi_1(p, x_0)$ dans $\pi_1(B, b_0)$. On associe alors à ces données une application (qui dépend de b_0 et de x_0)

$$\rho : N \to G(p)$$

de la façon suivante : soit α un élément de N. On considère un relèvement f de α et g le relèvement de f dans X d'origine x_0. Notons x_1 l'extrémité de g, qui est un élément de la fibre $p^{-1}(b_0)$. Vérifions qu'il existe un élément de $G(p)$ qui transforme x_0 en x_1.

Rappelons que l'on a $x_1 = x_0.\alpha$. On définira alors, comme dans le cas où p est galoisien, $\rho(\alpha)$ par l'égalité

$$\rho(\alpha)(x_0) = x_0.\alpha.$$

Les sous-groupes de $\pi_1(B, b_0)$, Im $\pi_1(p, x_0)$ et Im $\pi_1(p, x_1)$ sont liés par l'égalité

$$\alpha^{-1} \text{ Im } \pi_1(p, x_0)\ \alpha = \text{Im } \pi_1(p, x_1).$$

Puisque α appartient à N on a donc α^{-1} Im $\pi_1(p, x_0)$ $\alpha =$ Im $\pi_1(p, x_0)$, ce qui entraîne Im $\pi_1(p, x_0) =$ Im $\pi_1(p, x_1)$, et démontre notre assertion.

On démontre, comme dans le cas où p est galoisen le résultat suivant :

Proposition 6.1. *L'application ρ est un homomorphisme de groupes surjectif. L'image de l'homomorphisme $\pi_1(p) = \pi_1(p, x_0) : \pi_1(X, x_0) \to \pi_1(B, b_0)$ est contenu dans N (par définition) et c'est le noyau de ρ. On a ainsi une suite exacte de groupes*

$$1 \longrightarrow \pi_1(X, x_0) \overset{\pi_1(p)}{\longrightarrow} N \overset{\rho}{\longrightarrow} G(p) \longrightarrow 1.$$

Démonstration : Il suffit de démontrer que ρ est surjectif , le reste de la démonstration étant inchangé par rapport au cas où p est galoisien.

Soit f un élément de $G(p)$. Posons $x_1 = f(x_0)$. Soit γ un chemin de X d'origine x_0 et d'extrémité x_1. Posons $\alpha = [p \circ \gamma]$. Vérifions que α appartient à N. On remarque pour cela que l'on a l'égalité

$$[p \circ \gamma]^{-1}\text{Im } \pi_1(p, x_0)[p \circ \gamma] = \text{Im } \pi_1(p, x_1).$$

Or puisqu'il existe un élément de $G(p)$ transformant x_0 en x_1 (à savoir f) on a

$$\text{Im } \pi_1(p, x_1) = \text{Im } \pi_1(p, x_0).$$

Cela montre notre assertion. On a alors $\rho(\alpha)(x_0) = x_1$, et donc $\rho(\alpha) = f$. D'où la proposition.

Remarque. Le revêtement p est galoisien si et seulement si l'on a $N = \pi_1(B, b_0)$.

VII. Théorie de Galois

VII.1. Préliminaires

Partons d'un revêtement $p : X \to B$ galoisien, X et B étant toujours supposés connexes et LCA. Soit $G(p)$ son groupe de Galois.

Lemme 7.1. *Le groupe $G(p)$ opère continûment et proprement sans point fixe sur X.*

Démonstration : Montrons d'abord que $G(p)$ opère proprement sans point fixe sur X. Soit x_0 un élément de X. Posons $b_0 = p(x_0)$. Soit U un ouvert connexe (on peut

dans cette démonstration choisir U non connexe) trivialisant de p contenant b_0. Soit V la composante connexe de $p^{-1}(U)$ contenant x_0 que p envoie homéomorphiquement sur U. Vérifions que pour tout $\sigma \in G(p)$ autre que l'identité, l'on a $\sigma(V) \cap V = \emptyset$. Soit donc σ un élément de $G(p)$ distinct de l'identité de X tel que $\sigma(V) \cap V$ ne soit pas vide. Soit y un élément de $\sigma(V) \cap V$. On a $\sigma(v) = y$ pour un certain élément $v \in V$. Or $p \circ \sigma(v) = p(v)$. D'où l'égalité $p(v) = p(y)$, ce qui entraîne $v = y$. Cela implique que σ soit l'identité de X. D'où une contradiction et notre assertion. Montrons maintenant que $G(p)$ opère continûment sur X, autrement dit que l'application $G(p) \times X \to X$ définit par $(\sigma, x) \mapsto \sigma(x)$ est continue, $G(p)$ étant muni de la topologie discrète. Soit (σ, x) un point de $G(p) \times X$. Soit V un ouvert de X contenant $\sigma(x)$. Alors $\{\sigma\} \times \sigma^{-1}V$ est un ouvert de $G(p) \times X$ dont l'image par l'application précédente est contenue dans V. D'où le lemme.

Lemme 7.2. *Soit G un groupe discret opérant de façon continue, et proprement sans point fixe sur un espace Y connexe et LCA. Alors la surjection canonique $q : Y \to Y/G$ est un revêtement galoisien et son groupe de Galois est G. Plus précisément, le groupe de Galois de q est formé des homéomorphismes $Y \to Y$ définis par $y \mapsto gy$, lorsque g parcourt G. Autrement dit, l'application $g \mapsto \{y \mapsto gy\}$ est un isomorphisme de groupes Ψ de G sur $G(q)$.*

Démonstration : On sait déjà que q est un revêtement et que Y/G est aussi connexe et LCA. D'abord $\Psi(g)$ appartient à $G(q)$ pour tout $g \in G$, car $q(gy) = q(y)$ par définition. Par ailleurs, Ψ est clairement un homomorphisme de groupes. Il est injectif car G opère sur Y sans point fixe. Enfin il est surjectif : soit h un élément de $G(q)$. Pour tout $y \in Y$, on a $q \circ h(y) = q(y)$. Étant donné $y \in Y$, il existe donc $g \in G$ tel que l'on ait $h(y) = gy$. On remarque alors que les applications h et $z \mapsto gz$ sont deux relèvements de q qui coïncident en un point (à savoir y). Ils sont donc égaux (car Y est connexe) ; d'où la surjectivité de Ψ. Par ailleurs, du fait que $\Psi(g)$ est dans $G(q)$ pour tout $g \in G$, il résulte que $G(q)$ opère transitivement dans les fibres de q (par définition) et donc que q est galoisien. D'où le résultat.

Proposition 7.1. *L'application canonique $s : X \to X/G(p)$ est un revêtement. Le revêtement p se factorise en $X \to X/G(p) \to B$. Plus précisément on a $p = \varphi \circ s$, où $\varphi : X/G(p) \to B$ est un homéomorphisme (il existe un unique tel homéomorphisme). Autrement dit p s'identifie de la sorte au revêtement s.*

Démonstration : Le fait que s soit un revêtement résulte des lemmes 7.1 et 7.2. Par ailleurs, on constate facilement que p passe au quotient suivant la relation d'équivalence associée à $G(p)$, autrement dit que p se factorise à travers s. Il existe donc une application $\varphi : X/G(p) \to B$ tel que $p = \varphi \circ s$; on a ainsi $\varphi(s(x)) = p(x)$ pour tout $x \in X$, ce qui montre en particulier l'unicité de φ.

Montrons que φ est injective. Soient x et y deux éléments de X tels que $\varphi(s(x)) = \varphi(s(y))$. On a alors $p(x) = p(y)$. Puisque p est galoisien, $G(p)$ opère transitivement dans les fibres, et il existe donc $g \in G(p)$ tel que l'on ait $y = g(x)$, ce qui signifie l'égalité $s(x) = s(y)$. D'où l'assertion. Par ailleurs, φ est surjective, car p l'est.

Vérifions que φ est continue. Il suffit de remarquer que, si U est un ouvert de B, l'on a $\varphi^{-1}(U) = sp^{-1}(U)$ et que s est une application ouverte. L'argument est le même pour montrer que φ^{-1} est continue : si l'on pose $\psi = \varphi^{-1}$, on a pour tout ouvert U de $X/G(p)$ l'égalité $\psi^{-1}(U) = ps^{-1}(U)$ et on utilise le fait que p est une application ouverte. D'où la proposition.

VII.2. Correspondance de Galois

Nous allons démontrer dans ce paragraphe le théorème de la correspondance de Galois pour les revêtements. Tous les espaces considérés dans la suite sont supposés connexes et LCA (ils sont donc connexes par arcs).

Proposition 7.2. *Soit $p : (X, x_0) \to (B, b_0)$ un revêtement galoisien. Soient $G(p)$ le groupe de Galois de p et Γ un sous-groupe de $G(p)$. Soit $s_\Gamma : (X, x_0) \to (X/\Gamma, s_\Gamma(x_0))$ le revêtement pointé associé à la surjection canonique $X \to X/\Gamma$. Alors il existe un unique revêtement $r_\Gamma : (X/\Gamma, s_\Gamma(x_0)) \to (B, b_0)$ vérifiant l'égalité $r_\Gamma \circ s_\Gamma = p$.*

Démonstration : D'abord l'application p se factorise à travers s car Γ est un sous-groupe de $G(p)$. Il existe donc une application, $r_\Gamma : (X/\Gamma, s_\Gamma(x_0)) \to (B, b_0)$, nécessairement unique, telle que l'on ait $r_\Gamma \circ s_\Gamma = p$. Par ailleurs r_Γ est continue car si U est un ouvert U de B, on a l'égalité

$$s_\Gamma(p^{-1}(U)) = r_\Gamma^{-1}(U). \tag{1}$$

Vérifions que r_Γ est une application ouverte : il sufit pour cela de remarquer que si V est un ouvert de X/Γ, l'on a

$$r_\Gamma(V) = p(W),$$

où $W = s_\Gamma^{-1}(V)$, et que p est une application ouverte. Montrons maintenant que r_Γ est un revêtement. On doit pour cela recouvrir B par des ouverts trivialisants pour r_Γ. Soit b un élément de B. Soit U un ouvert connexe de B contenant b trivialisant pour le revêtement p. On va démontrer que U est un ouvert trivialisant pour r_Γ.

Soit V une composante connexe de $p^{-1}(U)$ qui s'envoie homéomorphiquement sur U via p. On peut écrire $p^{-1}(U)$ comme la réunion disjointe

$$p^{-1}(U) = \bigcup_{g \in G(p)} gV. \tag{2}$$

En fait cette égalité résulte de l'assertion suivante :

Assertion. *Soit $p : X \to B$ un revêtement galoisien. Soit U un ouvert connexe trivialisant pour p. Alors les composantes connexes de $p^{-1}(U)$ sont les $\sigma(V)$, où σ est dans $G(p)$ et où V est une composante connexe de $p^{-1}(U)$.*

Démonstration : Il suffit de prouver que si V_1 et V_2 sont deux composantes connexes de $p^{-1}(U)$, il existe σ dans $G(p)$ tel que $\sigma(V_1) = V_2$: il existe un élément a dans V_1 et un élément b dans V_2 tels que l'on ait $p(a) = p(b)$, car V_1 et V_2 sont homéomorphes à U via p. Puisque p est galoisien, il existe σ dans $G(p)$ tel que $\sigma(a) = b$, ce qui entraîne l'égalité $\sigma(V_1) = V_2$ (car σ induit un homéomorphisme de $p^{-1}(U)$ sur $p^{-1}(U)$, et $\sigma(V_1)$ et V_2 sont deux composantes connexes de $p^{-1}(U)$ contenant b). D'où l'assertion.

On considère alors un système de représentants $S = (g_i)_{i \in I}$ de l'ensemble des classes à droite de $G(p)$ modulo Γ. Vérifions que l'ensemble $r_\Gamma^{-1}(U)$ s'écrit comme la réunion disjointe

$$r_\Gamma^{-1}(U) = \bigcup_{i \in I} s_\Gamma(g_i V). \tag{3}$$

D'après les égalités (1) et (2), $r_\Gamma^{-1}(U)$ est la réunion des ensembles $s_\Gamma(gV)$ lorsque g parcourt $G(p)$. Par ailleurs, étant donnés i et j dans I, les conditions suivantes sont équivalentes :

(i) l'élément $g_i g_j^{-1}$ appartient à Γ ;
(ii) on a $s_\Gamma(g_i V) = s_\Gamma(g_j V)$;
(iii) on a $s_\Gamma(g_i V) \cap s_\Gamma(g_j V) \neq \emptyset$.

En effet, l'égalité $g_i = \alpha g_j$, où $\alpha \in \Gamma$, implique $g_i V = \alpha g_j V$ et donc $s_\Gamma(g_i V) = s_\Gamma(g_j V)$; Le fait que (ii) entraîne (iii) est clair. Il reste donc à prouver que (iii) implique (i). On considère pour cela deux éléments v et v' de V pour lesquels il existe g dans Γ tels que $g_i v = g g_j v'$. Puisque $G(p)$ opère proprement sans point fixe, cela entraîne $g_i = g g_j$ (cf. dém. du lemme 7.1). D'où notre assertion.

On déduit des équivalences précédentes l'égalité (3) et le fait que cette réunion soit disjointe. Il reste alors à démontrer que, pour tout $i \in I$, la restriction de r_Γ à $s_\Gamma(g_i V)$ induit un homéomorphisme de $s_\Gamma(g_i V)$ sur U (cela prouvera que r_Γ est un revêtement). D'abord cette restriction est surjective car p induit une bijection de $g_i V$ sur U. Supposons par ailleurs que l'on a l'égalité $r_\Gamma \circ s_\Gamma(g_i v) = r_\Gamma \circ s_\Gamma(g_i v')$, où v et v' sont deux éléments de V. On a alors $p(g_i v) = p(g_i v')$, et il existe donc un élément σ dans $G(p)$ tel que $g_i v = \sigma g_i v'$. D'où $g_i = \sigma g_i$ et σ est l'élément neutre de $G(p)$. D'où $v = v'$ et le fait que la restriction de r_Γ à $s_\Gamma(g_i V)$ soit injective. Mais on a déjà montré que r_Γ est continue et ouverte. D'où notre assertion et la proposition.

Remarque. L'ouvert U utilisé dans la démonstration peut en fait ne pas être connexe. Il suffit ensuite de prendre pour V *un* ouvert de $p^{-1}(U)$ qui s'envoie homéomorphiquement sur U via p. Pour tout $\sigma \in G(p)$ distinct de l'identité, on a encore $\sigma V \cap V = \emptyset$.

Définition 7.1. *Soit $p : (X, x_0) \to (B, b_0)$ un revêtement pointé. On appelle revêtement intermédiaire de p, tout revêtement $r : (Y, y_0) \to (B, b_0)$, tel qu'il existe une application continue $q : (X, x_0) \to (Y, y_0)$ vérifiant $r \circ q = p$. L'application q est alors unique, car c'est un relèvement pointé de p, et c'est un revêtement (prop. 7.2). Deux revêtements intermédiaires $r : (Y, y_0) \to (B, b_0)$ et $r' : (Y', y'_0) \to (B, b_0)$ sont dits équivalents s'il existe un homéomorphisme $h : (Y, y_0) \to (Y', y'_0)$ tel que $h \circ q = q'$ et $r' \circ h = r$, où $q' : (X, x_0) \to (Y', y'_0)$ vérifie comme ci-dessus $r' \circ q' = p$.*

Considérons désormais un revêtement galoisien pointé $p : (X, x_0) \to (B, b_0)$. On désigne par $\mathcal{R}$ l'ensemble des classes d'isomorphisme de revêtements intermédiaires $r : (Y, y_0) \to (B, b_0)$ de p et par $\mathcal{H}$ l'ensemble des sous-groupes de $G(p)$. Étant donné un revêtement pointé $q : (X, x_0) \to (Y, y_0)$, on notera $G(q)$ son groupe de Galois sans autre précision. Étant donné un revêtement intermédiaire $r : (Y, y_0) \to (B, b_0)$ de p, on désignera par $cl\big(r : (Y, y_0) \to (B, b_0)\big)$ sa classe d'équivalence.

Lemme 7.3. *Soit $r : (Y, y_0) \to (B, b_0)$ un revêtement intermédiaire de p. Soit $q : (X, x_0) \to (Y, y_0)$ le revêtement pointé de Y satisfaisant à l'égalité $r \circ q = p$. Alors le revêtement q est galoisien.*

Démonstration : De l'égalité $r \circ q = p$, on déduit que l'on

$$\pi_1(r, y_0) \circ \pi_1(q, x_0) = \pi_1(p, x_0).$$

Par ailleurs, l'application $\pi_1(r, y_0)$ est injective, et l'on a donc

$$\pi_1(r, y_0)^{-1}\big(\pi_1(p, x_0)(\pi_1(X, x_0)\big) = \pi_1(q, x_0)\big(\pi_1(X, x_0)\big).$$

Puisque $\pi_1(p, x_0)\big(\pi_1(X, x_0)\big)$ est un sous-groupe distingué de $\pi_1(B, b_0)$ (car p est galoisien), on en déduit que $\pi_1(q, x_0)\big(\pi_1(X, x_0)\big)$ est un sous-groupe distingué de $\pi_1(Y, y_0)$. D'où le lemme.

Énonçons maintenant le théorème relatif à la correspondance de Galois.

Théorème 7.1. *L'application $\Phi : \mathcal{R} \to \mathcal{H}$ définie par*

$$cl\big(r : (Y, y_0) \to (B, b_0)\big) \mapsto G(q), \quad \text{où} \quad r \circ q = p,$$

est une bijection de $\mathcal{R}$ sur $\mathcal{H}$. L'application réciproque $\Psi : \mathcal{H} \to \mathcal{R}$ est donnée par

$$\Gamma \mapsto cl\big(r_\Gamma : (X/\Gamma, s_\Gamma(x_0)) \to (B, b_0)\big),$$

où $r_\Gamma : (X/\Gamma, s_\Gamma(x_0)) \to (B, b_0)$ est le revêtement dont l'existence est affirmée dans la proposition 7.2. Les revêtements intermédiaires de p qui sont galoisiens correspondent aux sous-groupes distingués de $G(p)$.

Démonstration : 1) Vérifions que l'application Φ est bien définie. D'abord $G(q)$ est bien un sous-groupe de $G(p)$; en effet, il est contenu dans $G(p)$, car si f appartient à

$G(q)$, on a $q \circ f = q$, ce qui entraîne $r \circ q \circ f = r \circ q$, i.e. $p \circ f = p$. Considérons maintenant r et r' deux revêtements intermédiaires (pointés) isomorphes de p. Il s'agit de prouver que l'on a $G(q) = G(q')$, où q et q' sont définies par les égalités $p = r \circ q = r' \circ q'$. Soit f un élément de $G(q)$. On a $q \circ f = q$. Soit h un homéomorphisme de Y sur Y' tel que $h \circ q = q'$. On a alors les égalités $q' \circ f = h \circ q \circ f = h \circ q = q'$ et le fait que f appartienne à $G(q')$. Cela entraîne (pour des raisons de symétrie) que Φ soit bien définie.

2) Démontrons que les applications Φ et Ψ sont inverses l'une de l'autre. Vérifions d'abord que l'on a

$$\Psi \circ \Phi = 1_{\mathcal{R}}. \tag{1}$$

Considérons $C = cl\big(r : (Y, y_0) \to (B, b_0)\big)$ un élément de $\mathcal{R}$. Les revêtements $q : (X, x_0) \to (Y, y_0)$ et $s_q : (X, x_0) \to \big(X/G(q), s_q(x_0)\big)$ sont isomorphes (où q est le revêtement associé à r par définition). Autrement dit, il existe un unique homéomorphisme φ de (Y, y_0) sur $\big(X/G(q), s_q(x_0)\big)$ tel que l'on ait l'égalité $\varphi \circ q = s_q$. Soit r_q l'unique revêtement $\big(X/G(q), s_q(x_0)\big) \to (B, b_0)$ tel que $r_q \circ s_q = p$ dont l'existence est assurée par la proposition 7.1. Par définition de φ, on a $r_q \circ \varphi = r$. Cela montre que les revêtements r et s_q sont isomorphes. On a ainsi $\Psi(G(q)) = C$, ce qui entraîne l'égalité (1). Vérifions maintenant que l'on a

$$\Phi \circ \Psi = 1_{\mathcal{H}}. \tag{2}$$

Il suffit pour cela de vérifier que le groupe de Galois du revêtement $s_\Gamma : (X, x_0) \to \big(X/\Gamma, s_\Gamma(x_0)\big)$ est précisément le groupe Γ : d'abord Γ est évidemment contenu dans ce groupe de Galois. Inversement soit h un élément de $G(p)$ tel que $s_\Gamma \circ h = s_\Gamma$; soit x un élément de X. Il existe γ_x dans Γ tel que l'on ait $h(x) = \gamma_x(x)$; d'où $h = \gamma_x$ (car h et γ_x coïncident en un point) et h appartient à Γ. D'où l'égalité (2) et le fait que Φ et Ψ sont inverses l'une de l'autre.

Reste à montrer que les revêtements intermédiaires de p qui sont galoisiens et les sous-groupes distingués de $G(p)$ se correspondent par les applications Φ et Ψ.

3) Soit $r : (Y, y_0) \to (B, b_0)$ un revêtement *galoisien* de (B, b_0). Soit $q : (X, x_0) \to (Y, y_0)$ le revêtement associé à r tel que $r \circ q = p$. Montrons que $G(q)$ est un sous-groupe distingué de $G(p)$. Soient h un élément de $G(p)$ et f un élément de $G(q)$. Il s'agit de vérifier que hfh^{-1} appartient à $G(q)$, autrement dit que l'on a $q \circ (hfh^{-1}) = q$. Soit x un élément de X. Posons $y = h^{-1}(x)$. On remarque que l'on a les égalités

$$rq(x) = p(x) = p(y) = rq(y),$$

l'avant dernière égalité ayant lieu car h appartient à $G(p)$. Puisque r est par hypothèse galoisien, il existe donc un élément σ de $G(r)$ tel que l'on ait $\sigma(q(y)) = q(x)$. Considérons

alors les applications continues σq et qh de X dans Y. Elles coïncident au point y : en effet, $qh(y) = q(x) = \sigma q(y)$ d'après l'égalité ci-dessus. Par ailleurs, on a $r(qh) = (rq)h = ph = p$ et $r(\sigma q) = q = p$. Ainsi les applications σq et $qh : X \to Y$ sont deux relèvements de $(X, y) \to (B, p(y)$ à $(Y, q(y) \to (B, p(y)$ qui prennent la même valeur en y. Elles sont donc égales. On déduit alors les égalités : $q(hfh^{-1}) = \sigma qfh^{-1} = \sigma qh^{-1} = qhh^{-1} = q$. D'où notre assertion.

4) Considérons maintenant un revêtement $r : (Y, y_0) \to (B, b_0)$ tel que le sous-groupe $G(q)$ correspondant soit *distingué* dans $G(p)$. Montrons que r est galoisien.

On construit pour cela une application (de restriction) $\delta : G(p) \to G(r)$. Soit h un élément de $G(p)$. Il s'agit de voir qu'il existe une unique application $\delta(h) : Y \to Y$ qui soit un homéomorphisme de Y sur Y tel que

$$q \circ h = \delta(h) \circ q \quad \text{et} \quad r \circ \delta(h) = r. \tag{3}$$

a) Vérifions l'existence de $\delta(h)$ satifaisant à la première égalité ci-dessus. On considère pour cela x et x' deux éléments de X tels que $q(x) = q(x')$. Il s'agit de vérifier que l'on a $qh(x) = qh(x')$. Puisque q est un revêtement galoisien, il existe σ dans $G(q)$ tel que l'on ait $x' = \sigma(x)$. Or on a $h\sigma = (h\sigma h^{-1})h = \sigma_1 h$, où $\sigma_1 = h\sigma h^{-1}$ est un élément de $G(q)$ (car $G(q)$ est par hypothèse distingué dans $G(p)$). On a ainsi $h(x') = h\sigma(x) = \sigma_1 h(x)$, d'où l'on déduit que $qh(x') = q\sigma_1 h(x) = qh(x)$. D'où notre assertion. Par ailleurs l'application q étant surjective, $\delta(h)$ est entièrement déterminée par l'égalité $q \circ h = \delta(h) \circ q$, ce qui montre l'unicité d'une telle application.

b) L'application $\delta(h)$ est une bijection de Y sur Y. En effet, on a les égalités

$$\delta(h^{-1}) \circ \delta(h) = \delta(h^{-1}) \circ \delta(h) = 1_Y.$$

Pour le vérifier, il suffit de constater que l'on a $\delta(h^{-1}) \circ \delta(h) \circ q = \delta(h) \circ \delta(h^{-1}) \circ q = q$.

c) On a $r\delta(h) = r$. En effet, on a $r\delta(h)q = rqh = ph = p = rq$. D'où l'égalité annoncée car q est surjective.

d) Montrons maintenant que $\delta(h)$ est un homéomorphisme de Y sur Y. Il suffit pour cela de vérifier que $\delta(h)$ est continue, car cela prouvera aussi la continuité de $\delta(h^{-1})$. Soit U un ouvert de Y. Puisque q est une application ouverte et que q et h sont continues, il suffit en fait de démontrer la formule $q(h^{-1}q^{-1}(U)) = \delta(h)^{-1}(U)$, ce qui immédiat : en effet, soit y un élément de $\delta(h)^{-1}(U)$. Il existe t dans X tel que $q(t) = y$ (q est surjective) et l'on a $qh(t) = \delta(h)q(t) = \delta(h)(y)$ qui est donc dans U et y appartient à $q(h^{-1}q^{-1}(U))$. Inversement si z est dans $q(h^{-1}q^{-1}(U))$, on a $z = q(t)$, où t appartient à $h^{-1}q^{-1}(U)$. Donc $qh(t) = \delta(h)q(t)$ est dans U et z appartient à $\delta(h)^{-1}(U)$. D'où l'égalité annoncée.

On déduit de là que r est galoisien. En effet, soient y et y' deux éléments de Y tels que $r(y) = r(y')$. Soient x et x' dans X tels que $q(x) = y$ et que $q(x') = y'$. On a $p(x) = p(x')$ et donc il existe h dans $G(p)$ tel que l'on ait $h(x) = x'$ (car p est galoisien). On a alors

$\delta(h)(y) = \delta(h)q(x) = qh(x) = q(x') = y'$, ce qui montre que $G(r)$ agit transitivement dans les fibres de r, et donc que r est galoisien (cf. les alinéas a), b), c) et d) précédents).

Cela termine la démonstration du théorème.

Proposition 7.3. *Soit $r : (Y, y_0) \to (B, b_0)$ un revêtement intermédiaire de $p : (X, x_0) \to (B, b_0)$. Supposons que r soit galoisien. Soit q le revêtement $(X, x_0) \to (Y, y_0)$ correspondant. On a la suite exacte de groupes*

$$1 \longrightarrow G(q) \xrightarrow{i} G(p) \xrightarrow{\delta} G(r) \longrightarrow 1,$$

où i est l'inclusion canonique $G(q) \to G(p)$, et où $\delta : G(p) \to G(r)$ est l'application définie par l'égalité $\delta(h) \circ q = h \circ q$ pour tout h dans $G(p)$. En particulier, le groupe quotient $G(p)/G(q)$ est isomorphe à $G(r)$ via δ passée au quotient.

Démonstration : Il s'agit de démontrer que δ est un homomorphisme surjectif de groupes dont le noyau est $G(q)$.

Soient h et h' deux éléments de $G(p)$. On a $\delta(h)q = qh$ et $\delta(h')q = qh'$. On a ainsi $q(hh') = \delta(h)qh' = \delta(h)\delta(h')q$. Or $\delta(hh')$ est l'unique application de Y dans Y vérifiant $q(hh') = \delta(hh')q$. D'où l'égalité $\delta(hh') = \delta(h)\delta(h')$ et le fait que δ soit un homomorphisme de groupes.

Vérifions que δ est surjectif. Soit σ un élément de $G(r)$. Partons d'un élément x de X. Posons $y = q(x)$ et $y' = \sigma(y)$. Soit par ailleurs x' dans X tel que $q(x') = y'$. On a $p(x') = r(y') = r\sigma(y) = r(y) = p(x)$. Il existe donc h dans $G(p)$ tel que $h(x) = x'$. Montrons que l'on a $\delta(h) = \sigma$. Il s'agit de montrer que l'on a l'égalité $\sigma q = qh$ (σq et qh sont des applications de X dans Y). On a $r(\sigma q) = (r\sigma)q = rq = p = ph = rqh$, et $\sigma q(x) = qh(x)$. Ainsi σq et qh sont deux relèvements de $r\sigma q : X \to B$ à $r : Y \to B$ qui coïncident en un point. Ils sont donc égaux, ce qui prouve notre assertion.

Déterminons le noyau de δ. Soit h un élément de $G(p)$ tel que $\delta(h) = 1_Y$. On a alors $qh = q$ et h est donc dans $G(q)$. Inversement si h est dans $G(q)$, on a $qh = q$, et par définition de δ, $\delta(h)$ est l'identité de Y. D'où le fait que le noyau de δ soit le groupe $G(q)$ et la proposition.

VII.3. Cas d'un revêtement simplement connexe

Soit $p : (X, x_0) \to (B, b_0)$ un revêtement simplement connexe de B (s'il existe) : X est donc par définition simplement connexe. On a construit un homomorphisme de groupes $\rho : \pi_1(B, b_0) \to G(p)$ qui est défini par l'égalité $\rho(\alpha)(x_0) = x_0.\alpha$ pour tout α de $G(p)$ (où $x_0.\alpha$ est l'opération de α sur x_0 qui est dans la fibre $p^{-1}(b_0)$). Lorsque p est un revêtement simplement connexe de B, ρ est un isomomorphisme de groupes. On déduit de ce qui précède le résultat suivant :

Théorème 7.2. *Il existe une correspondance bijective entre les sous-groupes du groupe fondamental $\pi_1(B, b_0)$ et les classes d'isomorphisme de revêtements connexes pointés de*

base (B, b_0). *Dans cette correspondance, les revêtements galoisiens sont les revêtements qui correspondent aux sous-groupes distingués de* $\pi_1(B, b_0)$.

Démonstration : On remarque d'abord que le revêtement $p : (X, x_0) \to (B, x_0)$ est un objet initial dans la catégorie des revêtements pointés de base (B, b_0), autrement dit que les revêtements connexes pointés de base (B, b_0) sont des revêtements intermédiaires de p. Par ailleurs, l'ensemble des classes d'isomorphisme de revêtements connexes pointés de base (B, b_0) est exactement l'ensemble des classes d'isomorphisme de revêtements intermédiaires de p ; en effet, si $r : (Y, y_0) \to (B, b_0)$ et $r' : (Y', y_0') \to (B, b_0)$ sont deux revêtements de p équivalents comme revêtement connexes pointés, ils le sont aussi comme revêtements intermédiaires de p : soit h un homéomorphisme de (Y', y_0') sur (Y, y_0) tel que $rh = r'$. Si q et q' sont les deux revêtements $(X, x_0) \to (Y, y_0)$ et $(X, x_0) \to (Y', y_0')$ correspondant à r et r', il suffit pour le voir de vérifier que $hq' = q$, ce qui résulte du fait que q et hq' sont deux relèvements de p à r qui coïncident en x_0. Il suffit ensuite d'utiliser le théorème de la correspondance de Galois et le fait que $\rho : \pi_1(B, b_0) \to G(p)$ soit un isomorphisme de groupes pour obtenir le résultat.

Proposition 7.4. *Supposons toujours* X *simplement connexe. Soit* $r : (Y, y_0) \to (B, b_0)$ *un revêtement intermédiaire de* p. *Soit* q *le revêtement* $(X, x_0) \to (Y, y_0)$ *correspondant à* r. *Supposons que* r *soit fini, i.e. que les fibres de* r *soient finies de cardinal* n. *Alors l'image de* $\rho^{-1}\big(G(q)\big)$ *par* $\pi_1(r, y_0)$ *dans* $\pi_1(B, b_0)$ *est un sous-groupe d'indice* n *de* $\pi_1(B, b_0)$.

Démonstration : On a la suite exacte de groupes

$$1 \longrightarrow \pi_1(X, x_0) \xrightarrow{\pi_1(q)} \pi_1(Y, y_0) \xrightarrow{\rho} G(q) \longrightarrow 1.$$

Puisque X est par hypothèse simplement connexe, on a $\pi_1(X, x_0) = \{1\}$ et le groupe fondamental $\pi_1(Y, y_0)$ est donc isomorphe via ρ à $G(q)$. Par ailleurs l'ensemble des classes à droite de $\pi_1(B, b_0)$ modulo l'image de $\pi_1(Y, y_0)$ par $\pi_1(r, y_0)$ dans $\pi_1(B, b_0)$ est en bijection avec l'ensemble $r^{-1}(b_0)$. Or l'application $\pi_1(r, y_0)$ est injective. Donc $\pi_1(Y, y_0)$ et son image dans $\pi_1(B, b_0)$ sont des groupes isomorphes. On déduit de là que $\pi_1(r, y_0)\big(\rho^{-1}(G(q))\big)$ est d'indice n dans $\pi_1(B, b_0)$. D'où le résultat.

VII.4. Existence d'un revêtement simplement connexe

Dans toute la suite de ce paragraphe B est un espace connexe et LCA. On va démontrer le théorème suivant qui fournit une condition nécessaire et suffisante pour l'existence d'un revêtement simplement connexe de B.

Théorème 7.3. *Pour qu'il existe un revêtement* $p : X \to B$ *tel que* X *soit simplement connexe il faut et il suffit que* B *possède la propriété suivante :*

(Π) *: pour tout élément* b *de* B, *il existe un ouvert* U *connexe contenant* b *tel que l'homomorphisme* $\pi_1(U, b) \to \pi_1(B, b)$ *induit par l'inclusion* $U \to B$ *soit neutre, i.e. que son image soit réduite à l'élémént neutre de* $\pi_1(B, b)$.

Remarques. 1) Le fait que l'homomorphisme $\pi_1(U,b) \to \pi_1(B,b)$ soit neutre signifie que tout lacet de U d'origine b est homotope dans B au lacet constant d'origine b.

2) Soit b un élément de B et U un ouvert connexe de B contenant b tel que l'homomorphisme $\pi_1(U,b) \to \pi_1(B,b)$ soit neutre. Alors pour tout point b' de U l'homomorphisme $\pi_1(U,b') \to \pi_1(B,b')$ est aussi neutre (autrement dit la propriété (Π) relative à U ne dépend pas du point b de U).

Démonstration : On remarque d'abord que U est connexe par arcs, car il est connexe par hypothèse et B est LCA. On choisit ensuite un chemin c de U d'origine b et d'extrémité b'. L'application $\pi_1(U,b) \to \pi_1(U,b')$ définie par $[\gamma] \mapsto [c^{-1}\gamma c]$ est un isomorphisme de groupes. De même si $i : U \to B$ est l'injection canonique, l'application $[\delta] \mapsto [(i \circ c)^{-1}\delta(i \circ c)]$ est un isomorphisme de $\pi_1(B,b) \to \pi_1(B,b')$. Enfin si γ est un chemin de U d'origine b, on a l'égalité des chemins (d'origine et d'extrémité b') $(i \circ c^{-1})(i \circ \gamma)(i \circ c) = i \circ (c^{-1}\gamma c)$. Cela entraîne notre assertion.

Définition 7.2. *On dit qu'un ouvert U de B est privilégié s'il est connexe et si pour tout b dans U, l'homorphisme $\pi_1(U,b) \to \pi_1(B,b)$ est neutre.*

Le théorème peut alors se reformuler de la façon suivante :

Théorème 7.4. *Pour qu'il existe un revêtement $p : X \to B$ tel que X soit simplement connexe il faut et il suffit que B puisse être recouvert par des ouverts privilégiés.*

Corollaire 7.1. *Une variété topologique connexe possède un revêtement simplement connexe.*

Démonstration : En effet chaque point d'un tel espace topologique possède (par définition) un voisinage simplement connexe.

Avant de commencer la démonstration du théorème prouvons d'abord l'énoncé suivant :

Proposition 7.5. *Pour qu'un ouvert connexe U de B soit privilégié, il faut et il suffit que, pour tout couple de points b et b' de U, l'image de l'application $\Phi : \pi_1(U; b, b') \to \pi_1(B; b, b')$, définie par $[\gamma] \mapsto [i \circ \gamma]$, ait un seul élément.*

Démonstration : Considérons deux éléments β_0 et β_1 de $\pi_1(U; b, b')$. On a $\beta_0 = [c_0]$ et $\beta_1 = [c_1]$, où c_0 et c_1 sont deux chemins de U d'origine b et d'extrémité b'. Dans le groupoïde fondamental de U on a l'égalité $\beta_1 = \alpha.\beta_0$, où α appartient à $\pi_1(U,b)$. Il résulte de l'égalité des chemins $i \circ c_1 = (i \circ \tilde{\alpha})(i \circ c_0)$ (où $\tilde{\alpha}$ est un relèvement de α) que l'on a l'égalité $\Phi(\beta_1) = \Phi(\alpha).\Phi(\beta_0)$. Si U est privilégié, $\Phi(\alpha)$ est l'élément neutre, et donc $\Phi(\beta_1) = \Phi(\beta_0)$. Inversement, supposons que pour tout β_0 et β_1 de $\pi_1(U; b, b')$ on ait $\Phi(\beta_1) = \Phi(\beta_0)$. On a alors en particulier $\Phi(\beta_0) = \Phi(\alpha).\phi(\beta_0)$, pour tout α de $\pi_1(U,b)$. Cela montre que pour tout α de $\pi_1(U,b)$, $\Phi(\alpha)$ est l'élément neutre. D'où le résultat.

Démonstration du théorème

1) Montons que la condition (Π) est nécessaire pour l'existence d'un revêtement simplement connexe. Soient donc $p : X \to B$ un revêtement simplement connexe de B. Soient b un point de B et U un ouvert connexe trivialisant pour p. On montre que U est un ouvert privilégié. On considère pour cela une composante connexe V de $p^{-1}(U)$ qui s'envoie homéomorphiquement sur U via p. Soit x le point de V tel que $p(x) = b$. Soient $\gamma : [0,1] \to V$ un lacet d'origine x et $j : U \to B$ et $i : V \to X$ les inclusions canoniques. Les applications $j \circ p \circ \gamma$ et $p \circ i \circ \gamma$ sont égales (car $p \circ i = j \circ p$). En particulier les homomorphismes de groupes que l'on déduit par passage aux quotients $\pi_1(V,x) \to \pi_1(X,x) \to \pi_1(B,b)$ et $\pi_1(V,x) \to \pi_1(U,b) \to \pi_1(B,b)$ commutent. Puisque $\pi_1(X,x)$ est réduit à l'élément neutre car X est par hypothèse simplement connexe, cela entraîne que l'homomorphisme $\pi_1(U,b) \to \pi_1(B,b)$ est neutre. D'où notre assertion.

2) Inversement supposons que l'on puisse recouvrir B par des ouverts privilégiés. On va construire un revêtement $p : X \to B$ où X est un espace simplement connexe. On définit d'abord X en tant qu'ensemble. On choisit pour cela désormais un point b_0 de B. Par définition X est la réunion disjointe des ensembles $\pi_1(B; b_0, b)$ lorsque b parcourt B. L'ensemble X est donc par définition l'ensemble des classes de chemins de B d'origine b_0 et d'extrémité quelconque. On définit alors l'application $p : X \to B$ par l'égalité $p(\alpha) = x$, où x est l'extrémité de n'importe quel chemin qui représente α. Autrement dit, à un chemin de B d'originie b_0, p associe son extrémité. Il s'agit maintenant de définir sur X une topologie telle que l'application $p : X \to B$ soit un revêtement et que X, muni de cette topologie, soit simplement connexe.

2.1) Définition des sections privilégiées : pour tout ouvert U privilégié, et pour tout point x de $p^{-1}(U)$ on définit une section

$$s_x : U \to X,$$

telle que x appartienne à $s_x(U)$. Considérons donc un ouvert privilégié U et x un élément de $p^{-1}(U)$. Posons $b = p(x)$: par définition b est l'extrémité de x. Soit b' un élément de U. D'après la proposition ci-dessous, il existe un élément γ de $\pi_1(U; b, b')$ tel que l'image de l'application $\pi_1(U; b, b') \to \pi_1(B; b, b')$ soit réduite à $\{\gamma\}$. On pose alors par définition

$$s_x(b') = x.\gamma,$$

où $x.\gamma$ est le composé des chemins $x \in \pi_1(B; b_0, b)$ et de $\gamma \in \pi_1(B; b, b')$. Par définition $x.\gamma$ est donc un élément de $\pi_1(B; b_0, b')$, et l'on a ainsi l'égalité

$$p(s_x(b')) = b'.$$

Cette égalité définit donc une section $s_x : U \to X$. Toute section obtenue de cette manière est appelée une section privilégiée. Ces sections possèdent les propriétés suivantes :

(i) Soient U un ouvert privilégié et x un élément de $p^{-1}(U)$. Si $b = p(x)$, on a $s_x(b) = x$ (autrement dit x appartient à l'image de s_x) : cela résulte du fait que l'élément γ qui correspond à b est l'élément neutre de $\pi_1(B, b)$.

(ii) Les images de deux sections privilégiées sont soit disjointes soit égales. En effet, soit x' un point de $s_x(U)$. Posons $b = p(x)$. On a $x' = s_x(a)$ où a appartient à U. Par ailleurs, on a par définition $s_x(a) = x.\gamma_0$ où γ_0 appartient à l'image de l'application $\pi_1(U; b, a) \to \pi_1(B; b, a)$. Considérons alors un point b' de U. On a $s_{x'}(b') = x'.\gamma'$, où γ' appartient à l'image de $\pi_1(U; a, b') \to \pi_1(B; a, b')$. De même on a $s_x(b') = x.\gamma$, où γ appartient à l'image de $\pi_1(U; b, b') \to \pi_1(B; b, b')$. On a alors $x'.\gamma' = x.\gamma_0.\gamma'$. Or $\gamma_0.\gamma'$ appartient à l'image de l'application $\pi_1(U; b, b') \to \pi_1(B; b, b')$ (c'est facile à vérifier). Puisque U est privilégié , on a donc $\gamma = \gamma_0.\gamma'$ (cf. la proposition précedente). Cela conduit à l'égalité $x'.\gamma' = x.\gamma$, et montre que $s_{x'}(b') = s_x(b')$. D'où notre assertion.

(iii) Soient U et U' deux ouverts privilégiés tels que U' soit contenu dans U. Si $s : U \to X$ est une section privilégiée, la restriction de s à U' est aussi une section privilégiée : cela résulte des définitions.

Lemme 7.4. *Il existe sur X une topologie possédant la propriété suivante : pour tout ouvert privilégié U contenu dans B, et toute section privilégiée $s : U \to X$, s est un homéomorphisme de U sur $s(U)$, qui est ainsi un ouvert de X.*

Démonstration : On définit la topologie suivante sur X ; une partie O de X est ouverte si et seulement elle possède la propriété ci-dessous :

pour tout x de O il existe un ensemble de la forme $s(U)$, où U est un ouvert privilégié, et $s : U \to X$ une section privilégiée, qui contient x et qui est contenu dans O.

Vérifions qu'il s'agit bien d'une topologie sur X. D'abord l'ensemble vide appartient à la famille de parties de X définies de la sorte. Il en est de même de la partie X : en effet si x est dans X, il existe un ouvert privilégié U de B tel que x soit dans $p^{-1}(U)$. Ainsi x appartient à $s_x(U)$. Considérons maintenant une partie de la forme $s(U)$ et $s'(U')$. Soient x un élément de $s(U) \cap s'(U')$ et $b = p(x)$. L'élément b est dans $U \cap U'$. Puisque B est localement connexe, il existe un ouvert V connexe contenu dans $U \cap U'$ et contenant b. L'ensemble V est un ouvert privilégié. Soient s_1 et s'_1 les restrictions de s et s' à V. Ce sont des sections privilégiées et x est dans $s_1(V) \cap s'_1(V)$. On a donc $s_1 = s'_1$. Si l'on note $s'' : V \to X$ cette section privilégiée, $s''(V)$ est contenu dans $s(U) \cap s'(U')$ et contient x. Cela prouve notre assertion.

Démontrons maintenant le lemme. Soient donc U un ouvert privilégié, et $s : U \to X$ une section privilégiée. D'abord s est évidemment une bijection de U sur $s(U)$ dont l'application réciproque est p. Par ailleurs, p est continue : soit V un ouvert de B. Soit x un élément de $p^{-1}(V)$. Posons $b = p(x)$. Soit V' un ouvert privilégié contenant b et contenu dans B (il en existe un par définition). On a $p \circ s_x(V') = V'$ et donc $s_x(V')$, qui contient x, est contenu dans $p^{-1}(V)$. Cela montre que $p^{-1}(V)$ est un voisinage de chacun

de ses points, autrement dit que c'est un ouvert de X. Enfin l'application s est ouverte. En effet, soit V un ouvert de B contenu dans U. L'ensemble V est un ouvert privilégié, $s\mid_V : V \to X$ est une section privilégié, et donc $s(V)$ est par définition un ouvert de X. L'application s étant ouverte continue et bijective sur $s(U)$, cela montre le lemme.

Vérifions maintenant que $p : X \to B$ est un revêtement. En fait tout ouvert privilégié U de B est trivialisant pour p. En effet, $p^{-1}(U)$ est la réunion disjointe des ouverts $s(U)$, lorsque s parcourt les sections privilégiées $s : U \to X$. D'abord cette réunion est disjointe, car si $s(U) \cap s'(U)$ n'est pas vide,on a $s = s'$. Par ailleurs si x est dans $p^{-1}(U)$, x appartient à $s_x(U)$. Inversement pour toute section privilégiée $s : U \to X$, $p(s(U)) = U$ et $s(U)$ est contenu dans $p^{-1}(U)$. Or d'après l'alinéa précédent, si s est une section privilégiée de U dans X, p est un homéomorphisme de $s(U)$ sur U (les $s(U)$ sont alors nécessairement les composantes connexes de $p^{-1}(U)$ car U est connexe). Cela prouve notre assertion.

Il reste à vérifier que X est simplement connexe. On étudie pour cela les chemins de X d'origine la classe du chemin constant en b_0 de B. On notera x_0 cet élément $(x_0 \in \pi_1(B, b_0))$.

Lemme 7.5. *Soit $f : I \to X$ un chemin d'origine x_0. Posons $g = p \circ f : I \to B$ (g est un chemin de B). Pour tout $t \in I$, on a $f(t) = [g_t]$, où g_t est le chemin de B défini par l'égalité*

$$g_t(u) = g(tu) \quad \textit{pour tout} \quad u \in B.$$

(On a $g_t(0) = p(x_0) = b_0$ et $g_t(1) = g(t)$ pour tout $t \in I$).

Démonstration : Montrons que l'application de I dans X

$$t \mapsto [g_t],$$

qui à $t \in I$ associe la classe du chemin g_t de B est continue. On considère pour cela un élément t_1 de I. On pose $x_1 = [g_{t_1}]$. Soit U un ouvert privilégié de B contenant $p(x_1) = g(t_1)$. Puisque g est une application continue, il existe un voisinage ouvert J_{t_1} de t_1 dans I tel que pour tout $t \in J_{t_1}$, $g(t)$ appartienne à U. La section privilégiée $s_{x_1} : U \to X$ est telle que $s_{x_1}(g(t)) = [g_t] \in s_{x_1}(U)$ pour tout $t \in J_{t_1}$: en effet, cela résulte des égalités $s_{x_1}(g(t)) = s_{x_1}(g_t(1)) = s_{x_1}(p([g_t]))$. Puisque les applications s_{x_1} et g sont continues, l'application $t \mapsto [g_t]$ est continue sur J_{t_1}. Elle donc continue sur I tout entier.

Par ailleurs on a $p([g_t]) = g_t(1) = g(t)$ (par définition).L'application $t \mapsto [g_t]$ est donc un relèvement de $g : I \to B$ au revêtement $p : X \to B$ qui prend la valeur x_0 en 0. Or par définition f est aussi un tel relèvement. On a donc $f(t) = [g_t]$ pour tout $t \in I$ (cf. le théorème d'unicité des relèvements des chemins). Cela montre le lemme.

Fin de la démonstration du théorème : montrons d'abord que X est connexe par arcs. Soit x un point de X. Par définition x est la classe $[g]$ d'un chemin de B d'origine

b_0. D'après le lemme 7.5, l'application $t \mapsto [g_t]$ est le relèvement de g d'origine x_0. Son extrémité est x. En effet, l'extrémité de $t \mapsto [g_t]$ est $[g_1]$ qui, par définition, est $[g] = x$. Cela montre que, pour tout $x \in X$, x_0 et x peuvent être joints par un chemin. D'où notre assertion.

Il s'agit maintenant de prouver que le groupe $\pi_1(X, x_0)$ est réduit à l'élément neutre. Soit α un élément de $\pi_1(X, x_0)$. Soit $f : I \to X$ un lacet de X d'origine x_0 qui représente α. Posons $g = p \circ f$. D'après le lemme, l'extrémité de f est $[g_1] = [g]$. Or $f(1) = x_0$. Ainsi $[g] = x_0$ est la classe du lacet constant de B en b_0, autrement dit g est homotope au lacet de B constant d'origine b_0. Cela entraîne que f , qui est le relèvement de g d'origine x_0, est aussi homotope au lacet constant de X d'origine x_0. D'où le résultat.

Cela termine la démonstration du théorème.

Notions topologiques pr éliminaires

1. Homotopie de deux applications continues

On note I le segment $[0,1]$.

Définition 1.1. *Soient X et Y deux espaces topologiques. Étant données deux applications continues $f_0 : X \to Y$ et $f_1 : X \to Y$, on dit que f_0 est homotope à f_1 s'il existe une application continue*

$$F : X \times I \to Y,$$

telle que, pour tout x dans X, l'on ait les égalités

$$F(x,0) = f_0(x) \quad et \quad F(x,1) = f_1(x).$$

Proposition 1.1. *La relation d'homotopie est une relation d'équivalence dans l'ensemble des applications continues de X dans Y.*

Notation. *On notera $[X,Y]$ l'ensemble des classes d'équivalence d'applications continues pour la relation d'homotopie.*

Proposition 1.2. *Soient X, Y et Z trois espaces topologiques et pour $i = 0,1$, soient $f_i : X \to Y$, $g_i : Y \to Z$ deux applications continues. Si f_0 est homotope à f_1 et g_0 homotope à g_1, alors $g_0 \circ f_0$ est homotope à $g_1 \circ f_1$.*

Cette proposition permet de définir la composition de deux classes d'applications. On obtient ainsi une loi de composition

$$[Y,Z] \times [X,Y] \to [X,Z],$$

définie par $(\varphi, \psi) \mapsto \varphi \circ \psi$ qui est associative. Cela permet de définir une catégorie (Tophom) dont les objets sont les espaces topologiques et l'ensemble des morphismes de X dans Y est $[X,Y]$.

2. Équivalence d'homotopie, type d'homotopie

Définition 2.1. *On dit qu'une application continue $f : X \to Y$ est une équivalence d'homotopie si sa classe dans $[X,Y]$ est un isomorphisme de la catégorie (Tophom). Autrement dit, une application continue $f : X \to Y$ est une équivalence d'homotopie si et seulement si il existe une application continue $g : Y \to X$ telle que $g \circ f$ soit homotope à l'identité de X et que $f \circ g$ soit homotope à l'identité de Y.*

La composée de deux équivalences d'homotopie est une équivalence d'homotopie.

Définition 2.2. *On dit que deux espaces topologiques X et Y ont le même type d'homotopie s'il existe une équivalence d'homotopie $f : X \to Y$. Cela revient à dire que X et Y sont isomorphes dans la catégorie (Tophom).*

Deux espaces homéomorphes ont le même type d'homotopie, mais la réciproque est fausse.

3. Espaces contractiles

Définition 3.1. *On dit qu'un espace topologique est contractile s'il a le même type d'homotopie qu'un espace réduit à un point.*

Proposition 3.1. *Soit X un espace topologique. Les conditions suivantes sont équivalentes :*

(i) X est contractile ;
(ii) Pour tout espace Y, l'ensemble $[Y, X]$ possède un seul élément ;
(iii) X est non vide et $[X, X]$ possède un seul élément ;
(iv) l'application identique de X est homotope à une application constante.

Démonstration : (i) $\Rightarrow$ (ii) : par hyopthèse X est homotope à un espace P réduit à un point. Ainsi l'unique application $\varphi : X \to P$ est une équivalence d'homotopie. Si Y est un espace topologique, φ induit donc une bijection

$$[Y, X] \to [Y, P],$$

définie par $\psi \mapsto \bar{\varphi} \circ \psi$, où $\bar{\varphi}$ est la classe d'homotopie de φ. Or $[Y, P]$ a un seul élément. D'où l'implication.

Les implications (ii) $\Rightarrow$ (iii) et (iii) $\Rightarrow$ (iv) sont évidentes.

Démontrons maintenant l'implication (iv) $\Rightarrow$ (i). On suppose donc que l'application identique de X est homotope à une application constante $\varphi : X \to X$: on a $\varphi(x) = a$ pour tout x de X. Par définition on a $\varphi = i \circ f$, où $f : X \to \{a\}$ est l'application constante et $i : \{a\} \to X$ l'injection canonique. Puisque $i \circ f$ est homotope à l'identité, f est une équivalence d'homotopie, car $f \circ i : \{a\} \to \{a\}$ est l'application identique. Cela montre que X a le même type d'homotopie qu'un point, i.e. que X est contractile. D'où le résultat.

Exemples d'espaces contractiles : 1) Soit E un espace vectoriel normé sur $\mathbb{R}$. Tout sous-espace X de E qui est étoilé par rapport à l'un de ses points $\{a\}$ est contractile (cette condition signife que pour tout x de X, le segment $[a, x]$ est contenu dans X, autrement dit que l'application $x \mapsto a + t(x - a)$, avec t dans $[0, 1]$, envoie X dans lui même) : en effet, la fonction $F : X \times I \to X$, définie par $F(x, t) = a + t(x - a)$, est une homotopie de l'application constante $x \mapsto a$ à l'application identique de X. En particulier les ensembles convexes de E sont contractiles. Tel est par exemple le cas des boules ouvertes ou fermées de E.

2) Soit X un espace topologique. On définit le *cône* de X, que l'on note souvent $C(X)$, comme étant l'espace quotient de $X \times I$ par la relation d'équivalence qui identifie entre eux les points de $X \times \{0\}$, les autres classes d'équivalences étant réduites à un point. On peut démontrer que $C(X)$, muni de la topologie quotient, est un espace contractile.

4. Espaces connexes, localement connexes, connexes par arcs et localement connexes par arcs

Nous allons rappeler ces différentes notions qui sont fondamentales pour la théorie des revêtements des espaces topologiques. On considère désormais un espace topologique X.

4.1. Connexité

On dit que X est connexe si les seules parties de X qui sont à la fois ouvertes et fermées sont X et l'ensemble vide. Cela revient par exemple à demander que X ne soit pas réunion de deux ouverts non vides disjoints, ou bien que toute application continue de X dans un espace discret soit constante. Un sous-espace de X est connexe si, muni de la topologie induite, c'est un espace connexe.

1) Si X est connexe, son image par une application continue est aussi un espace connexe.
2) Si X est réunion d'une famille (A_i) de sous-espaces connexes dont l'intersection *n'est pas vide*, X est aussi connexe.
3) Si X et Y sont deux espaces connexes, le produit $X \times Y$ est connexe.
4) Soient A un sous-espace connexe de X et B un sous-espace de X contenant A et contenu dans l'adhérence de A. Alors B est connexe (en particulier l'adhérence de A est connexe).
5) Si X est connexe tout espace quotient de X est connexe.

Exemples. L'espace $\mathbb{R}^n$ est connexe. Les parties connexes de $\mathbb{R}$ sont les intervalles. Les parties connexes de $\mathbb{Q}$ sont les points. Un espace discret ayant plus d'un point n'est pas connexe. L'ensemble $\mathbb{GL}_n(\mathbb{R})$ n'est pas connexe.

Définition 4.1. *Une composante connexe de X est un sous-espace connexe maximal de X.*

6) Soit A un sous-espace connexe non vide de X. Soit (C_i) la famille de tous les sous-espaces connexes de X contenant A. Alors la réunion des parties C_i est un sous-espace de X connexe et fermé qui contient A. C'est la composante connexe de A dans X. Une composante connexe de X est donc toujours une partie *fermée* de X.

Supposons que X soit un *groupe topologique* d'élément neutre e.

a) La composante connexe de $\{e\}$ est un sous-groupe fermé distingué de X.
b) Supposons de plus X connexe. Soit U un voisinage de $\{e\}$. Alors le sous-groupe de X engendré par U est X tout entier.

4.2. Connexité locale

On dit que X est localement connexe si tout point de X possède un système fondamental de voisinages connexes. Tel est par exemple le cas d'un ouvert de $\mathbb{R}^n$ (tout ouvert d'un espace localement connexe est localement connexe). Un espace peut être localement connexe sans être connexe : tel est le cas d'un espace discret ayant plus d'un point. Si X est localement connexe, tout quotient de X est aussi localement connexe. Si X et Y sont deux espaces localement connexes, le produit $X \times Y$ est aussi localement connexe.

Proposition 4.1. *Pour que X soit localement connexe, il faut et il suffit que toute composante connexe d'un ensemble ouvert dans X soit ouverte dans X. En particulier si X est localement connexe, les composantes connexes de X sont des ensembles ouverts de X.*

Démonstration : La condition est suffisante : soient x un point de X et V un voisinage ouvert de X contenant x. La composante connexe de V contenant x est alors un voisinage de x dans X. Inversement, soient A un ensemble ouvert de X et B une composante connexe de A et x un point de B. Par hypothèse il existe un voisinage connexe V de x contenu dans A. Par définition V est contenu dans B, ce qui prouve que B est un ouvert de X. D'où le résultat.

Corollaire 4.1. *Si X est localement connexe, les composantes connexes de X constituent une partition de X formée d'ensembles ouverts dans X.*

On déduit de là que dans un espace localement connexe tout point possède un système fondamental de voisinages *ouverts* connexes.

4.3. Connexité par arcs

On dit que X est connexe par arcs si pour tous points x et y dans X, il existe un chemin de X joignant x à y. Si X est connexe par arcs son image par une application continue est connexe par arcs. Le produit de deux espaces connexes par arcs est connexe par arcs. Un espace réduit à un seul point, un sous-ensemble convexe de $\mathbb{R}^n$, et $\mathbb{R}^n - \{0\}$ si n est ≥ 2, sont des espaces connexes par arcs. Si X est réunion d'une famille (A_i) de sous-espaces connexes par arcs dont l'intersection *n'est pas vide*, X est aussi connexe par arcs. Si X et Y sont deux espaces connexes par arcs , le produit $X \times Y$ est connexe par arcs.

Proposition 4.2. *Si X est connexe par arcs, il est connexe.*

Démonstration : Soit x un point de X. Pour tout point y de X, il existe par hypothèse un chemin c_y de X qui joint x à y. Par suite on a l'égalité $X = \cup_{y \in X} c_y(I)$. D'où le résultat, car I est connexe, c_y est continue et x appartient à tous les $c_y(I)$.

Définition 4.2. *Une composante connexe par arcs de X est un sous-espace connexe par arcs maximal de X.*

Étant donnée une partie A de X, la composante connexe par arcs de A est contenue dans la composante connexe de A. Ces deux composantes sont en général distinctes.

Soit A un sous-espace connexe par arcs non vide de X. Soit (C_i) la famille de tous les sous-espaces connexes par arcs de X contenant A. La réunion des parties C_i est un sous-espace de X connexe par arcs qui contient A. C'est la composante connexe par arcs de A dans X.

4.4. Connexité par arcs locale

On dit que X est localement connexe par arcs si tout point de X possède un système fondamental de voisinages connexes par arcs. Un ouvert de $\mathbb{R}^n$ est localement connexe par arcs (tout ouvert d'un ensemble localement connexe par arcs est localement connexe par arcs). Si X et Y sont deux espaces localement connexes par arcs, le produit $X \times Y$ est aussi localement connexe par arcs.

Proposition 4.3. *Pour que X soit localement connexe par arcs, il faut et il suffit que toute composante connexe par arcs d'un ensemble ouvert dans X soit ouverte dans X. En particulier si X est localement connexe par arcs, les composantes connexes par arcs de X sont des ensembles ouverts de X.*

Démonstration : La condition est suffisante : soient x un point de X et V un voisinage ouvert de X contenant x. La composante connexe par arcs de V contenant x est alors par définition un voisinage de x dans X. Inversement, soient A un ensemble ouvert de X, B une composante connexe par arcs de A et x un point de B. Par hypothèse il existe un voisinage connexe par arcs V de x contenu dans A. Par définition V est contenu dans B, ce qui prouve que B est un ouvert de X. D'où le résultat.

Proposition 4.4. *Si X est connexe et localement connexe par arcs, il est connexe par arcs.*

Démonstration : Cela résulte du fait que les composantes connexes par arcs de X sont ouvertes et fermées, et que X est connexe.

Corollaire 4.2. *Si X est localement connexe par arcs, ses composantes connexes et ses composantes connexes par arcs sont identiques.*

Démonstration : Soit C une composante connexe de X. Il suffit de montrer qu'elle est connexe par arcs : puisque C est un ensemble ouvert, C est localement connexe par arcs, ce qui entraîne le résultat d'après la proposition précédente.

Si X est localement connexe par arcs tout point de X possède un système fondamental de voisinages *ouverts* connexes par arcs.

5. Espaces simplement connexes

Soit X un espace topologique non vide.

Proposition 5.1. *Les conditions suivantes sont équivalentes:*

(i) pour tout x et y de X, l'ensemble $\pi_1(X; x, y)$ possède un seul élément ;

(ii) l'espace X est connexe par arcs, et pour tout x de X, le groupe $\pi_1(X, x)$ est réduit à l'élément neutre ;

(iii) l'espace X est connexe par arcs, et il existe x dans X, tel que le groupe $\pi_1(X, x)$ soit réduit à l'élément neutre.

Définition 5.1. *On dit que X est simplement connexe s'il satisfait aux conditions équivalentes de la proposition ci-dessus. Un espace simplement connexe est donc un espace connexe par arcs tel que tout lacet d'origine $x \in X$ soit homotope au lacet constant d'origine x.*

Proposition 5.2. *Pour que X soit simplement connexe, il faut et il suffit que l'ensemble $[\mathbb{S}^1, X]$, des classes d'homotopie d'applications continues du cercle unité $\mathbb{S}^1$ de $\mathbb{R}^2$ dans X, soit un ensemble à un élément.*

Démonstration : 1) Montrons d'abord que cette condition est nécessaire. Supposons donc X simplement connexe. Puisque X n'est pas vide, l'ensemble $[\mathbb{S}^1, X]$ possède au moins un élément, à savoir la classe d'une application constante (toutes les applications constantes $\mathbb{S}^1 \to X$ sont en fait homotopes car X est connexe par arcs : prendre comme homotopie l'application $\varphi : \mathbb{S}^1 \times I \to X$ définie par $\varphi(x, t) = \gamma(t)$, où γ est un chenin de X joignant deux points a et b). Considérons alors $f : \mathbb{S}^1 \to X$ une application continue. Il suffit donc de montrer que f est homotope à une application constante. Si $\mathcal{R}$ est la relation d'équivalence sur I consistant à identifier 0 et 1, l'espace quotient $I/\mathcal{R}$ est homéomorphe à $\mathbb{S}^1$ via l'application $t \mapsto \exp(2i\pi t)$ passée au quotient. On déduit de là l'existence d'une application $g : I \to X$ telle que, pour tout t dans I, l'on ait

$$g(t) = f\big(\exp(2i\pi t)\big).$$

L'application g, qui est continue, est un lacet de X d'origine $g(0) = g(1) = f(1) = a$. Puisque X est simplement connexe, g est homotope au lacet constant de base a : soit $G : I \times I \to X$ une homotopie de de g à ce lacet constant. On a par définition les égalités

$$G(t, 0) = g(t), \quad G(t, 1) = a, \quad G(0, s) = a \quad \text{et} \quad G(1, s) = a.$$

On considère alors l'application $\bar{G} : \mathbb{S}^1 \times I \to X$ définie pour tout $(x, s) \in \mathbb{S}^1 \times I$ par

$$\bar{G}(x, s) = G(t, s), \quad \text{où} \quad x = \exp(2\pi i t).$$

On constate alors que l'application $\bar{G}$ définit une homotopie de f à l'application constante $x \mapsto a$.

2) Inversement supposons que $[\mathbb{S}^1, X]$ soit un ensemble à un élément. Montrons que X est simplement connexe. D'abord X est connexe par arcs. En effet, soient a et b deux points de X. Soit G une homotopie des applications de $\mathbb{S}^1$ dans X définies par $x \mapsto a$ et $x \mapsto b$. Si l'on fixe un point x_0 de $\mathbb{S}^1$, l'application $\gamma : I \to X$ définie par $\gamma(t) = G(x_0, t)$ est un chemin de X joignant a à b. Soit alors x un élément de X et un lacet $g : I \to X$ d'origine x. Il s'agit de montrer que g est homotope au lacet constant de base x. On considère pour cela l'application h définie sur le bord du carré $I \times I$ à valeurs dans X par les égalités

$$h(t,0) = g(t), \quad h(t,1) = x, \quad h(0,s) = x \quad \text{et} \quad h(1,s) = x.$$

D'abord cette application est continue. Il s'agit ensuite de pouvoir prolonger h en une application continue sur $I \times I$ tout entier. Soient $\mathbb{B}^2$ la boule unité fermée de $\mathbb{R}^2$ et ω un homéomorphisme $I \times I \to \mathbb{B}^2$ qui transforme le bord du carré $I \times I$ dans le cercle $\mathbb{S}^1$ (une telle application existe : le vérifier !). Par hypothèse, l'application continue $h \circ \omega^{-1} : \mathbb{S}^1 \to X$ est homotope à une application constante. Elle se prolonge donc en une application continue $H : \mathbb{B}^2 \to X$ (cf. $(*)$). L'application $G = H \circ \omega : I \times I \to X$ est continue et coïncide avec h sur le bord du carré $I \times I$, ce qui prouve que G est une homotopie de g au lacet constant de base x. D'où le résultat.

$(*)$ On a utilisé le lemme suivant :

Lemme 5.1. *Soit $f : \mathbb{S}^1 \to X$ une application continue de $\mathbb{S}^1$ dans X homotope à une application constante. Alors f se prolonge en une application continue $\mathbb{B}^2 \to X$.*

Démonstration : Supposons que f soit homotope à l'application constante $x \mapsto a$ via une homotopie G. On vérifie que l'application $g : \mathbb{B}^2 \to X$ définie par

$$g(x) = \begin{cases} a & \text{si } \ 0 \leq \|x\| \leq 1/2 \\ G\big(\frac{x}{\|x\|}, 2 - 2\|x\|\big) & \text{si } \ 1/2 \leq \|x\| \leq 1. \end{cases}$$

est un prolongement cherché de f.

Corollaire 5.1. *Tout espace contractile est simplement connexe.*

Ce corollaire fournit des exemples d'espaces simplement connexes.

Table des matières

Théorie des revêtements d'un espace topologique

Théorie de Galois des revêtements

Notions topologiques préliminaires

Bibliographie

[1]. Cours d'Henri Cartan, sur l'homotopie, le groupe fondamental et les revêtements topologiques, 1968-1969.

[2]. R. et A. Douady, algèbre et théories galoisiennes, vol. 1 et 2, Cedic/Fernand Nathan 1978.

[3]. D.W. Erbach, J. Fischer, J. McKay, *Polynomials with* $\mathbb{PSL}_2(\mathbb{F}_7)$ *as Galois Group*, J. Number Theory 11 (1979), 69-75.

[4]. S. Francinou et H. Gianella, Exercices de Mathématiques pour l'agrégation, Algèbre 1, Masson 1994.

[5]. C. Godbillon, Éléments de topologie algébrique, Hermann 1971.

[6]. I. Gozard, Théorie de Galois, ellipses 1997.

[7]. S. Lang, Algebra, Addison Wesley 1965.

[8]. M.-P. Malliavin, algèbre commutative, Masson 1984.

[9]. J. Querré, Cours d'algèbre, Masson 1976.

[10]. P. Samuel, Théorie algébriques des nombres, deuxième édition, Hermann, Paris 1971.

[11]. E.S. Selmer, *On the irreductibility of certain trinomials*, Math. Scand. 4 (1956), 287-302.

[12]. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331.

[13]. J.-P. Serre, *Groupes de Galois sur* $\mathbb{Q}$, Sem. Bourbaki 1987-1988, n89.

[14]. J.-P. Serre, Topics in Galois Theory, Research Notes in Mathematics, Jones and Bartlett Publishers, 1992.