Analogies entre un résultat de théorie algébrique des nombres et un résultat de topologie

Soudères Ismaël

Table des matières

introduction **1**

1 L'aspect théorie des nombres **3**
1.1 Anneaux de valuation discrète et anneaux de Dedekind 3
1.1.1 Définitions et propriétés 3
1.1.2 Extensions 9
1.2 Cohomologie des groupes 17
1.2.1 Définitions et premières propriétés 17
1.2.2 Le cas fini 24
1.3 Corps 26
1.3.1 Le corps $\mathbb{Q}_p$ 26
1.3.2 Calcul de la cohomologie dans le cas G cyclique d'ordre premier 30

2 Topologie **33**
2.1 Revêtements 33
2.1.1 Généralités 33
2.1.2 Revêtements branchés ou revêtements ramifiés 48
2.2 Théorie des nœuds et entrelacs 49
2.2.1 Généralités 49

3 Une analogie **52**
3.1 Énoncé des théorèmes 52
3.2 Le dictionnaire MKR 53
3.3 Démonstration du théorème 3.1.2 53

introduction

généralités

Ce rapport est l'explicitation d'un article de Adam S. Sikora [Sik01] sur les analogies entre l'action d'un groupe cyclique d'ordre p sur des variétés de dimension 3 et des corps de nombres. Les analogies commencent en mathématiques par être une curiosité. Mais rapidement si une analogie n'est pas anecdotique, elle devient un vrai moteur de recherche. J'ai voulu dans ce rapport expliquer ce qu'il m'avait été nécessaire de comprendre pour saisir quels étaient les objets mis en jeu dans les résultats que démontre A . Sikora. Plutôt que d'apprendre quelques définitions et d'admettre l'ensemble des résultats intermédiaires nécessaire, j'ai préféré essayer de me familiariser avec les théories qui permettent de prouver ces résultats. La première partie est donc consacrée aux bases de la théorie algébrique des nombres. elle comprend une étude des anneaux de valuation discrète et de Dedekind, et des extensions de corps, une section sur la cohomologie des groupes puis une partie succincte sur le cas de $\mathbb{Q}$ et des corps de nombres p-adique. Une deuxième partie est consacrée à la topologie. On s'intéresse alors dans un premier temps aux revêtements dans leurs généralités. En effet, Dans l'article de A. Sikora il est question de revêtements ramifiés de variétés de dimension 3, il m'a semblé logique de commencer par étudier les revêtement d'espaces topologiques de manière général. L'aspect topologie de l'article de A. Sikora est d'autre part lié à la théorie des nœuds, c'est pourquoi une seconde section présente les définitions et quelques rudiments de théorie des nœuds. Enfin la dernière partie présente le premier théorème énoncé dans l'article étudié, une version du dictionnaire MKR qui permet de lier topologie des variétés et théorie des nombres, pour terminer nous donnerons les idées directrices de la démonstration du théorème énoncé précédemment dans son aspects théorie des nombres. J'ai bien conscience que ce rapport est peut-être un peu long mais j'ai souhaité montrer quelle avait été ma démarche pour approcher l'article de A.Sikora

notions supposées connues

Nous supposerons dans cet exposé que sont connues des bases d'algèbre commutative, de théorie de Galois, de topologie, d'algèbre homologique et de topologie algébrique. Nous utiliseront en particulier la notion de foncteur dérivé, de faisceau... On suppose aussi connue la topologie générale ainsi que des notion élémentaire sur l'homotopie (des espaces et des fonctions).

Chapitre 1

L'aspect théorie des nombres

1.1 Anneaux de valuation discrète et anneaux de Dedekind

Tous les anneaux considérés sont commutatifs et intègres. On notera (x) l'idéal engendré par x.

1.1.1 Définitions et propriétés

Anneaux de valuation discrète

Définitions

Définition 1.1.1. On dit qu'un anneau A est de *valuation discrète* si c'est un anneau principal et qu'il possède un unique idéal premier (non nul) $\mathfrak{m}(A)$

L'élément π qui engendre $\mathfrak{m}(A)$ est appelé uniformisante de A

On appelle le corps $A/\mathfrak{m}(A)$ *corps résiduel*

Remarque 1. Tous élément x de A peut s'écrire sous la forme $x = \pi^n u$. L'entier n est appelé valuation de x. Il ne dépend pas du choix de π.

Proposition 1.1.1. *Soit A un anneau de valuation discrète et $\mathbb{K}$ son corps des fractions. On peut définir un homomorphisme $v : \mathbb{K}^* \to \mathbb{Z}$ qui a $x = \pi^n u \in \mathbb{K}^*$ (u inversible de A, $n \in \mathbb{Z}$) associe n. Cet homomorphisme vérifie les propriétés suivantes :*

1) L'application v est surjective

*2) $v(x+y) \geqslant \mathrm{Inf}(v(x),v(y)) \quad \forall \quad x,y \in \mathbb{K}^*$

Réciproquement: Soit $\mathbb{K}$ un corps et soit $v : \mathbb{K}^* \to \mathbb{Z}$ un homomorphisme vérifiant 1) et 2). Alors l'ensemble A des $x \in \mathbb{K}$ tel que $v(x) \geqslant 0$ est un anneau de valuation discrète dont v est la valuation associée.

On prendra la convention $v(0) = +\infty$ qui sera utile par la suite

Démonstration. Soit π tel que $v(\pi) = 1$ alors tout x dans A s'écrit $x = \pi^n u$ avec $n = v(x)$ et $v(u) = 0$ i.e. u inversible. L'idéal engendré par π est donc premier et les idéaux de A sont de la forme (π^n). Donc A est de valuation discrète. □

Exemple 1.1.1. Soit p un nombre premier et soit $\mathbb{Z}_{(p)}$ le sous ensemble de $\mathbb{Q}$ des fractions $\frac{r}{s}$ où $s \nmid p$ (le localisé de $\mathbb{Z}$ en p). $\mathbb{Z}_{(p)}$ est un anneau de valuation discrète. Son corps résiduel est $\mathbb{F}_p$ et v_p sa valuation est l'exposant de p dans la décomposition en facteurs premiers.

Caractérisation des anneaux de valuation discrète

Lemme 1.1.2. *Soit A un anneau de valuation discrète et n éléments x_i de son corps des fractions tels que $\forall i \neq 1$ $v(x_i) > v(x_1)$ avec $i \geqslant 2$ alors :*

$$x_1 + ... + x_n \neq 0$$

Démonstration. Le cas $x_1 = 0$ est exclu car on a pris la convention $v(0) = +\infty$ En divisant par x_1 on se ramène à $x_1 = 1$ et $v(x_i) \geq 1$ $\forall i \neq 1$. Donc pour $x_i \in \mathfrak{m}(A)$ si $i \neq 1$ et $x_2 + ... + x_N \in \mathfrak{m}(A)$ comme $x_1 \notin \mathfrak{m}(A)$ on a $x_1 + x_2 + ... + x_n \notin \mathfrak{m}(A)$ et le résultat. □

Proposition 1.1.3. *Soit A un anneau nœthérien. Pour que A soit de valuation discrète il faut et il suffit qu'il vérifie les deux condition suivantes :*

i *A est intégralement clos*

ii *A possède un unique idéal premier non nul.*

Démonstration. $\Rightarrow$ Soit A un anneau de valuation discrète. ii est vérifié.

Mq A est intégralement clos.

Soit $\mathbb{K}$ le corps des fractions de A et $x \in \mathbb{K}$ entier sur A. Soient donc $n \in \mathbb{N}$ et a_0,...,$a_{n-1} \in A$ tel que

$$x^n + a_{n-1}x^{n-1} ... + a_1 x + a_0 = 0$$

Si $x \notin A$ alors $v(x) \leqslant 0$ On alors $v(x^n) = nv(x) \leqslant v(a_i x^i)$ $\forall i \in \{0,...,n-1\}$ ce qui est en contradiction avec le lemme précédent. donc $x \in A$

$\Leftarrow$ Soit A un anneau nœthérien vérifiant i et ii et $\mathbb{K}$ son corps des fractions. Soit $\mathfrak{m}$ l'idéal premier de A. Soit $\mathfrak{m}' = \{x \in \mathbb{K}$ tel que $x\mathfrak{m} \subset A\}$ On a $\mathfrak{m}.\mathfrak{m}' \subset A$ et comme $A \subset \mathfrak{m}$ on a $\mathfrak{m} \subset \mathfrak{m}.\mathfrak{m}'$. Comme un idéal maximal est premier on a que $\mathfrak{m}$ est maximal (d'après ii) et donc $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$ ou $\mathfrak{m}.\mathfrak{m}' = A$

Nous allons maintenant suivre le programme suivant :

I Mq sous ii on a $\mathfrak{m}' \neq A$

II Mq que si $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$ et que i est vérifiée alors $\mathfrak{m}' = A$

On a ainsi que $\mathfrak{m}.\mathfrak{m}' = A$

III Mq si $\mathfrak{m}.\mathfrak{m}' = A$ alors $\mathfrak{m}$ est principal. Puis que A est de valuation discrète

Démonstration de I

Soit $x \neq 0 \in \mathfrak{m}$. On considère

$$A_x = \{y/x^n \text{ tel que } y \in A \text{ et } n \in \mathbb{N}\} \subset \mathbb{K}$$

Supposons que $A_x \neq K$. Soit alors $\mathfrak{p}$ un idéal maximal de A_x . Alors $\mathfrak{p} \cap A = \mathfrak{m}$ D'après ii ($\mathfrak{p} \bigcap A$ est un idéal maximal de A) donc $x \in \mathfrak{p}$. Or x est inversible dans A_x et donc $\mathfrak{p} = \mathbb{K}$. Contradiction. Donc $A_x = \mathbb{K}$.

On fixe $z \neq 0 \in \mathfrak{m}$. Soient x_1,...,x_k les générateurs de $\mathfrak{m}$ (A est nœthérien). On alors $y_i \in A$ et $n_i \in \mathbb{N}$ tel que $\frac{1}{z} = \frac{y_i}{x_i^{n_i}}$ ($A_{x_i} = \mathbb{K}$). Donc avec n assez grand $\forall i \;\; x_i^n \in zA$

Comme $\mathfrak{m}^N$ est engendré par des monômes en les x_i de degré total N, avec $N \geqslant k(n-1)$ on a $\mathfrak{m}^n \subset zA$. On peut considérer N le plus petit entier vérifiant la propriété précédente. Alors $N \geq 1$.

Soit $y \in \mathfrak{m}^{N-1}$. On a $\mathfrak{m}y \subset zA$ et donc $y/z \in \mathfrak{m}'$. Comme $y \notin zA$, $y/z \notin A$ et $\mathfrak{m}' \neq A$

Démonstration de II

Supposons que $\mathfrak{m}.\mathfrak{m}' = \mathfrak{m}$ et que i est vérifié. Mq $\mathfrak{m}' = A$ Soit $x \neq 0 \in \mathfrak{m}'$. On a $x.\mathfrak{m} \subset \mathfrak{m}$. En itérant on obtient $\forall n \in \mathbb{N}\; x^n.\mathfrak{m} \subset \mathfrak{m}$. On considère la suite croissante de A-modules $\mathfrak{a}_n$ engendrée par $\{1,x,...,x^n\}$. Les $\mathfrak{a}_n$ son inclus dans $\mathfrak{m}'$ qui est nœthérien (cf ci-dessous) [on dit qu'un module M est nœthérien si toutes suite croissante de sous-modules de M est stationnaire] et l'on a $\mathfrak{a}_{n-1} = \mathfrak{a}_n$ *a.p.c.r.* On a alors $x^n \in \mathfrak{a}_{n-1}$ et donc $x^n = b_0 + b_1 x + ... + b_{n-1}x^{n-1}$. Comme A est intégralement clos on a que $x \in A$

Mq $\mathfrak{m}'$ est nœthérien :

Lemme 1.1.4. **a** *La définition est équivalente à : Tout sous-module de M est de type fini.*

b *Un module de type fini sur un anneau nœthérien est nœthérien.*

c *Tous sous module d'un module nœthérien est nœthérien.*

Démonstration. **démonstration de a** $\Rightarrow$ Soit M un module nœthérien et M' un sous module de M. On construit une suite de sous module de M la manière suivante: soir $x_0 \in M' \setminus \{0\}$ et M_0 le sous module engendré par x_0. Si $M_0 \neq M'$ on prend $x_1 \in M' \setminus M_0$ et on pose M_1 le module engendré par x_0 et x_1. Sinon on arrête la construction. On continue. Si la construction des modules M_i ne s'arrête pas on obtient ainsi un suite strictement croissante de sous module de M, ce qui est impossible. On a donc n tel que $M_n = M'$ et Comme M_n est de type fini, M' aussi.

$\Leftarrow$ Soit $(M_n)_{n\in\mathbb{N}}$ une suite croissante de sous module de M. Comme la suite est croissante, $\bigcup M_n$ est un sous module de M donc de type fini. Soient x_0,...,x_k ses générateurs. On a i_0 tel que x_0,...,$x_k \in M_{i_0}$. Donc $\bigcup M_n = M_{i_0}$ et la suite est stationnaire.

démonstration de b On fait une recurrence sur le nombre minimal de générateurs.

n=1 : Soit M un module engendré par un élément x et M' un sous module de M. On considère $\varphi : 1 \overset{\varphi}{\mapsto} x$. Alors $\varphi^{-1}(M')$ est un sous module (donc un idéal I de A). Soit x_0,..,x_k les images par φ des générateurs de I. M' est alors engendré par x_0,..,x_k.

On suppose le résultat vrai pour $n-1$ générateurs. Soit M un A module tel que $0 \to A^n \overset{\mathrm{f}}{\to} M \to 0$

Soit M' un sous module de M. Alors $N = \mathrm{f}^{-1}(M')$ est un sous module de A^n. Si on montre que N est de type fini engendré par x_1,...,x_k alors M' sera engendré par $f(x_1)$,...,$f(x_n)$.

On note e* la projection sur la dernière coordonnée Si $N \subset \ker(\text{e}^*) = A^{n-1}$ on applique l'hypothèse de récurrence. Sinon, soit $x_1,...x_k \in N$ tel que $\text{e}^*(x_i) = y_i$ et $\text{e}^*(N) = Ay_1 + ... + Ay_k$. Il reste a Mq $N = (\ker(\text{e}^*) \bigcap N) + x_1A + ... + x_kA$ ce qui est clair.

démonstration de c évident.

□

Démonstration de III

Comme $\mathfrak{m}.\mathfrak{m}' = A$ on une relation : $\sum x_iy_i = 1$ avec $x_i \in \mathfrak{m}$ et $y_i \in \mathfrak{m}'$ Tous les produit sont dans A et il existe au moins un i tel que $x_iy_i \notin \mathfrak{m}$. Cet élément u est donc inversible. On pose $x = x_iu^{-1} \in \mathfrak{m}$. On a alors : $xy_i = x_i(x_iy_i)^{-1}y_i = 1$. Si on prend $z \in \mathfrak{m}$ on a $z = x(y_iz)$. Comme $y_i\mathfrak{m}'$ et $z \in \mathfrak{m}$ on a que $y_iz \in A$. Donc $x \mid z$ et finalement $\mathfrak{m} = (x)$.

Mq A est de valuation discrète.

On va Mq tout y dans A s'écrit sous la forme x^nu où u est inversible. Soit $y \in \bigcap \mathfrak{m}^n$ On a $y = x^na_n$ $\forall n$ On a donc $\forall n$ $a_n - xa_{n+1} = 0$ De la la suite des Aa_n est croissante et donc stationnaire a.p.c.r., on a donc $a_{n+1} = ba_n$ pour n assez grand. Donc $0 = a_n - xa_{n+1} = (1 - xa)a_n$. Comme $1 - ax$ est inversible ($\notin \mathfrak{m}$) $a_n = 0$ et donc $y = 0$. Ainsi $\bigcap \mathfrak{m}^n = 0$ c'est à dire $\bigcup \mathfrak{m}^n = A$.

De là on définit $v : y = x^nu \mapsto n$ qui par prolongement à $\mathbb{K}$ défini une valuation discrète sur $\mathbb{K}$ donc l'anneau de valuation est A

□

Anneaux de Dedekind

On notera K le corps des fractions d'un anneau A

Localisation

Définition 1.1.2. Soit A un anneau, et S une partie multiplicative ($1 \in S$ et S est stable par multiplication). On définit le localisé en S, $S^{-1}A$ par un quotient: Sur $A \times S$ on définit la relation d'équivalence suivante :

$$(a; s)\mathcal{R}(a'; s') \Leftrightarrow \exists\ s'' \in S, \text{ tel que } s''(as' - a's) = 0$$

Le s'' inutile si l'anneau est intègre (et $0 \notin S$). Il sert sinon pour la transitivité. On définit ensuite deux lois sur $S^{-1}A = A \times S/\mathcal{R}$:

$$\overline{(a; s)} + \overline{(a'; s')} = \overline{(as' + a's; ss')} \text{ et } \overline{(a; s)}.\overline{(a'; s')} = \overline{(aa'; ss')}$$

Proposition 1.1.5. *L'inclusion de A dans $S^{-1}A$ $i : a \mapsto i(a) = \overline{(a; 1)}$ est un homomorphisme et permet d'établir une bijection entre les idéaux propre de $S^{-1}A$ et les idéaux de A ne rencontrant pas S.*

Démonstration. On considère :$\varphi : I \mapsto i(I)S^{-1}A$ et $\psi : I \mapsto i^{-1}(I)$. Soit I un idéal de A ne rencontrant pas S. Alors $\varphi(I)$ est un idéal propre de $S^{-1}A$. De même ψ à les bons ensembles d'arrivée et de départ. On a clairement $\varphi \circ \psi(I) = I$ et $\psi \circ \varphi(I) : I$ □

Exemple 1.1.2. **1** le corps des fractions d'un anneau intègre ($S = A \setminus 0$)

2 On prend pour S le complémentaire d'un idéal premier P. Le fait que l'idéal soit premier assure que S est multiplicative. L'anneau $S^{-1}A$ se note alors A_P et c'est un anneau local (i.e. possède un unique idéal maximal). (la démonstration est évidente en utilisant la propriété précédente)

Définitions

Définition 1.1.3. Soit A un anneau intègre. On dit que A est un anneau de Dedekind s'il est nœthérien, intégralement clos, et si tout idéal premier non nul de A est maximal.

Exemple 1.1.3. 1. Les anneaux principaux ;

2. l'anneau d'entiers d'un corps de nombres (i.e. une extension fini de $\mathbb{Q}$). Voir 1.1.21

Proposition 1.1.6. *Soit A un anneau nœthérien intègre. Il y a équivalence entre :*

a) A est un anneau de Dedekind

b) pour tout idéal premier $\mathfrak{p}$ de A, le localisé $A_\mathfrak{p}$ est un anneau de valuation discrète.

Démonstration. a) $\Rightarrow$ b). Soit $\mathfrak{p}$ un idéal premier non nul de A. Comme A est intègre et nœthérien, On sait déjà que $A_\mathfrak{p}$ l'est aussi et qu'il est local d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$.

Soit $\mathfrak{B}$ un idéal premier de $A_\mathfrak{p}$ alors si $\mathfrak{B} \neq \mathfrak{p}A_\mathfrak{p}$ on a que $\mathfrak{B} \bigcap A$ est un idéal premier non nul de A strictement inclus dans $\mathfrak{p}$ ce qui est absurde (tout idéal premier non nul de A est maximal). donc $\mathfrak{B} = \mathfrak{p}A_\mathfrak{p}$. Donc $\mathfrak{p}A_\mathfrak{p}$ est l'unique idéal premier de $A_\mathfrak{p}$.

Mq $A_\mathfrak{p}$ est intégralement clos.

Soit x un élément du corps des fractions de $A_\mathfrak{p}$ qui s'identifie à celui de A et un équation de dépendance intégrale sur $A_\mathfrak{p}$. En multipliant cette équation par le dénominateur des coefficients on obtient un élément $s \in A \setminus \mathfrak{p}$ et des éléments $a_i \in A$ tels que : $sx^n + a_1x^{n-1} + ... + a_n = 0$. En multipliant par s^{n-1} on a que sx est entier sur A donc est dans A. Donc x appartient à $A_\mathfrak{p}$. La proposition 1.1.3 permet de conclure.

b) $\Rightarrow$ a) Soient $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers non nul de A avec $\mathfrak{p} \subset \mathfrak{p}'$ Alors $\mathfrak{p}A_{\mathfrak{p}'}$ et $\mathfrak{p}'A_{\mathfrak{p}'}$ sont deux idéaux premiers non nul de $A_{\mathfrak{p}'}$ qui est de valuation discrète. Donc $\mathfrak{p}A_{\mathfrak{p}'} = \mathfrak{p}'A_{\mathfrak{p}'}$ car $A_{\mathfrak{p}'}$ est principal et possède un unique idéal maximal. On a donc que tout idéal premier de A est maximal.

Mq A est intégralement clos.

Soit x un élément du corps des fractions de A entier sur A. Alors pour tout idéal premier $\mathfrak{p}$ non nul de A, x est entier sur $A_\mathfrak{p}$ et donc appartient à $A_\mathfrak{p}$ par hypothèse. Cela entraîne que x est dans A par le lemme suivant. □

Lemme 1.1.7. *Soit A un anneau intègre. On a*

$$A = \bigcap_{\mathfrak{m}} A_\mathfrak{m}$$

où $\mathfrak{m}$ parcourt l'ensemble des idéaux maximaux de A.

Démonstration. [1] Puisque A est intègre, il est contenu dans l'intersection des $A_\mathfrak{m}$. Inversement, soit x dans l'intersection des $A_\mathfrak{m}$. Soit I l'idéal de A formé des éléments a tels que $ax \in A$. Soit

1. Ici tous les ensembles sont plongés dans le corps des fractions de A

$\mathfrak{m}$ un idéal maximal de A. On a d et e dans A tel que $d/e = x$ et $e \notin \mathfrak{m}$. On a alors que ex est dans A donc $e \in I$. Donc I n'est pas inclus dans $\mathfrak{m}$. Comme cela est vrai pour tous les idéaux maximaux, $I = A$ et donc x est dans A. □

Définition 1.1.4. On appelle *idéal fractionnaire* de A tous sous A-module I non nul de K (corps des fractions de A) pour lequel il existe un élément non nul d de A tel que dI soit inclus dans A.

Lemme 1.1.8. *Un sous A-module de type fini de K est un idéal fractionnaire de A. Si A est nœthérien, un idéal fractionnaire est un sous A-module de type fini de K.*

Démonstration. Soit I un sous A-module de type fini de K. En considérant le dénominateur commun de ses générateurs on obtient le résultat cherché. On a $d \in A$ tel que $d^{-1}A$ contienne I. Or $d^{-1}A$ est un module nœthérien 1.1.4 et I est de type fini. □

Soient I et I' deux idéaux fractionnaires de A. Alors $I + I'$, $I \bigcap I'$ et II' sont des idéaux fractionnaires. On rappelle que le produit II' est l'ensemble des sommes finies d'éléments $x_i y_i$ avec $x_i \in I$ et $y_i \in I'$.

Notation. On notera $\mathrm{Id}(A)$ l'ensemble des idéaux fractionnaires de A.

La multiplication des idéaux munit $\mathrm{Id}(A)$ d'une structure de monoïde commutatif. L'élément neutre est A.

Exemple 1.1.4. Soit A un idéal principal. Alors $\mathrm{Id}(A)$ est un groupe abélien. Soit I un idéal fractionnaire de A. On a $d \neq 0$ dans A tel que dI soit un idéal de A. On a donc $dI = aA$ En posant $J = (d/a)A$, on a que $IJ = A$

Définition 1.1.5. Soient I et J dans $\mathrm{Id}(A)$. On appelle transporteur de J dans I l'ensemble des $x \in K$ tels que $xJ \subset I$. On le note $(I : J)$.

On a $(I : J)$ appartient à $\mathrm{Id}(A)$: on considère $d \in A \setminus 0$ tel que $dI \subset A$ et $b \neq\in J$. Alors $db(I : J) \subset A$ et $db \neq 0$.

Lemme 1.1.9. *Soit $I \in \mathrm{Id}(A)$. I est inversible ssi $(A : I)I = A$*

Démonstration. Supposons que I soit inversible. Soit J son inverse. On a par définition $J \subset (A : I)$. D'autre part comme $(A : I)I \subseteq A$ on a $(A : I)IJ \subset J$ et donc que $(A : I)$ est inclus dans J. □

Décomposition en idéaux premiers On ne considère ici que de anneaux de Dedekind.

Théorème 1.1.10. *Soit A un anneau qui n'est pas un corps. Alors tout idéal maximal est inversible dans* $\mathrm{Id}(A)$

Démonstration. Soit $\mathfrak{m}$ un idéal maximal de A. Comme A n'est pas un corps, $\mathfrak{m}$ n'est pas nul et donc est dans $\mathrm{Id}(A)$. On a $(A : \mathfrak{m})\mathfrak{m} \subset A$ et c'est un idéal de A. Comme $A \subset (A : \mathfrak{m})$ on a $\mathfrak{m} \subset (A : \mathfrak{m})\mathfrak{m}$. $\mathfrak{m}$ étant maximal on a : $(A : \mathfrak{m})\mathfrak{m} = A$ ou $(A : \mathfrak{m})\mathfrak{m} = \mathfrak{m}$. On raisonne alors comme dans la proposition 1.1.3 I et II. On en déduit que $(A : \mathfrak{m})\mathfrak{m} = A$. □

On désigne par **P** l'ensemble des idéaux premier non nul de A

Théorème 1.1.11. a *Tout élément I de* $\mathrm{Id}(A)$ *s'écrit de manière unique sous la forme*

$$I = \prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \qquad (1.1.1.1)$$

où les $v_{\mathfrak{p}}(I)$ sont des entiers relatif presque tous nuls.

b *le monoïde* $\mathrm{Id}(A)$ *est un groupe.*

Démonstration. Voir [Kra00, pages 23-24] □

Définition 1.1.6. L'ensemble $Pr(A)$ des éléments de $Id(A)$ de la forme dA où $d \neq 0 \in K$ sont dit principaux et forment un sous groupe de $\mathrm{Id}(A)$. Le groupe quotient

$$Cl(A) = \mathrm{Id}(A)/Pr(A)$$

s'appelle groupe des classes d'idéaux de A

Proposition 1.1.12. *Si A est un l'anneau d'entiers d'un corps de nombre on peut montrer que $Cl(A)$ est un groupe fini*

On ira voir [Sam71, pages 69-71]

Théorème 1.1.13 (Théorème d'approximation). *Voir [Kra00, page 28] ou [Ser80, page 23]. Soit k un entier. Pour tout $1 \leqslant i \leqslant k$, soient des idéaux $\mathfrak{p}_i$ premiers de A distincts deux à deux, $x_i \in \mathbb{K}$ et n_i des entiers. Alors il existe un élément x de $\mathbb{K}$ tel que $v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$ pour tout i, et $v_{\mathfrak{q}}(x) \geqslant 0$ pour $\mathfrak{q} \neq \mathfrak{p}_1,...,\mathfrak{p}_k$.*

Pour une démonstration, voir [Kra00, pages 28]

Nous finissons ce paragraphe par un lemme utile par la suite qui trouve bien se place ici :

Lemme 1.1.14. *Soit i un entier et $\mathfrak{p}$ un idéal premier non nul de A. Soit a un élément de $\mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$. Alors l'application $\varphi_i : A \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ définie par $\varphi_i(x) = ax + \mathfrak{p}^{i+1}$ est un morphisme de groupe additif surjectif de noyau $\mathfrak{p}$. On en déduit un isomorphisme de $A/\mathfrak{p}$ sur $\mathfrak{p}^i/\mathfrak{p}^{i+1}$*

Démonstration. On a un idéal I tel que $a.A = \mathfrak{p}^i I$ avec $v_{\mathfrak{p}}(I) = 0$. L'application de $A/\mathfrak{p}$ dans $\mathfrak{p}^i I/\mathfrak{p}^{i+1}I$ qui envoie $x + \mathfrak{p}$ sur $ax + \mathfrak{p}^{i+1}I$ est un isomorphisme (de groupe additif). De plus l'application $\psi_i \mathfrak{p}^i I \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ qui envoie y sur $y + \mathfrak{p}^{i+1}$ est surjective ($\mathfrak{p}^i I + \mathfrak{p}^{i+1} = \mathfrak{p}^i$) et de noyau $\mathfrak{p}^{i+1}I$. D'où le résultat. □

1.1.2 Extensions

Dans cette section on se donne un corps $\mathbb{K}$ et une extension de degré fini $\mathbb{L}$. Son degré $[\mathbb{L} : \mathbb{K}]$ sera noté n. On se donne aussi un anneau A nœthérien, intégralement clos, de corps des fractions $\mathbb{K}$. On note B la fermeture intégrale de A dans $\mathbb{L}$. On remarque que le corps des fractions de B est $\mathbb{L}$.

On fera l'hypothèse que : $\mathbb{L}/\mathbb{K}$ est séparable

Propriétés générales

Premières propriétés

Définition 1.1.7. Soit $x \in \mathbb{L}$. La trace (resp. la norme) de x relativement à $\mathbb{L}$ et $\mathbb{K}$ est la trace (resp. le déterminant) de l'application $\mathbb{K}$-linéaire $m_x : y \mapsto xy$. On la note $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ (resp. $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)$).

On définit ainsi une forme $\mathbb{K}$-linéaire $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \to \mathbb{K}$ et un morphisme de groupe $\mathrm{N}_{\mathbb{L}/\mathbb{K}} : \mathbb{L}^* \to \mathbb{K}^*$. En considérant le polynôme caractéristique de x on a les formule suivante :

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = \sum_{i=1}^{n} x_i \text{ et } \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = \prod_{i=1}^{n} x_i$$

où les x_i sont les racines du polynôme caractéristique de x dans une extension convenable.

On définit aussi une forme bilinéaire

$$\begin{array}{rccc} \varphi_{\mathbb{L}/\mathbb{K}} : & \mathbb{L} \times \mathbb{L} & \to & \mathbb{K} \\ & (x ; y) & \mapsto & \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy) \end{array}$$

Théorème 1.1.15. *Si $\mathbb{L}/\mathbb{K}$ est separable (ce qui sera toujours le cas ici) alors $\varphi_{\mathbb{L}/\mathbb{K}}$ est non dégénérée*

Démonstration. On se donne une base $(e_i)_{1 \leqslant i \leqslant n}$ de $\mathbb{L}$ sur $\mathbb{K}$. Soient $(\sigma_i)_{1 \leqslant i \leqslant n}$ les n plongements de $\mathbb{L}$ dans $\overline{\mathbb{K}}$ (une cloture algébrique de $\mathbb{K}$) égaux à l'identité sur $\mathbb{K}$. On a :

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j) = \sum_{k=1}^{n} \sigma_k(e_i e_j) = \sum_{k=1}^{n} \sigma_k(e_i)\sigma_k(e_j)$$

(pour le voir on considère le polynôme minimal de x et l'extension engendré par x)

Soit $M = (\sigma_i(e_j))_{(i;j)}$ (c'est un matrice à coefficients dans $\overline{\mathbb{K}}$) Alors ${}^tMM$ est la matrice de la forme bilinéaire $\varphi_{\mathbb{L}/\mathbb{K}}$. Il suffit donc de Mq le determinant de M est non nul. Sinon on a un famille d'éléments $(\lambda_i)_{1 \leqslant i \leqslant n}$ de $\overline{\mathbb{K}}$ non tous nuls tel que

$$\forall j \quad \sum_{i=1}^{n} \lambda_i \sigma_i(e_j) = 0 \text{ (combinaison linéaire des lignes)}$$

On a donc $\displaystyle\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0 \ \forall x \in \mathbb{L}$. Ce qui est absurde en vertu du lemme suivant :

Lemme 1.1.16. *Soit G un groupe et M un corps, et $(\psi_i)_{1 \leqslant i \leqslant n}$ une famille d'homorphismes distinct de groupe de G dans M^*. Alors la famille est libre dans l'espace vectoriel des fonctions de G à valeur dans M.*

La démonstration est laissée au lecteur (considérer une équation de dépendance linéaire avec un minimum de termes)

cela conclut la démonstration du théorème. □

Lemme 1.1.17. *Soit $x \in B$ alors $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ et $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)$ appartiennent à A*

Démonstration. facile [Kra00, page 35] □

Proposition 1.1.18. *B est un A-module de type fini*

Démonstration. Soit $(y_i)_{1\leqslant i\leqslant n}$ une $\mathbb{K}$-base de $\mathbb{L}$. On a $d \neq 0 \in A$ tel que $z_i = dy_i \in B$. On a ainsi une $\mathbb{K}$-base de $\mathbb{L}$ formée d'élément de B. Soit $(z'_i)_{1\leqslant i\leqslant n}$ la base dual de $(z_i)_{1\leqslant i\leqslant n}$ par rapport à la forme $\varphi_{\mathbb{L}/\mathbb{K}}$ (possible car elle est non dégénérée).

Soit $x \in B$ on a des $x_j \in \mathbb{K}$ tels que $x = \sum_{j=1}^{n} x_j z'_j$. Soit i compris entre 1 et n. xz_i est dans B. Donc $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xz_i)$ est dans A et on a

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xz_i) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sum_{j=1}^{n} x_j z'_j z_i) = \sum_{j=1}^{n} x_j \,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(z'_j z_i) = x_j.$$

On a donc que

$$B \subseteq \sum_{i=1}^{n} Az'_i \qquad *\,.$$

On en déduit que B est inclus dans un A-module de type type fini et comme A est nœthérien B est aussi de type fini (lemme 1.1.4). □

Corollaire 1.1.19. *Si A est nœthérien, il en est de même pour B*

Démonstration. B est type fini sur A qui et nœthérien, donc B est un A-module nœthérien. Les idéaux de B sont donc de type fini sur A, donc aussi sur B. D'où le résultat □

Corollaire 1.1.20. *Supposons que A soit un anneau principal. Alors B est un A-module libre de rang $n = [\mathbb{L} : \mathbb{K}]$*

Démonstration. D'après la démonstration de la proposition précédente (en $*$), on a que B est inclus dans un A-module libre de rang n. Comme A est principal, B est libre rang $\leqslant n$. Cependant, toujours à la proposition 1.1.18 on a remarquer que B contient une base de $\mathbb{L}/\mathbb{K}$ et donc son rang est au moins n. Finalement il est libre de rang n. □

Proposition 1.1.21. *Supposons que A soit de Dedekind alors B aussi.*

Démonstration. On sait déjà que B est nœthérien. B est intégralement clos car si $x \in \mathbb{L}$ est entier sur B, il l'est aussi sur A, donc il est dans B. En vertu de 1.1.3 Il reste à monter que tout idéal premier non nul de B est maximal. Soit $\mathfrak{B}$ un idéal premier non nul de B. Soit x dans $\mathfrak{B}$ différent de 0. On considère une équation de dépendance intégrale de x : $x^n + ... + a_1 + a_0 = 0$ avec n minimal. Donc $a_0 \neq 0$ et a_0 est dans $\mathfrak{B} \bigcap A = \mathfrak{p}$. Comme $\mathfrak{p}$ est un idéal premier non nul de A il est maximal. Donc $A/\mathfrak{p}$ est un sous corps de $B/\mathfrak{B}$. Soit $b \neq 0 \in B/\mathfrak{B}$. Alors $A/\mathfrak{p}[b]$ est un espace vectoriel de dimension fini et la multiplication par b est injective ($B/\mathfrak{B}$ est intègre car $\mathfrak{B}$ est premier), elle est donc surjective et b est inversible. Donc $B/\mathfrak{B}$ est un corps et $\mathfrak{B}$ est maximal □

Définition de la ramification On se place maintenant dans le cas où A est un anneau de Dedekind. On va appliquer les résultats sur les anneaux de Dedekind à A et à B pour étudier les liens qu'il existe entre ces deux anneaux et leur idéaux.

Définition 1.1.8. Soit $\mathfrak{B}$ un idéal premier non nul de B, si $\mathfrak{p} = \mathfrak{B} \bigcap A$ on dira que $\mathfrak{B}$ *divise* $\mathfrak{p}$ (ou que $\mathfrak{B}$ est au-dessus de $\mathfrak{p}$). On notera $\mathfrak{B} \mid \mathfrak{p}$. Cette relation équivaut à dire que $\mathfrak{B}$ contient l'idéal $\mathfrak{p}B$. On notera $e_{\mathfrak{B}}$ l'exposant de $\mathfrak{B}$ dans la decomposition en idéaux premiers de $\mathfrak{p}B$. C'est à dire :

$$e_{\mathfrak{B}} = v_{\mathfrak{B}}(\mathfrak{p}B), \qquad \mathfrak{p}B = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}}}$$

L'entier $e_{\mathfrak{B}}$ est appelé *indice de ramification* de $\mathfrak{B}$ dans l'extension $\mathbb{L}/\mathbb{K}$

Si $\mathfrak{B} \mid \mathfrak{p}$ on a les propriétés suivantes : le corps $B/\mathfrak{B}$ est une extension de $A/\mathfrak{p}$, et cette extension est de degré fini car B est de type fini sur A. Ce degré est appelé *degré résiduel* de $\mathfrak{B}$ dans l'extension $\mathbb{L}/\mathbb{K}$ et est noté $f_{\mathfrak{B}} = [B/\mathfrak{B} : A/\mathfrak{p}]$

Remarque 2. Parfois, pour préciser le corps $\mathbb{K}$, on mettra en indice de e ou de f $\mathfrak{B}/\mathfrak{p}$ à la place de $\mathfrak{B}$

Terminologie. On dit que $\mathbb{L}/\mathbb{K}$ est *totalement ramifiée* en $\mathfrak{p}$ lorsqu'il y a un et un seul idéal premier $\mathfrak{B}$ qui divise $\mathfrak{p}$ et que $f_{\mathfrak{B}} = 1$

On dit que $\mathbb{L}/\mathbb{K}$ est *non ramifiée* en $\mathfrak{B}$ si $e_{\mathfrak{B}} = 1$ et que $B/\mathfrak{B}$ est séparable sur $A/\mathfrak{p}$. Si $\mathbb{L}/\mathbb{K}$ est non ramifiée pour tous les idéaux premiers divisant $\mathfrak{p}$, on dit que $\mathbb{L}/\mathbb{K}$ est non ramifiée au dessus de $\mathfrak{p}$ (ou en $\mathfrak{p}$).

Proposition 1.1.22. *Soit $\mathfrak{p}$ un idéal premier non nul de A. L'anneau $B/\mathfrak{p}B$ est une $A/\mathfrak{p}$-algèbre de degré $n = [\mathbb{L} : \mathbb{K}]$, isomorphe au produit $\prod_{\mathfrak{B}|\mathfrak{p}} B/\mathfrak{B}^{e_{\mathfrak{B}}}$. On a de plus la formule :*

$$n = \sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}} f_{\mathfrak{B}}$$

Démonstration. Par localisation on va se ramener au cas d'anneaux de valuation discrète.

Soit $S = A \setminus \mathfrak{p}$, on pose $A' = S^{-1}A = A_{\mathfrak{p}}$ et $B' = S^{-1}B$. A' est un anneau de valuation discrète et B' est sa fermeture intégrale dans $\mathbb{L}$. On a $A'/\mathfrak{p}A' = A/\mathfrak{p}A$ ainsi que $B'/\mathfrak{p}B' = B/\mathfrak{p}B$ (voir [Kra00, pages38-39]). Comme A' est principal on a que B' est un A'-module libre de rang n (cf corollaire 1.1.20). Donc $B'/\mathfrak{p}B'$ est libre de rang n sur $A'/\mathfrak{p}A'$. Et donc $B/\mathfrak{p}B$ est bien une algèbre de degré n.

D'autre part On a que $\mathfrak{p}B = \bigcap \mathfrak{B}^{e_{\mathfrak{B}}}$ et que les idéaux $\mathfrak{B}^{e_{\mathfrak{B}}}$ sont deux à deux comaximaux. En appliquant le lemme du chinois on obtient :

$$B/\mathfrak{p}B \cong \prod_{\mathfrak{B}|\mathfrak{p}} B/\mathfrak{B}^{e_{\mathfrak{B}}}$$

En notant $n_{\mathfrak{B}}$ la dimension de $B/\mathfrak{B}^{e_{\mathfrak{B}}}$ sur $A/\mathfrak{p}$ on a : $n = \sum_{\mathfrak{B}|\mathfrak{p}} n_{\mathfrak{B}}$. Or d'après le lemme 1.1.14 $\mathfrak{B}^i/\mathfrak{B}^{i+1}$ est isomorphe pour tout i à $B/\mathfrak{B}$ et l'on a la suite de exacte de $A/\mathfrak{p}$-algèbre :

$$0 \longrightarrow \mathfrak{B}^i/\mathfrak{B}^{i+1} \longrightarrow B/\mathfrak{B}^{i+1} \longrightarrow B/\mathfrak{B}^i \longrightarrow 0.$$

On en déduit que

$$n_{\mathfrak{B}} = \sum_{i=0}^{e_{\mathfrak{B}}-1} f_{\mathfrak{B}}$$

Ce qui termine la démonstration. □

Remarquons pour finir ce paragraphe que si $\mathfrak{B}$ est un idéal premier non nul de B et que $\mathfrak{p} = \mathfrak{B} \bigcap B$ alors $v_{\mathfrak{B}}(x) = e_{\mathfrak{B}} v_{\mathfrak{p}}(x)$ pour $x \in \mathbb{K}$. On dit alors que la valuation $v_{\mathfrak{B}}$ prolonge $v_{\mathfrak{p}}$ avec l'indice $e_{\mathfrak{B}}$. Réciproquement si w est une valuation discrète de $\mathbb{L}$ qui prolonge $v_{\mathfrak{p}}$ avec l'indice e, alors il existe un idéal premier $\mathfrak{B} \mid \mathfrak{p}$ tel que $w = v_{\mathfrak{B}}$ et $e = e_{\mathfrak{B}}$ (voir [Ser80, p.27 prop 11]).

Extensions galoisiennes

Nous supposerons ici que l'extension $\mathbb{L}/\mathbb{K}$ est galoisienne, et on notera $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ son groupe de Galois. Nous conservons les notations et les hypothèses du paragraphe précédent.

Propriétés

Proposition 1.1.23. *Soit $\mathfrak{p}$ un idéal premier non nul de A. Le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ opère transitivement sur les idéaux au dessus de $\mathfrak{p}$.*

Démonstration. Il est clair que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ opère sur les idéaux au dessus de $\mathfrak{p}$. Soit $\mathfrak{B} \mid \mathfrak{p}$, et soit $\mathfrak{B}'$ un idéal premier de B au dessus de $\mathfrak{p}$ qui soit distinct des $s(\mathfrak{B})$ $\forall s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. D'après le théorème d'approximation (th. 1.1.13), on a a dans $\mathfrak{B}'$ qui n'est pas dans $s(\mathfrak{B})$ pour tout $s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. On pose $x = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(a)$. Alors x est dans A (lemme 1.1.17) et $x = \prod_{s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} s(a)$ donc x est dans $\mathfrak{B}'$ et $x \notin \mathfrak{B}$. D'où une contradiction car $A \bigcap \mathfrak{B} = A \bigcap \mathfrak{B}'$. □

Corollaire 1.1.24. *Soit $\mathfrak{p}$ un idéal premier non nul de A, les entiers $e_{\mathfrak{B}}$ et $f_{\mathfrak{B}}$ (pour $\mathfrak{B}$ divisant $\mathfrak{p}$) ne dépendent que de $\mathfrak{p}$, on les note alors $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$. Si $g_{\mathfrak{p}}$ désigne le nombre d'idéaux premiers au-dessus de $\mathfrak{p}$ l'on a:*

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$$

On utilise, pour la première partie, l'unicité de la décomposition en idéaux premier, la seconde est une conséquence immédiate de la première (cf prop 1.1.22)

Définition 1.1.9. Soit $\mathfrak{B}$ un idéal premier non nul de B. Le sous groupe de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ formé des éléments qui fixe $\mathfrak{B}$ est appelé *groupe de décomposition* de $\mathfrak{B}$ dans l'extension $\mathbb{L}/\mathbb{K}$. On le note $D_{\mathfrak{B}}(\mathbb{L}/\mathbb{K})$ ou D s'il n'y a pas d'ambiguïté.

Lemme 1.1.25. *Soit $\mathfrak{B}$ et $\mathfrak{B}'$ deux idéaux premier de B au-dessus d'un même idéal premier $\mathfrak{p}$ de A. Alors leur groupes de décomposition sont conjugués dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. En fait si $s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est tel que $s(\mathfrak{B}) = \mathfrak{B}'$ alors:*

$$s D_{\mathfrak{B}} s^{-1} = D_{\mathfrak{B}'} \tag{1.1.2.1}$$

En particulier si l'extension $\mathbb{L}/\mathbb{K}$ est abélienne alors $D_{\mathfrak{B}} = D_{\mathfrak{B}'}$ et le groupe de décomposition de $\mathfrak{B}$ ne dépend que de $\mathfrak{B} \bigcap A$

Démonstration. il suffit de vérifié l'inclusion $s D_{\mathfrak{B}} s^{-1} \subset D_{\mathfrak{B}'}$ qui est immédiate. □

Soit $\mathfrak{B}$ un idéal premier non nul fixé de B. On pose $\mathfrak{p} = \mathfrak{B} \cap A$. Le théorème de correspondance de Galois fait correspondre au groupe de décomposition D de $\mathfrak{B}$ une extension $\mathbb{K}_D \subset \mathbb{L}$ de $\mathbb{K}$. Avec les notation du corollaire 1.1.24 on a $[\mathbb{K}_D : \mathbb{K}] = g_\mathfrak{p}$, $|D| = e_\mathfrak{p} f_\mathfrak{p}$ et $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_D) = D$

On pose désormais $k = A/\mathfrak{p}$ et $l = B/\mathfrak{B}$. Comme B est de type fini sur A, l est une extension fini de k de degré $f_\mathfrak{p}$ que l'on identifiera à un sur-corps de k. Cette extension n'est pas nécessairement galoisienne mais on a :

Lemme 1.1.26. *L'extension l/k est normale (quasi-galoisienne).*

Démonstration. Soit P un polynôme irréductible à coefficients dans k possédant une racine $\alpha = a + \mathfrak{B}$ dans l. Il faut montrer que toutes les racines de P sont dans l. On pose donc $Q = \prod_{s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - s(a))$. C'est un polynôme à coefficients dans A dont a est racine. On note $\overline{Q}$ le polynôme de $k[X]$ déduit Q en réduisant ses coefficients modulo $\mathfrak{p}$. On a $\overline{Q}(\alpha) = 0$ et toutes les racines de $\overline{Q}$ sont dans l (ce sont les $s(a) + \mathfrak{B}$ $s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$). Or P étant le polynôme minimal de α on a que P divise $\overline{Q}$ et le résultat. □

À un élément s de D on peut associer un élément $\bar{s}$ de $\mathrm{Gal}(l/k)$ par $\bar{s}(x + \mathfrak{B}) = \bar{s}(x) + \mathfrak{B}$. $\bar{s}$ est bien définie car s fixe $\mathfrak{B}$ et A. On obtient ainsi un morphisme de groupe :

$$\begin{array}{rccc} \epsilon : & D & \to & \mathrm{Gal}(l/k) \\ & s & \mapsto & \bar{s} \end{array}$$

Définition 1.1.10. Le noyau de ϵ est appelé *groupe d'inertie* de $\mathfrak{B}$ dans l'extension $\mathbb{L}/\mathbb{K}$. On le note $I_\mathfrak{B}(\mathbb{L}/\mathbb{K})$ ou simplement I s'il n'y a pas d'ambiguïté.

On a l'analogue pour I du lemme 1.1.25

Proposition 1.1.27. *L'application $\epsilon : D \to \mathrm{Gal}(l/k)$ passé au quotient est un isomorphisme de groupe de D/I sur $\mathrm{Gal}(l/k)$.*

Démonstration. Il s'agit de montrer que ϵ est surjective. Soit $u \in \mathrm{Gal}(l/k)$.

On commence par supposer que l/k est séparable. Soit α un élément primitif de l sur k. Il résulte du théorème d'approximation (th. 1.1.13) qu'on a un représentant de α qui soit dans tous les $s(\mathfrak{B})$ pour $s \notin D$. On considère alors le polynôme : $P = \prod_{s \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - s(a))$. Les racines non nulles du polynôme réduit $\bar{P}$ sont de la forme $\bar{s}(a + \mathfrak{B}) = s(a) + \mathfrak{B}$ avec $s \in D$. En particulier les racines du polynôme minimal de α sur k sont de la forme $\bar{s}(a + \mathfrak{B})$ avec $s \in D$. On a donc $s \in D$ tel que $\bar{s}(a + \mathfrak{B}) = u(a + \mathfrak{B})$ et donc $u = \bar{s}$. On a donc le résultat si l/k est séparable.

Si l/k n'est pas séparable, on considère la fermeture séparable l_s de k dans l. En raisonnant comme précédemment on trouve $s \in D$ tel que $\bar{s}$ coïncide avec u sur l_s. On utilise alors le fait que les restriction de $\bar{s}$ et de u se prolonge de manière unique en un élément de $\mathrm{Gal}(l/k)$ □

Corollaire 1.1.28. *Si l'extension l/k est séparable alors $|I| = e_\mathfrak{p}$*

C'est immédiat

Le cas G cyclique d'ordre premier Nous allons ici traiter un cas très particulier qui nous intéresse car il est celui que nous traiterons dans la dernière partie. On se place dans le cas d'une extension galoisienne dont le groupe de Galois est cyclique d'ordre p premier.

Proposition 1.1.29. *Soit $\mathfrak{p}$ un idéal premier non nul de A. Avec les notations des paragraphes précédents, on est alors dans l'un des trois cas suivants :*

$\mathfrak{p}B = \mathfrak{B}_1\mathfrak{B}_2...\mathfrak{B}_p$, $\mathfrak{p}$ *est totalement décomposé et* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *permute les idéaux premiers au-dessus de* $\mathfrak{p}$.

$\mathfrak{p}B = \mathfrak{B}^p$, $\mathfrak{p}$ *est totalement ramifié et* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *agit trivialement sur* $\mathfrak{B}$.

$\mathfrak{p}B = \mathfrak{B}$, *on dit que* $\mathfrak{p}$ *est inerte et* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *agit non trivialement sur* $\mathfrak{B}$.

Démonstration. On part de la suite exacte :

$$0 \to I \to D \to \mathrm{Gal}(k/l) \to 0$$

Comme $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est cyclique et d'ordre premier on est dans l'un des deux cas suivants : $D = \{1\}$ ou $D = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Si $D = \{1\}$ alors on est dans le premier cas. Sinon on a $I = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ ou $I = \{1\}$ ces deux cas correspondent respectivement au deuxième et troisième cas. □

Discriminant et ramification

Le but de ce dernier paragraphe est, étant donnés un anneau de Dedekind A de corps des fractions $\mathbb{K}$, $\mathbb{L}$ une extension de finie séparable $\mathbb{K}$ et B la fermeture intégrale de A dans $\mathbb{L}$, de savoir quels sont les idéaux premiers $\mathfrak{B}$ de B tel que $e_{\mathfrak{B}} > 1$.

Discriminant On se donne un anneau A et un anneau B qui contient A et qui est un A-module libre de rang fini n. Étant donné un élément x de B on note m_x l'application de multiplication par x. On définit comme précédemment la trace $\mathrm{Tr}_{B/A}(x)$ et la norme $\mathrm{N}_{B/A}(x)$ comme la trace et le déterminant de m_x. Ce sont des éléments de A.

Définition 1.1.11. Soit $(x_i)_{1\leqslant i\leqslant n}$ un élément de B^n. On appelle *discriminant* du système $(x_i)_{1\leqslant i\leqslant n}$ l'élément de A

$$D(x_1,...,x_n) = \det\Big(\big(\mathrm{Tr}_{B/A}(x_ix_j)\big)_{i,j}\Big)$$

Lemme 1.1.30. *Soient $(x_i)_{1\leqslant i\leqslant n}$ et $(y_i)_{1\leqslant i\leqslant n}$ deux éléments de B^n tel que, pour tout $1 \leqslant i \leqslant n$, l'on ait :*

$$y_i = \sum_{j=1}^{n} a_{ij}x_j \quad \textit{avec } a_{ij} \in A.$$

Alors on a

$$D(y_1,...,y_n) = \det(a_{ij})^2 D(x_1,...,x_n)$$

.

Démonstration. C'est un petit calcul matriciel. Voir [Kra00, p. 47 Lemme 4.1] □

Les discriminants de bases de B sur A sont donc associé, d'où :

Définition 1.1.12. On appelle *discriminant* de B sur A, et on notera $\delta_{B/A}$ l'idéal principal engendré par le discriminant de n'importe quelle base de B sur A;

Quelques propriétés

Lemme 1.1.31. *Pour que qu'un élément $(x_i)_{1\leqslant i\leqslant n}$ de B^n soit une base de B sur A il faut et il suffit que $D(x_1,...,x_n)$ soit un générateur de $\delta_{B/A}$.*

Démonstration. C'est évidement nécessaire.

Supposons que $d = D(x_1,...,x_n)$ soit un générateur de $\delta_{B/A}$. Soit $(e_i)_{1\leqslant i\leqslant n}$ une base de B sur A. On a alors des éléments $a_{ij} \in A$ tel que $\forall i\ x_i = \sum_j a_{ij}e_j$ et en notant $d' = D(e_1,...,e_n)$ on a : $d = \det(a_{ij})^2 d'$. Mais comme d et d' engendre $\delta_{B/A}$, on a u inversible de A tel que $d' = ud$. Finalement

$$d(1 - \det(a_{ij})^2 u) = 0.$$

Comme les anneaux sont tous considérés intègre on a que la matrice (a_{ij}) est inversible et que $(x_i)_{1\leqslant i\leqslant n}$ est une base de B sur A. □

Lemme 1.1.32. *Soient $(x_i)_{1\leqslant i\leqslant n}$ une A-base de B et I un idéal de A. On pose $\bar{x}_i = x_i + IB$ Alors $(\bar{x}_i)_{1\leqslant i\leqslant n}$ est une A/I-base de B/I et $D(\bar{x}_1,...,\bar{x}_n) = D(x_1,...,x_n) + I$*

Voir [Kra00, page 49]

Lemme 1.1.33. *Soit $(C_i)_{1\leqslant i\leqslant t}$ une famille d'anneaux contenant A et C l'anneau produit des C_i. L'anneau A s'identifie diagonalement à un sous anneau de C. On suppose que, pour tout i, C_i est un A-module libre de rang fini. Alors C aussi et on a :*

$$\delta_{C/A} = \prod_{i=1}^{t} \delta_{C_i/A}.$$

Pour la démonstration voir encore [Kra00, page 49]

Lemme 1.1.34. *Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension fini séparable de degré n de $\mathbb{K}$. si $(x_i)_{1\leqslant i\leqslant n}$ est une $\mathbb{K}$-base de $\mathbb{L}$ on a $D(x_1,...,x_n) = \det((\sigma_i(x_j))_{ij})^2 \neq 0$ où les σ_i sont les n plongements de $\mathbb{L}$ dans un cloture algébrique de $\mathbb{K}$.*

Voir la démonstration du théorème 1.1.15

Proposition 1.1.35. *Soit $\mathbb{K}$ un corps parfait et $\mathbb{L}$ une $\mathbb{K}$-algèbre de dimension finie sur $\mathbb{K}$. Pour que $\mathbb{L}$ soit réduite (i.e. que tel qu'il n'existe pas d'élément nilpotent non nul), il faut et il suffit que $\delta_{\mathbb{L}/\mathbb{K}} \neq 0$.*

Démonstration. Si $\mathbb{L}$ n'est pas réduite, on a un élément nilpotent x non nul. Soit $(x_1 = x, x_2,...,x_n)$ une base de $\mathbb{L}$ sur $\mathbb{K}$. Pour tout j, x_1x_j est nilpotent et donc l'endomorphisme $m_{x_1x_j}$ l'est aussi. Les valeurs propres de $m_{x_1x_j}$ sont donc nulles. La première ligne de la matrice $(\mathrm{Tr}(x_ix_j))_{i,j}$ est donc formée de 0, son déterminant est donc nul et $\delta_{\mathbb{L}/\mathbb{K}} = 0$

Si $\mathbb{L}$ est réduite on a que $(0) = \bigcap_{i=1}^{t} \mathfrak{p}_i$ où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathbb{L}$ (pour le voir on utilise le th. 1.1.11, pour plus de précisions voir [Kra00, page 50]). D'autre part $\mathbb{L}/\mathfrak{p}_i$ est une algèbre intègre de dimension finie sur $\mathbb{K}$, donc c'est un corps et $\mathfrak{p}_i$ est maximal. On a ainsi que $\mathfrak{p}_i + \mathfrak{p}_j = \mathbb{L}\ \forall i \neq j$. En utilisant le théorème chinois et le lemme 1.1.33 on a :

$$\delta_{\mathbb{L}/\mathbb{K}} = \prod_{i=1}^{t} \delta_{(\mathbb{L}/\mathfrak{p}_i)/\mathbb{K}}.$$

Comme $\mathbb{K}$ est parfait, $\mathbb{L}/\mathfrak{p}_i$ est une extension finie séparable de $\mathbb{K}$ le lemme 1.1.34 assure que $\delta_{\mathbb{L}/\mathbb{K}} \neq 0$. □

Lien avec la ramification On considère ici un anneau de Dedekind A de corps des fractions $\mathbb{K}$, une extension finie séparable de degré n de $\mathbb{K}$ et B la fermeture intégrale de A dans $\mathbb{L}$.

Soit $(x_i)_{1\leqslant i\leqslant n}$ une $\mathbb{K}$-base de $\mathbb{L}$ contenu dans B alors $\mathrm{Tr}_{B/A}(x_ix_j)$ est dans A (lemme 1.1.17), et donc $D(x_1,...,x_n)$ est dans A. La définition suivante est donc correcte.

Définition 1.1.13. On appelle *discriminant* de B sur A et on notera $\delta_{B/A}$ l'idéal de A engendré par les discriminants des bases de $\mathbb{L}$ sur $\mathbb{K}$ contenu dans B.

Théorème 1.1.36. *Soit $\mathfrak{p}$ un idéal premier non nul de A. Pour qu'il existe un idéal premier $\mathfrak{B}$ de B au-dessus de $\mathfrak{p}$ tel que $e_{\mathfrak{B}} > 1$, il faut et il suffit que $\mathfrak{p}$ divise le discriminant $\delta_{B/A}$. En particulier, il n'y a qu'un nombre fini d'idéaux premiers $\mathfrak{B}$ qui sont ramifiés.*

Démonstration. D'après la démonstration du théorème 1.1.22, pour qu'il existe un idéal premier $\mathfrak{B}$ de B tel que $e_{\mathfrak{B}} > 1$ il faut et il suffit que l'anneau $B/\mathfrak{B}$ ne soit pas réduit.

Posons $S = A \setminus \mathfrak{p}$. Puisque A est de Dedekind, $S^{-1}A$ est principal et $S^{-1}B$ est libre de rang n. Soit $(e_i)_{1\leqslant i\leqslant n}$ une base de $S^{-1}B$ sur $S^{-1}A$. D'après le lemme 1.1.32 $(e_i + \mathfrak{p}B.S^{-1}B)_{1\leqslant i\leqslant n}$ est une $S^{-1}A/\mathfrak{p}S^{-1}A$-base de $S^{-1}B/\mathfrak{p}B.S^{-1}B$ et :

$$D(e_1,...,e_n) + \mathfrak{p}S^{-1}A = D(e_1 + \mathfrak{p}B.s^{-1}B,...,e_n + \mathfrak{p}B.S^{-1}B).$$

Or d'après la démonstration du théorème 1.1.22 $B/\mathfrak{p}B$ et $S^{-1}B/\mathfrak{p}B.S^{-1}B$ sont isomorphes. On déduit donc de la proposition 1.1.35 l'équivalence (*) : Il existe un idéal premier $\mathfrak{B}$ de B au-dessus de $\mathfrak{p}$ tel que $e_{\mathfrak{B}} > 1$ ssi $D(e_1,...,e_n)$ appartient à $\mathfrak{p}S^{-1}A$

Supposons maintenant qu'on ait un idéal $\mathfrak{B}$ ayant les propriétés voulues. Soit $(x_i)_{1\leqslant i\leqslant n}$ une base de $\mathbb{L}$ contenue dans B. On a des éléments a_{ij} de $S^{-1}A$ tel que $x_i = \sum_j a_{ij}e_j$ et d'après le lemme 1.1.30 on a $D(x_1,...x_n) = \det(a_{ij})^2 D(e_1,...,e_n)$, et on déduit de (*) que $D(x_1,...,x_n)$ appartient à $\mathfrak{p}S^{-1}A \bigcap A = \mathfrak{p}$. Donc $\mathfrak{p}$ divise $\delta_{\mathbb{L}/\mathbb{K}}$.

Inversement supposons que $\mathfrak{p}$ divise $\delta_{\mathbb{L}/\mathbb{K}}$. On considère une base $(e_i)_{1\leqslant i\leqslant n}$ de $S^{-1}B$ sur $S^{-1}A$. On alors un $s \in S$ tel que (y_i) avec $y_i = se_i$ soit une base de $\mathbb{L}$ sur $\mathbb{K}$ contenue dans $\mathfrak{B}$. Finalement $D(e_1,...,e_n) = \frac{1}{s^{2n}} D(y_1,...,y_n)$ et $D(e_1,...,e_n)$ appartient à $\mathfrak{p}S^{-1}A$. l'équivalence (*) permet de conclure. □

Corollaire 1.1.37. $\mathbb{Q}$ *ne possède pas d'extension non ramifiée non trivial.*

1.2 Cohomologie des groupes

1.2.1 Définitions et premières propriétés

$\mathbb{Z}[G]$-module

Soit G un groupe abélien libre. On note $\mathbb{Z}[G]$ le groupe abélien libre sur $\mathbb{Z}$ ayant pour base les éléments de G $(\oplus_{g\in G}\mathbb{Z})$. Les éléments de $\mathbb{Z}[G]$ sont donc des sommes finies de la forme $\sum n_g g$. On munit ce groupe d'une multiplication ce qui lui confère une structure d'anneau. La multiplication est donner par la loi de G pour les éléments de G puis étendu par linéarité. $(\sum n_i g_i)(\sum n'_j g_j) = \sum n_i n'_j (g_i g_j)$

Définition 1.2.1. Soit G un groupe (noté multiplicativement) et M un groupe abélien (noté additivement). Si l'on a une action du groupe G dans M, on dit que M est un G-module. Cette structure est équivalente à celle de $\mathbb{Z}[G]$-module sur M.

Un *homomorphisme* ou (morphisme) de G modules ou G-homomorphisme est un morphisme de groupe abélien $\varphi : M \to N$ tel que $\varphi(gm) = g(\varphi(m))$ pour tout $g \in G,\ \ m \in M$. On note $\mathrm{Hom}_G(M;N)$ l'ensemble des G-homomorphismes de M dans N.

On identifiera par la suite les deux structures équivalentes de G-module et de $\mathbb{Z}[G]$-module, ainsi que les catégories qui leur correspondent.

Soit G un groupe et H un sous groupe. Pour un H-module M, on définit $\mathrm{Ind}_H^G(M)$ comme l'ensemble des applications $\varphi : G \to M$ tel que $\varphi(hg) = h\varphi(g)$ pour tout $h \in H$. $\mathrm{Ind}_H^G(M)$ est munit d'une structure de G-module par les opérations suivantes :

$$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x) \qquad (g.\varphi)(x) = \varphi(xg)$$

Pour tout $x \in G$.

Lemme 1.2.1. a *Pour tout G-module M et H-module N (H sous groupe de G) on a :*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M,N)$$

b *Le foncteur* $\mathrm{Ind}_H^G : \mathrm{Mod}(\mathbb{Z}[H]) \to \mathrm{Mod}(\mathbb{Z}[G])$ *est exact.*

Démonstration. Soit $\alpha : M \to \mathrm{Ind}_H^G(N)$. On définit $\beta : M \to N$ par $\beta(m) = \alpha(m)(1_G)$, On a alors $\beta(gm) = \alpha(m)(g)\ \forall g \in G$. Pour h dans H on a alors $\beta(hm) = \alpha(m)(h) = h(\alpha(m)(1_g)) = h\beta(m)$. Inversement, à $\beta \in \mathrm{Hom}_H(M,N)$ on associe $\alpha \in \mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N))$ tel que $\alpha(m)(g) = \beta(gm)$. Les applications $\alpha \to \beta$ et $\beta \to \alpha$ sont inverses l'une de l'autre ce qui donne a .

Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte de H-module. Il faut montrer que

$$0 \to \mathrm{Ind}_H^G(M') \to \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M'') \to 0$$

est exacte.

Il suffit de le montrer pour le dernier cran. Pour cela considère un ensemble S de représentants des classe de G modulo H (à gauche). On a donc $G = \cup_{s \in S} Hs$. Soit $\varphi \in \mathrm{Ind}_H^G(M'')$. Pour $s \in S$ on choisit $m(s) \in M$ qui s'envoit sur $\varphi(s)$. On définit alors $\tilde{\varphi}(hs) = h.n(s)$. $\tilde{\varphi}$ appartient à $\mathrm{Ind}_H^G(M)$ et s'envoit sur φ. □

Définition 1.2.2. Soit M_0 un groupe abélien. Il peut être considéré comme un H-module pour H réduit à l'élément neutre. On omet alors H dans la notation de l'induit et

$$\mathrm{Ind}^G(M_0) = \{\varphi : G \to M_0\} = \mathrm{Hom}(\mathbb{Z}[G],M_0)$$

(dans le terme du milieu ce sont juste des applications mais dans le dernier terme c'est de morphismes de groupes qu'il s'agit).

Proposition 1.2.2. *La catégorie des $\mathbb{Z}[G]$-modules possède assez d'injectifs et assez de projectifs.*

On pourra ainsi dériver les foncteurs qui ne seront pas exacts.

Cohomologie

Définitions

Définition 1.2.3. Soit A un G-module. On note A^G l'ensemble des éléments fixes sous l'action de G. Si $f : A \to B$ est un G-homomorphisme, f envoie A^G dans B^G. On parlera donc du foncteur A^G

Le foncteur A^G est covariant et exact à gauche

Les foncteurs dérivés à droite de A^G sont par définition les *groupes de cohomologie de G à valeur dans A*. On les note $\mathrm{H}^q(G,A)$ pour q positif.

On peut calculer les groupes de cohomologie à l'aide de résolution injective de G-module. Cependant on donnera au paragraphe suivant une autre caractérisation de ces groupes qui nous permettra de les calculer autrement.

On a la propriété générale des foncteurs dérivés :

Soit une suite exacte courte de G-module :

$$0 \to A \to B \to C \to 0$$

alors on a une suite exacte longue

$$... \to \mathrm{H}^q(G,B) \to \mathrm{H}^q(G,C) \overset{\delta^q}{\to} \mathrm{H}^{q+1}(G,A) \to \mathrm{H}^{q+1}(G,B) \to ...$$

L'application δ^q est appelé cobord.

Remarque 3. Soit une suite exacte courte $0 \to A \to B \to C \to 0$ de G-module. Si pour $q \geqslant 1$ $\mathrm{H}^q(G,B) = 0$ alors on a :$0 \to A^G \to B^G \to C^G \to \mathrm{H}^1(G,A) \to 0$ et

$$\mathrm{H}^q(G,C) \cong \mathrm{H}^{q+1}(G,A), \qquad \forall q \geqslant 1$$

On peut généraliser : Si on a $0 \to A \to B^1 \to ... \to B^s \to C \to 0$. On a en découpant cette suite exacte longue en suite exactes courtes $\mathrm{H}^q(G,C) \cong \mathrm{H}^{q+s}(G,A)$

Soit A un G-module. Si l'on regarde $\mathbb{Z}$ comme un G-module avec l'action trivial ($gm = m$ pour tout g dans G et m dans $\mathbb{Z}$), alors un morphisme α de G-module de $\mathbb{Z}$ dans M est uniquement déterminé par $\alpha(1)$, et un élément m de M est l'image de 1 par un G-homomorphisme $\mathbb{Z} \to M$ si et seulement si il est fixé par G. On a donc :

$$\mathrm{Hom}_G(\mathbb{Z},M) = M^G$$

. C'est cette description que l'on utilisera au paragraphe suivant. Elle nous est utile pour la proposition suivante :

Proposition 1.2.3 (Lemme de Shapiro). *Soit H un sous groupe de G. Pour tout H-module A on a un isomorphisme canonique :*

$$\mathrm{H}^q(G, \mathrm{Ind}_H^G(A)) \to \mathrm{H}^q(H,A) \quad \forall q \geqslant 0.$$

Démonstration. Pour $q = 0$ on a

$$A^H \cong \mathrm{Hom}_H(\mathbb{Z},A) \overset{1.2.1}{\cong} \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(A)) \cong \mathrm{Ind}_H^G(A)^G.$$

Maintenant on prend $I^\bullet$ une résolution injective de A. Puis on applique le foncteur Ind_H^G et on obtient une résolution injective de $\mathrm{Ind}_H^G(A)$ car le foncteur est exact (1.2.1) et conserve les injectifs (voir [Mil97, page 43 prop1.5]) On a alors :

$$\mathrm{H}^q(G, \mathrm{Ind}_H^G(A)) = \mathrm{H}^q((\mathrm{Ind}_H^G(I^\bullet))^G) = \mathrm{H}^q(I^{\bullet H}) = \mathrm{H}^q(H,A).$$

□

Corollaire 1.2.4. *Si A est un G-module induit, alors* $\mathrm{H}^q(G,A) = 0 \ \forall q > 0$

Démonstration. Si $A = \mathrm{Ind}^G(A_0)$ alors $\mathrm{H}^q(G,A) = \mathrm{H}^q(\{1\},A_0) = 0$ □

Résolution projective et cochaines Comme nous l'avons remarquer au paragraphe précédent, le foncteur A^G est équivalent au foncteur $\mathrm{Hom}_G(\mathbb{Z},A)$. Et donc $\mathrm{H}^q(G,A) = \mathrm{Ext}_G^q(\mathbb{Z},A)$, or pour calculer les Ext on peut aussi le faire avec une résolution projective de $\mathbb{Z}$ en tant que G-module. Les modules libres étant en particulier projectifs on va construire une $\mathbb{Z}[G]$-résolution libre de $\mathbb{Z}$. Soit L_i le $\mathbb{Z}[G]$-module libre ayant pour base $\left((g_o,...g_i)_{(g_0,...,g_i)\in G^{i+1}}\right)$. G opère sur L_i par translation : $s.(g_0,...g_i) = (sg_0,...,sg_i)$. Le morphisme $d : L_i \to L_{i-1}$ est définit par la formule :

$$d(g_0,...,g_i) = \sum_{j=0}^{i}(-1)^j(g_0,...,\hat{g_j},...,g_i)$$

où le symbole $\hat{}$ signifie que la lettre au-dessus duquel il se trouve doit être omise. L'homomorphisme $L_0 \to \mathbb{Z}$ est définit par $g \mapsto 1 \ \forall g \in G$.

On obtient ainsi un complexe $L^\bullet : ... \to L_1 \to L_0 \to \mathbb{Z} \to 0$. Cette suite est exacte. On a de plus la proposition suivante qui découle directement des remarques précédentes :

Proposition 1.2.5. *Pour tout G-module A on a :*

$$\mathrm{H}^q(G,A) \cong \mathrm{H}^q(\mathrm{Hom}_G(L^\bullet,A))$$

Un élément de $\mathrm{Hom}_G(L_i,A)$ peut être identifié à une fonction $\varphi : G^{i+1} \to A$ et tel que $\varphi(gg_0,...,gg_i) = g(\varphi(g_0,...,g_i))$. On peut ainsi identifier $\mathrm{Hom}_G(L_i,A)$ avec l'ensemble $\tilde{C}^i(G,A)$ des applications vérifiant les conditions précitées. Une telle application φ est appelle *i-cochaine homogène de G à valeur dans A*. Et le cobord $\tilde{d^i} : \tilde{C}^i(G,M) \to \tilde{C}^{i+1}(G,M)$ est définit par : $(\tilde{d^i}\varphi)(g_0,...,g_{i+1}) = \sum(-1)^j\varphi(g_0,...,\hat{g_j},...,g_{i+1})$. On a alors

$$\mathrm{H}^q(G,A) = \frac{\ker(\tilde{d^q})}{\mathrm{im}(\tilde{d^{q-1}})}.$$

Cependant une cochaine homogène est déterminée par sa valeur sur les éléments de la forme $(1,g_1,g_1g_2,...,g_1g_2...g_r)$ On introduit donc le groupe $C^i(G,A)$ des *cochaines non homogènes* de toutes les applications de G^i dans A. On définit $d^i : C^i(G,A) \to C^{i+1}(G,A)$ par

$$(d^i\varphi)(g_1,...,g_{i+1}) = g_1\varphi(g_2,...,g_{i+1}) + \sum_{j=1}^{i}(-1)^j\varphi(g_1,...,g_jg_{j+1},...,g_{i+1}) + (-1)^{i+1}\varphi(g_1,...g_r)$$

On appelle groupe des i-cocycle $\ker(d^i)$ et groupe des i-cobord $\mathrm{im}(d^{i-1})$.

Proposition 1.2.6. *On a une suite exacte longue :*

$$C^0(G,A) \xrightarrow{d^0} C^1(G,A) \xrightarrow{d^1} \ldots \xrightarrow{d^{i-1}} C^i(G,A) \xrightarrow{d^i} C^{i+1}(G,A) \to \ldots$$

et l'on a un isomorphisme (canonique)

$$\mathrm{H}^i(G,A) = \frac{\ker(d^i)}{\mathrm{im}(d^i)}.$$

Exemple 1.2.1. On montre qu'un 1-cocycle est une application de G dans A tel que $\varphi(gg') = g\varphi(g') + \varphi(g)$. Une tel application est appelée *homomorphisme croisé*. Un homomorphisme croisé est un cobord ssi il existe a tel que $\varphi(g) = g.a - a \ \forall g \in G$. Ce type d'application est appelé *homomorphisme croisé principal*. On a donc :

$$\mathrm{H}^1(G,A) = \frac{\text{homomorphismes croisés } G \to A}{\text{homomorphismes croisés principaux}}$$

et si l'action de G est trivial on a $\mathrm{H}^1(G,A) = \mathrm{Hom}(G,A)$ morphisme de groupe abélien.

Exemple 1.2.2. Soit G un groupe cyclique d'ordre m et A un G-module. On définit $\mathrm{Nm}_G : M \to M$ l'application $m \mapsto \sum_{g\in G} gm$ Soit g un générateur de G, alors $\varphi \mapsto \varphi(g)$ est un isomorphisme

$$\mathrm{H}^1(G,M) \xrightarrow{\sim} \frac{\ker(\mathrm{Nm}_G)}{(g-1)A}.$$

En effet, soit φ un homomorphisme croisé. Alors $\varphi(1) = \varphi(1 \times 1) = 1\varphi(1) + \varphi(1) = 2\varphi(1)$. Et $\varphi(1) = 0$. De là,

$$0 = \varphi(g^m) = g\varphi(g^{m-1}) + \varphi(g) = g^2\varphi(g^{m-2}) + g\varphi(g) = \varphi(g) = \mathrm{Nm}_G(\varphi(g)).$$

Ainsi $\varphi(g) \in \ker(\mathrm{Nm}_G)$. Pour conclure on remarque que φ est principal ssi $\varphi(g) = ga - a$ pour un certain a et donc ssi $\varphi(g) \in (g-1)A$

Homomorphismes :Inflation, Restriction, Corestriction Soient A et A' respectivement un G et un G' modules. Des homomorphismes $\alpha : G' \to G, \quad \beta : A \to A'$ sont dit compatibles si $\beta(\alpha(g)m) = g(\beta(m))$. Le couple (α,β) définit alors un morphisme de complexe

$$C(G,A) \to C(G',A'), \quad \varphi \mapsto \beta \circ \varphi \circ \alpha$$

et de là des homomorphismes

$$\mathrm{H}^q(G,A) \to \mathrm{H}^q(G',A').$$

Les exemples suivants sont importants pour la suite.

Exemple 1.2.3. a Soit H un sous groupe de G. Si on prend pour α l'inclusion $H \hookrightarrow G$ et pour β l'indentité, on obtient ainsi les homomorphismes de *restriction* :

$$\mathrm{Res} : \mathrm{H}^q(G,M) \to \mathrm{H}^q(H,M).$$

Une autre construction possible est de considérer l'homomorphisme de A dans $\mathrm{Ind}_H^G(A)$ qui envoie a sur φ_a avec $\varphi_a(g) = ga$. Il induit des homomorphismes sur les groupes de cohomologie que l'on compose avec les isomorphismes du lemme de Shapiro.

$$\mathrm{H}^q(G,A) \to \mathrm{H}^q(G, \mathrm{Ind}_H^G(A,A)) \xrightarrow{\sim} \mathrm{H}^q(H,A)$$

b Soit H un sous groupe distingué de G. Avec pour α l'application de passage au quotient et pour β l'inclusion $A^H \hookrightarrow A$, on obtient les homomorphismes de *inflation* :

$$\mathrm{Inf} : \mathrm{H}^q(G/H, A^H) \to \mathrm{H}^q(G,A)$$

Exemple 1.2.4. Soit H un sous groupe d'indice fini de G et S un ensemble de représentants des classes de G modulo H (à gauche). On a donc $G = \cup_{s\in S} sH$. Soit A un G-module. Pour $m \in A^H$ on a définit :

$$\mathrm{Nm}_{G/H}\, m = \sum_{s\in S} sm.$$

Cela est bien définit car la somme est indépendante du choix de S, cette somme est de plus fixée par G. On a ainsi un homomorphisme $\mathrm{Nm}_{G/H} : A^H \to A^G$. On peut l'étendre en des homomorphismes sur les groupes de cohomologie : les homomorphismes de *corestriction* :

$$\mathrm{Cor} : \mathrm{H}^q(H,A) \to \mathrm{H}^q(G,A).$$

On procède comme suit : on a un homomorphisme canonique $\mathrm{Ind}_H^G(A) \to A$, qui a φ associe $\sum_{s\in S} s\varphi(s^{-1})$. Il induit des morphismes sur les groupes de cohomologie qui composés avec les isomorphismes du lemme de Shapiro donne Cor :

$$\mathrm{H}^q(H,A) \xrightarrow{\sim} \mathrm{H}^q(G, \mathrm{Ind}_H^G(A,A)) \to \mathrm{H}^q(G,A)$$

Proposition 1.2.7. *Soit H un sous groupe de G d'indice fini. La composée* $\mathrm{Cor} \circ \mathrm{Res} : \mathrm{H}^q(G,A) \to \mathrm{H}^q(G,A)$ *est la multiplication par $(G : H)$.*

Démonstration. L'application $\mathrm{Cor} \circ \mathrm{Res}$ est la composition

$$a \mapsto \varphi_a \mapsto \sum_{s\in S} s\varphi_a(a^{-1}) = \sum_{s\in S} m = (G : H)$$

□

Corollaire 1.2.8. *Si m est l'ordre de G, alors $m\,\mathrm{H}^q(G,A) = 0$ $\forall q > 0$*

Démonstration. La multiplication par m se factorise d'après la proposition précédente à travers $\mathrm{H}^q(\{1\},M) = 0$ □

Remarque 4. Si G est d'ordre premier, cela permet de munir $\mathrm{H}^q(G,A)$ d'une structure de $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel.

Corollaire 1.2.9. *Si G est fini et que A est, en tant que groupe abélien, engendré par un nombre fini d'éléments alors* $\mathrm{H}^q(G,A)$ *est fini.*

Démonstration. D'après la description de $\mathrm{H}^q(G,A)$ comme quotient des cocycle par le cobord c'est un groupe abélien de type fini. Comme la multiplication par l'ordre de G y est nulle, il est fini. □

Proposition 1.2.10. *Soit H un sous groupe distingué de G et A un G-module. Soit q un entier > 0. Si $\mathrm{H}^i(H,M) = 0$ pour tout i, $0 < i < q$, alors la suite*

$$0 \to \mathrm{H}^q(G/H,M^H) \overset{\mathrm{inf}}{\to} \mathrm{H}^q(G,M) \overset{\mathrm{Res}}{\to} \mathrm{H}^q(H,M)$$

est exact.

Pour une démonstration voir [Mil97, page 55 prop 1.34] ou [Ser80, page 126 prop 5]

Homologie

Définitions

Définition 1.2.4. Soit G un groupe et A un G-module. Soit M_G le plus grand quotient sur lequel G agit trivialement. En fait A_G est le quotient de A par le sous-groupe engendré par $\{ga - a \ / \ g \in G,\ a \in A\}$.

C'est la notion dual de A^G qui est le plus grand sous-objet de A sur lequel G agit trivialement. C'est un foncteur covariant exacte à droite. Ses foncteurs dérivés à gauche sont, par définition, les *groupes d'homologie de G à coefficients dans A.*

On peut calculer ces groupes par une résolution projective de A, cependant comme pour pour la cohomologie on a une description en terme de q-cycle et de q-bord. Pour cela on commence par remarquer que $A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$. On a alors que $\mathrm{H}_q(G,A) = \mathrm{Tor}_q^{\mathbb{Z}[G]}(\mathbb{Z},A)$. La résolution projective de $\mathbb{Z}$ donnée précédemment permet de calculer les groupes d'homologie. On a la résolution suivante : $L^\bullet : ... \to L_1 \to L_0 \to \mathbb{Z} \to 0$ qu'on tensorise par A. Un élément de $L_q \otimes A$ peut être identifié à une fonction $x(g_1,...,g_q)$ à valeur dans A nulle pour presque tous les systèmes $(g_1,...,g_q)$.

On construit de manière analogue à la cohomologie les homomorphismes de restriction, de corestriction et d'inflation.

Le groupe $\mathrm{H}_1(G,\mathbb{Z})$ L'application $\mathbb{Z}[G] \to \mathbb{Z}$ qui à $\sum n_g g$ associe $\sum n_g$ est appelé *application d'augmentation.* Son noyau est appelé *idéal d'augmentation* et est noté I_G. I_G est un $\mathbb{Z}$-module libre de base $\{g - 1 \ g \in G\}$ et

$$M/I_G M = M_G = H_0(G,M)$$

On considère alors la suite exacte $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$. Comme $\mathbb{Z}[G]$ est libre, il est projectif et $\mathrm{H}_1(G,\mathbb{Z}[G]) = 0$, En passant à la suite longue d'homologie on trouve :

$$0 \to \mathrm{H}_1(G,\mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G] \to \mathbb{Z} \to 0$$

La flèche du milieu est induite par l'inclusion $I_G \hookrightarrow \mathbb{Z}[G]$ et est donc nulle. En conséquence :

$$\mathrm{H}_1(G,\mathbb{Z}) \overset{\sim}{\to} I_G/I_G^2 \qquad (*)$$

et $\mathbb{Z}[G]_G = \mathbb{Z}$.

Lemme 1.2.11. *Soit G^c le sous groupe des commutateurs de G, en conséquence G/G^c est le plus grand quotient abélien G^{ab} de G. Alors l'application $g \mapsto (g-1) + I_G^2$ induit un isomorphisme de $G/G^c \to I_G/I_G^2$*

Démonstration. Comme $gg' - 1 = (g-1)(g'-1) + (g-1) + (g'-1) \equiv (g-1) + (g+1) \bmod I_G^2$, l'application $G \to I_g/I_G^2$ qui envoie g sur $(g-1) + I_G^2$ est bien un homomorphisme. Comme I_G/I_G^2 est commutatif l'application se factorise a travers G^{ab}. On considère ensuite le morphisme de I_G dans G^{ab} qui envoie $g-1$ sur la classe de g. Il se factorise à travers I_G/I_G^2 et les deux morphismes sont inverses l'un de l'autre. □

Proposition 1.2.12. *On a un isomorphisme canonique* $\mathrm{H}_1(G,\mathbb{Z}) \to G^{ab}$

Démonstration. On combine le lemme et l'isomorphisme $(*)$ □

1.2.2 Le cas fini

Dans toute cette section on ne considérera que des groupes finis.

Groupes d'homologie modifiés : Les groupes de Tate

On rappelle que l'application de norme $\mathrm{Nm}_G : A \to A$ est définie par $m \mapsto \sum_{g\in G} gm$. On a de manière évidente que $I_G A \subset \ker(\mathrm{Nm}_G)$ et $\mathrm{im}(\mathrm{Nm}_G) \subset A^G$. Comme $\mathrm{H}_0(G,A) = A/I_G A$ et $\mathrm{H}^0(G,A) = A^G$, on en déduit que Nm_G définit un homomorphisme $\mathrm{Nm}_G : \mathrm{H}_0(G,A) \to \mathrm{H}^0(G,A)$.

Pour toute suite exacte courte $0 \to A' \to A \to A'' \to 0$ on a un diagramme :

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & \mathrm{H}_1(G,A'') & \longrightarrow & \mathrm{H}_0(G,A') & \longrightarrow & \mathrm{H}_0(G,A) & \longrightarrow & \mathrm{H}_0(G,A'') & \longrightarrow & 0 & \\
 & & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & & \\
0 \longrightarrow & \mathrm{H}^0(G,A') & \longrightarrow & \mathrm{H}^0(G,A) & \longrightarrow & \mathrm{H}^0(G,A') & \longrightarrow & \mathrm{H}^1(G,A') & \longrightarrow & \cdots &
\end{array}$$

En appliquant une version un peu modifier du lemme du serpent on obtient la suite exacte longue :

$$\cdots \to \widehat{\mathrm{H}}^q(G,A') \to \widehat{\mathrm{H}}^q(G,A) \to \widehat{\mathrm{H}}^q(G,A'') \to \widehat{\mathrm{H}}^{q+1}(G,A') \to \cdots \quad \text{pour } -\infty < q < +\infty$$

avec

$$\widehat{\mathrm{H}}^q(G,A) = \begin{cases} \mathrm{H}^q(G,A) & \text{si } r > 0 \\ A^G/\,\mathrm{Nm}_G(A) & \text{si } r = 0 \\ \ker(\mathrm{Nm}_G)/I_G A & \text{si } r = -1 \\ \mathrm{H}_{-q-1}(G,A) & \text{si } r < -1 \end{cases}$$

La plupart des résultats pour les groupes H^q s'étendent à tous les groupes $\widehat{\mathrm{H}}^q$. En particulier le lemme de Shapiro et ses conséquences. On a donc des morphismes :

Res : $\widehat{\mathrm{H}}^q(G,A) \to \widehat{\mathrm{H}}^q(H,A)$ (H est un sous groupe de G);

Cor : $\widehat{\mathrm{H}}^q(H,A) \to \widehat{\mathrm{H}}^q(G,A)$ (H est un sous groupe de G);

Inf : $\widehat{\mathrm{H}}^q(G/H,A^H) \to \widehat{\mathrm{H}}^q(G,A)$ (H est un sous groupe distingué de G).

La composition Res $\circ$ Cor est toujours la multiplication par $(G:H)$, et comme $\widehat{\mathrm{H}}^q(\{1\},A) = 0$ on a toujours que $\widehat{\mathrm{H}}^q(G,A)$ est tué par la multiplication par $\mid G \mid$

Le cas G cyclique

On se donne un groupe cyclique G d'ordre m et de générateur s et A un G-module. Alors par définition :

$$\widehat{\mathrm{H}}^0(G,A) = \frac{\ker(s-1)}{\mathrm{im}(\mathrm{Nm}_G)} \text{ et } \widehat{\mathrm{H}}^{-1}(G,A) = \frac{\ker(\mathrm{Nm}_G)}{\mathrm{im}(s-1)}$$

car $s^k - 1 = (s-1)(1+s+...+s^{k-1})$.

Proposition 1.2.13. *Soit G un groupe cyclique d'ordre fini et A un G-module. Alors pour tout q on a un isomorphisme*

$$\widehat{\mathrm{H}}^q(G,A) \xrightarrow{\sim} \widehat{\mathrm{H}}^{q+2}(G,A)$$

qui ne dépend que du choix de d'un générateur de G.

Démonstration. Soit s un générateur de G. On a la suite exacte

$$0 \to \mathbb{Z} \xrightarrow{a \mapsto \sum_0^{m-1} as^i} \mathbb{Z}[G] \xrightarrow{s-1} \mathbb{Z}[G] \xrightarrow{s^i \mapsto 1} \mathbb{Z} \to 0$$

Comme les groupes de la suite et le noyau de $\mathbb{Z}[G] \to \mathbb{Z}$ sont des $\mathbb{Z}$-modules libres on a qu'en tensorisant par A sur $\mathbb{Z}$ la suite reste exacte : $0 \to A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to A \to 0$

Si on note A_0, A dont on a oublié la structure de G-module, on peut définir un isomorphisme de G-modules entre $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ et $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A_0$ par $g \otimes a \mapsto g \otimes ga$. D'autre part on a un isomorphisme : $\mathrm{Ind}^G(A_0) = \oplus_{g \in G} g.A_0 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A_0$ donné par $\varphi \mapsto \sum_{g \in G} g \otimes \varphi(g^{-1})$ On a donc $\widehat{\mathrm{H}}(G,\mathbb{Z}[G] \otimes A) = \widehat{\mathrm{H}}(G, \mathrm{Ind}^G(A_0)) = 0$ en vertu du corollaire 1.2.4. La remarque 3 permet de conclure que

$$\widehat{\mathrm{H}}^q(G,A) = \widehat{\mathrm{H}}^{q+2}(G,A)$$

□

Définition 1.2.5. Soit G est un groupe cyclique fini et A un G-module. Quand les groupes de cohomologie sont finis on peux définir le *quotient de Herbrand* par :

$$h(A) = \frac{\mid \widehat{\mathrm{H}}^0(G,M) \mid}{\mid \widehat{\mathrm{H}}^1(G,A) \mid}$$

Lemme 1.2.14. *Soit $0 \to A_0 \to A_1 \to ... \to A_r \to 0$ une suite exacte finie de groupes finis. Alors*

$$\frac{\mid A_0 \mid\mid A_2 \mid ...}{\mid A_1 \mid\mid A_3 \mid ...} = 1$$

Démonstration. C'est évident pour une suite exacte courte (r=2). Dans le cas ou la suite comporte plus de trois termes on la "coupe" en suites exactes courtes :

$$\begin{gathered} 0 \to A_0 \to A_1 \to C_1 \to 0 \\ 0 \to C_1 \to A_2 \to C_2 \to 0 \\ \cdots \\ 0 \to C_{r-1} \to A_{r-1} \to A_r \to 0 \end{gathered}$$

On trouve alors $1 = \frac{|A_0||C_1|}{|A_1|} = \frac{|A_0||A_2|}{|A_1||C_2|} = ...$ □

Proposition 1.2.15. *Soit une suite exacte courte de G-modules $0 \to A' \to A \to A'' \to 0$. Si deux des quotients de Herbrand $h(A')$, $h(A)$, $h(A'')$ sont définis alors le troisième aussi et $h(A) = h(A')h(A'')$.*

Démonstration. On tronque la suite exacte longue de cohomologie :

$$0 \to K \to \mathrm{H}^0(G,A') \to \mathrm{H}^0(G,A) \to \mathrm{H}^0(G,A'') \to \mathrm{H}^1(G,A') \to \mathrm{H}^1(G,A) \to \mathrm{H}^1(G,A'') \to K' \to 0$$

où $K \cong \mathrm{coker}(\mathrm{H}^{-1}(G,A) \to \mathrm{H}^{-1}(G,A'')) \cong \mathrm{coker}(\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,A'')) = K'$. Ce qui permet de conclure la première partie. L'égalité se déduit du lemme précédent. □

Proposition 1.2.16. *Si A est un module fini alors $h(A) = 1$*

Démonstration. On a $0 \to A^G \to A \overset{g-1}{\to} A \to A_G \to 0$ où g est un générateur de G. On en déduit que A^G et A_G sont de même ordre. On a d'autre part : $0 \to \widehat{\mathrm{H}}^{-1}(G,A) \to A_G \overset{\mathrm{Nm}_G}{\to} A^G \to \widehat{\mathrm{H}}^0(G,A) \to 0$. On en déduit que $\widehat{\mathrm{H}}^{-1}(G,A)$ et $\widehat{\mathrm{H}}^0(G,A)$ on même ordre et le résultat en utilisant la proposition 1.2.13. □

Corollaire 1.2.17. *Soit $\alpha : A \to B$ un homomorphisme de G-module ayant un noyau et un conoyau finis. Alors si $h(A)$ ou $h(B)$ est défini alors l'autre aussi et ils sont égaux*

Démonstration. On suppose par exemple que $h(B)$ est définit. La suite exacte $0 \to \alpha(A) \to B \to \mathrm{coker}(\alpha) \to 0$, nous apprend en utilisant la propriété 1.2.15 que $h(\alpha(A))$ est bien définie et égale à $h(B)$ (le coker est fini et d'après la proposition précédente son quotient de Herbrand est égal à 1). Le même raisonnement avec la suite exacte $0 \to \ker(\alpha) \to A \to \alpha(A) \to 0$ permet de conclure. □

1.3 Corps

1.3.1 Le corps $\mathbb{Q}_p$

les différentes valeurs absolues de $\mathbb{Q}$

les valeurs absolues d'un corps

Définition 1.3.1. Soit $\mathbb{K}$ un corps. Une valeur absolue sur $\mathbb{K}$ est une fonction $|.|$ non nulle de $\mathbb{K}$ dans $\mathbb{R}_+$ tel que

1 $|x| = 0$ si et seulement si $x = 0$

2 $|xy| = |x||y|$

3 $|x + y| \leqslant |x| + |y|$

Une telle valeur absolue définit un morphisme de $\mathbb{K}^* \to \mathbb{R}_+^*$. Pour tout sous corps $\mathbb{L}$ de $\mathbb{K}$, une valeur absolue sur $\mathbb{K}$ induit une valeur absolue sur $\mathbb{L}$. Une valeur absolue définit une distance, on remarque alors que les opérations d'addition, de multiplication et de passage à l'inverse sont continues. La fonction caractéristique de $\mathbb{K}^*$ est une valeur absolue, on l'appelle valeur absolue triviale et on l'exclue en générale. En notant $|.|_\infty$ la valeur absolue usuelle de $\mathbb{C}$ et si on a un plongement $i : \mathbb{K} \to \mathbb{C}$ alors les fonctions définies par $x \mapsto |i(x)|_\infty^k$ et $x \mapsto |i(\bar{x})|_\infty^k$ (pour $k > 0$) sont des valeurs absolues de $\mathbb{K}$. Un tel plongement définit une place de $\mathbb{K}$ dans $\mathbb{C}$.

Définition 1.3.2. Une valeur absolue est dite *non-archimédienne* si pour tout $(x,y) \in \mathbb{K}^2$ on a

$$|x + y| \leqslant \max(|x|,|y|).$$

Définition 1.3.3. On dit que deux valeurs absolues sont équivalentes si l'une est égale à l'autre élevée à une certaine puissance. Une valeur absolue est dite *archimédienne* si elle n'est pas équivalente à une valeur absolue non archimédienne.

Si on a un corps $\mathbb{K}$ munit d'une valuation discrète v alors l'application $x \mapsto a^{-v(x)}$ avec $a > 1$ est une valeur absolue sur $\mathbb{K}$ dont la classe d'équivalence est indépendante de a.

les valeurs absolues de $\mathbb{Q}$ Sur $\mathbb{Q}$ on peut définir comme précédemment des valeur absolue dites *p-adiques*, associé à la valuation en p (p premier) sur $\mathbb{Q}$. On rappelle que la valuation en p sur $\mathbb{Q}$ est l'application qui à un rationnel associe la puissance de p dans sa décomposition en nombre premier. On note $|x|_p = p^{-v_p(x)}$ la valuation p-adique On a le théorème suivant :

Théorème 1.3.1 (théorème d'Ostrowski). *Soit $|.|$ une valeur absolue non trivial de $\mathbb{Q}$. Alors $|.|$ est équivalente à $|.|_p$ pour un certain p ou à $|.|_\infty$.*

Complétion et corps p-adique

Pour construire le complété d'un corps $\mathbb{K}$ munit d'une valeur absolue, On considère l'anneau A des suites de Cauchy dans $\mathbb{K}$, On fait le quotient de A par l'idéal I des suites de Cauchy qui tendent vers 0 et on montre que $\hat{\mathbb{K}} = A/I$ est un corps et qu'il est complet. Si la valeur absolue $|.|$ est non-archimédienne sur $\mathbb{K}$ il en est de même du prolongement de $|.|$ à $\hat{\mathbb{K}}$.

Dans le cas des anneaux de valuation discrète, on a une autre construction que nous allons expliciter après. Cette deuxième construction nous donne une description explicite des éléments du complété qui est parfois utile.

On se donne donc un anneau de valuation discrète A, on note $\mathbb{K}$ son corps des fractions et $\mathfrak{p}$ son unique idéal premier non nul. La valuation définie un valeur absolue dont la classe d'équivalence ne dépend pas de a par $|x|_a = a^{-v(x)}$. Lorsque $A/\mathfrak{p}$ est fini on prend $a = |A/\mathfrak{p}|$.

Définition 1.3.4. Le *complété $\mathfrak{p}$-adique de A* est par définition la limite projective des $A/\mathfrak{p}^n$.

$$A_\mathfrak{p} = \lim_{\leftarrow} A/\mathfrak{p}^n.$$

C'est à dire le sous anneau de $\prod A/\mathfrak{p}^n$ formé des éléments $(a_1,...,a_n,...)$ tels que $a_{n+1} + \mathfrak{p}^n = a_n$.

On a les propriétés suivantes que nous ne démontrerons pas.

Proposition 1.3.2. *L'anneau $A_\mathfrak{p}$ est intègre*

L'homomorphisme de A dans $A_\mathfrak{p}$ qui envoie envoie a sur $(a+\mathfrak{p}, a+\mathfrak{p}^2, ..., a+\mathfrak{p}^n, ...)$ est injectif

Soit $a = (\alpha_1 + \mathfrak{p}, ..., \alpha_n + \mathfrak{p}^n, ...)$ un élément non nul de $A_\mathfrak{p}$. La suite d'entier $(v(\alpha_n))$ est stationnaire. On note $v(a)$ sa valeur d'adhérence. la fonction $a \mapsto v(a)$ coïncide avec v sur A (via $A \hookrightarrow A_\mathfrak{p}$), elle se prolonge au corps des fractions $\mathbb{K}_\mathfrak{p}$ de $A_\mathfrak{p}$ et définit une valuation discrète sur $\mathbb{K}_\mathfrak{p}$. $A_\mathfrak{p}$ est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$.

Proposition 1.3.3. *Si on note $\hat{\mathbb{K}}$ le complété de $\mathbb{K}$ pour la valeur absolue définie par $\mathfrak{p}$, alors les corps $\hat{\mathbb{K}}$ et $\mathbb{K}_\mathfrak{p}$ sont isomorphes.*

Exemple 1.3.1. Soit p un nombre premier. Si $A = \mathbb{Z}_{(p)}$ le localisé en p. On note $\mathbb{Z}_p = A_\mathfrak{p}$. c'est l'*anneau des entiers p-adiques*. Son corps des fractions, *le corps des nombres p-adiques* est noté $\mathbb{Q}_p$.

Les boules ouvertes pour la valeur absolue de centre $x \in \mathbb{K}_\mathfrak{p}$ sont les ensembles de la forme $x + \mathfrak{p}^n A_\mathfrak{p}$ $(n \geqslant 0)$. elles sont donc fermées. Tout élément d'une boule ouverte en est un centre. Un singleton est une boule fermée non ouverte. Soitπ une uniformisante de $\mathfrak{p}$, c'est aussi une uniformisante de $\mathfrak{p}A_\mathfrak{p}$. Soit $(a_n)_{n\geqslant 0}$ une suite d'éléments de A. La série $\sum_{k=0}^{n} a_k \pi^k$ converge dans $A_\mathfrak{p}$ vers un élément noté $\sum_{n=0}^{\infty} a_k \pi^k$.

Proposition 1.3.4. *Soit R un système de représentants de $A/\mathfrak{p}$. Tout élément non nul de $\mathbb{K}_\mathfrak{p}$ s'écrit de manière unique sous la forme*

$$\sum_{n=k}^{\infty} a_n \pi^n, \quad \forall n\, a_n \in R, k \in \mathbb{Z} \text{ et } a_k \neq 0.$$

Proposition 1.3.5. *Si le corps résiduel $A/\mathfrak{p}$ est fini alors le corps $\mathbb{K}_\mathfrak{p}$ est localement compact pour la topologie définie par la valeur absolue $\mathfrak{p}$-adique et $A_\mathfrak{p}$ est un sous ensemble compact de $K_\mathfrak{p}$.*

Comportement vis à des extensions

extension d'un corps complet On se donne dans cette section un anneau A de valuation discrète,on note $\mathfrak{p}$ son idéal premier non nul, $\mathbb{K}$ son corps des fractions, complet pour la topologie induite par la valuation v. Soit d'autre part une extension $\mathbb{L}/\mathbb{K}$ finie et séparable. On note B la cloture intégrale de A dans $\mathbb{L}$.

Proposition 1.3.6. *L'anneau B est de valuation discrète et $\mathbb{L}$ est complet pour la topologie définie par cette valuation*

Cette proposition montre que la structure topologique de $\mathbb{L}$ est imposée par celle de $\mathbb{K}$.

Corollaire 1.3.7. *En notant e l'indice de ramification et f le degré résiduel de l'idéal premier de B qui divise $\mathfrak{p}$, on a :*

$$[\mathbb{L} : \mathbb{K}] = ef.$$

Démonstration. C'est un cas particulier de la formule qui lie les indice de ramification et les degrés résiduels des idéaux premier de $\mathfrak{B}$ quand $\mathfrak{B}$ est simplement de Dedekind. On tient ici compte du fait qu'il n'existe qu'un seul idéal premier. □

Corollaire 1.3.8. *Deux éléments de* $\mathbb{L}$ *conjugués sur* $\mathbb{K}$ *ont même valuation.*

Démonstration. On note w l'unique valuation de $\mathbb{L}$ qui prolonge v. Quitte à agrandir $\mathbb{L}$ on peut supposer l'extension galoisienne. Soit $s \in \mathrm{Gal}$, alors $w \circ s$ est une valuation de $\mathbb{L}$ qui prolonge v et est donc égale à w. □

Corollaire 1.3.9. *L'unique valuation de* $\mathbb{L}$ *qui prolonge* v *est donnée par*

$$w(x) = \frac{1}{f} v(\mathbb{N}_{\mathbb{L}/\mathbb{K}}(x))$$

Démonstration. On peut se ramener au cas où $\mathbb{L}$ est galoisienne: Si On a une extension $\mathbb{M}/\mathbb{L}$ tel que $\mathbb{M}/\mathbb{K}$ soit galoisienne on déduit alors la formule du corollaire des formules relatives aux extensions galoisiennes $\mathbb{M}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$.

On suppose donc $\mathbb{L}/\mathbb{K}$ galoisienne. D'après le corollaire précédent on a :

$$w(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} w(\mathbb{N}_{\mathbb{L}/\mathbb{K}}(x)) = \frac{1}{fe} w(\mathbb{N}_{\mathbb{L}/\mathbb{K}}(x)).$$

On se donne π une uniformisante de $\mathfrak{p}$. On a donc $v(\pi) = 1$ et $w(\pi) = e$ et $v(\mathbb{N}_{\mathbb{L}/\mathbb{K}}(\pi)) = ef$. La formule est donc vrai pour $x = \pi$. On en déduit la formule pour x quelconque en écrivant $\mathbb{N}_{\mathbb{L}/\mathbb{K}}(x)$ comme produit d'une puissance de π et d'une unité de A. □

extension de complétion d'anneaux de valuation discrète Soit A un anneau de valuation discrète, K son corps des fractions et $\mathbb{L}/\mathbb{K}$ une extension finie séparable de $\mathbb{K}$. On note $\mathfrak{p}$ l'idéal premier non nul de A et B la cloture intégrale de A dans $\mathbb{L}$. pour chaque idéal $\mathfrak{B}$ de B divisant $\mathfrak{p}$, notons $\mathbb{K}_{\mathfrak{p}}$ et $\mathbb{L}_{\mathfrak{B}}$ les complétés de $\mathbb{K}$ et $\mathbb{L}$ pour les valeurs absolues associées à $\mathfrak{p}$ et $\mathfrak{B}$.

Proposition 1.3.10. *L'extension* $\mathbb{L}_{\mathfrak{B}}/\mathbb{K}_{\mathfrak{p}}$ *est de degré* $e_{\mathfrak{B}} f_{\mathfrak{B}}$ *et il existe une unique valuation de* $\mathbb{L}_{\mathfrak{B}}$ *qui prolonge la valuation de* $\mathbb{K}_{\mathfrak{p}}$

On a de plus un isomorphisme continue de $\mathbb{K}_{\mathfrak{p}}$*-espace vectoriels* φ *:*

$$\mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_{\mathfrak{p}} \simeq \prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{L}_{\mathfrak{B}},$$

induit par les injections canoniques diagonales $L \to \prod \mathbb{L}_{\mathfrak{B}}$ *et* $\mathbb{K}_{\mathfrak{p}} \to \prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{L}_{\mathfrak{B}}$.

Démonstration. Les deux premières assertions résultent du paragraphe précédent. Pour prouver la dernière assertion on remarque que par le théorème d'approximation (th 1.1.13) l'image de $\mathbb{L}$ dans $\prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{L}_{\mathfrak{B}}$ est dense. L'image de φ est donc dense. Comme $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_{\mathfrak{p}}$ est isomorphe en tant qu'espace vectoriel topologique à $\mathbb{K}_{\mathfrak{p}}^{[\mathbb{L}:\mathbb{K}]}$ c'est un espace complet. φ étant continue $\varphi(\mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_{\mathfrak{p}})$ est complet donc fermé. φ est donc surjective. On conclue par l'égalité des dimensions des deux $\mathbb{K}_{\mathfrak{p}}$ espaces vectoriels. □

Corollaire 1.3.11. *Supposons que* $\mathbb{L}/\mathbb{K}$ *soit galoisienne. Soit* $/B$ *un idéal au dessus de* $\mathfrak{p}$. *Notons* $D_{\mathfrak{B}}$ *son groupe de décomposition. Tout élément* σ *de* $D_{\mathfrak{B}}$ *se prolonge par continuité en un élément* $\tilde{\sigma}$ *de* $\mathrm{Gal}(\mathbb{L}_{\mathfrak{B}}/\mathbb{K}_{\mathfrak{p}})$. *De plus l'application* $\sigma \mapsto \tilde{\sigma}$ *est un isomorphisme de groupes*

$$D_{\mathfrak{B}} \simeq \mathrm{Gal}(\mathbb{L}_{\mathfrak{B}}/\mathbb{K}_{\mathfrak{p}}).$$

1.3.2 Calcul de la cohomologie dans le cas G cyclique d'ordre premier

la cohomologie de $\mathbb{L}$ et $\mathbb{L}^*$

On se donne $\mathbb{L}$ une extension galoisienne finie d'un corps $\mathbb{K}$ et on pose $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Alors $\mathbb{L}$ et $\mathbb{L}^*$ sont des G-modules.

Proposition 1.3.12. *Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne finie de groupe de Galois G. Alors* $\mathrm{H}^1(G,\mathbb{L}^*) = 0$

Démonstration. Soit $\varphi : G \to \mathbb{L}^*$ un homomorphisme croisé. On a $\varphi(sg) = s\varphi(g).\varphi(s)$. Soit $a \in \mathbb{L}^*$ On pose

$$b = \sum_{s\in G} \varphi(s).sa.$$

Si $b \neq 0$, alors

$$gb = \sum_{s\in G} g\varphi(s).gsa = \sum_{s\in G} \varphi(g^{-1})\varphi(gs)gsa = \varphi(g)^{-1}b.$$

En conséquence $\varphi(g) = b/gb = gx/x$ avec $x = b^{-1}$. Cela montre que φ est principal, et le résultat en vertu de l'exemple 1.2.1.

Il reste à montrer qu'on a un a tel que $b \neq 0$. On utilise le lemme 1.1.16 qui dit qu'une famille fini de morphisme vers un corps sont linéairement indépendants donc $\sum \varphi(s)s$ est une fonction non nulle de $\mathbb{L}^* \to \mathbb{L}^*$ et on a un a tel que $b \neq 0$ □

Corollaire 1.3.13. *Soit $\mathbb{L}/\mathbb{K}$ une extension cyclique et soit s un générateur de* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. *Si* $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(a) = 1$, *alors a est de la forme $\frac{sb}{b}$*

Démonstration. on a $1 = \mathrm{H}^1(G,\mathbb{L}^*) = \ker(\mathrm{N}_G)/(s-1)\mathbb{L}^*$ □

Le corollaire précédent est le "théorème 90" de Hilbert, la proposition qui le précède est aussi appelée théorème 90.

Proposition 1.3.14. *Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne finie de groupe de Galois G. Alors* $\mathrm{H}^q(G,\mathbb{L}) = 0$ *pour tout $q > 0$*

Démonstration. Le théorème de la base normale (le lemme suivant) nous apprend que $\mathbb{L} \cong K[G]$ en tant que G module. Cependant $K[G] \cong \mathrm{Ind}_{\{1\}}^G$. Les groupes de cohomologie sont donc nuls. □

Lemme 1.3.15 (Théorème de la base normale). *Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne finie de groupe de Galois G. Alors il existe un α dans $\mathbb{L}$ tel que $\{s\alpha \ / \ \alpha \in G\}$ soit une $\mathbb{K}$-base de $\mathbb{L}$*

Pour une démonstration voir [Mil97, page 50 lemme 1.24]

Extensions non ramifiées

On se donne ici $\mathbb{K}$ un corps local complet et $\mathbb{L}$ un autre corps local complet qui est une extension galoisienne, finie, cyclique et non ramifiée de $\mathbb{K}$ de groupe de Galois G. On note $\mathfrak{m}_{\mathbb{L}}$ ($\mathfrak{m}_{\mathbb{K}}$) l'idéal maximal de $\mathbb{L}$ ($\mathbb{K}$). On note l (respectivement k) le corps résiduel de $\mathbb{L}$ (resp. de $\mathbb{K}$) et on suppose que k est fini et parfait (donc l sera aussi fini, et l'extension l/k sera même galoisienne). On note $U_{\mathbb{L}}$ le groupe des unités de $\mathbb{L}$ et $U_{\mathbb{K}}$ celui de $\mathbb{K}$.

Lemme 1.3.16. *Pour $m > 0$, soit $U_{\mathbb{L}}^{(m)} = 1 + \mathfrak{m}_{\mathbb{L}}^m$. Alors*

$$U_{\mathbb{L}}/U_{\mathbb{L}}^{(1)} \xrightarrow{\sim} l^*$$
$$U_{\mathbb{L}}^{(m)}/U_{\mathbb{L}}^{(m+1)} \xrightarrow{\sim} l$$

cela en tant que G-module

Démonstration. Soit π un élément premier de $\mathbb{K}$. π reste un élément premier dans $\mathbb{L}$. On a $U_{\mathbb{L}}^{(m)} = \{1 + a\pi^m \ / \ a \in \mathcal{O}_{\mathbb{L}}\}$ Les applications suivantes donnent le résultat par passage au quotient.

$$u \mapsto u \qquad \bmod \mathfrak{m}_{\mathbb{L}} : \quad U_{\mathbb{L}} \to l^*$$
$$1 + a\pi^m \mapsto a \quad \bmod \mathfrak{m}_{\mathbb{L}} : \quad U_{\mathbb{L}}^{(m)} \to l$$

□

Lemme 1.3.17. *Pour tout q, $\widehat{\mathrm{H}}^q(G,l^*) = 0$. En particulier, la norme $l^* \to k^*$ est surjective.*

Démonstration. Hilbert 90 (1.3.12) donne $\mathrm{H}^1(G,l^*) = 0$. Comme l^* est fini son quotient de Herbrant $h(l^*) = 1$ (voir prop 1.2.16). De là on déduit que $\widehat{\mathrm{H}}^0(G,l^*) = 0$ et donc que tout les groupes sont nuls par 1.2.13.

Comme $0 = \widehat{\mathrm{H}}^0(G,l^*) = l^{*G}/\operatorname{im}(\mathrm{Nm}_G)$ et que d'une part Nm_G est l'application norme et que d'autre part $l^{*G} = k^*$, on a que la norme est surjective. □

Lemme 1.3.18. *Pour tout q, $\widehat{\mathrm{H}}^q(G,l) = 0$ En particulier l'application trace $l \to k$ est surjective.*

Démonstration. pour la première partie on applique la proposition 1.3.14. Ensuite on remarque que dans ce cas l'application Nm_G correspond à l'application trace et que $l^G = k$. □

Proposition 1.3.19. *L'application norme $\mathrm{N}_{\mathbb{L}/\mathbb{K}} : U_{\mathbb{L}} \to U_{\mathbb{K}}$ est surjective*

Démonstration. Soit $u \in U_{\mathbb{K}}$. Comme la norme $l^* \to k^*$ est surjective on a v_0 tel que $\mathrm{N}(v_0) \equiv u \bmod U_{\mathbb{K}}^{(1)}$. Comme la trace $l \to k$ est surjective, On en déduit que la norme $U_{\mathbb{L}}^{(m+1)}/U_{\mathbb{L}}^{(m)} \to U_{\mathbb{K}}^{(m+1)}/U_{\mathbb{K}}^{(m+1)}$ est surjective en vertu du lemme 1.3.16 appliqué à $\mathbb{L}$ mais aussi à $\mathbb{K}$. De là on trouve $v_1 \in U_{\mathbb{L}}^{(1)}$ tel que $\mathrm{N}(v_1) \equiv u/\mathrm{N}(v_0) \bmod U_{\mathbb{K}}^{(2)}$. En continuant on construit ainsi une suite d'éléments $v_0, v_1, \ldots, v_i \in U_{\mathbb{L}}^{(i)}$ tel que $u/\mathrm{N}(v_o v_1 \ldots v_i) \in U_{\mathbb{K}}^{(i+1)}$. Soit donc $v = \lim_{m\to+\infty} \prod_{j=0}^{m} v_j$ qui est bien défini. Alors $u/\mathrm{N}(v) \in \cap U_{\mathbb{K}}^{(i)} = \{1\}$. □

Proposition 1.3.20. *Soit $\mathbb{L}/\mathbb{K}$ une extension cyclique, galoisienne et non ramifiée de groupe de Galois G et soit $U_{\mathbb{L}}$ son groupe des unités. Alors $\widehat{\mathrm{H}}^q(G,U_{\mathbb{L}}) = 0$ pout tout q.*

Démonstration. Soit π un élément premier de $\mathbb{K}$, alors il reste premier dans $\mathbb{L}$ et $\mathbb{L}^* \cong U_{\mathbb{L}} \times \pi^{\mathbb{Z}}$. Comme par Hilbert 90 (1.3.12) on a $\mathrm{H}^1(G,\mathbb{L}^*) = 0$ et que le produit commute à la cohomologie, $\mathrm{H}^1(G,U_{\mathbb{L}})$ est un facteur direct de $\mathrm{H}(G,\mathbb{L}^*)$ et est donc nul. La proposition 1.3.19 assure que $\widehat{\mathrm{H}}^0(G,U_{\mathbb{L}}) = 0$ et donc tous les groupes sont nuls en vertu de 1.2.13. □

Extensions totalement ramifiées

On reprend les mêmes hypothèses qu'au paragraphe précédent mais cette fois l'extension est totalement ramifiée.

Lemme 1.3.21. *Soit $\mathbb{L}$ une extension galoisienne finie de $\mathbb{K}$. Soit G son groupe de Galois. Il existe un sous groupe ouvert de $\mathcal{O}_\mathbb{L}$ stable sous l'action de G et tel que $\mathrm{H}^q(G,V) = 0$ pour tout $q > 0$*

Démonstration. Soit $\{x_g \ / \ g \in G\}$ une base normal de $\mathbb{L}$ sur $\mathbb{K}$ (voir 1.3.15). Les x_g ont un dénominateur commun d dans $\mathcal{O}_\mathbb{L}$. Quitte à les remplacer par dx_g on peut les supposer dans $\mathcal{O}_\mathbb{L}$. On pose $V = \sum \mathcal{O}_\mathbb{L} x_g$. On a alors

$$V \cong \mathcal{O}_\mathbb{L}[G] = \mathrm{Ind}^G(\mathcal{O}_\mathbb{L})$$

et donc $\mathrm{H}^q(G,V) = 0$ pour tout $q > 0$. □

Lemme 1.3.22. *Soit $\mathbb{L}$ une extension galoisienne finie de $\mathbb{K}$ de groupe de Galois G. Alors il existe un sous groupe ouvert de $U_\mathbb{L}$ stable sous G tel que $\mathrm{H}^q(G,V) = 0$ pour tout $q > 0$.*

Démonstration. On suppose que la $\mathrm{char}(\mathbb{K}) = 0$. La série $e^x = 1 + x + ... + x^n/n! + ...$ converge pour sur un voisinage assez petit de 0. Elle définit un isomorphisme de voisinage ouvert de 0 dans un voisinage ouvert de 1 dans $\mathbb{L}^*$. Son inverse est la série $\log(x) = (x-1) - (x-1)^2/2 + ...$ Ces deux applications commutent avec l'action de G. Si on prend V' comme au lemme précédent, c'est un voisinage ouvert de 0 et $\pi^M V'$ aura les même propriétés voulues. On prend $V = \exp(\pi^M V')$ avec M assez grand pour que cela soit défini. V répond alors au problème. □

Lemme 1.3.23. *Soit $\mathbb{L}/\mathbb{K}$ une extension cyclique de degré n alors $h(U_\mathbb{L}) = 1$*

Démonstration. Soit V comme au lemme précédent. Comme $U_\mathbb{L}$ est compact, le groupe $U_\mathbb{L}/V$ est fini et d'après 1.2.17 $h(U_\mathbb{L}) = h(V) = 1$ □

Proposition 1.3.24. *Avec les hypothèses du lemme précédent* $\mid \widehat{\mathrm{H}}^0(G,U_\mathbb{L}) \mid = n$

Démonstration. $1 = h(U_\mathbb{L}) = \mid \widehat{\mathrm{H}}^0(G,U_\mathbb{L}) \mid / \mid \widehat{\mathrm{H}}^1(G,U_\mathbb{L}) \mid$ Il reste ensuite a montrer que $\widehat{\mathrm{H}}^1(G,U_\mathbb{L}) = n$. On peut aller voir dans [Lan86, page 188] pour le calcul (un peu rapide à mon gout). □

Chapitre 2

Topologie

2.1 Revêtements

2.1.1 Généralités

Cette section s'appuyera fortement sur le livre de Godbillon Éléments de topologie algébrique.

Définitions et propriétés

la catégorie des revêtements

Définition 2.1.1. Soit X et B deux espaces topologiques, et $f : X \to B$ une application continue. On dit que f est un *revêtement* si pour tout b dans B il existe un voisinage V de b, un espace discret non vide F et un homéomorphisme $h : V \times F \to f^{-1}(V)$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} V \times F & \xrightarrow{h} & f^{-1}(V) \\ & \searrow^{pr_1} & \downarrow f \\ & & V \end{array}$$

On dit que B est la *base*, X l'*espace total*, $f^{-1}(b)$ la *fibre* au-dessus de b, V un *voisinage distingué* de b et h une *trivialisation locale* de f au-dessus de V. On notera $X(b)$ la fibre au-dessus de b.

On a une notion de morphismes de revêtements. Soit $f : X \to B$ et $f' : X' \to B$ un *morphisme de revêtements* de f sur f' est une application continue $\varphi : X \to X'$ qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ & \searrow_{f} \quad \swarrow_{f'} & \\ & B & \end{array}$$

Si $f'' : X'' \to B$ est un autre revêtement et qu'on a un morphisme φ' de f' sur f'' alors $\varphi' \circ \varphi$ est un morphisme de revêtement de f sur f''. Quand le morphisme φ est un homéomorphisme et que sont inverses est aussi un morphisme de revêtement on parle d'*isomorphisme de revêtements* ou lorsque $X = X'$ d'*automorphisme de revêtements*.

On dit que $f : X \to B$ est un revêtement *trivial* s'il est isomorphe au revêtement $pr_1 : B \times F \to B$ où F est discret et non vide.

On a une autre définition équivalente de la notion de revêtement.

Proposition 2.1.1. *une application continue $f : X \to B$ est un revêtement si et seulement si pour tout b dans B on a un voisinage V de b tel que $f^{-1}(V) = \cup_{i \in I} U_i$ où les U_i sont des ouverts non vides disjoints de X et que $f\,|_{U_i} : U_i \to V$ est un homéomorphisme.*

Démonstration. Si f est un revêtement on prend pour V un voisinage distingué de b puis on pose $I = F$ et $U_i = h(V \times i)$.

Réciproquement on munit I de la topologie discrète. On définit $g : \cup U_i \to V \times I$ par $g(x) = (f(x),i)$ si $x \in U_i$. g est bien un homéomorphisme et son inverse est une trivialisation locale de f au-dessus de V. □

Exemple 2.1.1. *revêtement induit.* Soit $p : X \to B$ un revêtement et soit A un sous espace de B. Alors $p\,|_{p^{-1}(A)} : p^{-1}(A) \to A$ est un revêtement de A : le revêtement induit au-dessus de A.

Exemple 2.1.2. l'application $x \mapsto e^{2i\pi x}$ de $\mathbb{R}$ dans S^1 est un revêtement.

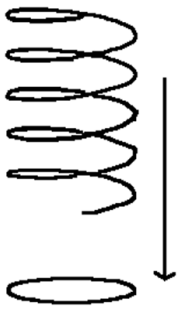


FIG. 2.1 – *revêtement de S^1 par $\mathbb{R}$*

homéomorphismes locaux et revêtements D'après les définitions du paragraphe précédent, un revêtement est un homéomorphisme local. Cependant la réciproque n'est pas vrai. Nous allons donner d'abord une condition suffisante pour qu'un homéomorphisme soit un revêtement fini (c'est à dire que $\{f^{-1}(b)\}$ est fini et de cardinal indépendant de b, on parle alors de revêtement à $n = |f^{-1}(b)|$ feuillets). Puis nous donnerons un exemple d'un homéomorphisme local qui n'est pas un revêtement.

Proposition 2.1.2. *Soit $f : X \to Y$ un homéomorphisme local avec X séparé. Si l'une des conditions suivantes*

- le cardinal de chaque fibre $f^{-1}(y)$ est fini constant non nul,

- f est propre et Y est connexe

est vérifié, alors f est un revêtement fini.

Démonstration. Soit $y \in Y$ pour tout $x \in X(y) = f^{-1}(y)$ on a un voisinage U_x tel que la restriction de f à U_x soit un homéomorphisme. Comme X est séparé, on peut supposer que les U_x sont deux à deux disjoints.

Sous la première hypothèse on pose $V = \cap_{x \in X(y)} f(U_x)$ qui est ouvert car f est ouverte. Alors $f^{-1}(V) \supset \cup_{x \in X(y)} f^{-1}(V) \cap U_x$ (union disjointe) et il y a égalité car le cardinal des fibres est constant. Comme la restriction de f à $f^{-1}(V) \cap U_x$ est un homéomorphisme on a le résultat.

Si f est propre alors f est fermée et, comme c'est un homéomorphisme local, f est ouverte. De plus Y est connexe donc $f(X) = Y$ et f est surjective. Pour y dans Y la fibre $X(y)$ est compacte car f est propre et discrète car X est séparé et que f est un homéomorphisme local, $X(y)$ est donc fini. Soit U_x pour x dans $X(y)$ définit comme précédemment. f induit un homéomorphisme de U_x sur un ouvert V_x voisinage de y. On pose

$$V = \bigcap_{x \in X(y)} f(U_x) \setminus f(X \setminus \cup_{x \in X(y)} U_x).$$

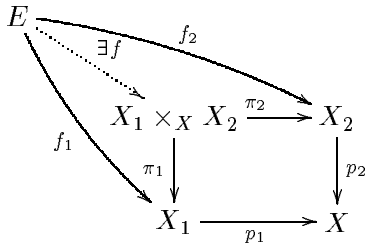
V est ouvert car f est fermée. $f^{-1}(V) = \cup_{x \in X(y)} f^{-1}(V) \cap U_x$ l'union étant disjointe. On a que la restriction de f à $f^{-1}(V) \cap U_x$ est un homéomorphisme sur V donc f est un revêtement. On a que toutes les fibres ont le même cardinal par le lemme suivant □

Lemme 2.1.3. *Soit $f = X \to B$ un revêtement. Si B est connexe et si il existe $b \in B$ tel que $f^{-1}(b)$ soit fini alors toutes les fibres sont finies et ont le même cardinal.*

Démonstration. On note A l'ensemble des points de B dont la fibre est finie et a le même cardinal que celle de b. Soit $y \in A$. Soit V un ouvert distingué de y. Alors $f^{-1}(V)$ est homéomorphe à $V \times F$ où $\mid F \mid = \mid f^{-1}(b) \mid$. On a donc que A est ouvert. Si $A \neq B$, soit $y \in B \setminus A$ alors de la même manière on montre qu'on a un voisinage de y inclue dans $B \setminus A$. Donc A et son complémentaire sont tous les deux ouvert et non vide. Cela contredit la connexité de B □

Exemple 2.1.3. l'application $]0;2[\to S^1$ avec $t \mapsto e^{2i\pi t}$ est un homéomorphisme local mais pas un revêtement (il n'y a pas de voisinage distingué de 1)

propriétés On rappel que le produit fibré de X_1 et X_2 au-dessus de X dans une catégorie est l'objet et les morphismes π_1 et π_2 qui répondent au problème universel suivant :



Si l'on a deux revêtements au dessus de B , $X_1 \xrightarrow{p_1} B$ et $X_2 \xrightarrow{p_2} B$, le produit fibré topologique de X_1 et X_2 au-dessus de B est un revêtement de B ($X_1 \times_B X_2 \xrightarrow{\pi_1 \circ p_1} B$). C'est le produit dans la catégorie des revêtement au-dessus de B. On a aussi aussi des sommes dans cette catégorie.

On peut se demander comment à partir de la donnée d'un revêtement $X \to B$ et d'une application continue $h : B' \to B$ on peut construire un revêtement de B' (comment changer de base). L'espace topologique $X' = B' \times_B X$ munit de la première projection $X' \to B'$ est un revêtement, on le note $h^*(X)$.

Nous allons à présent étudier les propriétés qui lient deux revêtements d'un même espace B. Nous supposerons à partir de maintenant que les espaces considérés sont séparé et localement connexes.

Proposition 2.1.4. *Soit X et Y deux revêtements au-dessus de B et f et g deux B-morphismes de Y dans X (morphismes de revêtements au-dessus de B). Alors l'ensemble des $y \in Y$ tels que $f(y) = g(y)$ est ouvert et fermé dans Y. En particulier, si Y est connexe et s'il existe un y tel que $f(y) = g(y)$ alors f et g coïncident.*

Démonstration. Soit y tel que $f(y) \neq g(y)$. Comme B est séparé, il existe deux ouverts U et V qui séparent $f(y)$ et $g'y)$. On a donc un voisinage U de y tel que $f(U) \subset U_f$ et $g(U) \subset U_g$. Donc l'ensemble des points où f et g coïncide est fermé. On montre qu'il est ouvert en remarquant est la projection $X \to B$ est localement injective. □

Corollaire 2.1.5. *Si B est connexe et qu'il existe $b \in B$ tel que f et g coïncide sur l'image réciproque de b dans Y alors $f = g$.*

Démonstration. Chaque composante connexe de Y contient un point de $Y(b)$ □

Proposition 2.1.6. *Soit X un revêtement de B.*

a Pour qu'une partie Y de X soit un revêtement de B il faut et il suffit que Y soit ouvert et fermé dans X.

b Soit $\mathfrak{R}$ une relation d'équivalence sur X. Pour que $X/\mathfrak{R}$ soit un revêtement de B, il faut et il suffit que le graphe de $\mathfrak{R}$ soit ouvert et fermé dans $X \times_B X$.

Démonstration. voir [eAD79, page 19, 4.2.8] □

Définition 2.1.2. Soit $p : X \to B$ une application continue. Une *section* de p au-dessus d'un sous espace $A \subset B$ est une application continue s de A dans E telle que $p \circ s = \mathrm{id}_A$.

Proposition 2.1.7. *Soit $p : X \to B$ une application continue. Pour que ce soit un revêtement, il faut et il suffit que pour tout $b \in B$ il existe un voisinage V de b et une famille non vide $(s_i)_{i \in I}$ de sections au-dessus de V tel que*

i pour tout i dans I, $s_i(V)$ est un ouvert de $p^{-1}(V)$

ii $s_i(V) \cap_j (V) = \emptyset$ pour $i \neq j$

iii $p^{-1}(V) = \cup s_i(V)$

Démonstration. Cette condition est clairement équivalente à la condition de la proposition 2.1.1 □

Proposition 2.1.8. *Soit $p : X \to B$ un homéomorphisme local et soient s et s' deux sections de p au-dessus de B. Si s et s' coïncident en un point b alors elles coïncident sur un voisinage de b.*

Démonstration. p est un homéomorphisme d'un voisinage ouvert U de $x = s(b) = s'(b)$ sur un voisinage ouvert V de b. On a alors nécessairement $s = s' = (p \mid_U)^{-1}$ sur $s^{-1}(U) \cap s'^{-1}(U) \cap V$ □

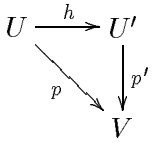
Corollaire 2.1.9. *Soit $p : X \to B$ un homéomorphisme local, et soit A un sous espace connexe de B. Alors si deux sections au-dessus de A coïncident en un point alors elles sont égales.*

Démonstration. Comme X est séparé les deux sections coïncident sur un sous espace non vide ouvert et fermé de A. □

Proposition 2.1.10. *Soient $p : X \to B$ et $p' : X \to B$ deux revêtements et $h : X \to X'$ un B-morphisme. On suppose que X et X' sont connexes. Alors $h : X \to X'$ est un revêtement.*

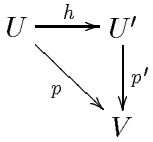
Démonstration. On va commencer par montrer que h est surjectif. [1]

Soit $x' \in h(X)$. On se donne $x \in h^{-1}(x')$ et un voisinage V de $p'(x')$ trivialisant X et X'. on note U l'ouvert de $p^{-1}(V)$ contenant x et U' celui contenant x'. Comme h fait permuter le diagramme



on a que $h = p|_U \circ (p'|_{U'})^{-1}$ est un homéomorphisme et donc $U' \in h(X)$. Donc $h(x)$ est ouvert.

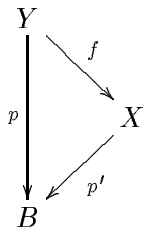
On se donne maintenant x dans le complémentaire de $h(X)$ que l'on suppose non vide. À nouveau on considère un voisinage V de $p'(x)$ trivialisant X et X'. On note U' l'ouvert de $p'^{-1}(V)$ contenant x'. On suppose qu'il existe $\alpha' \in h(X)$ dans U. On note α un antécédent de α'. α appartient alors a un ouvert U de $p^{-1}(V)$. En remarquant comme précédemment que h fait commuter,



on en déduit que $x' \in h(X)$ ce qui est absurde. Le complémentaire de $h(X)$ est donc ouvert. Cela contredit la connexité de X'.

On se donne maintenant un point x' de X'. Soit V un voisinage de $b = p'(x')$ trivialisant X et X' ainsi que $s_y : V \to X$, $y \in p^{-1}(b)$ et $s'_z : V \to X'$, $z \in p'^{-1}(b)$ deux familles de sections au-dessus de V vérifiant les propriétés de la proposition 2.1.7 tel que $s_y(b) = y$ et $s'_z(b) = z$. Alors pour $x \in h^{-1}(x')$ on a $h \circ s_x = s_{x'}$ d'après le corollaire précédent. On pose $U = s_{x'}(V)$ et pour $x \in h^{-1}(x')$ on pose $\sigma_x = s_x \circ p' : U \to U_x = s_x(V)$. La famille $(\sigma_x)_{x \in h^{-1}(x)}$ vérifie les conditions de la proposition 2.1.7 □

Une manière plus graphique de voir les chose est la suivante :



1. la démonstration faite dans [God71, page 112 proposition 4.3] s'abstient de cette vérification mais je ne comprends pas pourquoi

Si p et p' sont des revêtements alors f aussi.

Si X est un revêtement de B et que Y est un revêtement de X alors Y munit de l'application composée n'est pas forcément un revêtement (voir l'exemple 2.1.4). La proposition suivante donne une condition suffisante pour qu'il est soit ainsi.

Proposition 2.1.11. *Soit $X \xrightarrow{p} B$ un revêtement et soit $y \xrightarrow{p'} X$ un revêtement de X. Soient $b \in B$ et U un voisinage connexe de b trivialisant X. On note $(U_t)_{t\in F}$ la famille des composantes connexes de $p^{-1}(U)$ (munie de la topologie induite). Pour un ouvert V de U posons $V_t = U_t \cap p^{-1}(V)$. Pour que qu'il existe un voisinage ouvert V de b tel que $(p\circ p')^{-1}(V)$ soit un revêtement de V il faut et il suffit que qu'il existe un voisinage ouvert V de b inclus dans U tel que pour tout t dans F, l'ouvert V_t trivialise Y*

Démonstration. La condition est nécessaire en vertu du lemme 2.1.10. Comme pour tout $t \in F$ V_t trivialise Y on a que $(p\circ p')^{-1}(V)$ est la réunion disjointe des $p'^{-1}(V)$ qui sont des revêtements triviaux de V, et est donc un revêtement trivial. □

Corollaire 2.1.12. *Si X est un revêtement fini de B alors tout revêtement de X est un revêtement de B*

Exemple 2.1.4. Dans $\mathbb{R}^2$ on note C_n le cercle de diamètre [(0,0),(1/n,0)]. On pose

$$B = \cup_{n\in\mathbb{N}} C_n$$

Si on prend $\mathbb{N}$ copie de B. Sur la n-ième copie, on coupe le n-ième cercle‘(fermé à gauche et ouvert à droite). on raccorde ensuite la branche de gauche du n-ième cercle de la n-ième copie à la branche de droite du n-ième cercle de la $n+1$-ième copie. Ceci est un revêtement de B tel que $p^{-1}(C_n)$ ne soit pas trivial. On note cet espace E_n

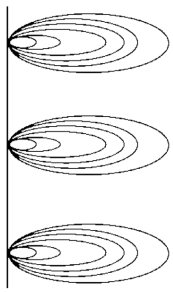


FIG. 2.2 – *E_n :c'est plus facile à dessiner qu'à écrire*

On note E la réunion disjointe des E_n. E munit de l'application qui envoie E_n sur $B \times \{n\}$ est un revêtement de $B \times \mathbb{N}^*$ qui est lui-même un revêtement de B. Cependant E n'est pas un revêtement de B car quelque soit le voisinage ouvert de 0 que l'on choisit, il existe au moins une composante connexe de son image réciproque qui ne lui sera pas homéomorphe. En effet un voisinage de 0 est une infinité de cercle concentrique et un nombre fini de branches. Si on note n_0 le plus petit entier tel que C_{n_0} soit dans le voisinage considéré, l'image réciproque de C_{n_0} dans E_{n_0} n'est pas homéomorphe à C_{n_0}. Comme on peut trouver un tel entier aussi petit que soit le voisinage de 0 choisi.

revêtements et groupes On note G un groupe et e son élément neutre.

Définition 2.1.3. Soit G un groupe et X un ensemble sur lequel G agit. l'action de G est dite *libre* si le stabilisateur G_x de chaque point x de X est réduit à l'élément neutre.

Définition 2.1.4. Soit X un espace topologique séparé et G un groupe topologique séparé, une action continue de G sur X est dite *propre* si l'application graphe

$$gr : \qquad G \times X \longrightarrow X \times X$$

$$(g,x) \longmapsto (x,gx)$$

est propre.

Proposition 2.1.13. *Si X est localement compact et G est séparé, une action continue de G sur X est propre si et seulement si, pour tout compact K de X l'ensemble $\{g \in G$ tels que $K \cap gK \neq \emptyset\}$ est compact dans G.*

Pour une démonstration voir [Pau01, page 29, proposition 3.3]

Proposition 2.1.14. *Si X et G sont séparés et si G agit proprement sur X l'espace quotient X/G est séparé.*

Démonstration. Soit x et y deux points de X qui ne sont pas dans la même orbite. Le couple (x,y) n'appartient alors pas à $\mathrm{im}(gr)$ qui est fermé dans $X \times X$. on a donc deux ouverts U et V tel que $(x,y) \in U \times V \subset X \times X \setminus \mathrm{im}(gr)$. On remarque alors que l'application $\pi : X \to X/G$ est ouverte : Soit U un ouvert de X, alors $\pi^{-1}(\pi(U)) = \cup_{g \in G} gU$ est un ouvert et donc $\pi(U)$ est ouvert. Ainsi $\pi(U)$ et $\pi(V)$ sont des ouverts disjoints (car $U \times V \cap \mathrm{im}(gr)$ est vide). Donc X/G est séparé. □

on en déduit que les orbites sont des fermés (image réciproque par π des singletons qui sont fermés car X/G est séparé).

Proposition 2.1.15. *Soit G un groupe discret agissant continûment, librement et proprement sur un espace topologique séparé X. Alors :*

1 pour tout x dans X on a un voisinage ouvert V de x tel que $gV \cap V = \emptyset$ quelque soit $g \in G \setminus \{e\}$

2 les orbites de X sont discrètes

3 la projection canonique $\pi : X \to X/G$ est un revêtement.

Démonstration. 2 est une conséquence de 1

Montrons 1. L'application graphe gr est continue, injective (car l'action est libre) et fermée (car propre); C'est donc un homéomorphisme sur son image. $\{e\} \times X$ étant ouvert dans $G \times X$, son image par gr qui est la diagonale de $X \times X$ est ouverte dans $\mathrm{im}(gr)$. Soit x dans X. On a donc un voisinage V ouvert de x tel que $(V \times V) \cap \mathrm{im}(gr)$ soit inclus dans la diagonale de $X \times X$. Si on suppose que $V \cap gV$ est non vide, on a $y \in V$ tel que $g.y$ soit aussi dans V. $(y,g.y)$ est donc dans $(V \times V) \cap \mathrm{im}(gr)$ et $g = e$.

Montrons 3. Soit $\alpha \in X/G$. On se donne x tel que $\pi(x) = \alpha$. Soit un voisinage de x vérifiant la propriété de 1, alors $U = \pi(V)$ est un ouvert de X/G car π est ouverte. $\pi^{-1}(U)$ est l'union disjointe des gV pour $g \in G$. En effet si $y \in gV \cap g'V$, alors $g^{-1}y$ appartient à $V \cap g^{-1}g'V$ et de là l'application π est un homéomorphisme de gV sur U.

□

On montre aussi (voir [God71, page 110, proposition 3.2 et page 27-28 proposition 6.1 et 6.2] ou [Pau01, page 31 corollaire 3.7])

Proposition 2.1.16. *soit H un sous-groupe discret d'un groupe topologique séparé G, alors H est fermé, G/H est séparé et la projection $G \to G/H$ est un revêtement.*

Exemple 2.1.5. i L'application $p : \mathbb{R}^n \to \mathbb{R}^n/\mathbb{Z}^n$ est un revêtement dont la base est homéomorphe au tore T^n. Pour le cas $n = 1$ voir l'exemple 2.1

ii La projection $p : \mathbb{C} \to \mathbb{C}/\mathbb{Z}$ est un revêtement. Comme l'application exp : $\mathbb{C} \to \mathbb{C}^*$ induit un homéomorphisme h de $\mathbb{C}/\mathbb{Z}$ sur $\mathbb{C}^*$. On a donc que exp est un revêtement.

iii Le groupe $\{1, -1\}$ opère librement et proprement sur la sphère S^n par $x \to -x$, l'espace quotient est homéomorphe au plan projectif réel $\mathbb{PR}^n$ et est donc un revêtement à deux feuillets.

iv *Espaces lenticulaires.* On note $S^{2n+1} = \{z \in \mathbb{C}^{n+1} \,/\, |z| = 1\}$ la sphère de dimension $n+1$. On se donne ξ une racine p-ième de l'unité. On a alors une action de $\mathbb{Z}/p\mathbb{Z}$ sur S^{2n+1} donner par :

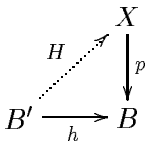
$$(\xi^r,(z_1,\ldots,z_{2n+1})) \mapsto (\xi^r z_1,\ldots\xi^r z_{2n+1}).$$

Cette action est libre et propre. L'espace quotient est une variété compact, sans bord de dimension $2n+1$, Il est noté L_p^{2n+1} et est appelé *espace lenticulaire de dimension* $2n+1$ *et de groupe* $\mathbb{Z}/p\mathbb{Z}$

Relèvement des applications

On se donne dans ce paragraphe un revêtement $p : X \to B$.

Définition 2.1.5. Soient $p : X \to B$ et $h : B' \to B$ deux applications continues. Un relèvement de h est une application continue $H : B' \to X$ telle que $p \circ H = h$, c'est à dire que H fait commuter le diagramme



Proposition 2.1.17 (Unicité des relèvements). *Soient $p : X \to B$ un revêtement et $h : B' \to B$. Si B' est connexe, alors deux relèvements de h qui coïncident en un point sont égaux.*

Démonstration. Soient H et H' deux relèvements de h coïncidant en un point b' de B'. On pose

$$A_0 = \{t \in B' \,/\, H(t) = H'(t)\} \quad \text{et} \quad A_1 = \{t \in B' \,/\, H(t) \neq H'(t)\}.$$

Soit t un point de B' et V un voisinage distingué de $h(t)$. On a un homéomorphisme $\varphi : V \times D \to p^{-1}(V)$. On note $V_d = \varphi(V \times \{d\})$ pour $d \in D$. Si t appartient à A_0, soit d dans D tel que $H(t) \in V_d$ alors $H^{-1}(V_d) \cap H'^{-1}(V_d)$ est un voisinage ouvert de t contenu dans A_0. Si t est dans A_1, soient d et d' tels que $H(t) \in v_d$ et $H'(t) \in V_{d'}$. On a donc que $d \neq d'$ et $H^{-1}(V_d) \cap H'^{-1}(V_{d'})$ est un voisinage ouvert de t inclus dans A_1. La connexité de B' permet de conclure car A_0 est supposer non vide. □

Corollaire 2.1.18. *1. Soient $p : X \to B$ et $p' : X' \to B$ deux revêtements. Si X est connexe deux morphismes de p sur p' qui coïncide en point sont égaux.*

2. Soit $p : X \to B$ un revêtement, alors le groupe des automorphismes de ce revêtement agit proprement et librement sur X.

3. Soit G un groupe discret agissant proprement et librement sur un espace connexe X, le groupe des automorphismes du revêtement $p : X \to X/G$ est isomorphe à G.

Démonstration. On ne montrera que 3. Un élément de G détermine un B-automorphisme de X. Soit h un B-automorphisme de X et x dans X. On a alors un élément g de G tel que $h(x) = g.x$. D'après le 1. h est alors égal à l'automorphisme défini par g. □

Proposition 2.1.19 (Relèvement des homotopies). *Soit $f : Y \to B$ une application continue, admettant un relèvement $\tilde{f} : Y \to X$. Pour toute homotopie $h : Y \times [0,1] \to B$ avec $h(.,0) = f$, il existe un unique relèvement $\tilde{h}$ de h tel que $\tilde{h}(.,0) = \tilde{f}$.*

Démonstration. Si p est trivial c'est immédiat.

Soit y dans Y. Pour $\alpha \in [0,1]$, on a un voisinage $U_{y,\alpha} \times]a_\alpha, b_\alpha[$ de (y,α) tel que $h(U_{y,\alpha} \times [a_\alpha, b_\alpha])$ soit inclue dans un voisinage distingué de $h(y,\alpha)$. On a donc un recouvrement de $[0,1]$ par les ouverts $]a_\alpha, b_\alpha[$. On en extrait un sous recouvrement fini $]a_{\alpha_1}, b_{\alpha_1}[, ...,]a_{\alpha_n}, b_{\alpha_n}[$. On se donne alors n_y tel que $[\frac{i}{n_y}, \frac{i+1}{n_y}] \subset]a_{\alpha_k}, b_{\alpha_k}[$ On pose alors $U_y = \cap_{k=1}^{n} U_{y,\alpha_k}$. U_y est alors tel que $h(U_y \times [\frac{i}{n_y}, \frac{i+1}{n_y}])$ Soit inclus dans un voisinage distingué de $h(y, \frac{i}{n_y})$.

Soit $\tilde{g}_0$ un relèvement de $h|_{U_y \times [0, \frac{1}{n}]}$ tel que $\tilde{g}_0(z,0) = \tilde{f}(z)$ pour tout $z \in U_y$. Par recurrence on construit un relèvement $\tilde{g}_i$ de $h|_{U_y \times [\frac{i}{n}, \frac{i+1}{n}]}$ tel que $\tilde{g}_i(z, \frac{i}{n}) = \tilde{g}_{i-1}(z, \frac{i}{n})$ pour tout $z \in U_y$. On recolle ensuite les différents relevés et on obtient un relèvement $\tilde{g}_y$ de $h|_{U_y \times [0,1]}$ tel que $\tilde{g}_y(z,0) = \tilde{f}(z)$ pour $z \in U_y$. On procède ainsi pour tout $y \in Y$ On obtient une famille de relèvements sur différents ouverts.

Soit $y' \in Y$. Pour $z \in U_y \cap U_{y'}$, $\tilde{g}_y$ et $\tilde{g}_{y'}$ coïncident en $(z,0)$ et donc sur $\{z\} \times [0,1]$ par connexité par arc de $\{z\} \times [0,1]$ en vertu de la proposition 2.1.17. $\tilde{g}_y$ et $\tilde{g}_{y'}$ coïncident donc sur $U_y \cap U_{y'}$ et l'on peut donc les recoller. On obtient ainsi le relèvement $\tilde{h}$ cherché.

Soit deux tels relèvements $\tilde{h}$ et $\tilde{h}'$. Pour $y \in Y$ ils coïncide en $(y,0)$ Et donc par connexité par arc de $\{y\} \times [0,1]$ sur $\{y\} \times [0,1]$. Ils sont donc égaux. □

Proposition 2.1.20 (Relèvement des chemins). *Pour tout chemin α dans B d'origine b et pour tout $x \in p^{-1}(b)$, il existe un unique relèvement $\tilde{\alpha}$ de α d'origine x*

Démonstration. On applique la proposition précédente avec Y réduit à un point. □

Corollaire 2.1.21. *Si α et β sont deux chemins homotopes dans B et si $\tilde{\alpha}$, $\tilde{\beta}$ sont des relèvements de α, β ayant même origine alors ils ont même extrémité et sont homotopes.*

Démonstration. Soit $h : [0,1] \times [0,1] \to B$ une homotopie de α à β avec

$$h(t,0) = \alpha(t), \quad h(t,1) = \beta(t), \quad h(0,s) = \alpha(0) = \beta(0), \quad h(1,s) = \alpha(1) = \beta(1).$$

Soit $\tilde{h}$ le relèvement de h avec $\tilde{h}(.,0) = \alpha$. Alors l'unicité dans la proposition 2.1.20 Et comme les chemins constants se relèvent en des chemins constants (encore l'unicité) on a :

$$\tilde{h}(t,1) = \tilde{\beta}(t), \quad \tilde{h}(0,s) = \tilde{\alpha}(0) = \tilde{\beta}(0), \quad \tilde{h}(1,s) = \tilde{\alpha}(1) = \tilde{\beta}(1)$$

□

Corollaire 2.1.22. *Soit $p : X \to B$ un revêtement avec X connexe par arcs, $b \in B$ et $x \in p^{-1}(b)$. Alors les propriété suivante sont équivalentes :*

1 X est simplement connexe,

2 deux lacets c, c' en b dans B sont homotopes si leur relèvement d'origine x ont même extrémité.

Démonstration. On suppose que X est simplement connexe. Soit deux lacets dans B en b dont les relèvements en x ont même extrémité. Ces deux relèvements ont même origine et même extrémité et sont donc homotopes par simple connexité de X. Leurs images par p sont donc aussi homotopes. On a donc $1 \Rightarrow 2$.

Soit α et α' deux chemins dans X ayant même origine x et même extrémité. Alors les chemins $p \circ \alpha$ et $p \circ \alpha'$ ayant des relevés en x qui ont la même origine et la même extrémité sont donc homotopes. Par le relèvement des homotopies, α et α' sont homotopes. Comme X est connexe par arcs, il est suffisant pour montrer que deux chemins de même origine et de même extrémité sont homotopes de le vérifier pour des chemin ayant la même origine x fixée. □

Le groupe fondamental

définitions et premières propriétés On se donne X un espace topologique

Définition 2.1.6. Soit X un espace topologique et $x \in X$. L'ensemble des lacets en x (c'est à dire l'ensemble des application $f : [0,1] \to X$ telle que $f(0) = f(1) = x$) peut être munit d'une loi de composition interne (on juxtapose les chemins). Cet espace munit de la composition des chemins et quotienté par la relation d'homotopie (c'est une relation d'équivalence compatible avec la loi) est un groupe noté $\pi_1(X,x)$, son élément neutre est la classe du lacet constant en x. Il est appelé *groupe fondamental* ou *groupe de Poincaré de X au point x*.

Pour plus de détail ont peu aller voir [God71, page 71 à 76]. On notera entre crochets $[c]$ la classe d'homotopie d'un chemin ou d'un lacet c

Proposition 2.1.23. *Soit c un lacet de x à y dans X. L'application*

$$\alpha_c : \quad \pi_1(X,y) \longrightarrow \pi_1(X,x)$$

$$[\gamma] \longmapsto [c\gamma c^{-1}]$$

est un isomorphisme qui ne dépend que de la classe d'homotopie de c.

Si c' est un deuxième chemin joignant x à y les isomorphismes α_c et $\alpha_{c'}$ sont conjugués dans $\pi_1(X,x)$.

Démonstration. voir [God71, page 76, propposition 2.3] □

On se donne à présent un autre espace topologique Y, $y \in Y$ et une application continue $f : X \to Y$ telle que $f(x) = y$.

Proposition 2.1.24. *Soit une application continue $f : X \to Y$ telle que $f(x) = y$. Alors f induit un morphisme*

$$f_* : \quad \pi_1(X,x) \longrightarrow \pi_1(Y,y) .$$

$$[c] \longmapsto [f \circ c]$$

De plus, si f est l'identité de X, f_* est l'identité de $\pi_1(X,x)$ et si g est une application continue de Y dans Z alors $(g \circ f)_* = g_* \circ f_*$.

Démonstration. cela découle des définitions □

On a donc l'invariance par homéomorphisme du groupe fondamental, on a aussi l'invariance du groupe fondamental entre deux espaces homotopes (voir [God71, page 77 théorème 3.4])

On peut voir π_1 comme un foncteur de la catégorie des espaces topologiques pointés dans celle des groupes. On peut donner une autre définition du groupe fondamental. On considère le foncteur Φ qui à un revêtement $p : X \to B$ associe l'ensemble $p^{-1}(b)$. On appelle alors groupe fondamental le groupe des automorphisme du foncteur Φ. Pour plus de précisions [eAD79, page 33 à 37]. Cette définition est équivalente à celle donnée ici, cela étant démontrer dans [eAD79, page 53 4.8.8].

Dans la suite nous garderons la première définition du groupe fondamental comme groupe des lacets quotienté par la relation d'homotopie.

Relation avec les revêtements On se donne à nouveau un revêtement $p : X \to B$

Proposition 2.1.25. *Soit x in X et $b = p(x)$. Le morphisme $p_* : \pi_1(X,x) \to \pi_1(B,b)$ est injectif.*

Démonstration. Soit α un lacet dans X d'origine x tel que $p \circ \alpha$ soit homotope au lacet constant dans B. Alors par l'unicité du relèvement α est le relevé de $p \circ \alpha$ et, en vertu du corollaire 2.1.21, α est homotope au chemin constant. □

Proposition 2.1.26. *Soit $x' \in p^{-1}(b)$ alors, si x et x' sont dans la même composante par arc de X, les sous-groupes $\mathfrak{p}_*\pi_1(X,x)$ et $p_*\pi_1(X,x')$ sont conjugués dans $\pi_1(B,b)$.*

Réciproquement pour tout sous-groupe H de $\pi_(B,b)$ conjugué du sous-groupe $p_*\pi_1(X,x)$, il existe x' tel que $H = p_*\pi_1(X,x')$.

Démonstration. voir [God71, page 131 proposition 2.5 et 2.6] □

Proposition 2.1.27. *On peut définir une application $\pi_1(B,b) \times p^{-1}(b) \to X$ en associant à un couple $(g = [\alpha],x)$ l'extremité $x.g = \tilde{\alpha}(1)$ de l'unique relevé de α d'origine x. Cette application est une action du $\pi_1(B,b)$ sur la fibre $F = p^{-1}(b)$. Le stabilisateur de $x \in F$ par l'action de $\pi_1(B,b)$ est $p_*\pi_1(X,x)$.*

Démonstration. Soient g et g' dans $\pi_1(B,b)$, et α et α' des représentants de g et g' respectivement. Le relèvement de la composition des chemin $\alpha.\alpha'$ est la concaténation du relèvement du chemin $\tilde{\alpha}$ de α d'origine x et du relèvement $\tilde{\alpha'}$ de α' d'origine $\alpha(1)$ (ce chemin convient et par unicité c'est le seul). Le relevé en x du chemin constant en b est le chemin constant en x. On a donc

$$\forall x \in F \, \forall g,g' \in \pi_1(B,b) \; x.(gg') = (x.g).g' \text{ et } x.e = x$$

où e est l'élément neutre de $\pi_1(B,b)$

Soit $g \in \pi_1(B,b)$ fixant x. Si α est un lacet en b représentant g, alors le relevé $\tilde{\alpha}$ de α en x est tel que $\tilde{\alpha}(1) = x$ et $\tilde{\alpha}$ est un lacet en x. Réciproquement si $g \in \pi_1(X,x)$ et que β est un représentant de g, β est est par unicité le relevé de $p \circ \beta$ et donc $x.p_*(g) = \beta(1) = x$. □

Proposition 2.1.28. *Si B est connexe par arcs, l'application $F \to \pi_0(X) = \left\{ \begin{array}{c} \text{composantes connexes} \\ \text{par arcs de } X \end{array} \right\}$ qui à $x \in F$ associe sa composante connexe, induit une bijection :*

$$F/\pi_1(B,b) \simeq \pi_0(X).$$

Démonstration. Soit $x \in X$. On a un chemin de $p(x)$ à b. Son relevé d'origine x est donc un chemin de y à un point de F. Donc $F \to \pi_0$ est surjective. D'autre part si x et x' sont deux points de F joints par un chemin α, alors $p \circ \alpha$ est un lacet en b et donc $x' = x.[p \circ \alpha]$. Enfin si x et x' dans F sont tels que $x' = x.g$ avec $g \in \pi_1(B,b)$, il existe un chemin de x à x'. □

Corollaire 2.1.29. *Si X est connexe par arcs, alors pour tout x dans F l'action de $\pi_1(B,b)$ induit une bijection :*

$$\pi_1(B,b)/\mathfrak{p}_*\pi_1(X,x) \simeq F$$

Démonstration. On utilise la proposition 2.1.1 et la deuxième partie de la proposition 2.1.27 □

Nous donnons ici une proposition qui,dans le cas où le revêtement est issue de l'action d'un groupe G, lie le groupe fondamental de l'espace total, celui de la base et G.

Proposition 2.1.30. *Soit G un groupe discret, agissant proprement et librement sur un espace topologique séparé et connexe par arc, $p : X \to B = X/G$ la projection canonique, $b \in B$ et $x \in F = p^{-1}(b)$. Pour tout $\gamma \in \pi_1(B,b)$, il existe un unique g_γ tel que $x.\gamma = g_\gamma.x$. L'application $\pi_1(B,b) \to G$ avec $\gamma \mapsto g_\gamma$ définie une bijection :*

$$\pi_1(B,b)/p_*\pi_1(X,x) \simeq G$$

Démonstration. F est par définition l'orbite de x sous l'action de G. Cela donne l'existence de g_γ. L'unicité vient du fait que l'action est libre.

On montre à présent qu'on a un morphisme de groupe. On a clairement $g_e = e$. On se donne $g \in G$, $\gamma \in \pi_1(B,b)$ et α un représentant de γ en b. $x.\gamma$ est l'extrémité du relèvement $\tilde{\alpha}$ de α d'origine x. $g.(x.\gamma)$ est donc l'extremité du relèvement $t \mapsto g.\tilde{\alpha}(t)$ de α d'origine $g.x$. Par unicité, on a donc $g.(x.\gamma) = (g.x).\gamma$. On en déduit donc :

$$g_{\gamma\gamma'}.x = x.(\gamma\gamma') = (x.\gamma).\gamma' = (g_\gamma.x).\gamma' = g_{\gamma'}.(g_\gamma.x) = (g_\gamma g_{\gamma'}).x$$

En vertu de la proposition 2.1.27 le noyau est bien $p_*\pi_1(X,x)$. □

Exemple 2.1.6. Comme S^{2n+1} est simplement connexe (son groupe fondamental est nul), On a que le groupe fondamental de L_p^{2n+1} (cf exemple 2.1.5 (iv)) est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Nous citons ici un résultat sur le relèvement des applications (et non plus seulement sur celui des chemins). Même si ce résultat n'a pas grande importance par la suite, il serait dommage de l'omettre car il est intéressant. Nous n'en feront cependant pas la démonstration que l'on peut trouver dans [God71, page 132 théorème 3.2] ou dans [Pau01, page 37 théorème 3.23]. Les démonstrations bien que n'employant pas les mêmes concepts fonctionnent sensiblement de la même façon.

Théorème 2.1.31 (Théorème du relèvement). *Soit $p : X \to B$ un revêtement, Y un espace connexe et localement connexe par arc, et $f : Y \to B$ une application continue. Soit $y \in Y$, $b = f(y)$ et $x \in p^{-1}(b)$. Il existe un relèvement $\tilde{f} : Y \to X$ de f tel que $\tilde{f}(y) = x$ si et seulement si*

$$f_*\pi_1(Y,y) \subset p_*\pi_1(X,x).$$

Revêtements galoisiens

Avant de donner le théorème principal nous avons encore besoin de quelques propositions. La première de ces propriétés est une caractérisation des B-morphismes.

Proposition 2.1.32. *Soient $p : X \to B$ et $p' : X' \to B$ deux revêtements, avec B connexe et localement connexe par arc. Soit $b \in B$, $F = p^{-1}(b)$ et $F' = p'^{-1}(b)$. Alors l'application*

$$\begin{array}{rccc} \Theta : & \mathrm{Hom}_B(X,X') & \to & \mathrm{Hom}_{\pi_1(B,b)}(F,F') \\ & f & \mapsto & f|_F \end{array}$$

est une bijection.

Démonstration. Commençons par montrer que l'application est bien définie. Si f est un B-morphisme $X \to X'$, alors il est clair que $f(F) \subset F'$. Soit $g = [\alpha] \in \pi_1(B,b)$ et $x \in X$, $x.g$ est alors l'extrémité du chemin $\tilde{\alpha}$ d'origine x qui relève α. Le chemin $f \circ \tilde{\alpha}$ est alors le relevé de α d'origine $f(x)$ et son extrémité $f(x.g)$ vaut donc $f(x).g$.

étape 1 : On se ramène au cas où X est connexe par arc.

Lemme 2.1.33. *Soit $p : X \to B$ un revêtement, avec B connexe et localement connexe par arc. Si C est une composante connexe de X, alors $p|_C : C \to B$ est un revêtement.*

Démonstration. Soit $b \in B$, V un voisinage distingué et connexe de b et $h : V \times F \to p^{-1}(V)$ une trivialisation de p au-dessus de V. Soit D' l'ensemble des d tel que $h(V \times \{d\}) \subset C$. Par connexité, on a $h(V \times \{d\}) \cap C = \emptyset$ si $d \notin D'$. $h|_{V \times D'}$ est donc une trivialisation de $p|_C$ au-dessus de V si D' est non vide. Soit x dans C et α un chemin de $p(x)$ à b. Soit $\tilde{\alpha}$ son relevé d'origine x, alors $\tilde{\alpha}(1) \in p^{-1}(V) \cap C$ et donc D' est non vide. □

Soit $(X_i)_{i \in I}$ la famille des composantes connexes par arcs de X. Les orbites de $\pi_1(B,b)$ dans F sont les $F \cap X_i$. Les restrictions à chaque X_i donnent donc des bijections :

$$\mathrm{Hom}_B(X,x') \simeq \prod_{i \in I} \mathrm{Hom}_B(X_i,X') \quad \text{et} \quad \mathrm{Hom}_{\pi_1(B,b)}(F,F') \simeq \prod_{i \in I} \mathrm{Hom}_{\pi_1(B,b)}(F \cap X_i,F')$$

Si le résultat est vrai pour chaque X_i il est donc vrai pour X.

Étape 2 : On suppose maintenant X connexe par arc. En particulier, l'action de $\pi_1(B,b)$ sur F est transitive. Soit f et g dans $\mathrm{Hom}_B(X,X')$ tel que $f|_F = g|_F$. Comme X est connexe (et F non vide) on a d'après le corollaire 2.1.18 que $f = g$. Θ est donc injective, on va montrer qu'elle est surjective. Soit $\varphi : F \to F'$ une application $\pi_1(B,b)$-équivariante. Soit x dans F, on pose $x' = \varphi(x)$. Comme X est connexe et localement connexe par arc on a d'après le théorème du relèvement (2.1.31) qu'il existe un relèvement $f : X \to X'$ de l'application $p : X \to B$ par le revêtement $p' : X' \to B$ tel que $f(x) = x'$si et seulement si $f_*\pi_1(Y,y) \subset p_*\pi_1(X,x)$. Soit $g \in p_*\pi_1(X,x)$, alors g fixe x d'après la proposition 2.1.27 et $x'.g = \varphi(x).g = \varphi(x.g) = \varphi(x) = x'$. g fixe donc x' et est donc dans $p_*(\pi_1(x',x'))$ toujours par la même proposition.

$f|_F$ et φ sont $\pi_1(B,b)$-équivariantes, comme l'action de $\pi_1(B,b)$ est transitive et que $f(x) = \varphi(x)$ on a $f|_F = \varphi$. Θ est donc surjective. □

Corollaire 2.1.34. *Sous les hypothèses de la proposition précédentes, la restriction à F induit une bijection entre les isomorphisme $X \to X'$ de revêtement au-dessus de B (X et X' sont fixé) et les isomorphismes $\pi_1(B,b)$-équivariants de F sur F'.*

La démonstration est simple (on peu la trouver dans [Pau01, page 41 corollaire 3.29]).

Donnons maintenant une proposition sur les groupes qui va nous être utile.

Lemme 2.1.35. *Soit G un groupe et H un sous-groupe de G. Alors les groupes $\mathrm{Aut}_G(G/H)$ et $N(H)/H$ sont isomorphes. $N(H)$ désigne ici le plus sous groupe de G dans le quel H soit distingué.*

En particulier l'action du groupe des bijection G-équivariantes agit transitivement sur G/H si et seulement si $G = N(H)$.

Proposition 2.1.36. *Soit $p : X \to B$, un revêtement, avec X connexe et séparé, et B localement connexe. Le groupe discret $\Gamma = \mathrm{Aut}_B(X)$ agit (continûment) proprement et librement sur X. Si Γ' est un sous groupe de Γ et $f : X/\Gamma' \to B$ est l'application induite par p, alors f est un revêtement et la projection canonique $\pi : X \to X/\Gamma'$ est un morphisme de revêtement.*

Démonstration. Comme X est connexe l'action de Γ est libre d'après le corollaire 2.1.18. Soit $gr : \Gamma \times X \to X \times X$ l'application graphe $(g,x) \mapsto (x,gx)$. Comme $\Gamma \times X$ est séparé et que l'action est libre l'image réciproque d'un point est un point, donc compact. On va montrer que l'application graphe est fermée ce qui permettra de conclure la première partie. Soit F un fermé de $\Gamma \times X$ et $(x,y) \in \overline{gr(F)}$. On montre que $(x,y) \in gr(F)$. Comme $p \times p$ est continue et que B est séparé, si Δ est la diagonale de $B \times B$, alors :

$$(p \times p)(x,y) \in (p \times p)(\overline{gr(F)}) \subset \overline{(p \times p)(gr(F))} \subset \overline{\Delta} = \Delta.$$

On a donc que $p(x) = p(y)$. Soit V un voisinage distingué connexe de $p(x)$, et V_x, V_y les composantes connexes de $p^{-1}(V)$ contenant x, y respectivement. L'intersection $(V_x \times V_y) \cap gr(F)$ est non vide car $(x,y) \in \overline{gr(F)}$. Soit donc $g \in \Gamma$ et u dans X tel que $u \in V_x$ et $gu \in V_y$. Comme g est un automorphisme de revêtement de p on a que $gV_x = V_y$, en particulier $y = gx$.

Un sous groupe Γ' de Γ agit aussi proprement et librement sur X. Si V est un voisinage distingué connexe dans B pour p, alors comme Γ' permute les composantes connexes de $p^{-1}(V)$, V est aussi un voisinage distingué pour $f : X/\Gamma' \to B$. □

Théorème 2.1.37. *Soit $p : X \to B$ un revêtement, avec X connexe et localement connexe par arcs, $x \in X$, $b = p(x)$ et $F = p^{-1}(b)$. Les conditions suivantes sont équivalentes :*

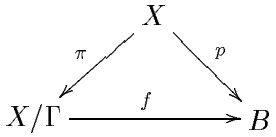
1 l'action de $\mathrm{Aut}_B(X)$ sur F est transitive

2 $p_*\pi_1(X,x)$ est distingué dans $\pi_1(B,b)$

3 $p_*\pi_1(X,y) = p_*\pi_1(X,z)$ pour tout y et z dans F

4 pour tout lacet α de B en b, ou bien tout relèvement de α est un lacet, ou bien aucun n'est un lacet.

5 Il existe un groupe discret Γ agissant proprement et librement sur X et un homéomorphisme $f : X/\Gamma \to B$ tel que si π est la projection canonique $X \xrightarrow{\pi} X/\Gamma$, alors le diagramme suivant commute :



Démonstration. Soir $G = \pi_1(B,b)$ et $H = p_*\pi_1(X,x)$. Comme X est connexe par arcs, il existe par le corollaire 2.1.29 une bijection G-équivariante de F sur G/H. Donc par le corollaire 2.1.34 $\mathrm{Aut}_B(X)$ agit transitivement sur F si et seulement si le groupe des bijections G équivariantes de G/H agit transitivement sur G/H. En vertu de la remarque 2.1.35, (1) et (2) sont équivalentes.

Si l'assertion (1) est vérifiée alors (4) aussi.

Supposons que l'assertion (4) soit vérifiée. Soient y et z dans F. Soit α un lacet en y dans X. Alors $p \circ \alpha$ est un lacet en b, son relèvement β en z est donc aussi un lacet avec $p_*[\alpha] = p_*[\beta]$. On a donc $p_*\pi_1(X,y) \subset p_*\pi_1(X,z)$. Par symétrie des roles jouer par y et z on a l'égalité.

Supposons que l'assertion (3) soit vérifiée. Soit α un lacet en b dans B. Soit c son relèvement d'origine x et y l'extrémité de c. On a un isomorphisme $\varphi_c : \pi_1(X,x) \to \pi_1(X,y)$ qui a $[\beta]$ associe $[c.\beta.c^{-1}]$. Comme $p_*[c.\beta.c^{-1}] = [\alpha].p_*(\beta).[\alpha]^{-1}$ on a :

$$[\alpha]p_*\pi_1(x,x)[\alpha]^{-1} = p_*(\varphi_c(\pi_1(X,x))) = p_*\pi_1(X,y) = p_*\pi_1(X,x).$$

Si l'assertion (5) est vérifiée, alors Γ est contenu dans $\mathrm{Aut}_B(X)$ et (1) est vérifiée. Réciproquement si (1) est vérifiée, par la proposition 2.1.36 le groupe $\Gamma = \mathrm{Aut}_B(X)$ agit proprement et librement sur X, et l'application $f : X/\Gamma \to B$ est un revêtement (d'après 2.1.10) à un feuillet (car l'action est transitive). C'est donc un homéomorphisme et (5) est vérifié. □

Définition 2.1.7. Un revêtement $p : X \to B$ avec X connexe et localement connexe par arcs qui vérifie l'une des propriété (1)-(4) du théorème est dit *galoisien*. Le groupe $\Gamma = \mathrm{Aut}_B(X)$ est alors appelé *groupe de Galois* de p.

On va en citant quelques propositions expliciter d'où vient l'appellation de galoisien. On se done un revêtement galoisien $p : X \to B$ on note G son groupe de Galois. On se donne aussi un espace discret F sur le quel G opère à droite. On a une action continue de G sur $X \times F$ donnée par $(x,f) \mapsto (gx,fg)$. Les démonstrations des propriétés qui suivent peuvent se trouver dans [God71, pages 121-125]. Elles sont assez proches voir extrêmement semblables à ce que avons fait pour démontrer le théorème. Tous les espaces sont supposés localement connexe par arcs.

Lemme 2.1.38. *Le groupe G opère proprement et librement sur $X \times F$.*

Lemme 2.1.39. *la projection $\pi_F : X \times F \to X_F = (X \times F)/G$ est un revêtement.*

De plus l'application $X \times F \to B$, $(x,f) \mapsto p(x)$ induit une application $p_F : X_F \to B$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} X \times F & \xrightarrow{p_1} & X \\ {\scriptstyle \pi_F}\downarrow & & \downarrow{\scriptstyle p} \\ X_F & \xrightarrow[p_F]{} & B \end{array}$$

Proposition 2.1.40. *L'application p_F est un revêtement.*

La fibre de ce revêtement est isomorphe à F. On dit alors que $p_F : X_F \to B$ est le *revêtement de fibre F associé* au revêtement galoisien $p : X \to B$.

Proposition 2.1.41. *Pour que le revêtement X_F associé à X soit tel que X_F soit connexe, il faut et il suffit que G opère transitivement sur F.*

Proposition 2.1.42. *Soit $p : X \to B$ un revêtement galoisien de groupe G et $p' : X' \to B$ un revêtement de B avec X' connexe. Pour que X' soit isomorphe à un revêtement $p_H : X/H \to B$ où H est un sous groupe de G , il faut et il suffit qu'il existe un B-morphisme h de X sur X'.*

Proposition 2.1.43. *Soient $p : X \to B$ un revêtement galoisien de groupe G, F et F' deux espaces discrets sur les quels G agit. On a alors une bijection entre* $\mathrm{Hom}_B(X_F,X_{F'})$ *et* $\mathrm{Hom}_G(F,F')$

Si X_F est un revêtement associé à X avec X_F connexe (c'est à dire que G opère transitivement sur F), X_F est isomorphe à $p_H : X/H \to B$, où H est le stabilisateur d'un point de F.

Théorème 2.1.44. *Soit $p : X \to B$ un revêtement galoisien.*

1l'ensemble des classes d'isomorphismes de revêtement connexes associés à X est en correspondance biunivoque avec l'ensemble des classes de sous groupes conjugués de G.

2 Un revêtement associé à X est galoisien si et seulement si il correspond à un sous groupe distingué H de G. Son groupe d'automorphisme est alors isomorphe au quotient G/H.

Ce théorème justifie l'appellation de galoisien; Il montre que la classification des revêtements connexes associé à un revêtement galoisien est formellement analogue à celle des extension intermédiaires d'une extension galoisienne d'un corps parfait $\mathbb{K}$.

2.1.2 Revêtements branchés ou revêtements ramifiés

Définitions

Nous donnons ici la définition d'une classe plus générale que celle des revêtements, celles des revêtements ramifiés. Cependant nous restreignons notre définition au cas des variétés différentiables. Intuitivement, c'est une application qui est un revêtement si l'on supprime de l'espace de départ (et donc de l'image) un ensemble assez petit de points.

Théorème 2.1.45. *Soit $f : M \to N$ une application différentiable entre deux variétés compactes, connexes et de même dimension n telle que son jacobien s'annule sur un espace A de dimension inférieur ou égal à $n-2$. Posons $N' = N \setminus f(A)$ et $M' = M \setminus f^{-1}(f(A))$. Alors l'application $f : M' \to N'$ est un revêtement à un nombre fini de feuillets et M' est connexe.*

Définition 2.1.8. L'application initiale $f : M \to N$ s'appelle alors *revêtement ramifié le long de A*. $f(A)$ est alors appelé *ensemble des points de ramification.*

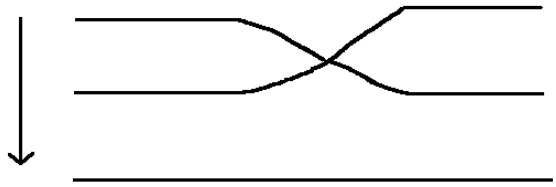


FIG. 2.3 – *une bonne idée intuitive de ce qui ce passe*

Dans la figure précédente il faut pour que cela soit correct considérer que les droites sont des plans (la figure étant invariante par rotation autour d'un axe vertical passant par le point ou cela ne marche pas). Cela correspond à une représentation du revêtement ramifié le long de 0 $\mathbb{C} \xrightarrow{z^2} \mathbb{C}$.

Démonstration. On commence par considéré le cas où A est vide. Comme M est compacte, le cardinal de chaque fibre $f^{-1}(y)$ est fini pour y dans N. En effet on considère un recouvrement de M par des ouvert U_i tels que $f|_{U_i}$ soit un difféomorphisme, on en extrait un sous recouvrement fini U_1,...,U_k, l'image réciproque d'un point y possède au plus un élément dans chaque U_j pour $j = 1,...k$. Par connexité tous les ensemble $f^{-1}(y)$ ont même cardinal. $f : M \to N$ est donc un revêtement en vertu de 2.1.2.

Dans le cas où A est non vide, on considère un ϵ-voisinage U_ϵ de $f(A)$ tel que $N \setminus U_\epsilon$ reste connexe (possible étant donner l'hypothèse sur la dimension de A). On applique le résultat précédent à $N_\epsilon = N \setminus U_\epsilon$ et à $M_\epsilon = M \setminus f^{-1}(U_\epsilon)$. Enfin on fait tendre ϵ vers 0 pour obtenir le résultat souhaité. □

2.2 Théorie des nœuds et entrelacs

Dans cette section nous donnerons la définition exacte de ce qu'est un nœud et un entrelac. Nous expliquerons rapidement comment décrire le groupe fondamental d'un nœud avec des générateurs et des relations

2.2.1 Généralités

Définitions

Définition 2.2.1. Soit $f : S^1 \to S^3$ (ou plus simplement $\mathbb{R}^3$) un plongement. On appelle *nœud de* S^3 l'image de S^1 par f.

Soit $g : \prod_{i=1}^{n} S^1 \to S^3$ (avec $n \in \mathbb{N}$) un plongement. On appelle *entrelacs de* S^3 l'image de

$\prod_{i=1}^{n} S^1$ par g.

Dans le cas où l'on munit S^1 d'une orientation, on parle de nœud orienté (ou d'entrelacs orienté dans le cas d'entrelacs).

On a le lemme suivant :

Lemme 2.2.1. *Soit L un entrelacs orienté de S^3 à n composantes. Alors il existe un voisinage $N(L)$ tubulaire de L assez petit tel que $\partial N(L)$ soit une union disjointe de n tores $S^1 \times S^1$ plongés dans S^3*

pour étudier la manière dont les nœuds sont noués on se limite à des classes d'équivalence de nœuds.

Définition 2.2.2. Deux nœuds $\mathcal{K}_1$ et $\mathcal{K}_2$ de $\mathbb{R}^3$ sont dit équivalents s'il existe un homéomorphisme de $\mathbb{R}^3$ qui envoie $\mathcal{K}_1$ dans $\mathcal{K}_2$. On dit que deux nœuds sont *de même type* s'ils sont dans la même classe.

On peut représenter un nœud symboliquement par sa projection sur un plan, en remplacement les lignes courbes par des lignes brisées avec la convention que lorsque ligne "passe sous" une autre, celle du dessous est coupées.

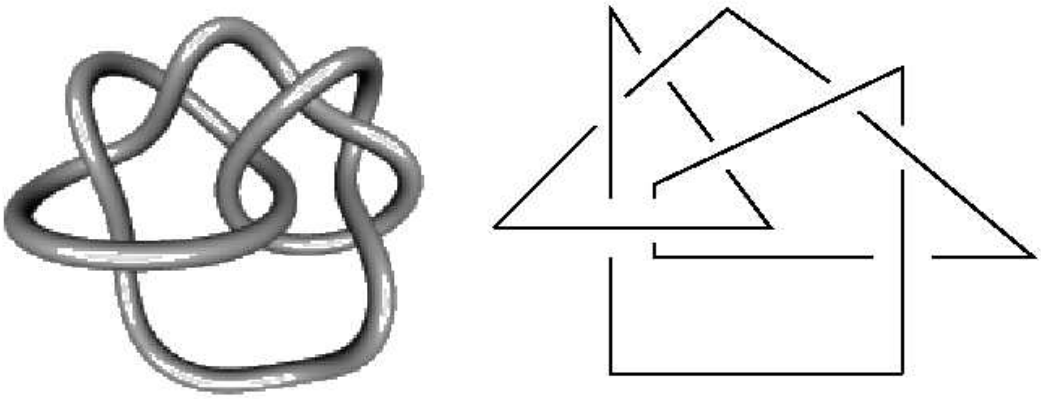


FIG. 2.4 – *un petit exemple*

On appelle cette manière de représenter un nœud la projection du nœud. Il y a des conditions supplémentaires pour que ce soit vraiment la projection : par exemple, en un point où deux segments se coupent il ne doit pas passer d'autre segment.

Groupe fondamental

Une des parties de la théorie des nœuds est de classifier les différents types de nœuds. Le groupe fondamental étant invariant par homéomorphisme, il définit un invariant des différents nœuds d'un même type.

Définition 2.2.3. On appelle *groupe du nœud* $\mathcal{K}$ le groupe fondamental pris en un point p_0 quelconque de $\mathbb{R}^3 \setminus \mathcal{K}$. On note $\pi_{\mathcal{K}} = \pi_1(\mathbb{R}^3 \setminus \mathcal{K}; p_0)$

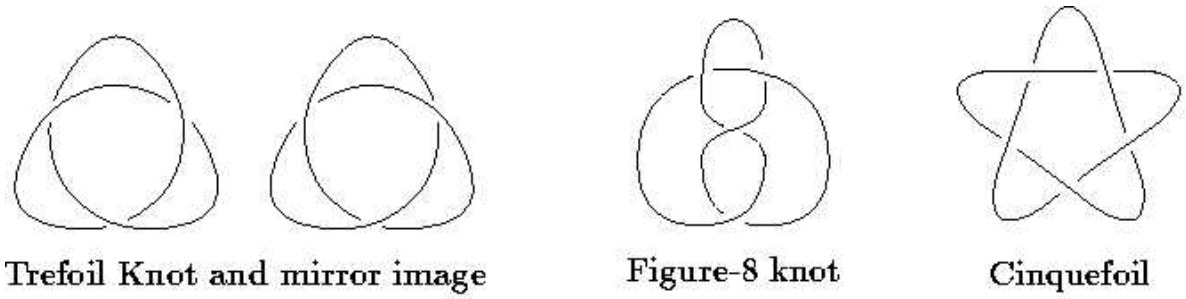


FIG. 2.5 – *d'autres exemples de nœuds*

On montre qu'on peut décrire le groupe d'un nœud par générateurs et relations. Soit $\mathcal{K}$ un nœud. À chaque composante connexe de la projection de $\mathcal{K}$, on associe un symbole g_i qui correspond à un lacet de $\pi_{\mathcal{K}}$ qui fait un tour au tour de cette composante en arrivant par en dessous.

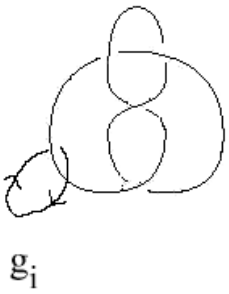


FIG. 2.6 –

Ensuite à un croisement on associe une relation :

FIG. 2.7 –

Chapitre 3

Une analogie

Comme nous l'avons dit dans l'introduction, le but de ce rapport est de comprendre les énoncés de deux théorèmes qui concernent deux domaines des mathématiques complètement différents : la topologie des variétés et la théorie des nombres. Avant de donner une version simplifiée du dictionnaire qui permet de passer d'un domaine à l'autre et d'en donner quelques limites, nous commencerons par énoncer les deux théorèmes qui sont une expression flagrante du lien qui existe entre ces deux domaines.

3.1 Énoncé des théorèmes

Problème T Soit C_p un groupe cyclique d'ordre premier p. Supposons que C_p agisse sur une variété M orientée, lisse, fermée et connexe de dimension 3. Dans cet situation la projection $\pi : M \to M/C_p$ est un revêtement ramifié. Une fois donnée l'action induite de C_p sur les groupe de torsion et sur la partie libre de $\mathrm{H}_1(M,\mathbb{Z})$ (notés $\mathrm{H}_{tor}(M)$ et $\mathrm{H}_{free}(M) = \mathrm{H}_1(M,\mathbb{Z})/\mathrm{H}_{tor}(M)$), on se propose de contrôler la borne supérieur du nombre s des composantes connexes de l'ensemble où il y a ramification. On a noté $\mathrm{H}_1(M,\mathbb{Z})$ le foncteur dérivé du foncteur section global appliqué au faisceau des fonctions localement constantes à valeur dans $\mathbb{Z}$

On a le théorème suivant :

Théorème 3.1.1. *Sous les hypothèses du problème T et avec l'hypothèse supplémentaire que* $\mathrm{H}_{free}(M/C_p) = 0$ *on a :*

$$s \leqslant 1 + \dim_{\mathbb{F}_p} \mathrm{H}^2(C_p, \mathrm{H}_{tor}(M)) + \dim_{\mathbb{F}_p} \mathrm{H}^1(C_p, \mathrm{H}_{free}(M)).$$

problème N Soient C_p un groupe cyclique d'ordre premier agissant sur un corps de nombre $\mathbb{L}$, $\mathbb{K} = \mathbb{L}^{C_p}$. Connaissant l'action de C_p sur le groupe des classes d'idéaux de $\mathbb{L}$ ($Cl(\mathbb{L})$) et sur le groupe des unités $O_{\mathbb{L}}^*$, on cherche un borne supérieure au nombre de place premières de $\mathbb{K}$ ramifiées dans $\mathbb{L}$. On notera s le nombre de places finies ramifiées et s_0 le nombre total de places ramifiées. On notera, en suivant le dictionnaire (voir la section suivante), $\mathrm{H}_{tor}(\mathbb{L}) = Cl(\mathbb{L})$ et $\mathrm{H}_{free}(\mathbb{L}) = O_{\mathbb{L}}^*/torsion$.

Théorème 3.1.2. *Sous les hypothèses du problème N on a :*

$$s_0 = 1 + \dim_{\mathbb{F}_p} \mathrm{H}^2(C_p, \mathrm{H}_{tor}(\mathbb{L})) + \dim_{\mathbb{F}_p} \mathrm{H}^1(C_p, \mathrm{H}_{free}(\mathbb{L})).$$

3.2 Le dictionnaire MKR

Kapranov et Reznikov on construit à partir des idées de Mazur un dictionnaire qui permet de traduire les objets et les concepts de la théorie des variétés de dimension 3 dans la théorie des nombres.

Topologie	Théorie des nombres
Une variété M lisse, fermée, orientée, connexe	Un corps de nombre $\mathbb{K}$ (extension finie de $\mathbb{Q}$). Plus précisément c'est $Spec\mathcal{O}_{\mathbb{K}}$ l'ensemble des idéaux premiers de $\mathbb{K}$
Un entrelac dans M	Un idéal dans $\mathcal{O}_{\mathbb{K}}$
Un nœud dans M	Un idéal premier de $\mathcal{O}_{\mathbb{K}}$
Une surface $S \subset M$.	Un entier algébrique $\omega \in \mathcal{O}_{\mathbb{K}}$
L'opération $S \to \partial S$	$\omega \to (\omega) \subset \mathcal{O}_{\mathbb{K}}$
Un entrelac de la forme ∂S est nul dans $\mathrm{H}_1(M,\mathbb{Z})$	un idéal de la forme (ω) est nul dans $Cl(\mathbb{K})$ (voir définition 1.1.6)
Une surface fermé $F \subset M$	Une unité de $\mathcal{O}_{\mathbb{K}}$
La partie de torsion de $\mathrm{H}_1(M,\mathbb{Z})$ notée $\mathrm{H}_{tor}(M)$	$Cl(\mathbb{K})$
la partie libre de $\mathrm{H}_1(M,\mathbb{Z})$ notée $\mathrm{H}_{free}(M) = \mathrm{H}_1(M,\mathbb{Z})/H H_{tor}(M)$	Le groupe des unités modulo la torsion (les racines de l'unité) $\mathcal{O}^*_{\mathbb{K}}/\mu(\mathbb{K})$
Les revêtements ramifiés finis $\pi : M \to N$	Les extensions finies $L \supset K$
Soit G un groupe fini qui agit sur M de manière lisse en conservant l'orientation, induit une application $M \to M/G$. M/G est encore une variété de dimension 3 et $M \to M/G$ est un revêtement fini ramifié.	Une extension galoisienne $\mathbb{K} \subset \mathbb{L}$ avec $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ induit un morphisme $Spec\mathcal{O}_{\mathbb{L}} \to Spec\mathcal{O}_{\mathbb{L}}/G = Spec\mathcal{O}_{\mathbb{K}}$.
S^3 qui n'a pas de revêtement non trivial non ramifié	$\mathbb{Q}$ qui n'a pas d'extension non triviale non ramifiée (voir 1.1.37)

Remarquons cependant que ce dictionnaire n'est pas fixe : A. Sikora précise dans son article [Sik01] que Reznikov qui est à l'origine du dictionnaire l'a modifié dans [Rez00] où il est question de "$3\frac{1}{2}$-variété". A. Sikora ne s'étend pas sur cette autre version que je n'ai pas eu le temps ni le courage de regarder, car les résultats qu'ils exposent dans son article ne s'applique pas au nouveau dictionnaire. Ceci mets en evidence la portée limitée du dictionnaire que nous venons de citer.

3.3 Démonstration du théorème 3.1.2

La première partie de ce rapport nous fournit tous les éléments nécessaires à la compréhension des objets qui sont mis en jeu dans cette démonstration. Cette démonstration sera cependant très elliptique car je n'est pas été en mesure de comprendre toutes les démonstrations intermédiaires qu'elle emploie. J'essaierais dans la mesure du possible de donner une référence (ce sera le plus

souvent la référence donnée par A. Sikora dans [Sik01]) où de préciser quelle théorie permet de justifier un affirmation.

On se donne donc $\mathbb{L}$ un corps de nombre, C_p un groupe cyclique d'ordre p et on note $\mathbb{K} = \mathbb{L}^{C_p}$. On fera l'abus de langage qui consiste à parler indifféremment des places de $\mathbb{L}$ ou des idéaux premiers de $\mathcal{O}_\mathbb{L}$ car il n'y a pas de différence pour les places non-archimédiennes (fini). On dit qu'une place infini v de $\mathbb{K}$ est ramifiée dans $\mathbb{L}$ si $i(\mathbb{K}) \subset \mathbb{R}$ et $i(\mathbb{L}) \nsubseteq \mathbb{R}$ où i est l'inclusion associée à v. On note $S_\mathbb{K}$ l'ensemble des places finies de $\mathbb{K}$ et $S_{\mathbb{K}\infty}$ l'ensemble des places infinies de $\mathbb{K}$. On note s_0 le nombre de places finies et s le nombre total de places. On notera $\mathbb{L}_v$ la complétion de $\mathbb{L}$ par rapport à la place v On considère le sous-groupe de $\prod_{v\in S_\mathbb{L}\cup S_{\mathbb{L}\infty}} \mathbb{L}_v^*$ composé des éléments $(x_v)_v$ tel que $x_v \in \mathcal{O}_{\mathbb{L},v}^*$ pour presque tout v. Ce groupe s'appelle groupe des idèles et est noté $\mathbb{I}_\mathbb{L}$. $\mathbb{L}$ s'injecte diagonalement dans $\mathbb{I}_\mathbb{L}$, et l'on note $C(\mathbb{L})$ le quotient. De plus $\mathbb{I}_\mathbb{L}$ s'envoit dans le groupe $I(\mathbb{L})$ des idéaux de $\mathbb{L}$ par $(x_v)_v \mapsto \prod \mathfrak{p}_v^{v(x_v)}$ où le produit est fait sur toutes les places finies. Le noyau de cette application est noté $U_\mathbb{L}$. On remarque que $\mathcal{O}_\mathbb{L}^* \hookrightarrow U_\mathbb{L}$.

Ces remarques nous permettent de construire le diagramme commutatif suivant :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_\mathbb{L}^* & \longrightarrow & \mathbb{L}^* & \longrightarrow & P(\mathbb{L}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_\mathbb{L} & \longrightarrow & \mathbb{I}_\mathbb{L} & \longrightarrow & I(\mathbb{L}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_\mathbb{L}/\mathcal{O}_\mathbb{L}^* & \dashrightarrow & C(\mathbb{L}) & \dashrightarrow & Cl(\mathbb{L}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Le lemme des 3×3 donne l'existence et l'unicité de la suite exacte du bas rendant le diagramme commutatif dans le cas de groupes quelconques.

Comme C_p agit sur chacun de ces groupes nous allons étudier les groupe de cohomologies de C_p à coefficient dans ces groupes.

Lemme 3.3.1.

$$\widehat{\mathrm{H}}^i(C_p, U_\mathbb{L}) = \begin{cases} \mathbb{F}_p^s & si\ i = 0 \\ \mathbb{F}_p^{s_0} & si\ i = 1 \end{cases}$$

Démonstration.

$$U_\mathbb{L} = \prod_{v\in S_\mathbb{L}} \mathcal{O}_{\mathbb{L},v}^* \prod_{v\in S_{\mathbb{L}\infty}} \mathbb{L}_v^*$$

En posant pour v' place de $\mathbb{K}$

$$M_{v'} = \begin{cases} \prod_{v|v'} \mathcal{O}_{\mathbb{L},v}^* & \text{si } v' \text{ est finie} \\ \prod_{v|v'} \mathbb{L}_v^* & \text{si } v' \text{ est infinie} \end{cases}$$

On a que $U_{\mathbb{L}} = \prod_{v'} M_{v'}$. Comme C_p est d'ordre premier une place est inerte, totalement décomposé ou totalement ramifié Dans les deux premier cas on a

$$\widehat{\mathrm{H}}^k(C_p, M'_v) = 0$$

pour tout k. (Si v' est inerte, il n'y a qu'un idéal v au dessus de v' et : $LL_v/\mathbb{K}_{v'}$ est non ramifié donc $\widehat{\mathrm{H}}^k(C_p, \mathcal{O}^*_{\mathbb{L},v}) = 0$ d'après voir 1.3.20 ; si v' est totalement décomposé, il y a p places au dessus de v' mais elles sont toutes non ramifiées.)

Si v' est totalement ramifié, il n'y a qu'une place au dessus de v' on déduit de 1.3.24 que

$$\widehat{\mathrm{H}}^i(C_p, M_{v'}) = \mathbb{F}_p$$

si v' est une place finie. Si v' est une place infinie on à : $\widehat{\mathrm{H}}^0(C_p, M_{v'} = \mathbb{F}_p$ $(p = 2)$ et $\widehat{\mathrm{H}}^1(C_p, M_{v'}) = 0$. Comme la cohomologie commute au produit on a le résultat cherché. □

Un des principaux résultat de la théorie du corps de classe est le calcul des groupes de cohomologie de C_p à valeur dans le groupe des classes d'idèles $C(\mathbb{L})$. On a le résultat suivant :

$$\widehat{\mathrm{H}}^k(C_p, C(\mathbb{L})) = \begin{cases} \mathbb{F}_p & \text{pour } k \text{ pair} \\ 0 & \text{pour } k \text{ impair} \end{cases}$$

On a un isomorphisme $\widehat{\mathrm{H}}^0(C_p, C(\mathbb{L})) \to C_p = \mathbb{F}_p$ qui induit une surjection de $\widehat{\mathrm{H}}^0(C_p, \mathcal{O}^*_{\mathbb{L},w})$ sur $\widehat{\mathrm{H}}^0(C_p, C(\mathbb{L}))$ pour un certain w ramifié. On a le résultat suivant : l'application $\widehat{\mathrm{H}}^0(C_p, U_{\mathbb{L}}/\mathcal{O}^*_{\mathbb{L}}) \to \widehat{\mathrm{H}}^0(C_p, C(\mathbb{L}))$ est une surjection, si $s > 0$.

On a le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow & & \downarrow & & \downarrow & \\
\cdots \longrightarrow & \widehat{\mathrm{H}}^0(C_p, \mathcal{O}^*_{\mathbb{L}}) & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, \mathbb{L}^*) & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, P(\mathbb{L})) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \downarrow & \\
\cdots \longrightarrow & \widehat{\mathrm{H}}^0(C_p, U_{\mathbb{L}}) = \mathbb{F}_p^s & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, \mathbb{I}_{\mathbb{L}}) & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, I(\mathbb{L})) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \downarrow & \\
\cdots \longrightarrow & \widehat{\mathrm{H}}^0(C_p, U_{\mathbb{L}}/\mathcal{O}^*_{\mathbb{L}}) & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, C(\mathbb{L})) = \mathbb{F}_p & \longrightarrow & \widehat{\mathrm{H}}^0(C_p, Cl(\mathbb{L})) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & \vdots & & \vdots & & \vdots &
\end{array}$$

D'après la remarque faite avant le diagramme, la dernière ligne de ce dernier est une suite exacte longue :

$$\cdots \longrightarrow \widehat{\mathrm{H}}^0(C_p, U_{\mathbb{L}}/\mathcal{O}^*_{\mathbb{L}}) \longrightarrow \widehat{\mathrm{H}}^0(C_p, C(\mathbb{L})) \xrightarrow{0} \widehat{\mathrm{H}}^0(C_p, Cl(\mathbb{L})) \longrightarrow \widehat{\mathrm{H}}^1(C_p, U_{\mathbb{L}}/\mathcal{O}^*_{\mathbb{L}}) \longrightarrow 0 = \widehat{\mathrm{H}}^0(C_p, C(\mathbb{L}))$$

On a donc

$$\widehat{\mathrm{H}}^0(C_p,Cl(\mathbb{L})) = \widehat{\mathrm{H}}^1(C_p,U_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}^*)$$

D'un autre coté la colonne de gauche donne la suite exacte suivante :

$$\widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) \to \widehat{\mathrm{H}}^1(C_p,U_{\mathbb{L}}) = \mathbb{F}_p^{s_0} \to \widehat{\mathrm{H}}^1(C_p,U_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}^*)$$

On en déduit que

$$\begin{aligned} s_0 &\leqslant \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,U_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}^*) \\ &\leqslant \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^0(C_p,Cl(\mathbb{L})) \end{aligned}$$

Soit μ^* le groupe de torsion de $\mathcal{O}_{\mathbb{L}}^*$ (c'est à dire le groupe des racines de l'unité dans $\mathbb{L}$). μ^* est cyclique et donc $\dim_{\mathbb{F}_p} \mu^* \leqslant 1$. Comme on a la suite exacte : $\widehat{\mathrm{H}}^1(C_p,\mu^*) \to \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) \to \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*/\mu^*)$, on a que $\dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) \leqslant 1 + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*/\mu^*)$. On se rappel que comme C_p est cyclique on a $\widehat{\mathrm{H}}^k = \widehat{\mathrm{H}}^{k+2}$. De la on a :

$$\begin{aligned} s_0 &\leqslant \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^0(C_p,Cl(\mathbb{L})) \\ &\leqslant 1 + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*/\mu^*) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^0(C_p,Cl(\mathbb{L})) \\ &\leqslant 1 + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathcal{O}_{\mathbb{L}}^*/\mu^*) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^2(C_p,Cl(\mathbb{L})) \text{ donc avec les notations de l'énoncé} \\ s_0 &\leqslant 1 + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^1(C_p,\mathrm{H}_{free}(\mathbb{L})) + \dim_{\mathbb{F}_p} \widehat{\mathrm{H}}^0(C_p,\mathrm{H}_{tor}(\mathbb{L})) \end{aligned}$$

Bibliographie

[eAD79] R. et A. Douady, *Algèbre et théories galoisiennes*, vol. 2/théories galoisiennes, CEDIC / Fernand Nathan, 1979.

[God71] Claude Godbillon, *éléments de topologie algébrique*, Herman, 1971.

[Kra00] Alain Kraus, *Corps locaux et applications*, cours accéléré de dea, université de Paris VI, septembre 2000.

[Lan86] Serge Lang, *Algebraic number theory*, Springer Verlag, 1986.

[Mil97] J. S. Milne, *Class field theory*, course note, university of Michigan, www.math.lsa.umich.edu/ jsmilne, Winter 1997, Math 776.

[Pau01] Frédéric Paulin, *Topologie algébrique élémentaire*, cours de magistère, École Normale Superieure, http://www.dma.ens.fr/edition/NotesCours/, 2001.

[Rez00] A. Reznikov, *Embedded incompressible surfaces and homology of ramified coverings of three-manifolds*, Selecta Math, 2000.

[Sam71] P. Samuel, *Théorie algébrique des nombres*, deuxième ed., Hermann, 1971.

[Ser80] Jean-Pierre Serre, *Corps locaux*, troisième ed., Hermann, 1980.

[Sik01] Adam S. Sikora, *Analogies between group action on 3-manifolds and number fields*, 2001, www.arvix.org/math.gt/0107210.