Pierre Dèbes

ARITHMÉTIQUE DES REVÊTEMENTS DE LA DROITE

Pierre Dèbes
Laboratoire Paul Painlevé, Université Lille 1,
59655 Villeneuve d'Ascq CEDEX, France.
E-mail : Pierre.Debes@univ-lille1.fr
Url : http://math.univ-lille1.fr/~pde/

ARITHMÉTIQUE DES REVÊTEMENTS DE LA DROITE

Pierre Dèbes

TABLE DES MATIÈRES

PREFACE

Ce document, en chantier, est consacré à l'arithmétique des revêtements de la droite projective avec le problème inverse de la théorie de Galois comme fil conducteur.

Il est conçu pour être de niveau intermédiaire entre les mathématiques classiques, telles qu'enseignées en France jusqu'au niveau "Bac + 4", et les mathématiques plus avancées utilisées pour la recherche. Il s'adresse par exemple aux étudiants souhaitant s'engager dans un doctorat dans une direction algébrique ainsi qu'à ceux qui préparent l'Agrégation.

Les revêtements de la droite projective peuvent être considérés sous de multiples points de vue. Ils correspondent ainsi à la donnée d'une fonction analytique algébrique, ou bien, d'une fonction méromophe sur une surface de Riemann compacte, ou bien d'une courbe algébrique et d'une fonction rationnelle, ou bien d'une extension algébrique de $k(T)$, ou bien d'une représentation d'un groupe fondamental, ou bien d'un uplet de permutations d'un groupe symétrique S_n, ou bien d'un point d'un espace de modules. Plus concrètement, c'est aussi la donnée d'un polynôme $P(T, Y)$ où T est vu comme paramètre et Y comme indéterminée.

Notre premier but sera de donner une présentation aussi complète et cohérente que possible de tous ces aspects et de leurs liens. Les techniques utilisées varieront, relevant de l'arithmétique des corps, la géométrie algébrique, la théorie des nombres, la topologie et l'analyse complexe, etc. Pour chacun de ces domaines, cela nous fournira l'occasion d'approfondir le bagage classique et d'introduire plusieurs thèmes de recherche actuels, comme la théorie inverse de Galois, l'arithmétique des espaces de modules et quelques autres problèmes de géométrie diophantienne.

Ce document est divisé en chapitres qui se répartissent en plusieurs parties.

L'aspect arithmétique que nous mettons en avant est développé dans une première partie correspondant aux chapitres 3 et 4 : les revêtements y sont vus

comme des extensions algébriques finies de $k(T)$. C'est la voie la plus directe vers le problème inverse de Galois sous sa forme géométrique, qui consiste à montrer que tout groupe fini est le groupe de Galois d'une extension finie de $\mathbb{Q}(T)$, régulière sur $\mathbb{Q}$. Les objets sont présentés et étudiés au chapitre 3 où nous introduisons aussi le groupe fondamental algébrique et faisons le lien avec le point de vue des revêtements de la géométrie algébrique. Dans le chapitre 4, nous donnons quelques éléments de base pour le "problème inverse", notamment la théorie de la rigidité (moyennant le théorème d'existence de Riemann qui sera vu plus tard). Cette partie correspond à un cours de Master 2ème année que j'ai donné à l'université de Lille en 2007/2008.

La seconde partie s'intéresse aux "spécialisations" des revêtements. Si on voit un revêtement comme un polynôme irréductible $P(T, Y)$, il s'agit de comprendre le lien entre sa structure arithmétique et galoisienne et celle des polynômes spécialisés $P(t, Y)$ où t est dans le corps de base k. Le résultat phare dans cette direction est le théorème d'irréductibilité de Hilbert selon lequel si $k = \mathbb{Q}$, ou plus généralement si k est hilbertien, il existe une infinité de $t \in k$ pour lesquels $P(t, Y)$ est irréductible et a même groupe de Galois sur k que $P(T, Y)$ sur $k(T)$. On voit l'intérêt pour la théorie inverse de Galois : il suffit de réaliser un groupe donné comme groupe de Galois sur $\mathbb{Q}(T)$ pour pouvoir le réaliser sur $\mathbb{Q}$. Le chapitre 5 étudie en toute généralité la propriété de spécialisation de Hilbert ainsi que plusieurs applications. Au chapitre 6, on s'intéresse, dans le cas où k est le corps $\mathbb{Q}$ ou un corps de nombres, aux parties hilbertiennes, c'est-à-dire, aux ensembles des "bonnes" spécialisations pour un ou plusieurs polynômes $P(T, Y)$ donnés. Ces deux chapitres constituent une deuxième partie qui correspond à un cours de DEA que j'ai donné à l'université de Pondichery en 1997 et à l'université de Lille en 2000/2001.

La troisième partie qui comprend les chapitres 7 et 8 est topologique et analytique. Le but est d'expliquer que les revêtements topologiques de la droite projective complexe $\mathbb{P}^1(\mathbb{C})$ — la sphère de Riemann — privée d'un nombre fini $\{t_1, \ldots, t_r\}$ de points ont une structure algébrique, c'est-à-dire, peuvent être définis à partir d'un polynôme $P(T, Y) \in \mathbb{C}[T, Y]$; c'est ce qu'on appelle le théorème d'existence de Riemann. On comprend là aussi l'intérêt pour le problème inverse de Galois : pour réaliser un groupe comme groupe de Galois d'une extension de $\mathbb{C}(T)$, il suffit de le réaliser topologiquement, c'est-à-dire, comme groupe d'automorphismes d'un revêtement topologique de $\mathbb{P}^1(\mathbb{C})\backslash\{t_1, \ldots, t_r\}$. Or le chapitre 7, qui est consacré à la théorie du groupe fondamental et des revêtements topologiques, montrera que c'est toujours possible dès que r est assez grand. L'équivalence "topologique-algébrique" est établie au chapitre 8 *via* un passage dans le monde analytique complexe des surfaces de Riemann. La pièce manquante pour résoudre le problème inverse est de comprendre dans quelle mesure les revêtements algébrique complexes que l'on sait construire peuvent être définis sur $\mathbb{Q}$, c'est-à-dire, par un polynôme

$P(T, Y) \in \mathbb{Q}[T, Y]$. La théorie de la rigidité vue au chapitre 4 est une première réponse, incomplète. On termine ce document par une introduction aux espaces de modules et à leur utilisation qui constituent une voie plus générale, donnant plus de résultats mais est elle aussi encore incomplète. Cette partie correspond à un cours de DEA donné à l'université de Lille en 1994/1995.

Le document commence par un prélude algébrique (chapitre 1) où nous avons regroupé un certain nombre de thèmes et d'outils importants pour la suite et pour d'autres domaines en algèbre et géométrie, mais qui pourraient manquer dans la formation du lecteur. Sont couvertes notamment la théorie des anneaux de Dedekind et des anneaux de valuation discrète, la théorie des extensions algébriques, des extensions intégrales, la théorie des extensions résiduelles et de la spécialisation, la théorie de la ramification, ainsi qu'une introduction à la géométrie algébrique (topologie de Zariski, Nullstellensatz, etc.). Suit un chapitre d'introduction aux thèmes développés dans la suite (chapitre 2). L'objectif est de faire un tour d'horizon du sujet avant de rentrer dans les détails de chaque partie. Le problème inverse de Galois sert de fil conducteur. On explique comment grâce au théorème d'irréductibilité de Hilbert, dont on prouve une première forme, on peut se ramener à l'étude de la forme géométrique du problème en termes de revêtements. On définit notamment la notion d'extension $E/k(T)$ régulière sur k, l'équivalent en termes de corps des revêtements. On introduit enfin le théorème d'existence de Riemann et la stratégie générale qu'il permet d'adopter. Ces deux premiers chapitres peuvent servir de base à un cours d'Algèbre approfondie.

CHAPITRE 1

PRÉLUDE ALGÉBRIQUE

1.1. Anneaux, idéaux : généralités

Convention 1.1.1. — Le mot "anneau" signifie "anneau commutatif". Un anneau intègre contient au moins les deux éléments distincts 0 et 1. En conséquence, un idéal premier d'un anneau A est distinct de A et l'idéal nul est le seul idéal premier d'un corps ; il est aussi maximal.

1.1.1. Anneaux locaux. —

1.1.1.1. Anneaux de fractions. — Soient A un anneau intègre, de corps des fractions K et S une partie multiplicative, c'est-à-dire, stable pour la multiplication, contenant 1 et ne contenant pas 0. L'ensemble des éléments de la forme x/s où $x \in A$ et $s \in S$ est un anneau que l'on note $S^{-1}A$. La correspondance $i_S : x \to x/1$ définit un morphisme d'anneau injectif (on a supposé A intègre), ce qui permet d'identifier A à un sous-anneau de $S^{-1}A$. Rappelons l'énoncé suivant qui décrit les idéaux de $S^{-1}A$.

Proposition 1.1.1. — *Soit S une partie multiplicative d'un anneau intègre A. Si I est un idéal de A, l'ensemble $S^{-1}I = \{i/s \,|\, i \in I, s \in S\}$ est un idéal de $S^{-1}A$, l'idéal engendré par $i_S(I)$. La correspondance $I \to S^{-1}I$ induit une bijection de l'ensemble ordonné, noté $\mathcal{I}d^*(A)$, des idéaux de A vérifiant la condition (*) $sa \in I, s \in S, a \in A \Rightarrow a \in I$, sur l'ensemble ordonné, noté $\mathcal{I}d(S^{-1}A)$, des idéaux de $S^{-1}A$. Cette bijection envoie l'ensemble des idéaux premiers de A tels que $I \cap S = \emptyset$ sur l'ensemble des idéaux premiers de $S^{-1}A$. La bijection réciproque est définie par la correspondance $I' \to I' \cap A$.*

Démonstration. — On vérifie que si $\mathcal{I} \in \mathcal{I}d(S^{-1}A)$, alors $\mathcal{I} \cap A \in \mathcal{I}d^*(A)$ (pour la condition (*), écrire $a = (sa) \cdot 1/s$).

Montrer ensuite que les deux correspondances sont récriproques l'une de l'autre revient à vérifier que
- pour $\mathcal{I} \in \mathcal{I}d(S^{-1}A)$, on a $S^{-1}(\mathcal{I} \cap A) = \mathcal{I}$, et
- pour $I \in \mathcal{I}d^*(A)$, on a $S^{-1}I \cap A = I$.

Pour l'inclusion $S^{-1}(\mathcal{I} \cap A) \supset \mathcal{I}$, voir que si $i/s \in \mathcal{I}$ ($i \in A$, $s \in S$), alors $i = s \cdot i/s \in \mathcal{I} \cap A$ et donc $i/s \in S^{-1}(\mathcal{I} \cap A)$. Pour l'inclusion $S^{-1}I \cap A \subset I$, voir que si $i/s = a \in A$ avec $i \in I$, $s \in S$, alors $sa \in I$ et la condition (*) entraîne que $a \in I$. Les autres inclusions sont faciles.

Enfin on vérifie sans peine que ces correspondances échangent les idéaux premiers de A et ceux de $S^{-1}A$ et que, pour I idéal premier de A, la condition (*) équivaut à $I \cap S = \emptyset$. □

Exemple 1.1.2. — Si A est un anneau et $f \in A$ un élément non nilpotent, l'ensemble des puissances entières f^n de f est une partie multiplicative. Nous noterons A_{f^∞} l'anneau de fractions correspondant. Par exemple, si $A = \mathbb{Z}$ et $f = 10$, A_{f^∞} est l'ensemble des nombres décimaux. D'après la proposition 1.1.1, les idéaux premiers de A_{f^∞} correspondent aux idéaux premiers de A ne contenant pas f ; par exemple les idéaux premiers de $\mathbb{Z}_{10^\infty}$ sont de la forme $p\mathbb{Z}_{10^\infty}$ avec $p \neq 2, 5$.

1.1.1.2. Anneaux locaux et anneaux localisés. —

Proposition 1.1.3. — *Soit A un anneau. Les conditions suivantes sont équivalentes :*
(i) *A ne possède qu'un idéal maximal $\mathcal{M}$.*
(ii) *Le complémentaire dans A de l'ensemble $A^\times$ des éléments inversibles de A est un idéal de A.*

Un anneau satisfaisant ces conditions est appelé anneau local. L'ensemble des inversibles est le complémentaire de l'unique idéal maximal de A.

Démonstration. — (i) ⇒ (ii). Montrons que le complémentaire de $A^\times$ est l'idéal $\mathcal{M}$. Si $x \in \mathcal{M}$ alors $x \notin A^\times$. Réciproquement, si $x \notin \mathcal{M}$, alors x n'appartient à aucun idéal maximal de A. D'où $Ax = A$ puisque d'après le lemme de Zorn, tout idéal propre peut être inclus dans un idéal maximal. L'égalité $Ax = A$ entraîne que $x \in A^\times$.

(ii) ⇒ (i). Le complémentaire I de $A^\times$ est un sous-ensemble propre de A ($1 \notin I$) qui contient nécessairement tout idéal propre $\mathcal{P}$ de A (car $\mathcal{P} \not\subset I \Rightarrow \mathcal{P} \cap A^\times \neq \emptyset \Rightarrow \mathcal{P} = A$). Si I est un idéal, il est donc nécessairement le plus grand idéal propre de A, et en particulier le seul idéal maximal de A. □

Les *localisés* d'anneaux sont des exemples fondamentaux d'anneaux locaux. Etant donné un anneau intègre A et $\mathfrak{p}$ un idéal premier de A, l'ensemble $S = A \setminus \mathfrak{p}$ est une partie multiplicative. L'anneau $S^{-1}A$ est un anneau local, qu'on note $A_\mathfrak{p}$: en effet, les inversibles de cet anneau sont les éléments de $S^{-1}S$ dont le complémentaire $S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ est un idéal, l'unique idéal maximal de A. Les idéaux premiers de $A_\mathfrak{p}$ correspondent aux idéaux premiers de A contenus dans $\mathfrak{p}$.

1.1.1.3. Anneaux locaux réguliers. — La définition suivante interviendra dans la définition de non-singularité d'un point sur une variété algébrique.

Définition 1.1.4. — Un anneau local noethérien A d'idéal maximal $\mathcal{M}$ et de corps des fractions K est dit régulier si $\mathcal{M}/\mathcal{M}^2$ est un K-espace vectoriel de dimension $\dim(A)$.

1.1.1.4. Lemme de Nakayama. — Soit A un anneau local d'idéal maximal $\mathcal{M}$. Si V est un A-module, $\mathcal{M}V$ est un sous A-module de V et $V/\mathcal{M}V$ est un $A/\mathcal{M}$-espace vectoriel.

***Lemme 1.1.5* (Lemme de Nakayama)**. — *On suppose que le A-module V est de type fini. Soient $v_1, \ldots, v_n$ des éléments de V dont les classes modulo $\mathcal{M}V$ engendrent le $A/\mathcal{M}$-espace vectoriel $V/\mathcal{M}V$. Alors $v_1, \ldots, v_n$ engendrent le A-module V.*

Démonstration. — Soient $t_1, \ldots, t_p \in V$ tels que $V = \langle v_1, \ldots, v_n, t_1, \ldots, t_p \rangle$. Par hypothèse, il existe $c_1, \ldots, c_n$ tels que $t_p - (c_1 v_1 + \cdots + c_n v_n)$ est dans $\mathcal{M}V$ et donc s'écrit comme combinaison linéaire de $v_1, \ldots, v_n, t_1, \ldots, t_p$. Grâce au fait que $m \in \mathcal{M} \Rightarrow 1 - m \in A^\times$, on en déduit que $t_p \in \langle v_1, \ldots, v_n, t_1, \ldots, t_{p-1} \rangle$. Le même argument appliqué ensuite successivement à $t_{p-1}, \ldots, t_1$ conduit à la conclusion souhaitée. □

1.1.2. Quelques résultats classiques utiles. —

1.1.2.1. Lemme chinois. —

***Lemme 1.1.6* (lemme chinois)**. — *Soient A un anneau et $I_1, \ldots, I_\ell$ des idéaux de A tels que $I_i + I_j = A$ pour $i \neq j$, par exemple des idéaux maximaux deux à deux distincts. Alors on a $I_1 \cap \ldots \cap I_\ell = I_1 \cdots I_\ell$ et il y a un isomorphisme canonique entre $A/I_1 \cdots I_\ell$ et $A/I_1 \times \cdots A/I_\ell$. En particulier le morphisme naturel $A \to A/I_1 \times \cdots A/I_\ell$ est surjectif.*

Démonstration. — Le cas $\ell = 1$ est banal ; supposons $\ell \geq 2$.

On observe d'abord que $I_1+(I_2\dots I_\ell)=A$. En effet, par hypothèse, il existe $c_i\in I_1$ et $j_i\in I_i$ tels que $c_i+j_i=1$, $i=2,\dots,n$. En multipliant membre à membre ces inégalités, on obtient $c+j_2\cdots j_\ell=1$ avec $c\in I_1$.

On en déduit $I_1\cap(I_2\dots I_\ell)=I_1I_2\cdots I_\ell$. L'inclusion "$\supset$" est imédiate et l'inclusion inverse résulte de l'écriture $x=cx+(j_2\cdots j_\ell)x$, valable pour tout $x\in I_1\cap(I_2\dots I_\ell)$.

L'égalité $I_1\cap\ldots\cap I_\ell=I_1\cdots I_\ell$ s'obtient ensuite aisément par récurrence.

On a un morphisme canonique $A/\bigcap_{i=1}^{\ell}I_i\ \to\ A/I_1\times\cdots A/I_\ell$ et il est évidemment injectif. Reste à montrer que tout élément $(x_1,\dots,x_\ell)$ de l'anneau d'arrivée est dans l'image. Par linéarité, on peut se ramener au cas où toutes les composantes sauf une sont nulles et donc à un changement d'indexation près au cas où $x_2=\cdots=x_\ell=0$. Mais d'après le premier point établi, il existe $x\in(I_2\dots I_\ell)$ tel que x soit dans la classe de x_1 modulo I_1 ; cet élément x est l'antécédent de $(x_1,0,\dots,0)$ cherché. □

Une conséquence utile est l'énoncé suivant qu'on appelle parfois le lemme d'*évitement des idéaux maximaux*.

Corollaire 1.1.7. — *Soient A un anneau et $I_1,\dots,I_\ell$ des idéaux maximaux de A tels que I_1 est distinct de $I_2,\dots,I_\ell$. Alors pour tout $\alpha\in A$*
(a) *il existe $a\in A$ tel que $a-\alpha\in I_1$ et $a\notin I_j$, $j=1,\dots,\ell$,*
(b) *il existe $a\in A$ tel que $a-\alpha\notin I_1$ et $a\in I_j$, $j=1,\dots,\ell$.*

Démonstration. — Les énoncés (a) et (b) se déduisent facilement du lemme chinois appliqué à l'ensemble des idéaux maximaux de A constitué de I_1 et de représentants distincts de l'ensemble $\{I_2,\dots,I_\ell\}$. □

1.1.2.2. Idéaux maximaux d'un anneau $A[Y]/\langle f\rangle$ avec A local. — Soient A un anneau et $f\in A[Y]$ un polynôme unitaire de degré $d\geq 1$. On note B_f l'anneau quotient $B_f=A[Y]/\langle f\rangle$. C'est une A-algèbre libre de rang d sur A. On s'intéresse aux idéaux maximaux de B_f. Si A est un corps, il résulte classiquement de la principalité de $A[Y]$ que les idéaux maximaux de B_f correspondent aux facteurs irréductibles distincts de f dans $A[Y]$.

On se place dans ce paragraphe dans la situation où A un anneau local. On note $\mathcal{M}$ son idéal maximal $\mathcal{M}$ et k son corps résiduel. On pose $\overline{B_f}=B_f/\mathcal{M}B_f$. Si $\overline{f}$ désigne l'image de f par réduction modulo $\mathcal{M}$, on a

$$\overline{B_f}=A[Y]/\langle\mathcal{M},f\rangle=k[Y]/\langle\overline{f}\rangle$$

Soient $\overline{f} = \prod_{i=1}^{r} \varphi_i^{e_i}$ la factorisation en irréductibles de f dans l'anneau $k[Y]$ et, pour $i = 1, \ldots, r$, $g_i \in A[Y]$ un polynôme tel que $\overline{g_i} = \varphi_i$ et $\mathcal{M}_i = \langle \mathcal{M}, g_i \rangle$ l'idéal de B_f engendré par $\mathcal{M}$ et la classe de g_i modulo $\langle f \rangle$.

Lemme 1.1.8. — *Les idéaux $\mathcal{M}_1, \ldots, \mathcal{M}_r$ sont les idéaux maximaux de B_f.*

Démonstration. — Il découle de l'isomorphisme $B_f/\mathcal{M}_i \simeq k[Y]/\langle \varphi_i \rangle$ que $\mathcal{M}_i$ est un idéal maximal, $i = 1, \ldots, r$. Inversement soit $M \subset B_f$ un idéal maximal. On a $\mathcal{M} \subset M$ car sinon on aurait $M + \mathcal{M}B_f = B_f$, ce qui conduirait en utilisant le lemme de Nakayama (lemme 1.1.5 ; B_f est un A-module de type fini) à $M = B_f$. Si $\rho : B_f \to \overline{B_f}$ désigne le morphisme de réduction modulo $\mathcal{M}$, il découle de $\mathcal{M} \subset M$ que $M = \rho^{-1}(\rho(M))$ et que $\rho(M)$ est un idéal maximal de $\overline{B_f}$, c'est-à-dire, comme nous l'avons rappelé en préambule de ce paragraphe, un des idéaux $\langle \varphi_i \rangle \subset k[Y]$, $i = 1, \ldots, r$. Pour l'indice i en question, on a bien $M = \rho^{-1}(\langle \varphi_i \rangle) = \langle \mathcal{M}, g_i \rangle = \mathcal{M}_i$. □

1.1.2.3. Radical d'un idéal. —

Définition 1.1.9. — Si I est un idéal d'un anneau A, on appelle radical de I l'idéal noté $\sqrt{I}$ intersection des idéaux premiers de A qui contiennent I.

Proposition 1.1.10. — *L'idéal $\sqrt{I}$ est l'ensemble des éléments $x \in A$ pour lesquels il existe $n \in \mathbb{N}$ tel que $x^n \in I$.*

Pour l'idéal nul $I = \{0\}$, le radical $\sqrt{0}$ est appelé nilradical de A. D'après la caractérisation ci-dessus, c'est l'ensemble des éléments nilpotents de A.

Démonstration. — Si $x \in A$ est tel que $x^n \in I$ ($n \in \mathbb{N}$), alors pour tout idéal premier $\mathcal{P} \supset I$, on a $x \in \mathcal{P}$. Cela prouve une des deux inclusions souhaitées. Inversement, soit $x \in \sqrt{I}$ et supposons que $x^n \notin I$ pour tout $n \in \mathbb{N}$. L'ensemble $\mathcal{F}_x$ des idéaux J de A contenant I et tels qu'aucune puissance de x ne soit dans J est donc non vide. Cet ensemble étant inductif, il existe, par le lemme de Zorn, un élément maximal P. Montrons que P est premier, ce qui fournira une contradiction, puisque $x \notin P$. Soient $a, b \in A \setminus P$. Par la maximalité de P, les idéaux $P + (a)$ et $P + (b)$ n'appartiennent pas à $\mathcal{F}_x$. Ainsi il existe $m, n \in \mathbb{N}$ tels que $x^m \in P + (a)$ et $x^n \in P + (b)$. Mais alors $x^{m+n} \in (P + (a))(P + (b)) \subset P + (ab)$, ce qui prouve comme désiré que $ab \notin P$. □

1.1.2.4. Une propriété des anneaux noethériens. —

Théorème 1.1.11. — *Soit A un anneau noethérien et I un idéal propre tel que $\sqrt{I} = I$. Alors il existe un nombre fini d'idéaux premiers $J_1, \ldots, J_n$ de A*

tels que $I = J_1 \cap \cdots \cap J_n$. Si on impose de plus aux idéaux J_i de vérifier $J_i \not\subset J_j$, $i \neq j$, une telle décomposition de I est unique à l'ordre près des facteurs.

En termes géométriques, cet énoncé correspond à l'écriture de tout ensemble fermé comme réunion de composantes irréductibles.

Démonstration. — Supposons que l'ensemble $\mathcal{F}$ des idéaux J de A tels que $J \neq A$, $\sqrt{J} = J$ et J n'est pas intersection finie d'idéaux premiers, est non vide. L'anneau A étant supposé noethérien, l'ensemble $\mathcal{F}$ possède un élément maximal I. Comme $I \in \mathcal{F}$, I n'est pas premier : il existe donc $a, b \in A \setminus I$ tel que $ab \in I$.

Considérons les idéaux $\sqrt{Aa + I}$ et $\sqrt{Ab + I}$. Ce sont des idéaux propres de A : en effet, si par exemple $1 \in \sqrt{Aa + I}$, il existerait $\omega \in A$ et $i \in I$ tels que $1 = \omega a + i$, ce qui donnerait $b = \omega ab + ib \in I$. On a ensuite les inclusions suivantes

$$\begin{cases} I \subsetneq Aa + I \subset \sqrt{Aa + I} = \sqrt{\sqrt{Aa + I}} \\ I \subsetneq Ab + I \subset \sqrt{Ab + I} = \sqrt{\sqrt{Ab + I}} \end{cases}$$

qui permettent de conclure que les idéaux $\sqrt{Aa + I}$ et $\sqrt{Ab + I}$ ne sont pas dans $\mathcal{F}$, et qu'il existe des idéaux premiers $\mathcal{P}_1, \ldots, \mathcal{P}_s$ et $\mathcal{Q}_1, \ldots, \mathcal{Q}_t$ tels que

$$\begin{cases} \sqrt{Aa + I} = \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_s \\ \sqrt{Ab + I} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_t \end{cases}$$

Montrons que $I = \sqrt{Aa + I} \cap \sqrt{Ab + I}$; cela fournira la contradiction cherchée. L'inclusion "$\subset$" est claire. Inversement soit $x \in \sqrt{Aa + I} \cap \sqrt{Ab + I}$: il existe des entiers $m, n \geq 1$ tel que $x^m \in Aa + I$ et $x^n \in Ab + I$. On en déduit $x^{m+n} \in (Aa + I)(Ab + I) \subset Aab + I \subset I$. D'où $x \in I$ puisque $I = \sqrt{I}$.

L'unicité de la décomposition découle du fait suivant : un idéal premier intervenant dans une décomposition de I contient l'intersection et donc le produit de tous les idéaux premiers de toute autre décomposition ; il en contient donc nécessairement l'un des facteurs. □

Corollaire 1.1.12. — *Soit A un anneau noethérien qui n'est pas un corps et $I \subset A$ un idéal non nul. Alors il existe un nombre fini d'idéaux premiers non nuls $I_1, \ldots, I_n$ de A tels que $I \supset I_1 \cdots I_n$.*

Démonstration. — Si $I = A$, l'énoncé est vrai car A n'étant pas un corps contient un idéal non nul, lequel est contenu dans un idéal maximal.

Supposons $I \neq A$. Alors $\sqrt{I} \neq A$ et $\sqrt{\sqrt{I}} = \sqrt{I}$. D'après le théorème 1.1.11, on peut écrire $\sqrt{I} = J_1 \cap \cdots \cap J_n$ avec $J_1, \ldots, J_n$ idéaux premiers de

A. En particulier, $J_1 \cdots J_n \subset \sqrt{I}$. Mais d'autre part, en utilisant que A est noethérien, on montre qu'il existe N tel que $\sqrt{I}^N \subset I$: si $\{x_1, \ldots, x_m\}$ est un système générateur de l'idéal $\sqrt{I}$ et n un entier tel que $x_i^n \in I$, $i = 1, \ldots, m$, on peut prendre $N = nm$. On obtient $(J_1 \cdots J_n)^N \subset I$ et par construction aucun des idéaux $J_1, \ldots, J_n$ n'est nul (puisque $\sqrt{I} \supset I$ n'est pas nul). □

1.1.3. Intégralité. —

Proposition 1.1.13. — *Soient A un sous-anneau d'un anneau B et $x \in B$. Les conditions suivantes sont équivalentes :*
(i) *Il existe $a_1, \ldots, a_n \in A$ tels que $x^n + a_1 x^{n-1} + \cdots + a_n = 0$,*
(ii) *Le sous-anneau $A[x]$ de B est un A-module de type fini,*
(iii) *Il existe un sous-anneau C de B tel que $A[x] \subset C$ et C est un A-module de type fini.*
Un élément $x \in B$ satisfaisant ces conditions est dit entier sur A et l'équation dans (i) *une équation de dépendance intégrale satisfaite par x.*

Démonstration. — (i) ⇒ (ii). Par (i), on obtient que toute puissance x^r ($r \in \mathbb{N}$) s'écrit comme combinaison A-linéaire de $x, \ldots, x^{n-1}$, ce qui donne (ii).

(ii) ⇒ (iii). Prendre $C = A[x]$.

(iii) ⇒ (i). Par hypothèse, le A-module C possède un système générateur fini $\mathbf{y} = (y_1, \ldots, y_n)$. Pour $i = 1, \ldots, n$, $xy_i \in C$. Il existe donc une matrice $M \in M_{n\times n}(A)$ tel que $(x\mathrm{Id} - M)^t\mathbf{y} = 0$. Les formules de Cramer conduisent alors à $\det(x\mathrm{Id} - M)y_j = 0, j = 1, \ldots, n$, ce qui donne, en posant $d = \det(x\mathrm{Id} - M)$, l'égalité $dC = 0$ et donc $d = 0$. En développant le déterminant, on obtient une équation de dépendance intégrale pour x. □

L'énoncé suivant se démontre aisément par récurrence.

Corollaire 1.1.14. — *Soient A un sous-anneau d'un anneau B et $x_1, \ldots, x_n \in B$. On suppose x_i entier sur $A[x_1, \ldots, x_{i-1}]$, $i = 1, \ldots, n$ (par exemple $x_1, \ldots, x_n$ entiers sur A). Alors $A[x_1, \ldots, x_d]$ est un A-module de type fini.*

Corollaire 1.1.15. — *Soit A un sous-anneau d'un anneau B. L'ensemble A' des éléments de B entiers sur A est un sous-anneau de B qui contient A.*

Démonstration. — Pour tous $x, y \in B$, l'anneau $A[x, y]$ est un A-module de type fini (corollaire 1.1.14). Donc $x \pm y$, xy sont dans A'. Il est clair que $A \subset A'$. □

Définition 1.1.16. — L'anneau A' défini ci-dessus s'appelle fermeture ou clôture intégrale de A dans B. Si $A' = B$, on dit que B est entier sur A. Si

$A' = A$, on dit que A est intégralement fermé dans B. Un anneau A intègre est dit intégralement clos si A est intégralement fermé dans son corps des fractions.

***Proposition 1.1.17* (Transitivité de l'intégralité)**
Soient A et B deux sous-anneaux d'un anneau C tels que $A \subset B$. Si C est entier sur B et B entier sur A, alors C est entier sur A.

Démonstration. — Soient $x \in C$ et $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ une équation de dépendance intégrale pour x sur B. L'anneau $A[b_1, \ldots, b_n, x]$ est un A-module de type fini contenant x. Donc x est entier sur A. □

Remarque 1.1.18. — (a) Si B est un anneau entier sur un sous-anneau A et $\mathcal{P}$ un idéal de B, alors $B/\mathcal{P}$ est entier sur $A/(\mathcal{P} \cap A)$.

(b) La clôture intégrale A' dans B d'un sous-anneau A est intégralement fermée dans B. Si A est intègre, la clôture intégrale A' de A (dans son corps des fractions) est un anneau intégralement clos.

(c) Tout anneau factoriel est intégralement clos (exercice).

Proposition 1.1.19. — *Soient B un anneau intègre, A un sous-anneau de B, A' la fermeture intégrale de A dans B et S une partie multiplicative de A. Alors la fermeture intégrale de $S^{-1}A$ dans $S^{-1}B$ est $S^{-1}A'$.*

Démonstration. — Le sous-anneau $S^{-1}A'$ de $S^{-1}B$ est entier sur $S^{-1}A$ et est donc inclus dans la fermeture intégrale de $S^{-1}A$ dans $S^{-1}B$. Inversement, soit x/s ($x \in B$, $s \in S$) un élément de $S^{-1}B$ entier sur $S^{-1}A$. En chassant les dénominateurs dans une équation de dépendance intégrale pour x/s sur $S^{-1}A$, on obtient que, pour un certain $t \in S$, tx est entier sur A et donc est dans A', ce qui donne bien $x/s \in S^{-1}A'$. □

Corollaire 1.1.20. — *Si A est un anneau intégralement clos, alors tout anneau de fractions $S^{-1}A$ est intégralement clos.*

Le lemme suivant sera utilisé de multiples fois.

Lemme 1.1.21. — *Soit B un anneau entier sur un sous-anneau A.*
(a) *Si B est intègre, alors B est un corps si et seulement si A est un corps.*
(b) *Si $\mathcal{P}$ est un idéal premier de B, alors $\mathcal{P}$ est maximal dans B si et seulement si $\mathcal{P} \cap A$ est un idéal maximal de A.*

Démonstration. — (a) ($\Rightarrow$) : Soit $a \in A$, $a \neq 0$. Alors $a^{-1} \in B$. Par hypothèse, il existe $a_1, \ldots, a_d \in A$ tels que $a^{-d} + a_1 a^{-(d-1)} + \cdots + a_d = 0$. D'où $a^{-1} = -(a_1 + \cdots + a_d a^{d-1}) \in A$ et A est un corps.

($\Leftarrow$) : Soit $b \in B$, $b \neq 0$. Par hypothèse, il existe $a_1, \ldots, a_d \in A$ tels que $b^d + a_1 b^{d-1} + \cdots + a_d = 0$. On peut supposer que $a_d \neq 0$ (grâce à l'hypothèse B intègre). L'identité précédente montre que l'élément $-a_d^{-1}(b^{d-1} + a_1 b^{d-2} \cdots + a_{d-1}) \in B$ est inverse de b dans B.

(b) Le morphisme naturel $A/(\mathcal{P} \cap A) \to B/\mathcal{P}$ est injectif. L'anneau intègre $B/\mathcal{P}$ est entier sur $A/(\mathcal{P} \cap A)$. Il suffit d'appliquer (a) pour conclure. □

1.2. Anneaux de Dedekind et anneaux de valuation discrète

Rappelons qu'étant donné un anneau A, on appelle dimension de A le supremum (éventuellement infini) des longueurs d des chaînes

$$\mathcal{P}_0 \underset{\neq}{\subset} \mathcal{P}_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathcal{P}_d$$

d'idéaux premiers $\mathcal{P}_0, \mathcal{P}_1, \ldots \mathcal{P}_d$ de A.

Un anneau intègre de dimension 0 est un corps. Un anneau intègre de dimension 1 est un anneau qui n'est pas un corps et où tout idéal premier non nul est maximal. La dimension de l'anneau $K[X_1, \ldots, X_n]$ est n. Les anneaux auxquels on s'intéresse dans cette section sont de dimension ≤ 1.

1.2.1. Anneaux de Dedekind. —

Définition 1.2.1. — Un anneau A est appelé anneau de Dedekind s'il est noethérien, intégralement clos (donc intègre) et de dimension ≤ 1 (c'est-à-dire, si tout idéal premier non nul de A est maximal)[(1)].

Définition 1.2.2. — Soient A un anneau intègre et K son corps des fractions. On appelle idéal fractionnaire de A tout sous A-module I de K pour lequel il existe $d \in A$, $d \neq 0$ tel que $I \subset d^{-1}A$. On dit que d est un dénominateur de I.

Tout sous-A-module de type fini de K est un idéal fractionnaire et la réciproque est vraie si A est noethérien. La somme, l'intersection, le produit de deux idéaux fractionnaires sont encore des idéaux fractionnaires. L'ensemble des idéaux fractionnaires non nuls d'un anneau A forment un monoïde commutatif pour la multiplication ; l'idéal fractionnaire A en est un élément neutre.

Lemme 1.2.3. — *Soit A un anneau de Dedekind. Tout idéal premier $\mathfrak{m}$ non nul de A est inversible dans le monoïde des idéaux fractionnaires de A.*

[(1)] Par notre convention 1.1.1, un corps est un anneau de Dedekind.

Démonstration. — Soit $\mathfrak{m}$ un idéal premier non nul de A. Posons $\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subset A\}$. C'est un sous-$A$-module de K et tout élément de $\mathfrak{m}$ en est un dénominateur ; c'est donc un idéal fractionnaire de A. Nous allons montrer que $\mathfrak{m}'\mathfrak{m} = A$. On a évidemment $\mathfrak{m}'\mathfrak{m} \subset A$. D'autre part, comme $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$ (puisque $A \subset \mathfrak{m}'$) et que $\mathfrak{m}$ est maximal, on a $\mathfrak{m}'\mathfrak{m} = A$ ou $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. Reste à montrer que $\mathfrak{m}'\mathfrak{m} \neq \mathfrak{m}$.

Supposons $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. On a alors $\mathfrak{m}' = A$. En effet, si $x \in \mathfrak{m}'$, il découle de $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ que $x^{n+1}\mathfrak{m} \subset x^n\mathfrak{m}$ et donc que $x^n\mathfrak{m} \subset \mathfrak{m}$ pour tout $n \geq 0$. Il en résulte que $A[x]$ est un idéal fractionnaire de K (tout élément de $\mathfrak{m}$ en est un dénominateur) et comme A est noethérien, c'est un A-module de type fini. D'où x est entier sur A et donc $x \in A$ puisque A est intégralement clos. D'où l'inclusion $\mathfrak{m}' \subset A$; l'autre est évidente.

Reste à montrer que $\mathfrak{m}' = A$ est impossible. Soit $a \in \mathfrak{m}$ non nul. D'après le corollaire 1.1.12, l'idéal Aa contient un produit fini $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'idéaux premiers non nuls ; on peut de plus supposer n minimal. De $a \in \mathfrak{m}$ on déduit que $\mathfrak{m}$ contient $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, et donc l'un des idéaux $\mathfrak{p}_i$, disons $\mathfrak{p}_1$. Mais comme $\mathfrak{p}_1$ est maximal, on a en fait $\mathfrak{m} = \mathfrak{p}_1$ et donc $Aa \supset \mathfrak{m}\mathfrak{b}$ avec $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. De plus, par la minimalité de n, $Aa \not\supset \mathfrak{b}$. Ainsi il existe $b \in \mathfrak{b}$ tel que $b \notin Aa$. L'élément b vérifie $\mathfrak{m}b \subset Aa$ et donc $\mathfrak{m}ba^{-1} \subset A$, d'où $ba^{-1} \in \mathfrak{m}'$. Mais de $b \notin Aa$ découle que $ba^{-1} \notin A$. D'où $\mathfrak{m}' \neq A$. □

Théorème 1.2.4. — *Soit A un anneau de Dedekind.*

(a) *Tout idéal fractionnaire non nul $\mathfrak{b}$ de A s'écrit de façon unique sous la forme $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$ où $\mathfrak{p}$ décrit l'ensemble des idéaux premiers non nuls de A et les $n_{\mathfrak{p}}(\mathfrak{b})$ sont des entiers relatifs, tous nuls sauf un nombre fini.*

(b) *Le monoïde des idéaux fractionnaires non nuls de A est un groupe.*

Démonstration. — Pour la partie "existence" du (a), fixons un idéal fractionnaire $\mathfrak{b}$ non nul de A. En écrivant $\mathfrak{b} = \mathfrak{b}\cdot(Ad)\cdot(Ad)^{-1}$ où d est un dénominateur de $\mathfrak{b}$, on se ramène au cas où $\mathfrak{b} \subset A$. Pour $\mathfrak{b} = A$, l'énoncé est vrai : on prend tous les $n_{\mathfrak{p}}(\mathfrak{b})$ égaux à 0. Supposons désormais que $\mathfrak{b} \neq A$ (en particulier A n'est pas un corps) et que la décomposition annoncée n'existe pas pour $\mathfrak{b}$. Faisons même l'hypothèse plus faible qu'elle n'existe pas avec des exposants $n_{\mathfrak{p}}(\mathfrak{b}) \geq 0$; la contradiction fournira une conclusion plus forte que nécessaire mais utile pour la suite (voir remarque 1.2.5). D'après le corollaire 1.1.12, $\mathfrak{b}$ contient un produit fini $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'idéaux premiers non nuls de A. Soit $\mathfrak{m}$ un idéal maximal de A contenant $\mathfrak{b}$; on a donc $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{b} \subset \mathfrak{m}$. Nécessairement $\mathfrak{m}$ contient l'un des idéaux $\mathfrak{p}_1, \ldots \mathfrak{p}_n$, disons $\mathfrak{p}_1$, et comme celui-ci est maximal, on a $\mathfrak{m} = \mathfrak{p}_1$. En multipliant la double inclusion précédente par $\mathfrak{p}_1^{-1}$ (qui

est donné par le lemme 1.2.3), on obtient $\mathfrak{p}_2 \cdots \mathfrak{p}_n \subset \mathfrak{b}\mathfrak{p}_1^{-1} \subset A$. De plus les inclusions sont strictes car sinon on obtient une décomposition pour $\mathfrak{b}$, avec des exposants ≥ 0. On peut alors répéter cet argument jusqu'à obtenir que $\mathfrak{p}_n \subset \mathfrak{b}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_{n-1}^{-1} \subset A$. Mais comme $\mathfrak{p}_n$ est maximal et qu'aucune des deux inclusions ne peut être une égalité, on obtient la contradiction souhaitée.

Pour la partie "unicité", on se ramène aisément à montrer qu'une égalité $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_n^{\beta_n}$ avec $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ idéaux premiers distincts deux à deux, $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ des entiers > 0 et avec n ou m non nul (c'est-à-dire l'une des deux écritures non triviale) n'est pas possible. Supposons le contraire. Alors $\mathfrak{p}_1$ contient $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_n^{\beta_n}$ et donc doit contenir l'un des idéaux $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$, mais ce dernier étant maximal, doit en fait lui être égal, ce qui est contradictoire.

La partie (b) est immédiate. □

Remarque 1.2.5. — La démonstration du théorème 1.2.4 fournit également cette conclusion : pour $\mathfrak{a}$ idéal fractionnaire de A,

(i) $\mathfrak{a} \subset A$ *si et seulement si* $n_\mathfrak{p}(\mathfrak{a}) \geq 0$ *pour tout idéal premier* $\mathfrak{p}$ *non nul.*

En conséquence, si $\mathfrak{b}$ est un deuxième idéal fractionnaire de A, en appliquant (i) à $\mathfrak{a}\mathfrak{b}^{-1}$, on obtient

(ii) $\mathfrak{a} \subset \mathfrak{b}$ *si et seulement si* $n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b})$ *pour tout idéal premier* $\mathfrak{p}$ *non nul.*

Il en découle que les idéaux premiers $\mathfrak{p}$ qui contiennent un idéal entier $\mathfrak{a}$ non nul sont ceux pour lesquels $n_\mathfrak{p}(\mathfrak{a}) > 0$; en particulier ils sont en nombre fini. Une autre conséquence est que pour $x \in A$ et $\mathfrak{p}$ un idéal premier non nul, $n_\mathfrak{p}(xA) \geq n$ si et seulement si $Ax \subset \mathfrak{p}^n$, c'est-à-dire $x \in \mathfrak{p}^n$. D'où

(iii) *pour* $x \in A$, $n_\mathfrak{p}(xA)$ *est le plus grand entier* n *tel que* $x \in \mathfrak{p}^n$. *En particulier,* $x \notin \mathfrak{p}$ *si et seulement si* $n_\mathfrak{p}(xA) = 0$.

On en déduit plus généralement que

(iv) *pour* $x \in K$, *on a* $x \in A_\mathfrak{p}$ *si et seulement si* $n_\mathfrak{p}(xA) \geq 0$, *et dans ce cas* $n_\mathfrak{p}(xA)$ *est le plus grand entier* $n \geq 0$ *tel que* $x \in \mathfrak{p}^n A_\mathfrak{p}$. *En particulier,* $x \in \mathfrak{p}A_\mathfrak{p}$ *si et seulement si* $n_\mathfrak{p}(xA) > 0$.

En effet, si $x \in \mathfrak{p}^n A_\mathfrak{p}$ (pour $n \geq 0$), c'est-à-dire $x = \pi/s$ avec $\pi \in \mathfrak{p}^n$ et $s \notin \mathfrak{p}$, alors $n_\mathfrak{p}(xA) = n_\mathfrak{p}(\pi A) - n_\mathfrak{p}(sA) \geq n - 0$ (d'après (iii)). Inversement, pour $x \in K$, $n_\mathfrak{p}(xA) \geq n$ entraîne qu'il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ distincts de $\mathfrak{p}$ et des entiers $\alpha_1, \ldots, \alpha_m > 0$ tels que $(xA)\,\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m} \subset \mathfrak{p}^n$. On choisit $b_i \in \mathfrak{p}_i^{\alpha_i} \setminus \mathfrak{p}$, $i = 1, \ldots, n$ (prendre $b_i = \beta_i^{\alpha_i}$ avec β_i dans l'ensemble $\mathfrak{p}_i \setminus \mathfrak{p}$ qui est non vide puisque $\mathfrak{p}_i \not\subset \mathfrak{p}$). L'inclusion précédente donne $xb_1 \cdots b_m \in \mathfrak{p}^n$ et donc $x \in \mathfrak{p}^n A_\mathfrak{p}$.

1.2.2. Anneaux de valuation discrète. —

1.2.2.1. Définitions. — Un groupe abélien Γ muni d'une relation $\leq$ est appelé *groupe ordonné* si $\leq$ est une relation d'ordre total compatible avec la loi de groupe de Γ (notée additivement). Etant donné un corps F, une valuation sur F est un homomorphisme $v : (F^\times, \times) \to (\Gamma, +)$ vérifiant $v(x+y) \geq \min(v(x), v(y))$. On convient généralement que $v(0) = \infty$. Le sous-groupe $v(F^\times) \subset \Gamma$ est appelé *groupe des valeurs* de v. L'ensemble $\mathcal{O}_v = \{a \in F \,|\, v(a) \geq 0\}$ est un anneau local appelé *anneau de valuation*; son idéal maximal est $\mathcal{M}_v = \{a \in F \,|\, v(a) > 0\}$ et le groupe des inversibles de $\mathcal{O}_v$ est $\mathcal{O}_v^\times = \{a \in F \,|\, v(a) = 0\}$. Le corps $\mathcal{O}_v/\mathcal{M}_v$ est appelé *corps résiduel* de v.

La valuation v est dite *réelle* si $v(F^\times) \subset \mathbb{R}$ et *discrète* si $v(F^\times)$ est isomorphe à $\mathbb{Z}$; quitte à diviser v par un élément de Γ, on peut alors supposer que $v(F^\times) = \mathbb{Z}$.

Définition 1.2.6. — Un *anneau de valuation discrète* est l'anneau de valuation d'une valuation discrète sur un corps.

Un anneau de valuation discrète $\mathcal{O}_v$ est un anneau local et il est aussi principal : tout élément de valuation minimale d'un idéal donné en est un générateur. Tout élément π de valuation 1 est un générateur de $\mathcal{M}_v$, appelé *uniformisante* de $\mathcal{O}_v$ et les idéaux de $\mathcal{O}_v$ sont les puissances $\mathcal{M}_v^n = \pi^n \mathcal{O}_v$ de $\mathcal{M}_v$ ($n > 0$). L'idéal $\mathcal{M}_v^n$ est l'ensemble des éléments de $\mathcal{O}_v$ de valuation $\geq n$. L'idéal de valuation détermine donc la valuation; en particulier, la valuation discrète v est unique.

Réciproquement, tout anneau A local principal qui n'est pas un corps[(2)] est un anneau de valuation discrète. En effet, si π est un générateur de l'idéal maximal (non nul), les idéaux de A sont les idéaux principaux $A\pi^n$ ($n \geq 0$). Tout élément $x \neq 0$ dans le corps des fractions F de A, s'écrit de façon unique $x = \pi^n u$ avec $n \in \mathbb{Z}$ et u inversible. L'entier n ne dépend pas du choix de π; on le note $v(x)$. On vérifie sans peine que l'application $v : K^\times \to \mathbb{Z}$ définit une valuation discrète sur F pour laquelle $\mathcal{O}_v = A$ et $\mathcal{M}_v = A\pi$.

1.2.2.2. Caractérisation. — On peut affiner la caractérisation précédente.

Théorème 1.2.7. — *Soit A un anneau local noethérien d'idéal maximal $\mathcal{M}$. Les assertions suivantes sont équivalentes :*
(a) *A est un anneau de valuation discrète,*
(b) *A est un anneau local intègre régulier de dimension* 1,

[(2)] Un corps n'est pas un anneau de valuation discrète car on aurait $F^\times = \mathcal{O}_v^\times$ et $v(F^\times) = \{0\}$.

(c) *A est un anneau de Dedekind qui n'est pas un corps,*
(d) *$\mathcal{M}$ est engendré par un élément non nilpotent.*

Démonstration. — (a) $\Rightarrow$ (c) est facile.

Pour (b) $\Leftrightarrow$ (c) voir [**AM69**, proposition 9.2 p. 94].

(c) $\Rightarrow$ (d) Soit $\pi \in \mathcal{M} \setminus \mathcal{M}^2$ ($\mathcal{M} \neq \mathcal{M}^2$ en raison de la partie "unicité dans le théorème 1.2.4). Pour tout $m \in \mathcal{M}$, l'exposant en $\mathcal{M}$ de la décomposition de l'idéal $m\pi^{-1}A$ est ≥ 0. Mais comme $\mathcal{M}$ est le seul idéal premier, cela donne $m\pi^{-1} \in A$ (voir remarque 1.2.5), d'où $\mathcal{M} = \pi A$. L'élément π n'est pas nilpotent puisque A est intègre.

(d) $\Rightarrow$ (a) Soit π un générateur de $\mathcal{M}$. Nous allons montrer que $\bigcap_{n\geq 0} \mathcal{M}^n = \{0\}$. On déduira la conclusion souhaitée *via* l'argument suivant (déjà rencontré dans le §1.2.2.1). Il résulte de $\bigcap_{n\geq 0} \mathcal{M}^n = \{0\}$ et de l'hypothèse "π non nilpotent" que tout élément $x \neq 0$ dans A s'écrit de façon unique $x = \pi^{v(x)}u$ avec $v(x) \in \mathbb{N}$ et $u \notin \mathcal{M}$ et donc u inversible dans A. Il en découle d'une part que A est intègre. D'autre part, on vérifie sans peine que l'entier $v(x)$ ne dépend pas du choix de π et que l'application $v : A \setminus \{0\} \to \mathbb{Z}$ se prolonge en une valuation discrète sur le corps des fractions de A pour laquelle $\mathcal{O}_v = A$ et $\mathcal{M}_v = \pi A$.

Soit $y \in \bigcap_{n\geq 0} \mathcal{M}^n$. Pour tout $n \geq 0$, on peut écrire $y = \pi^n x_n$ avec $x_n \in A$, d'où l'on tire $\pi^n(x_n - \pi x_{n+1}) = 0$. Notons $\mathcal{I}$ l'idéal de A des éléments x tels que $x\pi^n = 0$ pour n suffisamment grand. Ainsi $x_n - \pi x_{n+1} \in \mathcal{I}$ pour tout $n \geq 0$. Il en découle que la suite des idéaux $\mathcal{I} + Ax_n$ est croissante. Comme l'anneau A est noethérien, elle est stationnaire et donc pour n suffisamment grand, $x_{n+1} \in \mathcal{I} + Ax_n$, c'est-à-dire $x_{n+1} = z + tx_n$ avec $z \in \mathcal{I}$ et $t \in A$. Mais comme $x_n = \pi x_{n+1} + z'$ avec $z' \in \mathcal{I}$, on obtient $(1 - \pi t)x_{n+1} \in \mathcal{I}$. L'élément $1 - \pi t$ n'étant pas dans $\mathcal{M}$ est inversible dans A, d'où $x_{n+1} \in \mathcal{I}$. Enfin, comme l'idéal $\mathcal{I}$ est de type fini (A étant noethérien), il existe un entier N fixe tel que $x\pi^N = 0$ pour tout $x \in \mathcal{I}$. Prenons $n \geq N$ et suffisamment grand pour que la conclusion précédente $x_{n+1} \in \mathcal{I}$ soit valable. On peut alors conclure que $y = \pi^{n+1}x_{n+1} = 0$, ce qui achève la preuve de $\bigcap_{n\geq 0} \mathcal{M}^n = \{0\}$. □

Corollaire 1.2.8. — *Soient A un anneau de valuation discrète, d'idéal de valuation $\mathcal{M}$, de corps résiduel k et $f \in A[Y]$ un polynôme unitaire de degré $d \geq 1$. Si le polynôme $\overline{f} \in k[Y]$ obtenu par réduction de f modulo l'idéal $\mathcal{M}$ est irréductible dans $k[Y]$ et sans racine multiple dans $\overline{k}$, alors l'anneau $B_f = A[Y]/\langle f\rangle$ est un anneau de valuation discrète, son idéal maximal est l'idéal $\mathcal{M}B_f$ et B_f est la clôture intégrale de A dans le corps $E_f = K[Y]/\langle f\rangle$.*

Démonstration. — L'anneau B_f est noethérien. D'après le lemme 1.1.8, c'est un anneau local et son unique idéal maximal est engendré dans B_f par une uniformisante de A, laquelle ne peut être un élément nilpotent puisque A est intègre. Le théorème 1.2.7 permet de conclure que B_f est un anneau de valuation discrète. L'anneau B_f peut être identifié à un sous-anneau de $E_f = K[Y]/\langle f\rangle$ *via* le morphisme naturel (qui est bien injectif) déduit de l'inclusion $A \subset K$. Du caractère intégralement clos de B_f combiné au fait que B_f est entier sur A (puisque f est unitaire), on déduit que B_f est la fermeture intégrale de A dans $K[Y]/\langle f\rangle$. □

1.2.2.3. Valuations discrètes associées à un anneau de Dedekind. — Si A est un anneau de Dedekind, tout idéal premier $\mathfrak{p}$ non nul détermine une valuation discrète sur le corps des fractions K, appelée valuation $\mathfrak{p}$-adique : à tout élément $x \in K$ non nul, on associe l'exposant en $\mathfrak{p}$ dans la décomposition de l'idéal fractionnaire xA. D'après la remarque 1.2.5, l'anneau local $A_\mathfrak{p}$ en est l'anneau de valuation ; en particulier $A_\mathfrak{p}$ est un anneau de valuation discrète.

Les deux propriétés suivantes sont également utiles :
(*) l'idéal de valuation $\mathfrak{p}A_\mathfrak{p}$ possède des générateurs dans l'anneau A : tout élément $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ est en effet de valuation 1.
(**) pour tout $n \geq 0$, $\mathfrak{p}^n A_\mathfrak{p} + A = A_\mathfrak{p}$, ce qui signifie que A est dense dans $A_\mathfrak{p}$ pour la valuation $\mathfrak{p}$-adique (au sens de la métrique introduite au §1.2.2.4). En effet, pour $s \in A \setminus \mathfrak{p}$, l'idéal $\mathcal{P} = \langle \mathfrak{p}^n, s\rangle$ est égal à A puisque, en utilisant la remarque 1.2.5, on déduit des inclusions $\mathcal{P} \supset \mathfrak{p}^n$ et $\mathcal{P} \supset As$ que $n_\mathfrak{q}(\mathcal{P}) = 0$ pour tout idéal premier $\mathfrak{q} \neq \mathfrak{p}$ et que $n_\mathfrak{p}(\mathcal{P}) \leq n_\mathfrak{p}(As) = 0$, et donc que $\mathcal{P} = A$. Ainsi si $x = b/s \in A_\mathfrak{p}$, il existe $a \in A$ tel que $b - as \in \mathfrak{p}^n$, ce qui donne $b/s - a \in \mathfrak{p}^n A_\mathfrak{p}$.

On en déduit notamment que $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq A/\mathfrak{p}$: en effet le morphisme naturel $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est injectif (proposition 1.1.1) et la propriété de densité (**) ci-dessus donne la surjectivité.

Exemple 1.2.9. — (a) Pour tout nombre premier p, la valuation p-adique est une valuation discrète sur $\mathbb{Q}$. L'anneau de valuation discrète correspondant est l'anneau local $\mathbb{Z}_{(p)}$.

(b) Un autre cas particulier important est celui où $A = k[X]$ où k est un corps et $\mathfrak{p} = (P(X))$ avec $P(X) \in k[X]$ polynôme irréductible. Par exemple, la valuation $(X - x_0)$-adique notée v_{X-x_0} ou ord_{x_0} qui correspond à $P(X) = X - x_0$ avec $x_0 \in k$. La valuation $1/X$-adique $v_{1/X}$, notée aussi ord_∞, est un autre exemple de valuation discrète sur $k(X)$: elle est définie, pour tout $f(X) \in k(X)^\times$, par $v_\infty(f(X)) = -n$ si et seulement si on peut écrire $f(X) =$

$X^n \frac{a(1/X)}{b(1/x)}$ avec $a, b \in k[T]$ premiers entre eux tels que $a(0) \neq 0$, $b(0) \neq 0$. Pour cette valuation, $1/X$ est une uniformisante (ainsi que tout élément du type $1/(X-x)$ avec $x \in k$).

(c) L'idéal $I = (X_1, \ldots, X_n)$ de l'anneau $A = k[X_1, \ldots, X_n]$ (où k est un corps) est un idéal maximal. Mais l'anneau local A_I n'est pas un anneau de valuation discrète si $n \geq 2$: en effet, les idéaux (X_1) et (X_1, X_2) dans l'anneau A_I sont premiers, et (X_1) est strictement inclus dans (X_1, X_2) ; il existe dans A_I donc des idéaux premiers non maximaux, au contraire des anneaux principaux. Notons cependant que I vérifie $\bigcap_{n\geq 0} I^n = \{\underline{0}\}$.

1.2.2.4. Métrique associée à une valuation discrète. — Soit v une valuation discrète sur un corps K. On définit une valeur absolue $|\ |_v$ et une distance d sur K en posant, pour a un nombre réel fixé avec $0 < a < 1$

$$\begin{cases} |x|_v = a^{v(x)},\ x \in K \\ d(x,y) = |x-y|_v,\ x, y \in K \end{cases}$$

La valeur absolue $|\ |_v$ et la distance d sont *ultramétriques* ; c'est-à-dire, l'inégalité triangulaire prend la forme

$$|x+y|_v \leq \max(|x|_v, |y|_v)$$

De plus $$|x|_v \neq |y|_v \Rightarrow |x+y|_v = \max(|x|_v, |y|_v).$$

(La seconde inégalité $\geq$ s'obtient en notant que, si par exemple $|x|_v > |y|_v$, alors $|x|_v \leq \max(|-y|_v, |x+y|_v)$ et ce dernier terme est nécessairement $|x+y|_v$).

Il en résulte des propriétés métriques particulières (laissées en exercice [**Ami75**, §2.2]) :

- tous les triangles sont isocèles,
- tout point d'une boule en est le centre,
- deux boules sont soit disjointes soit comparables (pour l'inclusion),
- toute boule est une partie à la fois ouverte et fermée, en particulier l'anneau de valuation $\mathcal{O}_v$ (qui est la boule de rayon 1 centrée en 0),
- un espace métrique ultramétrique est totalement discontinu, c'est-à-dire : ses seules parties connexes sont les singletons,
- une suite $(x_n)_{n>0}$ est de Cauchy si et seulement si $d(x_n, x_{n+1})$ tend vers 0 quand $n \to +\infty$, etc.

Proposition 1.2.10. — *Deux valeurs absolues $|\ |_1$ et $|\ |_2$ sur le corps K définissent la même topologie sur K si et seulement si $|\ |_2 = |\ |_1^c$ avec $c \in \mathbb{R}$, $c > 0$. En particulier, deux valuations discrètes v_1 et v_2 sur K définissent la même topologie sur K si et seulement si $v_2 = cv_1$ avec $c > 0$. On dit alors de*

$|\ |_1$ et $|\ |_2$, et de v_1 et v_2, qu'elles sont équivalentes et on appelle places de K les classes d'équivalence correspondantes.

Démonstration. — L'implication ($\Leftarrow$) est évidente. Pour l'autre direction, supposons que $|\ |_1$ et $|\ |_2$ définissent la même topologie sur K. Alors l'ensemble des $x \in K$ tels que la suite $(x^n)_{n\geq 0}$ converge vers 0 est le même pour les deux valeurs absolues. Donc, pour $x \in K$ on a $|x|_1 < 1$ si et seulement si $|x|_2 < 1$. Si seul 0 vérifie ces conditions, alors, $|\ |_1$ et $|\ |_2$ sont nécessairement triviales, et égales. Supposons qu'il existe $b \neq 0$ tel que $|b|_1 < 1$ et $|b|_2 < 1$. Pour tout couple (m, n) d'entiers > 0, on a alors, pour $x \in K$ non nul, $n \log |x|_1 < m \log |b|_1$ si et seulement si $n \log |x|_2 < m \log |b|_2$ (puisque cela équivaut à x^n/b^m de valeur absolue < 1). On peut conclure alors que $\log |x|_1 / \log |b|_1 = \log |x|_2 / \log |b|_2$. □

***Exemple 1.2.11* (Ostrowski).** — Les places non archimédiennes du corps $\mathbb{Q}$ correspondent exactement aux valuations p-adiques décrites dans l'exemple 1.2.9. De même les places du corps $k(X)$ triviales sur k correspondent aux valuations $P(X)$-adiques décrites dans le même exemple. Pour voir que ce sont les seules, par exemple pour $k(X)$, on peut procéder comme suit. Etant donnée une valuation v sur $k(X)$ triviale sur k, on distingue un premier cas où v ne prend que des valeurs ≥ 0 sur $k[X]$. Si v est non triviale (sur $k(X)$), il existe $p(X) \in k[X]$ tel que $v(p) > 0$ et qu'on peut choisir de degré minimal. On montre alors que $p(X)$ est irréductible et que v est équivalente à la valuation $p(X)$-adique v_p : voir que si $q \in k[X]$ est premier à p, alors $v(q) = 0$ en écrivant une relation de Bezout pour p^n et q^n avec n assez grand. Dans le second cas, il existe $f(X) \in k[X]$ tel que $v(f) < 0$ (si v non triviale). On montre alors que $v(X) < 0$ (sinon $v(X) \geq 0$ et en fait $v(X) = 0$ d'après l'hypothèse faite, ce qui entraîne que $v(P(X)) = 0$ pour tout $P(X) \in k[X]$ et donc que v est triviale). On conclut ensuite facilement que v est équivalente à $v_{1/X}$. Le raisonnement est similaire pour le résultat sur $\mathbb{Q}$ (qu'on appelle le théorème d'Ostrowski ; voir [**Ami75**, §1.7] pour plus de détails).

1.2.2.5. Complétion d'un corps discrètement valué. — Le procédé général de complétion d'un espace métrique s'applique au corps valué (K, v). Le complété $\widetilde{K}$ est encore un corps valué : pour $x = \lim_{n\to+\infty} x_n \in \widetilde{K}$ (avec $x_n \in K$), la suite réelle $(|x_n|_v)_{n>0}$ est de Cauchy et converge donc vers une limite $|x|_{\tilde{v}} \in \mathbb{R}$; la correspondance $x \to |x|_{\tilde{v}}$ définit une valeur absolue ultramétrique sur $\widetilde{K}$. Cette valeur absolue provient d'une valuation $\widetilde{v}$, égale à $-\log |\ |_{\tilde{v}}$ à un multiple réel > 0 près. De plus, si $|x|_{\tilde{v}} \neq 0$, comme la valuation v est discrète et que la suite $(v(x_n))_{n>0}$ converge vers $\tilde{v}(x)$, on a $\tilde{v}(x) = v(x_n)$ pour tout $n \gg 0$.

Proposition 1.2.12. — *Si $\widetilde{\mathcal{O}_v}$ et $\widetilde{\mathcal{M}_v}$ désignent les complétés respectifs dans $\widetilde{K}$ de l'anneau de valuation $\mathcal{O}_v$ et de l'idéal de valuation $\mathcal{M}_v$ (c'est-à-dire leur adhérence topologique), on a :*

(a) $\widetilde{\mathcal{O}_v} = \mathcal{O}_{\tilde{v}}$ *et en conséquence* $\mathrm{Frac}(\widetilde{\mathcal{O}_v}) = \widetilde{K}$.

(b) *pour tout* $\nu \in \mathbb{N}$, $\nu \neq 0$, $\widetilde{\mathcal{M}_v}^{\nu} = \mathcal{M}_{\tilde{v}}^{\nu}$. *En particulier toute uniformisante* π_v *de la valuation* v *est une uniformisante de la valuation* $\tilde{v}$.

(c) *Les groupes de valeurs de* v *et* $\tilde{v}$ *concident.*

(d) *pour tout* $\nu \in \mathbb{N}$, $\nu \neq 0$, *les anneaux quotient* $\widetilde{\mathcal{O}_v}/\widetilde{\mathcal{M}_v}^{\nu}$ *et* $\mathcal{O}_v/\mathcal{M}_v^{\nu}$ *sont canoniquement isomorphes. En particulier, les corps résiduels de* v *et de* $\tilde{v}$ *sont canoniquement isomorphes.*

Remarque 1.2.13. — On sait aussi que toute uniformisante π_v de la valuation v est une uniformisante de la valuation $\tilde{v}$. Il résulte alors de (b) que $\widetilde{\mathcal{M}_v}^{\nu} = \widetilde{\mathcal{M}_v^{\nu}}$ ($\nu > 0$).

Démonstration. — (a) et (b) Les inclusions $\widetilde{\mathcal{O}_v} \subset \mathcal{O}_{\tilde{v}}$, $\widetilde{\mathcal{O}_v^{\times}} \subset \mathcal{O}_{\tilde{v}}^{\times}$ et $\widetilde{\mathcal{M}_v}^{\nu} \subset \mathcal{M}_{\tilde{v}}^{\nu}$ ($\nu > 0$) résultent facilement de la définition de $\tilde{v}$. Les inclusions inverses se déduisent du fait suivant, où π_v désigne une uniformisante de v :

(*) *pour tout* $x \in \widetilde{K}$, $x \neq 0$, *si* $\tilde{v}(x) = \nu$ *alors* x *s'écrit* $x = y\pi_v^{\nu}$ *avec* $y \in \widetilde{\mathcal{O}_v^{\times}}$.

En effet, x s'écrit comme limite d'une suite d'éléments $x_n \in K$ de valuation $v(x_n) = \tilde{v}(x) = \nu$ ($n > 0$). Si on pose $y_n = \pi_v^{-\nu} x_n$, alors $v(y_n) = 0$, c'est-à-dire $y_n \in \mathcal{O}_v^{\times}$ ($n > 0$), et la suite $(y_n)_{n>0}$ tend vers $y = \pi_v^{-\nu} x$.

(c) est une conséquence immédiate de la définition de $\tilde{v}$.

(d) Soit $\nu \in \mathbb{N}$, $\nu \neq 0$. En factorisant le morphisme $p_v^{\nu} : \mathcal{O}_v \to \widetilde{\mathcal{O}_v}/\widetilde{\mathcal{M}_v}^{\nu}$ par l'idéal $\mathcal{M}_v^{\nu}$, on obtient un morphisme

$$\mathcal{O}_v/\mathcal{M}_v^{\nu} \to \widetilde{\mathcal{O}_v}/\widetilde{\mathcal{M}_v}^{\nu}$$

Ce morphisme est injectif car $\ker(p_v^{\nu}) = \{x \in \mathcal{O}_v \mid \tilde{v}(x) = v(x) \geq \nu\} = \mathcal{M}_v^{\nu}$. Il est surjectif car pour tout $x \in \widetilde{\mathcal{O}_v}$, il existe $a \in \mathcal{O}_v$ tel que $\tilde{v}(x - a) \geq \nu$ (densité de $\mathcal{O}_v$ dans $\widetilde{\mathcal{O}_v}$). □

Pour tout $m \in \mathbb{N}$, $m \neq 0$, notons p_v^m la surjection canonique

$$p_v^m : \widetilde{\mathcal{O}_v} \to \mathcal{O}_v/\mathcal{M}_v^m$$

(où $\mathcal{O}_v/\mathcal{M}_v^m$ est identifié à $\widetilde{\mathcal{O}_v}/\widetilde{\mathcal{M}_v}^{\nu}$) et notons pareillement sa restriction $\mathcal{O}_v \to \mathcal{O}_v/\mathcal{M}_v^m$ à $\mathcal{O}_v$. Pour $m, n \in \mathbb{N}$ tels que $n \geq m$, notons aussi

$$p_v^{n,m} : \mathcal{O}_v/\mathcal{M}_v^n \to \mathcal{O}_v/\mathcal{M}_v^m$$

l'épimorphisme naturel vérifiant $p_v^m = p_v^{n,m} \circ p_v^n$.

Corollaire 1.2.14. — *Le complété $\widetilde{\mathcal{O}_v}$ est isomorphe à la limite projective $\varprojlim_m \mathcal{O}_v/\mathcal{M}_v^m$ du système projectif formé par les épimorphismes $(p_v^m)_{m>0}$ et $(p_v^{n,m})_{n>m>0}$.*

Démonstration. — Rappelons que $\varprojlim_m \mathcal{O}_v/\mathcal{M}_v^m$ est le sous-ensemble du produit $\prod_m \mathcal{O}_v/\mathcal{M}_v^m$ formé des familles $(u_m)_{m>0}$ telles que pour $n, m \in \mathbb{N}$ tels que $n \geq m > 0$, on a $p_v^{n,m}(u_n) = u_m$. Le morphisme produit $\prod_m p_v^m$ fournit un morphisme

$$\prod_m p_v^m : \widetilde{\mathcal{O}_v} \to \varprojlim_m \mathcal{O}_v/\mathcal{M}_v^m$$

Ce morphisme est injectif car $\bigcap_{m>0} \widetilde{\mathcal{M}_v}^m = \{0\}$. Il est également surjectif : si $(u_m)_{m>0} \in \varprojlim_m \mathcal{O}_v/\mathcal{M}_v^m$ et x_m est choisi dans $\mathcal{O}_v$ tel que $p_v^m(x_m) = u_m$ $(m > 0)$, alors $(x_m)_{m>0}$ est une suite de $\mathcal{O}_v$ de Cauchy, qui converge donc vers un élément x du complété $\widetilde{\mathcal{O}_v}$, lequel vérifie $(\prod_m p_v^m)(x) = (u_m)_{m>0}$. □

Exemple 1.2.15. — (a) L'anneau $\mathbb{Z}_{(p)}$, le corps $\mathbb{Q}$ ne sont pas complets pour la métrique p-adique : on montre ci-après (§1.2.2.7) grâce au lemme de Hensel qu'il existe des équations quadratiques sans solutions dans $\mathbb{Q}$ qui se résolvent dans le complété[3]. Leurs complétés sont respectivement notés $\mathbb{Z}_p$ et $\mathbb{Q}_p$ et appelés l'anneau des *entiers p-adiques* et le corps des *nombres p-adiques*. De même, $k[X]$ et $k(X)$ ne sont pas complets pour la valeur absolue $(X - x_0)$-adique $(x_0 \in k)$. Les complétés sont respectivement appelés l'anneau $k[[X-x_0]]$ des *séries formelles* et le corps $k((X - x_0))$ des *séries de Laurent formelles* ($k[[1/X]]$ et $k((1/X))$ pour $1/X$ à la place de $X - x_0$). D'après le corollaire 1.2.14, on a

$$\mathbb{Z}_p = \varprojlim_m \mathbb{Z}/p^m\mathbb{Z} \quad \text{et} \quad k[[X - x_0]] = \varprojlim k[[X - x_0]]/\langle (X - x_0)^m \rangle$$

(b) Dans le cas où A est un anneau supposé seulement posséder un idéal I vérifiant $\bigcap_{n\geq 0} I^n = \{0\}$, on peut définir sur A une distance ultramétrique similaire aux précédentes : pour $x, y \in K$, on pose $d(x, y) = a^{v(x-y)}$ où $v(x-y)$ est ici défini comme le plus grand entier n tel que $x - y \in I^n$ et $a \in \mathbb{R}$ est fixé avec $0 < a < 1$. Prenons par exemple $A = k[X_1, \ldots, X_n]$ et $I = (X_1, \ldots, X_n)$. On appelle *anneau de séries formelles à n indéterminées* sur le corps k le complété de l'anneau $A = k[X_1, \ldots, X_n]$ pour la distance d ; on note

[3] Pour montrer que $\mathbb{Z}$ n'est pas complet, on peut montrer plus simplement que la suite de terme général $1 + p + \cdots + p^n$ est de Cauchy mais ne converge pas dans $\mathbb{Z}$. *Idem* pour la suite de terme général $1 + X + \cdots + X^n$ dans $k[X]$.

$k[[X_1, \ldots, X_n]]$ cet anneau. C'est un anneau local d'idéal maximal engendré par $(X_1, \ldots, X_n)$.

1.2.2.6. Développement de Hensel. — Donnons-nous de plus une suite $(D_v^m)_{m>0}$ de *domaines fondamentaux* pour v, c'est-à-dire, d'ensembles $D_v^m \subset \mathcal{O}_v$ tels que, pour tout $m > 0$, toute classe dans le quotient $\mathcal{O}_v/\mathcal{M}_v^m$ soit représentée par exactement un élément de D_v^m. On note

$$s_v^m : \mathcal{O}_v/\mathcal{M}_v^m \to D_v^m$$

la correspondance associée, c'est-à-dire la réciproque de la restriction $p_v^m|_{D_v^m}$. Pour $K = \mathbb{Q}$ et v la valuation p-adique, on prendra $D_v^m = [0, p^m - 1] \cap \mathbb{N}$ et pour $K = k(X)$ et v la valuation $(X - x_0)$-adique ($x_0 \in k$), on prendra pour D_v^m le sous-ensemble $k[X]_{m-1} \subset k[X]$ des polynômes de degré $\leq m - 1$.

Etant donné $x \in \widetilde{\mathcal{O}_v}$, considérons la suite $(x_m)_{m>0}$ définie par

$$x_m = s_v^m \circ p_v^m(x) \quad (m > 0)$$

Pour tout $m > 0$, on a $p_v^m(x_m) = p_v^m(x)$, c'est-à-dire $x - x_m \in \widetilde{\mathcal{M}_v}^m$. La suite $(x_m)_{m>0}$ converge donc vers x dans $\widetilde{\mathcal{O}_v}$. On a de plus pour tout $n \geq m$

$$\begin{aligned} p_v^m(x_n) &= p_v^{n,m} \circ p_v^n(x_n) \\ &= p_v^{n,m} \circ p_v^n(x) \\ &= p_v^m(x) \end{aligned}$$

et donc aussi $s_v^m \circ p_v^m(x_n) = x_m$. Autrement dit, l'unique représentant dans D_v^m de x_n modulo $\mathcal{M}_v^m$ est égal à x_m.

Dans le cas où $K = \mathbb{Q}$ et v est la valuation p-adique, l'entier $x_m \in [0, p^m - 1]$ s'écrit de façon unique $x_m = \sum_{k=0}^{m_1} a_k^m p^k$. La propriété précédente montre que, pour $n \geq m$, les entiers $a_0^n, \ldots a_m^n$ sont indépendants de n : ils valent respectivement $a_0^m, \ldots a_m^m$.

Corollaire 1.2.16. — (a) *Tout entier p-adique $x \in \mathbb{Z}_p$ s'écrit de façon unique comme somme $\sum_{k=0}^{\infty} a_k p^k$ d'une série de terme général $a_k p^k$ avec $a_k \in [0, p-1] \cap \mathbb{N}$. Tout nombre p-adique $y \in \mathbb{Q}_p$ s'écrit de façon unique comme somme $\sum_{k=-\nu}^{\infty} b_k p^k$ d'une série de terme général $b_k p^k$ avec $b_k \in [0, p-1] \cap \mathbb{N}$, $\nu \in \mathbb{Z}$ et $b_{-\nu} \neq 0$.*

(b) *Tout élément $x \in k[[x - x_0]]$ s'écrit de façon unique comme somme $\sum_{k=0}^{\infty} a_k (X - x_0)^k$ d'une série de terme général $a_k (X - x_0)^k$ avec $a_k \in k$. Tout élément $y \in \mathbb{Q}_p$ s'écrit de façon unique comme somme $\sum_{k=-\nu}^{\infty} b_k (X - x_0)^k$ d'une série de terme général $b_k (X - x_0)^k$ avec $b_k \in k$, $\nu \in \mathbb{Z}$ et $b_{-\nu} \neq 0$.*

Les séries $\sum_{k=0}^{\infty} a_k p^k$ et $\sum_{k=-\nu}^{\infty} b_k p^k$ sont appelées *développements de Hensel* de $x \in \mathbb{Z}_p$ et de $y \in \mathbb{Q}_p$. La série $\sum_{k=0}^{\infty} a_k (X - x_0)^k$ est appelée *développement en série formelle en* $(X - x_0)$ de $x \in k[[X - x_0]]$ et la série $\sum_{k=-\nu}^{\infty} b_k (X - x_0)^k$ *développement en série de Laurent formelle en* $(X - x_0)$ de $y \in k((X - x_0))$. Comme d'habitude, $(X - x_0)$ doit être changé en $1/X$ quand la valuation considérée sur $k(X)$ est la valuation $1/X$-adique.

Démonstration. — Pour (a) l'existence a été établie ci-dessus. Pour l'unicité, supposons que x ait deux développements de Hensel distincts $\sum_{k=0}^{\infty} a_k p^k$ et $\sum_{k=0}^{\infty} a'_k p^k$. On a $\sum_{k=0}^{\infty} (a'_k - a_k) p^k = 0$. Si n_0 est alors le plus petit entier ≥ 0 tel que $a'_{n_0} - a_{n_0} \neq 0$. Comme $a'_{n_0} - a_{n_0} \in]-(p-1), (p-1)[$, on a $v_p(\sum_{k=0}^{\infty} (a'_k - a_k) p^k) = n_0$ ce qui est absurde. Le développement de Hensel d'un nombre p-adique $y \in \mathbb{Q}_p$ s'obtient ensuite aisément en écrivant $y = p^{-\nu} x$ avec $-\nu = v_p(y)$ et $x \in \mathbb{Z}_p$. La preuve de (b) est similaire. □

On a également de tels développements en série dans le cas où A est un anneau supposé seulement posséder un idéal I vérifiant $\bigcap_{n \geq 0} I^n = \{0\}$ [**Mal79**].

1.2.2.7. Lemme de Hensel. —

Théorème 1.2.17. — *Soit A un anneau de valuation discrète complet d'idéal de valuation I, ou plus généralement un anneau A local dont l'idéal maximal I vérifie $\bigcap_{n \geq 0} I^n = \{0\}$ et qui est complet pour la métrique associée à I. Soit $\kappa = A/I$ le corps résiduel. Soit $f(X) \in A[X]$ un polynôme tel que le polynôme réduit $\bar{f} \in \kappa[X]$ ait une racine simple $\lambda \in \kappa$. Alors il existe une racine x de f dans A, et une seule, telle que $\bar{x} = \lambda$.*

Cela fournit en particulier l'incomplétude de $k(T)$ et de $\mathbb{Q}$ pour chacune de leurs valuations. En effet, si par exemple $k(T)$ était complet pour la valuation T-adique, il serait fermé dans son complété $k[[T]]$ et donc égal à $k[[T]]$ puisqu'il y est dense. Or l'équation $y^2 - (1 + T) = 0$ n'a pas de solution dans $k(T)$ alors qu'elle en a dans le complété.

Démonstration. — L'unicité est facile. Pour l'existence, on utilise la *méthode d'approximation de Newton*. Soit $x_1 \in A$ tel que $\bar{x}_1 = \lambda$; on a $f(x_1) \equiv 0 \pmod{I}$.

Supposons avoir trouvé $x_n \in A$ tel que $\bar{x}_n = \lambda$ et $f(x_n) \equiv 0 \pmod{I^n}$. Pour $h \in I^n$, la formule de Taylor donne

$$f(x_n + h) = f(x_n) + f'(x_n) h + y h^2 \text{ avec } \ y \in A$$

Comme $yh^2 \in I^{2n} \subset I^{n+1}$, on a $f(x_n + h) \equiv 0 \pmod{I^{n+1}}$ si et seulement si

$$f(x_n) + f'(x_n)h \equiv 0 \pmod{I^{n+1}}$$

Comme λ est racine simple de $\bar{f}$, on a $\bar{f}'(\lambda) \neq 0$; cela donne $f'(x_n) \notin I$ et donc $f'(x_n)$ est inversible dans l'anneau local A. Comme $f(x_n)$ et h sont dans I^n, on en déduit que l'équation ci-dessus a une solution (unique) h_n. Posons $x_{n+1} = x_n + h_n$

Le procédé précédent fournit une suite $(x_n)_{n>0}$ d'éléments $x_n \in A$ vérifiant $\bar{x}_n = \lambda$, $x_{n+1} \equiv x_n \pmod{I^n}$ et $f(x_n) \equiv 0 \pmod{I^n}$. Cette suite est clairement de Cauchy. Dans l'espace métrique complet A, elle converge donc vers un élément $x \in A$, lequel vérifie $f(x) = 0$. □

Définition 1.2.18. — Un anneau A muni d'un idéal maximal I pour lequel la conclusion du lemme de Hensel est vraie est dit hensélien. Un corps est appelé hensélien si c'est le corps des fractions d'un anneau hensélien.

1.3. Extensions algébriques

1.3.1. Généralités. — Etant donnés un anneau R et un sous-corps K, un élément $x \in R$ est dit *algébrique* sur K s'il est entier sur K, c'est-à-dire, s'il existe une équation de dépendance $x^d + a_1 x^{d-1} + \cdots + a_d = 0$ à coefficients $a_1, \ldots, a_d \in K$, ou, de façon équivalente, si la dimension $[K[x] : K]$ (comme K espace vectoriel), appelée *degré* de x sur K, est finie. La théorie des extensions intégrales pourra donc être appliquée aux extensions algébriques. Si x n'est pas algébrique sur K, il est dit *transcendant* sur K.

L'anneau R est dit algébrique sur K si tout élément $x \in R$ est algébrique sur K ; si R est un corps on parle d'*extension algébrique* E/K. La dimension $[E : K]$ s'appelle le *degré* de E sur K. Par exemple, l'ensemble K' des éléments $x \in R$ algébriques sur K est un sous-anneau de R, contenant K et qui est algébrique sur K ; de plus si R est intègre, K' est un corps (lemme 1.1.21). Une extension E/K de degré fini est nécessairement algébrique ; la réciproque est fausse (prendre par exemple $K = \mathbb{Q}$ et $E = \overline{\mathbb{Q}}$). Une extension E de degré fini de $\mathbb{Q}$ est appelée *corps de nombres*. On vérifie sans peine qu'il y a multiplicativité des degrés, c'est-à-dire, si E est une extension algébrique de K et F une extension algébrique de E, alors F est une extension algébrique de K et $[F : K] = [F : E][E : K]$.

Soit $x \in R$ un élément algébrique sur un corps K. L'ensemble des polynômes $P(X) \in K[X]$ tels que $P(x) = 0$ est un idéal de l'anneau principal $K[X]$; son unique générateur unitaire $P(X)$ (c'est-à-dire, de coefficient dominant égal à

1 est appelé *polynôme minimal* de x sur K. On a un isomorphisme d'anneau $K[x] \simeq K[X]/(P(X))$. Si $K[x]$ est intègre, c'est un corps (la réciproque "$K[x]$ corps $\Rightarrow$ x algébrique" est également vraie) et donc le polynôme minimal $P(X)$ est irréductible.

Inversement, étant donné un polynôme irréductible $P(X) \in K[X]$, l'anneau intègre $K[X]/(P(X))$ est un corps, extension algébrique de degré $\deg(P)$ de K, de la forme $K[x]$ avec $P(x) = 0$ (prendre x égal à la classe de X modulo $P(X)$). Un corps vérifiant ces propriétés est appelé *corps de rupture* du polynôme $P(X)$.

Pour $P \in K[X]$, non nécessairement irréductible, on montre ensuite, par récurrence sur $d = \deg(P)$, l'existence d'un *corps de décomposition* de P, c'est-à-dire d'un corps E tel que $P(X) = c\prod_{i=1}^{d}(X - x_i)$ avec $x_i \in E$ et $E = K(x_1, \ldots, x_d)$ (considérer le corps de rupture $K[x]$ d'un facteur irréductible de P et appliquer l'hypothèse de récurrence au polynôme $P(X)/(X - x) \in K[x][X]$).

Une itération "transfinie" de ce procédé conduit au théorème de Steinitz.

Théorème 1.3.1. — *Tout corps K possède une clôture algébrique, c'est-à-dire, une extension algébrique $\widetilde{K}$ telle que $\widetilde{K}$ est un corps algébriquement clos.*

1.3.2. K-morphismes. — Etant donnés deux corps E et E' contenant un corps K, on appelle K-isomorphisme de E sur E' tout isomorphisme $E \to E'$ induisant l'identité sur K. Il est fréquent d'utiliser le terme "K-isomorphisme" même si le morphisme n'est pas surjectif : il faut le comprendre comme "K-isomorphisme sur son image". Si de plus E et E' sont algébriques sur K, les deux corps sont dits *K-conjugués*. Deux éléments x et x' (dans des anneaux contenant K) sont dits K-conjugués s'il existe un K-isomorphisme $K[x] \to K[x']$ envoyant x sur x'. Si x et x' sont algébriques, cela est équivalent à dire que x et x' ont le même polynôme minimal sur K.

1.3.2.1. Résultats de prolongements. — Le lemme 1.3.2 est le point de départ de la plupart des questions de prolongement des K-morphismes.

Lemme 1.3.2. — *Soient A un anneau intègre de corps des fractions K, R un anneau contenant K, y un élément de R algébrique sur K de polynôme minimal $X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$ à coefficients dans A* [(4)]*. Soit f :*

[(4)] Cette hypothèse est satisfaite quand y est entier sur A et A est intégralement clos (et donc en particulier quand A est un corps). En effet, si y est entier sur A, ses conjugués le sont aussi et donc les coefficients $a_1, \ldots, a_d \in K$ également. Si A est intégralement clos, ces coefficients $a_1, \ldots, a_d$ sont en fait dans A.

$A \to C$ un morphisme d'anneau à valeurs dans un corps C. Alors, si $\alpha \in C$ est une racine du polynôme $f(P) = X^d + f(a_1)X^{d-1} + \cdots + f(a_{d-1})X + f(a_d)$, le morphisme f se prolonge de façon unique en un morphisme d'anneau $f : A[y] \to C$ tel que $f(y) = \alpha$.

Démonstration. — Pour tout polynôme $Q \in A[X]$, on pose $f(Q(y)) = f(Q)(\alpha)$ (où $f(Q)$ est le polynôme obtenu en appliquant f aux coefficients de Q). Ce prolongement est bien défini : si $Q(y) = R(y)$ pour $R(X) \in A[X]$, alors $X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$ divise $P - Q$, *a priori* dans $K[X]$ mais en fait dans $A[X]$ (car $P - Q \in A[X]$ et le polynôme minimal de y est unitaire) ; il en résulte que $f(P)(\alpha) = f(Q)(\alpha)$. Autrement dit, sous les hypothèses considérées, l'ensemble des polynômes $P \in A[X]$ tels que $P(y) = 0$ est un idéal principal de $A[X]$. Le prolongement f ainsi défini vérifie les conditions de l'énoncé ; de plus un tel prolongement est déterminé par la condition $f(y) = \alpha$. □

L'énoncé suivant découle aisément, par récurrence sur $\deg(P)$.

Corollaire 1.3.3. — *Si $\sigma : K \to K'$ est un isomorphisme de corps, $P(X) \in K[X]$ un polynôme, $x_1, \ldots, x_n$ (resp. $x'_1, \ldots, x'_{n'}$) les racines distinctes de $P(X)$ (resp. de $\sigma(P)(X)$) dans un corps où $P(X)$ (resp. $\sigma(P)(X)$) est décomposé, il existe un isomorphisme $K(x_1, \ldots, x_n) \to K'(x'_1, \ldots, x'_{n'})$ prolongeant σ et envoyant $\{x_1, \ldots, x_n\}$ sur $\{x'_1, \ldots, x'_{n'}\}$. En particulier $n = n'$.*

Du corollaire 1.3.3 résulte en particulier l'unicité à K-isomorphisme près, du corps de décomposition d'un polynôme. Il en résulte aussi que le nombre de racines distinctes d'un polynôme ne dépend pas du corps où le polynôme est totalement décomposé.

Une autre conséquence classique du lemme 1.3.2 est l'énoncé ci-dessous.

Théorème 1.3.4. — *Etant données une extension algébrique E/K (non nécessairement de degré fini) et C un corps algébriquement clos, tout morphisme $K \to C$ se prolonge en un morphisme $E \to C$. En particulier la clôture algébrique d'un corps K est unique à K-isomorphisme près.*

Démonstration. — La première partie s'obtient par récurrence sur $[E : K]$ si l'extension E/K est finie ; si elle est infinie, il faut utiliser le lemme de Zorn. Pour la seconde partie, si C_1 et C_2 sont deux clôtures algébriques de K, alors l'identité $K \to K$ se prolonge en un K-morphisme $\sigma : C_1 \to C_2$. On observe alors que pour tout $x \in C_2$, si $P(X) \in K[X]$ est le polynôme minimal de

x sur K, alors σ envoie l'ensemble des racines distinctes de P dans C_1 dans l'ensemble des racines distinctes de P dans C_2. Comme σ est injective et que ces deux ensembles ont même cardinal, cette restriction est bijective. □

1.3.2.2. Séparabilité. —

Définition 1.3.5. — Etant donnée une extension algébrique E/K, un élément $x \in E$ est dit séparable sur K si son polynôme minimal (sur K) n'a que des racines simples, ou, de façon équivalente, a exactement $\deg(P)$ racines distinctes, dans tout corps où il est décomposé (par exemple dans un corps algébriquement clos contenant K). L'extension E/K est dite séparable si tous les éléments de E sont séparables sur K.

Proposition 1.3.6. — *Si E/K est une extension algébrique de degré fini d, alors E/K est séparable si et seulement si le nombre de K-morphismes distincts $E \to C$ dans un corps C algébriquement clos contenant K vaut $[E : K]$. En toute généralité, c'est-à-dire sans l'hypothèse de séparabilité, ce nombre est $\leq [E : K]$; plus généralement, cette majoration vaut pour le nombre de morphismes distincts $E \to C$ prolongeant un morphisme donné $\chi : K \to C$.*

Cette caractérisation de la séparabilité montre en particulier que le sous-ensemble E_s des éléments de E qui sont séparables sur K est un sous-corps de E : si x et y sont séparables sur K, alors l'extension $K(x)(y)/K$ est séparable, c'est-à-dire $K(x, y) \subset E_s$.

Démonstration de la proposition 1.3.6. — Observons d'abord que le lemme 1.3.2, dans le cas où A est un corps (et donc $A = K$), fournit la conclusion suivante qui correspond au cas particulier de la proposition 1.3.6 où E est une extension algébrique monogène $E = K(y)$) :

(*) *Le nombre de prolongements d'un morphisme $\varphi : K \to C$ en un morphisme $K(y) \to C$ est égal au nombre de racines distinctes du polynôme minimal $P(Y)$ de y sur K (dans un corps où P est décomposé). En particulier, ce nombre vaut $[K(y) : K]$ si et seulement si y est séparable sur K.*

Passons au cas général de la proposition 1.3.6.

($\Rightarrow$) : En écrivant $E = F(x)$ pour F un sous-corps propre de E contenant K et $x \in E$[5] utilisant le fait (*), on obtient aisément par récurrence sur $[E : K]$ que si E/K est séparable, alors le nombre de morphismes $E \to C$ prolongeant un morphisme donné $\varphi : K \to C$ vaut $[E : K]$. On obtient de la même façon

[5] Pour $E \neq K$, considérer le plus petit entier n tel que E s'écrive $E = K(x_1, \ldots, x_n)$ avec $x_1, \ldots, x_n \in E$ et prendre $x = x_n$ et $F = K(x_1, \ldots, x_{n-1})$.

que sans l'hypothèse de séparabilité, le nombre de K-morphismes distincts $E \to C$ est $\leq [E : K]$, et que la même majoration vaut pour le nombre de morphismes distincts $E \to C$ prolongeant un morphisme donné $\chi : K \to C$.

($\Leftarrow$) : pour $x \in E$, soit n_x le nombre de K-morphismes $K(x) \to C$ et $m_{x,\chi}$ le nombre de morphismes $E \to C$ prolongeant un morphisme donné $\chi : K(x) \to C$. L'hypothèse s'écrit $[E : K] = \sum_\chi m_{x,\chi}$ où la sommation porte sur l'ensemble des K-morphismes $K(x) \to C$. On sait de plus que $n_x \leq [K(x) : K]$ et que $m_{x,\chi} \leq [E : K(x)]$. Comme $[E : K] = [E : K(x)][K(x) : K]$, l'égalité précédente n'est possible que si les inégalités sont des égalités. On obtient donc $n_x = [K(x) : K]$, c'est-à-dire, x est séparable sur K. □

Proposition 1.3.7. — *Soit K un corps parfait, c'est-à-dire, ou bien de caractéristique 0, ou bien de caractéristique $p > 0$ et tel que l'application $x \to x^p$ de K dans K est surjective sur K. Si $P(X) \in K[X]$ est un polynôme unitaire irréductible, alors $P(X)$ n'a que des racines simples (dans tout corps C où $P(X)$ est décomposé). En conséquence, les extensions algébriques d'un corps parfait sont séparables.*

Exemple 1.3.8. — Les corps finis sont parfaits. Le corps $\mathbb{F}_p(T)$ ne l'est pas.

Démonstration. — Si $P(X)$ a une racine multiple $\alpha \in C$, alors $P'(\alpha) = 0$. Mais alors $P(X)$ divise $P'(X)$, ce qui impose $P'(X) = 0$. Cela n'est pas possible en caractéristique 0. En caractéristique $p > 0$, cela n'est possible que si $P(X)$ est de la forme $Q(X^p)$ avec $Q \in K[X]$ (nécessairement irréductible dans $K[X]$). Mais si K est parfait, chaque coefficient de Q est une puissance p-ième dans K, ce qui permet d'écrire $P(X) = Q(X^p) = (R(X))^p$ et contredit l'irréductibilité de P. □

La preuve ci-dessus montre également l'énoncé suivant.

Corollaire 1.3.9. — *Soient K un corps et x un élément algébrique et inséparable sur K. Alors K est de caractéristique $p > 0$ et il existe un plus petit entier $m \geq 1$ tel que le polynôme minimal de x sur K soit de la forme $Q(X^{p^m})$ avec $Q \in K[X]$. Le polynôme Q est irréductible dans $K[X]$ et sans racine multiple dans $\overline{K}$; x^{p^m} est séparable sur K.*

En particulier si K^{s} est l'extension séparable maximale de K contenue dans $K(x)$, alors p divise $[K^{\mathrm{s}}(x) : K^{\mathrm{s}}] : a = x^{p^m} \in K^{\mathrm{s}} \setminus (K^{\mathrm{s}})^p$ et $y = x^{p^{m-1}} \in K(x)$ est de polynôme minimal $X^p - a$ sur K^{s} ; on a donc $[K^{\mathrm{s}}(y) : K^{\mathrm{s}}] = p$, et ce degré divise $[K^{\mathrm{s}}(x) : K^{\mathrm{s}}]$.

1.3.3. Théorème de l'élément primitif. —

Théorème 1.3.10 **(théorème de l'élément primitif)**
Etant donnée une extension E de degré fini et séparable d'un corps K, il existe un élément $x \in E$ tel que $E = K[x]$; on dit alors que x est un élément primitif de l'extension E/K. De plus, pour une extension algébrique du type $K(\alpha, \beta)$ avec α et β séparables et K infini, on peut prendre x de la forme $\alpha + c\beta$ avec c quelconque en dehors d'un ensemble fini de K.

Démonstration. — Si K est fini, on a $K \simeq \mathbb{F}_q$ et $E = \mathbb{F}_{q^m}$ pour une puissance q d'un nombre premier et $m > 0$ un entier. On sait que $\mathbb{F}_{q^m}^\times$ est un groupe cyclique. Le résultat souhaité s'ensuit. Pour la suite, on peut donc supposer K infini. Nous donnons deux arguments pour ce cas.

1er argument. Etant donnés deux K-morphismes σ, σ' distincts de E dans un corps algébriquement clos C contenant K, l'ensemble $V_{\sigma,\sigma'}$ des $y \in E$ tels que $\sigma(y) = \sigma'(y)$ est un K-sous-espace vectoriel propre de E. Comme de tels K-morphismes sont en nombre fini et que K est infini, E n'est pas égal à la réunion des $V_{\sigma,\sigma'}$ quand σ, σ' varient dans l'ensemble $\{\sigma_1, \ldots, \sigma_n\}$ des K-morphismes $E \to C$. Il existe donc $x \in E$ tels que tous les éléments $\sigma_i(x)$, $i = 1, \ldots, n$, soient distincts. On obtient donc que $[K(x) : K] \geq n$. Mais l'extension E/K étant séparable, on a aussi $n = [E : K]$. D'où $K(x) = E$.

2ème argument. Il suffit de montrer que toute extension algébrique du type $K(\alpha, \beta)$ avec β séparable possède un élément primitif. Une récurrence immédiate donne ensuite le cas général.

Soient $P(X)$ et $Q(X)$ les polynômes minimaux respectifs de α et β sur K. Notons $\alpha_1, \ldots, \alpha_n$ avec $\alpha_1 = \alpha$ (resp. $\beta_1, \ldots, \beta_n$ avec $\beta_1 = \beta$) les racines de $P(X)$ et $Q(X)$ dans un corps algébriquement clos C contenant K. Posons $\theta = \alpha + c\beta$ pour $c \in K$. L'élément β est racine du polynôme $Q(X) \in K[X]$ et du polynôme $P(\theta - cX) \in K(\theta)[X]$. Notons $\Delta(X)$ le pgcd dans $K(\theta)[X]$ de $Q(X)$ et de $P(\theta - cX)$; on a $\deg(\Delta) \geq 1$. D'autre part une autre racine commune éventuelle de $Q(X)$ et de $P(\theta - cX)$ est un élément β_i $(1 < i \leq m)$, $\beta_i \neq \beta$, satisfaisant $\theta - c\beta_i = \alpha_j$, soit $\alpha + c\beta = \alpha_j + c\beta_i$, pour un certain indice $j \in \{1, \ldots, n\}$. Cela n'est possible que pour un nombre fini de valeurs de c. Si c est choisi en dehors de ces valeurs, ce qui est possible puisque K est infini, on obtient que β est la seule racine commune dans C des polynômes $Q(X)$ et de $P(\theta - cX)$. D'où $\Delta(X) = (X - \beta)^e$, pour un entier $e \geq 1$. Mais la séparabilité de β implique $e = 1$. D'où $\Delta(X) = (X - \beta)$ et $\beta \in K(\theta)$, ce qui donne $K(\theta) = K(\alpha, \beta)$. □

1.3.4. Normes et traces. — Soient B un anneau et A un sous-anneau tel que B soit un A-module libre de rang d. On appelle *trace*, *norme*, *polynôme caractéristique* d'un élément $x \in B$, la trace, la norme, le polynôme caractéristique (respectivement) de l'endomorphisme m_x du A-module B correspondant à la multiplication par x dans B. On les note $\mathrm{Tr}_{B/A}(x)$, $\mathrm{N}_{B/A}(x)$, $\det(m_x - X\mathrm{Id})$.

Considérons le cas où B/A est une extension E/K de corps de degré fini.

Si x est un élément primitif de E/K et $X^d + a_1X^{d-1} + \cdots + a_d$ est son polynôme minimal sur K, l'endomorphisme m_x est représenté dans la base $(1, x, \ldots, x^{n-1})$ par une matrice compagnon de dernière colonne ${}^t[-a_d, \ldots, -a_1]$. On en déduit que $\mathrm{Tr}_{E/K}(x) = -a_1$, $\mathrm{N}_{E/K}(x) = (-1)^d a_d$ et $\det(m_x - t\mathrm{Id}) = (-1)^d(X^d + a_1X^{d-1} + \cdots + a_d)$. Si $x_1, \ldots, x_d$ sont les d racines (éventuellement répétées) de $X^d + a_1X^{d-1} + \cdots + a_d$, on obtient alors les formules suivantes :

$$\begin{cases} \mathrm{Tr}_{E/K}(x) = x_1 + \cdots + x_d \\ \mathrm{N}_{E/K}(x) = x_1 \cdots x_d \\ \det(m_x - X\mathrm{Id}) = \prod_{i=1}^{d}(x_i - X) \end{cases}$$

Si $x \in E$ n'est plus supposé primitif, les formules doivent être ajustées. Pour la trace, le terme de droite doit être multiplié par $[E : K(x)]$; pour la norme, le terme de droite doit être élevé à la puissance $[E : K(x)]$-ième. On obtient ces formules générales à partir des précédentes en représentant l'endomorphisme m_x dans une base $(e_if_j)_{i,j}$ de E/K construite à partir d'une base $(e_i)_i$ de $K(x)/K$ et une base $(f_j)_j$ de $E/K(x)$: la matrice de m_x dans cette base est un tableau diagonal de $[E : K(x)]$ fois la matrice M correspondant à la multiplication m_x dans $K(x)$ dans la base $(e_i)_i$ (voir que $x(e_if_j) = (xe_i)f_j$ et que xe_i s'écrit comme combinaison linéaire des e_k à coefficients dans K).

Corollaire 1.3.11. — *Soient A un anneau intègre, K son corps des fractions et E/K une extension finie séparable. Soit $x \in E$ entier sur A. Alors les coefficients du polynôme* $\det(m_x - X\mathrm{Id})$*, par exemple* $\mathrm{Tr}_{E/K}(x)$ *et* $\mathrm{N}_{E/K}(x)$*, sont entiers sur A ; il en est de même des coefficients du polynôme minimal de x sur K. Si de plus, A est intégralement clos, ces coefficients sont dans A.*

Démonstration. — Les coefficients des polynômes considérés dans cet énoncé s'écrivent comme fonctions symétriques élémentaires de conjugués de x. Ils sont donc entiers sur A. Comme ils sont aussi dans K, si A est intégralement clos, ils sont alors dans A. □

Sous l'hypothèse supplémentaire E/K séparable, les formules se réécrivent

$$\begin{cases} \mathrm{Tr}_{E/K}(x) = \sum_\sigma \sigma(x) \\ \mathrm{N}_{E/K}(x) = \prod_\sigma \sigma(x) \\ \det(m_x - X\mathrm{Id}) = \prod_\sigma (\sigma(x) - X) \end{cases}$$

où la sommation et les produits portent sur l'ensemble des K-morphismes distincts de E dans une clôture algébrique.

1.3.5. Structure des extensions d'entiers. —

1.3.5.1. Lemme de Dedekind. —

Théorème 1.3.12. — *Soient G un groupe, C un corps et $\sigma_1, \ldots, \sigma_n$ des homomorphismes distincts de G dans le groupe multiplicatif $C^\times$. Alors les homomorphismes $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants sur C.*

Démonstration. — Supposons que $\sigma_1, \ldots, \sigma_n$ sont linéairement dépendants sur C et considérons une relation non triviale $\sum_{i=1}^n u_i\sigma_i = 0$ telle que le nombre s des coefficients u_i non nuls soit minimal. Après renumérotation, on peut supposer que cette relation est

$$\sum_{i=1}^{s} u_i\sigma_i(g) = 0 \quad \text{pour tout } g \in G$$

Multiplions cette relation par $\sigma_1(h)$ pour $h \in G$ et soustrayons la relation ci-dessus avec gh substitué à g. En utilisant $\sigma_i(gh) = \sigma_i(g)\sigma_i(h)$, on obtient

$$\sum_{i=2}^{s} u_i(\sigma_1(h) - \sigma_i(h))\sigma_i(g) = 0 \quad \text{pour tout } g \in G$$

La minimalité de s donne $\sigma_1(h) = \sigma_i(h)$ pour tout $h \in G$, $i = 1, \ldots, s$, ce qui contredit l'hypothèse que les σ_i sont distincts. □

1.3.5.2. Discriminants. —

Définition 1.3.13. — Soient B un anneau et A un sous-anneau tel que B soit un A-module libre de rang d. Pour $(e_1, \ldots, e_d) \in B^d$, on appelle *discriminant* du système $(e_1, \ldots, e_d)$ l'élément de A, noté $\Delta(e_1, \ldots, e_d)$ et défini par $\Delta(e_1, \ldots, e_d) = \det\big((\mathrm{Tr}_{B/A}(e_ie_j))_{1\leq i,j\leq d}\big)$.

Si $(f_1, \ldots, f_d) \in B^d$ est un système tel que $f_i = \sum_{j=1}^d a_{ij}e_j$ avec $a_{ij} \in A$, on déduit de $\mathrm{Tr}_{B/A}(f_pf_q) = \sum_{ij} a_{pi}a_{qj}\mathrm{Tr}_{B/A}(e_pe_q)$, ce qui matriciellement s'écrit $(\mathrm{Tr}_{B/A}(f_pf_q))_{p,q} = P\,(\mathrm{Tr}_{B/A}(e_ie_j))_{i,j}\,{}^tP$, où P est la matrice des a_{ij}, que

$$\Delta(f_1, \ldots, f_d) = \det(P)^2\,\Delta(e_1, \ldots, e_d)$$

En particulier, les discriminants des bases du A-module B sont égaux à des inversibles de A près ; on appelle discriminant de B sur A l'idéal noté $\mathcal{D}_{B/A}$ qu'ils engendrent.

Plaçons-nous dans la situation où B/A est une extension E/K de corps et supposons-la de plus séparable. Soient $\sigma_1, \dots, \sigma_d$ les d K-morphismes de E dans une clôture algébrique C de K. La formule $\mathrm{Tr}_{E/K}(e_i e_j) = \sum_{k=1}^{d} \sigma_k(e_i)\sigma_k(e_j)$ permet d'écrire la matrice des traces $\left[(\mathrm{Tr}_{E/K}(e_i e_j))_{i,j}\right]$ comme produit des matrices $[(\sigma_k(e_i))_{i,k}]$ et $[(\sigma_k(e_j))_{k,j}]$, d'où

$$\Delta(e_1, \dots, e_d) = \det\left((\sigma_i(e_j))_{1\leq i,j\leq d}\right)^2$$

Si de plus $e_1, \dots, e_d$ constituent une base du K-espace vectoriel E, alors, d'après le lemme de Dedekind, $\Delta(e_1, \dots, e_d) \neq 0$, et donc aussi $\mathcal{D}_{E/K} \neq \{0\}$.

Remarque 1.3.14. — Si $P(Y) \in K[Y]$ est le polynôme minimal d'un élément primitif y de E/K, le calcul ci-après montre que le discriminant $\Delta(1, y, \dots, y^{d-1})$ de la base $(1, y, \dots, y^{d-1})$ de E sur K est égal au signe près au discriminant Δ_P de P. Notons $y_1, \dots, y_d \in E$ les racines de $P(Y) \in K[Y]$, c'est-à-dire les K-conjugués de y. On a alors

$$\begin{aligned}
\Delta(1, y, \dots, y^{d-1}) &= \det\left(y_i^j\right)_{\substack{1\leq i\leq d \\ 0\leq j\leq d-1}}^2 \\
&= (-1)^{d(d-1)/2} \textstyle\prod_{i\neq j}(y_i - y_j) \\
&= (-1)^{d(d-1)/2} \textstyle\prod_i P'(y_i) \\
&= (-1)^{d(d-1)/2}\ \Delta_P
\end{aligned}$$

1.3.5.3. Résultat principal. —

Théorème 1.3.15. — *Soit A un anneau intégralement clos, de corps des fractions K. Soient E/K une extension de corps séparable de degré d et A'_E la clôture intégrale de A dans E*[(6)].

(a) *L'anneau A'_E est contenu dans un A-module libre de rang $\leq d$. Plus précisément, si $y_1, \dots, y_d$ est une base de E/K avec $y_i \in A'_E$, $i = 1, \dots, d$ et $\Delta \in A$ est le discriminant de cette base, alors $\Delta A'_E$ est contenu dans le A-module libre engendré par $y_1, \dots, y_d$. En particulier, si $\Delta \in A^\times$ (par exemple si A est remplacé par A_{Δ^∞}), on a $A'_E = Ay_1 \oplus \cdots \oplus Ay_d$.*

(b) *Si A est noethérien, A'_E est un A-module de type fini et un anneau noethérien.*

(c) *Si A est un anneau de Dedekind, alors A'_E est un anneau de Dedekind.*

(6) Noter que E est automatiquement le corps des fractions de A'_E ; on a même $E = KA'_E$ (pour l'inclusion "$\subset$", voir que si $y \in E$ et si $a \in A$ est un dénominateur commun des coefficients de son polynôme minimal sur K, alors $ay \in A'_E$).

(d) *Si A est principal, alors A'_E est un A-module libre de rand d.*

(e) *Soient A un anneau de valuation discrète d'idéal de valuation $\mathcal{M}$ et y un élément primitif de E/K entier sur A de polynôme minimal $P \in K[Y]$. Si le polynôme obtenu par réduction de P modulo $\mathcal{M}$ n'a que des racines simples (dans $\overline{A/\mathcal{M}}$), alors $A'_E = A \oplus Ay \oplus \cdots Ay^{d-1}$. De façon équivalente, A'_E est isomorphe à $B_f = A[Y]/\langle f\rangle$ via le morphisme $B_f \to A'_E$ envoyant Y sur y.*

(f) *Si (K, v) est un corps muni d'une valuation discrète v complet pour la métrique induite, alors il existe, à équivalence près, une unique valuation w de E qui prolonge v et E est complet pour la métrique induite. De plus, si A est l'anneau de valuation de v, alors A'_E est l'anneau de valuation de w.*

Démonstration. — (a) Tout élément $z \in A'_E$ s'écrit $z = \sum_{j=1}^{d} c_j y_j$ avec $c_1, \ldots, c_d \in K$. On en déduit le système de d équations

$$\mathrm{Tr}_{E/K}(zy_i) = \sum_{j=1}^{d} c_j \mathrm{Tr}_{E/K}(y_j y_i) \quad i = 1, \ldots, d$$

Les élément $z, y_1, \ldots, y_d$ étant entiers et A intégralement clos, on a $\mathrm{Tr}_{E/K}(zy_i) \in A$, $i = 1, \ldots, d$ (corollaire 1.3.11). Les formules de Cramer conduisent alors à $\Delta c_i \in A$, $i = 1, \ldots, d$.

(b) Si A est noethérien, le A-module libre engendré par $y_1/\Delta, \ldots, y_d/\Delta$ est un A-module noethérien. Donc le A-module A'_E est de type fini sur A et est un A-module noethérien (comme sous-A-module d'un module noethérien). Tout idéal de A'_E, étant un sous-A-module de A'_E, est de type fini sur A, et donc sur A'_E. L'anneau A'_E est donc noethérien.

(c) Vu le (b) et comme A'_E est intégralement clos, il reste à montrer que tout idéal premier $\mathcal{P} \subset A'_E$ non nul est maximal. Cela découlera de l'énoncé (b) du lemme 1.1.21 une fois montré que $\mathcal{P}_A = \mathcal{P} \cap A$ est *non nul*. Si $x \in \mathcal{P}$ est non nul et $x^n + \cdots + a_1 x + a_0 = 0$ est une relation de dépendance intégrale de x sur A et si $a_0 \neq 0$ (ce à quoi on peut se ramener car B est intègre), alors $a_0 \in \mathcal{P}_A = \mathcal{P} \cap A$.

(d) D'après un résultat classique, un sous-module d'un module libre de rang n sur un anneau principal est lui-même libre [**Sam67**, chapitre1], de rang $\leq n$. Donc si A est principal, (a) entraîne que A'_E est un A-module libre, de rang d.

(e) Sous l'hypothèste faite, le discriminant $\Delta_P \in A$ du polynôme P est non nul dans $A/\mathcal{M}$, c'est-à-dire, $\Delta_P \notin \mathcal{M}$. Comme A est local, Δ_P est inversible dans A et le résultat découle alors du (a) et de la remarque 1.3.14.

(f) Comme (K, v) est complet et E de dimension finie sur K, toutes les normes sont équivalentes sur E et E est complet pour ces normes. Si w est une valuation discrète sur E prolongeant v, la valeur absolue associée fait de E un espace vectoriel normé sur (K, v). Il n'existe donc qu'un prolongement possible de v. D'après (c), A'_E est un anneau de Dedekind. Considérons les valuations $v_{\mathfrak{p}'}$ de E associées aux idéaux premiers $\mathfrak{p}'$ non nuls de A'_E (§1.2.2.3) ; il existe au moins un tel idéal $\mathfrak{p}'$ (sinon A'_E serait un corps et A aussi). Ces valuations prolongent toutes v puisque $\mathfrak{p}' \cap A$ est nécessairement égal au seul idéal premier non nul de A, l'idéal de valuation de v. D'après ce qui précède, toutes ces valuations induisent des métriques équivalentes. Leurs boules unité ouvertes, c'est-à-dire les idéaux $\mathfrak{p}'(A'_E)_{\mathfrak{p}'} \subset (A'_E)_{\mathfrak{p}'}$, sont donc égales (proposition 1.2.10). Comme $\mathfrak{p}' = \mathfrak{p}'(A'_E)_{\mathfrak{p}'} \cap A'_E$, on conclut qu'il n'existe qu'un seul idéal premier dans A'_E, lequel est donc un anneau de valuation discrète (théorème 1.2.7). Plus précisément, A'_E est l'anneau de valuation de la valuation, disons w, correspondant à l'idéal $\mathfrak{p}'$ qui est construite dans la preuve du théorème 1.2.7 : pour $x \in A'_E$, $w(x)$ est le plus grand entier n tel que $x \in (\mathfrak{p}')^n$, ce qui est aussi la définition de $v_{\mathfrak{p}'}$. D'où $w = v_{\mathfrak{p}'}$. Il reste à dire que l'anneau de valuation de $w = v_{\mathfrak{p}'}$ est l'anneau $(A'_E)_{\mathfrak{p}'}$ qui vaut évidemment A'_E puisque A'_E est local. □

Corollaire 1.3.16. — *Soient K un corps complet pour une valuation discrète v et $\overline{K}$ une clôture algébrique de K. Alors il existe une unique valuation sur $\overline{K}$ prolongeant v.*

Démonstration. — On utilise la conclusion (f) du théorème 1.3.15. Si E/K, E'/K sont deux extensions finies telles que $E \subset E'$ et w, w' sont les uniques prolongements de v à E et E' respectivement, alors nécessairement w' prolonge w. Les prolongements de v aux extensions finies de K définissent ainsi une valuation sur $\overline{K}$. L'unicité du prolongement résulte de l'unicité des prolongements aux extensions finies. □

1.4. Théorie de Galois

1.4.1. Théorie de Galois finie. — Dans cette sous-section les extensions considérées sont de degré fini.

Etant donnée une extension (finie) de corps E/K, l'ensemble des K-automorphismes de E est un groupe noté $\mathrm{Aut}(E/K)$. Etant donné un corps E et G un ensemble d'automorphismes de E, l'ensemble des $x \in E$ tels que

$\sigma(x) = x$ pour tout $\sigma \in G$, est un sous-corps de E, appelé sous-corps de E *fixé* par G (ou sous-corps des *invariants* de E sous G) et noté E^G.

Théorème 1.4.1. — *Etant donnée une extension E/K séparable de degré fini d, les conditions suivantes sont équivalentes :*
(a) *K est le sous-corps de E fixé par* $\mathrm{Aut}(E/K)$.
(b) *Pour tout $x \in E$, le polynôme minimal de x sur K a toutes ses racines dans E.*
(c) *Pour tout K-morphisme σ de E dans une clôture algébrique $\overline{K}$, on a $\sigma(E) \subset E$.*
(d) *Le nombre de K-automorphismes de E est égal au degré $[E : K]$.*
(e) *E est engendré par K et les racines d'un polynôme $P(X) \in K[X]$ sans racine multiple dans $\overline{K}$.*

Sous ces conditions, l'extension E/K est dite *galoisienne*; le groupe $\mathrm{Aut}(E/K)$ a d éléments, on l'appelle le groupe de Galois de l'extension E/K et on le note $\mathrm{Gal}(E/K)$. Si l'extension E/K n'est plus supposée séparable mais qu'elle vérifie les conditions équivalentes (b) et (c), elle est dite *normale*.

Démonstration du théorème 1.4.1. — L'équivalence entre (b) et (c) est facile et n'utilise pas la séparabilité; elle repose sur le fait qu'étant donné $x \in E$, un élément $y \in \overline{K}$ est racine du polynôme minimal de x si et seulement s'il existe un K-morphisme $\sigma : E \to \overline{K}$ tel que $\sigma(x) = y$.

L'équivalence de ces deux conditions avec la condition (d) sous l'hypothèse de séparabilité découle immédiatement : d'après la proposition 1.3.6, il y a $[E : K]$ K-morphismes $E \to \overline{K}$; il y a donc $[E : K]$ K-automorphismes $E \to E$ si et seulement si chacun des K-morphismes est un automorphisme.

Pour l'implication (e)⇒(c), on écrit $E = K(x_1, \ldots, x_d)$ avec $x_1, \ldots, x_d$ les racines de P (qui sont distinctes). Alors pour tout K-morphisme $\sigma : E \to \overline{K}$, on a $\sigma(E) = K(\sigma(x_1), \ldots, \sigma(x_d)) = E$ puisque $\{\sigma(x_1), \ldots, \sigma(x_d)\} = \{x_1, \ldots, x_d\}$ ($\sigma(x_1), \ldots, \sigma(x_d)$ sont les racines de $\sigma(P(X)) = P(X)$).

Pour l'implication (b)⇒(e), prenons pour P le polynôme minimal d'un élément primitif x de l'extension E/K. Sous la condition (b), toutes les racines $x_1, \ldots, x_d$ (où $d = [E : K]$) de P sont dans E. On a donc $E = K[x] = K(x_1, \ldots, x_d)$.

Supposons que E/K soit galoisienne, c'est-à-dire, que (b) et (c) soient satisfaites et que E/K soit séparable. L'argument ci-dessous montre qu'alors (a) est satisfaite. Il est toujours vrai que K soit inclus dans le sous-corps de E fixé par $\mathrm{Aut}(E/K)$. Inversement soit $x \in E$ tel que $x \notin K$. Son polynôme minimal

a alors une racine $y \in \overline{K}$ telle que $y \neq x$. Le K-morphisme $K[x] \to \overline{K}$ envoyant x sur y se prolonge en un K-morphisme $\sigma : E \to \overline{K}$ (théorème 1.3.4). D'après la condition (c), σ est un K-automorphisme de E et par construction $\sigma(x) \neq x$. L'élément x n'est donc pas dans le sous-corps de E fixé par $\mathrm{Aut}(E/K)$.

Quant à l'implication (a)⇒(b), elle résulte immédiatement du lemme d'Artin ci-dessous (et n'utilise pas l'hypothèse de séparabilité). □

***Théorème 1.4.2* (Artin).** — *Si G est un groupe fini d'automorphismes d'un corps E, alors E/E^G est une extension galoisienne de groupe G.*

Démonstration. — Considérons un élément $x \in E$. Notons $x_1, \ldots, x_d$ les transformés distincts de x par les automorphismes de G, avec $x_1 = x$; ce sont des éléments de E. Considérons ensuite le polynôme

$$\begin{aligned} g(X) &= (X - x_1) \cdots (X - x_d) \\ &= X^d - s_1 X^{d-1} + \cdots + (-1)^d s_d \end{aligned} \quad \text{où} \quad \begin{cases} s_1 &= \sum_{i=1}^d x_i \\ &\cdot \\ &\cdot \\ &\cdot \\ s_d &= \prod_{i=1}^d x_i \end{cases}$$

Autrement dit, les éléments $s_1, \ldots, s_d$ sont les valeurs des d fonctions symétriques élémentaires en les éléments de l'ensemble $G(x) = \{g(x) \mid g \in G\}$; ces valeurs ne dépendent pas de l'ordre des éléments. Cet ensemble étant invariant par l'action de tout automorphisme dans G, on obtient que $s_1, \ldots, s_d$ sont dans E^G, et donc que $g \in E^G[X]$.

On déduit de $g(x) = 0$ (par construction) que x est algébrique sur E^G et que son polynôme minimal $f \in E^G[X]$ divise g dans $E^G[X]$; en particulier f n'a que des racines simples. En fait, on a $f = g$ puisque pour tout $\sigma \in G$, on a $f(\sigma(x)) = \sigma(f(x)) = 0$; le polynôme minimal de x est donc totalement décomposé dans $E[X]$. Le raisonnement ci-dessus étant valable pour tout élément $x \in E$, on obtient que l'extension E/E^G est algébrique, séparable et normale, c'est-à-dire galoisienne.

L'argument précédent donne aussi que pour tout $x \in E$, $[E^G(x) : E^G] \leq |G|$. Choisissons x de degré maximal sur E^G et montrons que $E = E^G(x)$, ce qui donnera que $[E : E^G] \leq |G|$. L'inclusion $E \supset E^G(x)$ est claire. Inversement soit $y \in E$. L'extension $E^G(x, y)/E^G$ est séparable (car x et y, dans E, le sont). D'après le théorème de l'élément primitif (théorème 1.3.10), il existe $z \in E$ tel que $E^G(x, y) = E^G(z)$. Il résulte alors de $E^G(x) \subset E^G(z)$ et de la maximalité du degré de x sur E^G que $E^G(z) = E^G(x)$, c'est-à-dire que $y \in E^G(x)$.

Enfin on a évidemment $G \subset \mathrm{Gal}(E/E^G)$ et donc $|G| \leq |\mathrm{Gal}(E/E^G)|$. Combiné à $[E : E^G] \leq |G|$ (ci-dessus) et $[E : E^G] = |\mathrm{Gal}(E/E^G)|$ (l'extension E/E^G est galoisienne), on obtient que $\mathrm{Gal}(E/E^G) = G$. □

Le coeur de la théorie de Galois se situe dans la correspondance entre sous-extensions d'une extension galoisienne et sous-groupes du groupe de Galois.

Théorème 1.4.3. — *Soit E/K une extension galoisienne de groupe de Galois G. A tout sous-groupe G' de G, associons le sous-corps $h(G') = E^{G'}$ de E fixé par G', et à tout sous-corps K' de E contenant K, associons le sous-groupe $g(K') = \mathrm{Aut}(E/K')$ des K'-automorphismes de E.*

(a) *Les applications g et h sont des bijections réciproques l'une de l'autre, décroissantes pour l'inclusion. De plus E est extension galoisienne de tout corps K', intermédiaire entre K et E et* $\mathrm{Gal}(E/K') \subset \mathrm{Gal}(E/K)$.

(b) *Pour qu'un corps K' intermédiaire entre K et E soit une extension galoisienne de K, il faut et il suffit que $g(K') = \mathrm{Aut}(E/K') = \mathrm{Gal}(E/K')$ soit un sous-groupe distingué de* $\mathrm{Gal}(E/K) = G$. *Dans ce cas, le groupe de Galois* $\mathrm{Gal}(K'/K)$ *s'identifie au groupe quotient* $G/\mathrm{Gal}(E/K')$.

Démonstration. — (a) La décroissance des correspondances g et h est claire. Soit K' un corps intermédiaire entre K et E. L'extension E/K' est séparable car pour tout $x \in E$, la propriété de n'admettre que des racines simples passe du polynôme minimal de x sur K au polynôme minimal de x sur K', le second divisant le premier dans $K'[X]$. Pour la même raison, il en est de même de la propriété d'avoir toutes ses racines dans E, ce qui donne la normalité de l'extension (théorème 1.4.1). L'inclusion $\mathrm{Gal}(E/K') \subset \mathrm{Gal}(E/K)$ est évidente.

Etablir que les correspondances g et h sont réciproques l'une de l'autre revient à vérifier que
- pour tout corps $K \subset K' \subset E$, on a $E^{\mathrm{Gal}(E/K')} = K'$, et
- pour tout sous-groupe $G' \subset G$, on $\mathrm{Gal}(E/E^{G'}) = G'$.

Pour le premier point, fixons un corps K' tel que $K \subset K' \subset E$. L'inclusion $K' \subset E^{\mathrm{Gal}(E/K')}$ est évidente. D'après le lemme d'Artin, l'extension $E/E^{\mathrm{Gal}(E/K')}$ est galoisienne de groupe de Galois $\mathrm{Gal}(E/K')$. Comme il en est de même de l'extension E/K', les extensions $E/E^{\mathrm{Gal}(E/K')}$ et E/K' ont même degré et donc les corps $E^{\mathrm{Gal}(E/K')}$ et K' sont égaux. Le second point est encore plus directement une conséquence du lemme d'Artin.
(b) Fixons un corps K' tel que $K \subset K' \subset E$. Comme l'extension E/K' est galoisienne, on a $K' = E^{\mathrm{Gal}(E/K')}$. Mais alors pour tout $\sigma \in \mathrm{Gal}(E/K)$, on a

$$\sigma(K') = E^{\sigma\,\mathrm{Gal}(E/K')\,\sigma^{-1}}$$

L'équivalence annoncée en découle immédiatement. En toute généralité, l'application de restriction de E à K' fournit une bijection

$$\mathrm{Gal}(E/K)/\cdot\,\mathrm{Gal}(E/K') \to \mathrm{Mor}_K(K', \overline{K})$$

entre l'ensemble des classes à gauche du groupe $\mathrm{Gal}(E/K)$ modulo son sous-groupe $\mathrm{Gal}(E/K')$ et l'ensemble des K-morphismes de K' dans $\overline{K}$. Quand l'extension K'/K est galoisienne, cette application devient un isomorphisme de groupes entre le groupe quotient $\mathrm{Gal}(E/K)/\mathrm{Gal}(E/K')$ et le groupe $\mathrm{Aut}_K(K')$ des K-automorphismes de K'. □

Un intérêt de la théorie de Galois est que toute extension finie séparable E/K possède une clôture galoisienne $\widehat{E}/K$, qui est par définition l'intersection (dans $\overline{K}$) de toutes les extensions galoisiennes F/K telles que $F \supset E$. Cette intersection est elle-même galoisienne ; c'est la plus petite extension galoisienne contenant E. Si $\sigma_1, \ldots, \sigma_d$ sont les d K-morphismes de E dans $\overline{K}$, on voit facilement que $\widehat{E}$ est le compositum des corps $\sigma_1(E), \ldots, \sigma_d(E)$. Si x est un élément primitif de E/K, c'est-à-dire $E = K[x]$, on voit similairement que $\widehat{E} = K(x_1, \ldots, x_d)$ où $x_1, \ldots, x_d$ sont les K-conjugués de x.

Corollaire 1.4.4. — *Etant donnée une extension séparable finie E/K, il n'existe qu'un nombre fini de corps k tels que $K \subset k \subset E$.*

Ce résultat est faux si on ne suppose plus l'extension séparable. En effet, considérons le corps $E = \mathbb{F}_p(T)(\sqrt[p]{a}, \sqrt[p]{b})$, avec $a, b \in \mathbb{F}_p(T)$ choisis de telle sorte que l'extension $E/\mathbb{F}_p(T)$ soit de degré $> p$. Les extensions $\mathbb{F}_p(T)(\sqrt[p]{a} + c\sqrt[p]{b})$, où c décrit $\mathbb{F}_p(T) \setminus \{0\}$, sont distinctes et sont toutes strictement contenues dans E : en effet, l'élément $x = \sqrt[p]{a} + c\sqrt[p]{b}$ vérifie $x^p = a + c^p b$ et est donc de degré $\leq p$.

Exercice 1.4.5. — Montrer que si F/k est une extension galoisienne, alors $F(T)/k(T)$ en est une également et $\mathrm{Gal}(F(T)/k(T)) \simeq \mathrm{Gal}(F/k)$.

1.4.2. Théorie de Galois infinie. — La théorie de Galois s'étend aux extensions algébriques E/K de degré infini. On définit de la même façon $\mathrm{Aut}(E/K)$ et E^G. La normalité est définie par les conditions (b) et (c) du théorème 1.4.1, qui demeurent équivalentes, et sont équivalentes, sous l'hypothèse de séparabilité, à la condition (e) généralisée suivante [**Lan78**, VII, §3, théorème 4] :

(e-gen) E est engendré par K et les racines d'une famille de polynômes sans racine multiple dans $\overline{K}$.

Une extension E/K normale et séparable est dite galoisienne et le groupe $\mathrm{Aut}(E/K)$ est appelé groupe de Galois et noté $\mathrm{Gal}(E/K)$.

Une extension algébrique E/K est la réunion de ses sous-extensions de degré fini. Il en résulte que $\mathrm{Gal}(E/K)$ est isomorphe au groupe limite projective des groupes de Galois $\mathrm{Gal}(F/K)$ des extensions galoisiennes finies contenues dans F. On peut alors équiper le groupe $\mathrm{Gal}(E/K)$ de la topologie naturelle de cette limite projective, qu'on appelle la topologie de Krull. Le groupe topologique $\mathrm{Gal}(E/K)$ est un groupe *profini*, c'est-à-dire, une limite projective de groupes finis munis de la topologie discrète. En particulier, c'est un groupe compact.

Le théorème 1.4.3 s'étend aux extensions algébriques en général à condition de ne considérer que les sous-groupes *fermés* G' de G [**FJ04**, prop.1.3.1]. De la compacité $\mathrm{Gal}(F/K)$ résulte que les sous-groupes ouverts sont fermés d'indice fini, et réciproquement, et donc que les sous-extensions correspondantes sont les extensions de K de degré fini.

En pratique, dans un situation donnée, le groupe de Galois $\mathrm{Gal}(E/K)$ peut être compris comme "le groupe de Galois $\mathrm{Gal}(F/K)$ d'une extension galoisienne finie suffisamment grande de K".

Ce qui précède s'applique en particulier à la clôture séparable K^{s} de K. C'est une extension galoisienne et son groupe de Galois est appelé *groupe de Galois absolu* de K et note G_K.

Pour plus de détails sur limites projective, topologie de Krull, groupes profinis et théorie de Galois infinie, nous renvoyons à [**FJ04**].

1.5. Extensions résiduelles et ramification

1.5.1. Généralités. — On suppose donnés ici, de façon générale, une extension E/K de degré fini d, un anneau (intègre) $A \subset K$ et un sous-anneau $B \subset E$ entier sur A.

Soit $\mathcal{P}$ un idéal premier de B. L'idéal $\mathcal{P}_A = \mathcal{P} \cap A$ est un idéal premier (non nul si $\mathcal{P}$ est non nul d'après la preuve du (c) du théorème 1.3.15). On dit que $\mathcal{P}$ *divise* $\mathcal{P}_A$ (ou est *au-dessus de* $\mathcal{P}_A$), et on écrit parfois $\mathcal{P}|\mathcal{P}_A$.

Le corps $\mathrm{Frac}(B/\mathcal{P})$, noté $\bar{E}$, est appelé *corps résiduel* de $\mathcal{P}$; c'est une extension du corps résiduel $\bar{K} = \mathrm{Frac}(A/\mathcal{P}_A)$ de $\mathcal{P}_A$, appelée *extension résiduelle*. L'idéal $\mathcal{P}$ est maximal dans B si et seulement si $\mathcal{P}_A$ est un idéal maximal de A (lemme 1.1.21). Dans ce cas on a $\bar{E} = B/\mathcal{P}$ et $\bar{K} = A/\mathcal{P}_A$.

Si B est un A-module de type fini, alors l'anneau $B/\mathcal{P}$ est un $A/\mathcal{P}_A$-module de type fini. En particulier si $\mathcal{P}$ (et $\mathcal{P}_A$) sont maximaux, l'extension résiduelle

est de degré fini, qu'on appelle *degré résiduel* de $\mathcal{P}$ sur A[7]. D'après le théorème 1.3.15, la condition de finitude du A-module B est satisfaite sous les hypothèses de la proposition ci-dessous.

Proposition 1.5.1. — *On suppose A noethérien, intégralement clos, de corps des fractions K, $B = A'_E$ et E/K séparable. Si $y_1, \dots, y_d$ est une base de E/K avec $y_i \in A'_E$, $i = 1, \dots, d$ et $\Delta \in A$ est le discriminant de cette base, alors pour tout idéal maximal $\mathcal{P}$ tel que $\Delta \notin \mathcal{P}$, on a*
(i) $[\bar{E} : \bar{K}] \leq [E : K]$
(ii) $\bar{E} = \bar{K}(\bar{y}_1, \dots, \bar{y}_d)$ *où $\bar{y}_i$ est l'image de y_i dans $A'_E/\mathcal{P}$.*

Démonstration. — D'après le théorème 1.3.15, ΔB est contenu dans le A-module libre engendré par $y_1, \dots, y_d$. Si $\mathcal{P}$ est un idéal maximal tel que $\Delta \notin \mathcal{P}$, Δ s'inverse dans $B/\mathcal{P}$. On obtient que les classes $\bar{y}_1, \dots, \bar{y}_d$ de $y_1, \dots, y_d$ modulo $\mathcal{P}$ constituent un système générateur du $A/\mathcal{P}_A$-espace vectoriel $B/\mathcal{P} = \bar{E}$. Les énoncés (i) et (ii) découlent aussitôt. □

1.5.2. Décomposition d'un idéal premier dans une extension. — On suppose que A est un anneau de Dedekind, $K = \mathrm{Frac}(A)$, E/K séparable de degré $d \geq 1$ et on prend $B = A'_E$. On sait que B est un anneau de Dedekind (théorème 1.3.15).

1.5.2.1. Définitions. — Soit $\mathfrak{p}$ un idéal premier non nul de A. D'après le théorème 1.2.4, l'idéal $\mathfrak{p}B$ s'écrit de façon unique

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

où les $\mathfrak{P}_i$ sont des idéaux premiers distincts de B et où les e_i sont des entiers ≥ 1. L'exposant e_i s'appelle l'*indice de ramification* de $\mathfrak{P}_i$ sur A et on note f_i désigne le degré résiduel de $\mathfrak{P}_i$ sur A, $i = 1, \dots, g$.

Définition 1.5.2. — On dit que :
- l'idéal $\mathfrak{P}_i$ est non ramifié dans l'extension E/K ou que E/K est non ramifiée en $\mathfrak{P}_i$ si $e_i = 1$ et que l'extension résiduelle $B/\mathfrak{P}_i$ de $A/\mathfrak{p}$ est séparable,
- l'idéal $\mathfrak{p}$ est non ramifié dans E/K ou que E/K est non ramifiée au-dessus de $\mathfrak{p}$ si E/K est non ramifiée en chaque idéal $\mathfrak{P}_i$, $i = 1, \dots, g$,

[7] Ceci est vrai plus généralement si pour tout $b \in \mathrm{Frac}(B/\mathcal{P})$, il existe $a \in A/\mathcal{P}_A$ non nul tel que $ab \in B/\mathcal{P}$ (c'est le cas par exemple si $A/\mathcal{P}_A$ est intégralement clos et l'extension résiduelle est normale : on peut alors prendre pour a la norme d'un dénominateur de b dans l'extension résiduelle).

- l'idéal $\mathfrak{p}$ est inerte dans E/K si $\mathfrak{p}B$ est un idéal premier de B, c'est-à-dire si $g = 1$ et $e_1 = 1$.
- l'idéal $\mathfrak{p}$ est totalement ramifié dans E/K ou que E/K est totalement ramifiée au-dessus de $\mathfrak{p}$ si $g = 1$ et $e_1 = [E : K]$.

1.5.2.2. Le résultat fondamental pour un anneau de Dedekind. —

Théorème 1.5.3. — (a) *Les idéaux $\mathfrak{P}_1, \dots \mathfrak{P}_g$ sont exactement les idéaux premiers $\mathfrak{P}$ de B tels que $\mathfrak{P} \cap A = \mathfrak{p}$, ou, de façon équivalente, tels que $\mathfrak{P} \supset \mathfrak{p}$. En particulier $\mathfrak{p}B \cap A = \mathfrak{p}$.*

(b) *L'anneau $B/\mathfrak{p}B$ est une $A/\mathfrak{p}$-algèbre de dimension $[E : K]$. De plus il est isomorphe à l'anneau produit $\prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ dont chaque facteur est une $A/\mathfrak{p}$-algèbre de dimension $e_i f_i$. On a en particulier*

$$\sum_{i=1}^{g} e_i f_i = [E : K]$$

En particulier, les idéaux premiers $\mathfrak{P}$ de B au-dessus d'un idéal premier $\mathfrak{p} \neq 0$ de A sont en nombre fini. Le théorème 1.6.1 généralisera cette propriété.

Démonstration. — Pour $\mathfrak{P}$ idéal premier de B, si $\mathfrak{P} \supset \mathfrak{p}$ alors $\mathfrak{P} \cap A \supset \mathfrak{p}$ et donc $\mathfrak{P} \cap A = \mathfrak{p}$ puisque $\mathfrak{p}$ est maximal et que $\mathfrak{P} \cap A \neq A$. La réciproque est immédiate. Ainsi $\mathfrak{P} \cap A = \mathfrak{p}$ équivaut à la condition $\mathfrak{P} \supset \mathfrak{p}B$. Or on sait que cette dernière équivaut au fait que l'exposant en $\mathfrak{P}$ de la décomposition de l'idéal $\mathfrak{p}B$ est > 0 (théorème 1.2.4 et remarque 1.2.5). D'où le (a).

Soit $S = A \setminus \mathfrak{p}$. L'anneau $A_\mathfrak{p}$ est un anneau de valuation discrète (§1.2.2.3) et l'anneau $S^{-1}B$ est la clôture intégrale de $A_\mathfrak{p}$ dans E (proposition 1.1.19). On a $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq A/\mathfrak{p}$ (§1.2.2.3). On a aussi $S^{-1}B/\mathfrak{p}S^{-1}B \simeq B/\mathfrak{p}B$: l'épimorphisme $B \to B/\mathfrak{p}B$ envoie les éléments de S sur des inversibles de $A/\mathfrak{p}$ et donc aussi du sur-anneau $B/\mathfrak{p}B$; il induit donc un épimorphisme $S^{-1}B \to B/\mathfrak{p}B$, lequel a pour noyau est $S^{-1}(\mathfrak{p}B) = \mathfrak{p}S^{-1}B$. Comme $A_\mathfrak{p}$ est principal, $S^{-1}B$ est un $A_\mathfrak{p}$-module libre de rang $d = [E : K]$ (théorème 1.3.15) et $S^{-1}B/\mathfrak{p}S^{-1}B$ est un $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$-espace vectoriel de dimension d : une base du $A_\mathfrak{p}$-module libre donne par réduction une base du $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$-espace vectoriel. On a ainsi obtenu que $B/\mathfrak{p}B$ est une $A/\mathfrak{p}$-algèbre de dimension d.

Pour $i \neq j$, on a $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = B$ car aucun idéal maximal $\mathfrak{P}$ ne peut contenir $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j}$ puisque devant contenir alors $\mathfrak{P}_i^{e_i}$ et $\mathfrak{P}_j^{e_j}$ ce devrait être $\mathfrak{P} = \mathfrak{P}_i = \mathfrak{P}_j$. L'isomorphisme $B/\mathfrak{p}B \simeq \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ découle alors du "lemme chinois" (lemme 1.1.6).

Pour conclure la preuve de (b), il nous reste à établir que $B/\mathfrak{P}_i^{e_i}$ est une $A/\mathfrak{p}$-algèbre de dimension $e_i f_i$, $i = 1, \ldots, g$. La structure de $A/\mathfrak{p}$-algèbre de $B/\mathfrak{P}_i^{e_i}$ est donnée par le morphisme $A/\mathfrak{p} \to B/\mathfrak{P}_i^{e_i}$ induit par l'inclusion $\mathfrak{p} \subset \mathfrak{P}_i^{e_i}$; ce morphisme est injectif car $A/\mathfrak{p}$ est un corps. Dans $B/\mathfrak{P}_i^{e_i}$ on a la suite décroissante suivante

$$B/\mathfrak{P}_i^{e_i} \supset \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supset \mathfrak{P}_i^2/\mathfrak{P}_i^{e_i} \cdots \supset \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supset \{0\}$$

de sous-$A/\mathfrak{p}$-espaces vectoriels dont la dimension décroit de f_i unités entre deux termes. En effet, le sous-espace quotient $(\mathfrak{P}_i^k/\mathfrak{P}_i^{e_i})/(\mathfrak{P}_i^{k+1}/\mathfrak{P}_i^{e_i})$ est isomorphe à $\mathfrak{P}_i^k/\mathfrak{P}_i^{k+1}$ et ce dernier est un $B/\mathfrak{P}_i$-espace vectoriel, dont les sous-espaces vectoriels sont de la forme $V/\mathfrak{P}_i^{k+1}$ avec V un B-module, c'est-à-dire un idéal de B, tel que $\mathfrak{P}_i^{k+1} \subset V \subset \mathfrak{P}_i^k$. Comme il n'y a pas d'idéaux strictement compris entre $\mathfrak{P}_i^k$ et $\mathfrak{P}_i^{k+1}$, on obtient que $\mathfrak{P}_i^k/\mathfrak{P}_i^{k+1}$ est de dimension 1 sur $B/\mathfrak{P}_i$ et lui est donc isomorphe comme $A/\mathfrak{p}$-espace vectoriel. □

La proposition suivante est utile. Elle découle aisément des définitions et de la forme de la décomposition des idéaux premiers.

Proposition 1.5.4. — *Soient E/K et A comme ci-dessus et L un corps intermédiaire entre K et E. Si $\mathcal{Q}$ est un idéal premier non nul de A'_E, $\mathcal{P}$ sa restriction à A'_L et $\mathfrak{p}$ sa restriction à A, on a, avec des notations évidentes, $e_{E/K}(\mathcal{Q}) = e_{E/L}(\mathcal{Q}) \cdot e_{L/K}(\mathcal{P})$ et $f_{E/K}(\mathcal{Q}) = f_{E/L}(\mathcal{Q}) \cdot f_{L/K}(\mathcal{P})$.*

1.5.2.3. Anneaux de valuation discrète complets. — On s'intéresse ici à la situation plus particulière où A est un anneau de valuation discrète complet.

Théorème 1.5.5. — *Soit K un corps muni d'une valuation discrète v complet pour la métrique induite. Soient E/K une extension finie séparable, A l'anneau de valuation de v et B la fermeture intégrale de A dans E.*

(a) *L'unique valuation w de E qui prolonge v est définie par*

$$w(x) = \frac{1}{[E:K]}\, v(\mathrm{N}_{E/K}(x)) \quad (x \in E)$$

En particulier des éléments de E qui sont K-conjugués ont la même valuation.

(b) *Si e (resp. f) est l'indice de ramification (resp. le degré résiduel) de l'idéal de valuation de w dans E/K, on a $e = [w(E^\times) : w(K^\times)]$ et $ef = [E:K]$.*

Démonstration. — (a) On commence par montrer la seconde partie. Soient $\widehat{E}/K$ la clôture galoisienne de E/K et $\widehat{w}$ l'unique valuation de $\widehat{E}$ prolongeant w et donc v. Pour tout $\sigma \in \mathrm{Gal}(\widehat{E}/K)$, $\widehat{w} \circ \sigma$ est une valuation de $\widehat{E}$ qui prolonge v. D'où $\widehat{w} \circ \sigma = \widehat{w}$ et $w(x) = w(\sigma(x))$ pour tout $x \in E$ tel que

$\sigma(x) \in E$. La formule explicite pour $w(x)$ résulte du fait que $\mathrm{N}_{E/K}(x) \in K$ et de $\mathrm{N}_{E/K}(x) = \prod_\sigma \tilde{\sigma}(x)$ où σ décrit l'ensemble des K-morphismes $E \to \overline{K}$ et pour chacun d'eux $\tilde{\sigma}$ désigne un élément de $\mathrm{Gal}(\widehat{E}/K)$ prolongeant σ.

(b) Si $\mathfrak{p}_v$ est l'idéal de valuation de v et $\mathfrak{P}_w$ celui de w, on a $\mathfrak{p}_v B = \mathfrak{P}_w^e$. La formule $ef = [E : K]$ est un cas particulier de la formule générale du théorème 1.5.3. La décomposition $\mathfrak{p}_v B = \mathfrak{P}_w^e$ montre aussi qu'une uniformisante de v est de valuation e pour w, d'où $e = [w(E^\times) : v(K^\times)]$. □

1.5.2.4. Complétion. — Soient E/K une extension finie séparable, v une valuation discrète de K, A son anneau de valuation et B la fermeture intégrale de A dans E. Le §1.5.2.2 s'applique. Soit $\mathfrak{p}$ l'idéal de valuation de v. L'idéal $\mathfrak{p}B$ s'écrit comme produit d'idéaux premiers de l'anneau de Dedekind B :

$$(*) \qquad \mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

On note e_i, f_i l'indice de ramification et le degré résiduel de chaque $\mathfrak{P}_i$.

Considérons par ailleurs les différents prolongements w_i de v à E. On note $\widetilde{K}$ le complété de K pour v et $\widetilde{v}$ l'unique prolongement de v à la clôture algébrique $\overline{\widetilde{K}}$ de $\widetilde{K}$ (corollaire 1.3.16). Pour chaque w_i, on note $\widetilde{E}_i$ le complété de E pour w_i et $\widetilde{w}_i$ le prolongement de w_i à $\widetilde{E}_i$.

Théorème 1.5.6. — (a) *L'ensemble des places w_i est en bijection avec l'ensemble des idéaux $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ (la correspondance est explicitée dans la preuve).*
(b) *La correspondance $\sigma \to \widetilde{v} \circ \sigma$ induit une surjection de l'ensemble des K-plongements $\sigma : E \to \overline{\widetilde{K}}$ sur l'ensemble des places $w_1, \ldots, w_g$. De plus si $w_i = \widetilde{v} \circ \sigma$ pour un K-plongement $\sigma : E \to \overline{\widetilde{K}}$, alors $\widetilde{E}_i$ peut être identifié à $\sigma(E)\widetilde{K}$ (via un isomorphisme isométrique) et la valuation $\widetilde{w}_i$ est l'unique valuation de $\widetilde{E}_i$ prolongeant $\widetilde{v}$ sur $\widetilde{K}$. Enfin deux places $\widetilde{v}\circ\sigma$ et $\widetilde{v}\circ\sigma'$ coincident sur E si et seulement si les K-plongements σ et σ' sont conjugués sur $\widetilde{K}$, c'est-à-dire, s'il existe un $\widetilde{K}$-isomorphisme entre $\widetilde{K}\sigma(E)$ et $\widetilde{K}\sigma'(E)$.*
(c) *Si $e(\widetilde{E}_i/\widetilde{K})$ et $f(\widetilde{E}_i/\widetilde{K})$ sont respectivement l'indice de ramification et le degré résiduel de l'unique idéal maximal au-dessus de l'idéal de valuation de $\widetilde{v}$ dans l'extension $\widetilde{E}_i/\widetilde{K}$, alors on a $e(\widetilde{E}_i/\widetilde{K}) = e_i$ et $f(\widetilde{E}_i/\widetilde{K}) = f_i$. En conséquence, on a $[\widetilde{E}_i : \widetilde{K}] = e_i f_i$.*

Démonstration. — (a) D'après le §1.2.2.3, pour chaque $i = 1, \ldots, g$, l'idéal $\mathfrak{P}_i$ induit une valuation discrète w_i de E ; l'anneau et l'idéal de valuation de w_i sont respectivement le localisé $B_{\mathfrak{P}_i}$, noté plus simplement B_i, et son idéal maximal $\mathfrak{P}_i B_i$. De plus w_i prolonge v en raison de l'égalité $\mathfrak{P}_i B_i \cap A = \mathfrak{p}$

($\mathfrak{P}_i B_i \cap A = \mathfrak{P}_i B_i \cap B \cap A = \mathfrak{P}_i \cap A = \mathfrak{p}$). Réciproquement à toute valuation discrète w sur E prolongeant v est associé un idéal $\mathfrak{P}_i$, à savoir $\mathfrak{P}_w \cap B$, où $\mathfrak{P}_w$ désigne l'idéal de valuation de w ; $\mathfrak{P}_w \cap B$ est un des idéaux $\mathfrak{P}_i$ car $\mathfrak{P}_w \cap B \supset \mathfrak{p}$ (théorème 1.5.3 (a)).

Ces deux correspondances sont inverses l'une de l'autre. Dans un sens, cela résulte de $\mathfrak{P}_i B_i \cap B = \mathfrak{P}_i$, $i = 1, \ldots, g$. Inversement si w est une valuation discrète sur E prolongeant v, il s'agit de voir que w et la valuation $v_{\mathfrak{P}_w \cap B}$ concident sur B (alors elles concideront sur $E = \mathrm{Frac}(B)$). Or pour $x \in B$, $w(x)$ (resp. $v_{\mathfrak{P}_w \cap B}(x)$) est le plus grand entier n tel que $x \in \mathfrak{P}_w^n$ (resp. $x \in (\mathfrak{P}_w \cap B)^n$. On voit facilement que ces deux entiers sont égaux (raisonner en utilisant une uniformisante π_w de w choisie dans $\mathfrak{P}_w \cap B$).

(b) On vérifie aisément que si $\sigma : E \to \overline{\widetilde{K}}$ est un K-plongement, alors $\widetilde{v} \circ \sigma$ est une valuation discrète sur E qui prolonge v. Réciproquement soit w une valuation de E qui prolonge v. Notons $\widetilde{E}_w$ le complété de E pour w et $\widetilde{w}$ la valuation de $\widetilde{E}_w$. On peut identifier l'adhérence de K dans E_w à $\widetilde{K}$. Le compositum $E\widetilde{K} \subset E_w$ est une extension finie de $\widetilde{K}$ et est donc un corps complet ; comme il contient E, on peut conclure que $\widetilde{E}_w = E\widetilde{K}$. De plus il existe un $\widetilde{K}$-plongement $\widetilde{\sigma} : E\widetilde{K} \to \overline{\widetilde{K}}$. D'après le théorème 1.3.15, on a $\widetilde{w} = \widetilde{v} \circ \widetilde{\sigma}$; en particulier, $\widetilde{w}$ prolonge $\widetilde{v}$ sur $\widetilde{K}$. La restriction de $\widetilde{\sigma}$ à E est le K-plongement $\sigma : E \to \overline{\widetilde{K}}$ désiré.

Il reste à établir l'équivalence concluant l'énoncé (b). La partie "réciproque" résulte du théorème 1.5.5. Pour la partie directe, donnons-nous deux K-plongements $\sigma, \sigma' : E \to \overline{\widetilde{K}}$ tels que $\widetilde{v} \circ \sigma$ et $\widetilde{v} \circ \sigma'$ coincident sur E. Soit $\lambda : \sigma'(E) \to \sigma(E)$ un K-isomorphisme. Il s'agit de montrer que λ s'étend en un $\widetilde{K}$-isomorphisme de $\sigma'(E)\widetilde{K}$ sur $\sigma(E)\widetilde{K}$. Le prolongement se fait par continuité. Plus précisément, tout élément $x \in \sigma'(E)\widetilde{K}$ s'écrit comme limite d'une suite $(\sigma'(x_n))_{n>0}$ avec $x_n \in E$. Grâce à l'hypothèse, on obtient que la suite $(\sigma(x_n))_{n>0}$ converge vers un élément, noté $\lambda(x)$, dans $\sigma(E)\widetilde{K}$. On vérifie que $\lambda(x)$ ne dépend pas de la suite $(\sigma'(x_n))_{n>0}$ et que la correspondance $x \to \lambda(x)$ induit un isomorphisme comme demandé.

(c) On sait que le complété $\widetilde{A}$ de A pour v est un anneau de valuation discrète d'idéal maximal le complété $\widetilde{\mathfrak{p}}$ de $\mathfrak{p}$ (c'est-à-dire, son adhérence dans $\widetilde{A}$), que le corps des fractions de $\widetilde{A}$ est égal à $\widetilde{K}$ et que le corps résiduel $\widetilde{A}/\widetilde{\mathfrak{p}}$ est isomorphe à $A/\mathfrak{p}$. Pour $i = 1, \ldots, g$, notons $\widetilde{B}_i$ le complété de B_i pour w_i ; c'est un anneau de valuation discrète et son idéal maximal, le complété $\widetilde{\mathfrak{P}_i B_i}$ de $\mathfrak{P}_i B_i$ est égal à $\mathfrak{P}_i \widetilde{B}_i$. Notons ensuite que pour $j \neq i$, l'adhérence $\overline{\mathfrak{P}_j B_i}$ de $\mathfrak{P}_j B_i$ dans $\widetilde{B}_i$ est l'anneau $\widetilde{B}_i$ tout entier puisque tout élément $x \in \mathfrak{P}_j \setminus \mathfrak{P}_i$ vérifie

$w_i(x) = 0$ (remarque 1.2.5) donc est inversible dans $\widetilde{B}_i$. La décomposition (*) conduit donc par passage à l'adhérence dans $\widetilde{B}_i$ à

$$(**) \qquad \mathfrak{p}\widetilde{B}_i = (\mathfrak{P}_i\widetilde{B}_i)^{e_i} \quad (i = 1, \ldots, g)$$

ce qui constitue la décomposition de l'idéal premier $\overline{\mathfrak{p}B} = \mathfrak{p}\widetilde{B}_i$ dans l'anneau $\widetilde{B}_i$. Cela fournit la conclusion $e_i = e(\widetilde{E}_i/\widetilde{K})$. Quant à $f_i = f(\widetilde{E}_i/\widetilde{K})$, elle découle de l'isomorphie entre les anneaux $\widetilde{B}_i/\mathfrak{P}_i\widetilde{B}_i$ et $B/\mathfrak{P}_i$. L'égalité $e_i f_i = [\widetilde{E}_i : \widetilde{K}]$ résulte alors du théorème 1.5.5. □

1.5.2.5. Localisation. — Soient E/K une extension finie séparable et $A \subset K$ un anneau de Dedekind. Le paragraphe §1.5.2.4 s'applique en particulier quand v est la valuation discrète $v_\mathfrak{p}$ associée à un idéal premier $\mathfrak{p}$ de A, c'est-à-dire où l'anneau noté A dans le §1.5.2.4 est le localisé $A_\mathfrak{p}$.

Posons $B = A'_E$. L'idéal $\mathfrak{p}B$ se décompose dans B sous la forme

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

avec e_i, f_i l'indice de ramification et le degré résiduel de l'idéal premier $\mathfrak{P}_i$.

Posons $S = A\backslash\mathfrak{p}$ et considérons l'anneau $S^{-1}B$ déjà introduit dans la preuve du théorème 1.5.3. Les anneaux $A_\mathfrak{p}$ et $S^{-1}B$ sont des anneaux de Dedekind ($A_\mathfrak{p}$ est de valuation discrète et $S^{-1}B$ est la clôture intégrale de $A_\mathfrak{p}$ dans E). L'anneau $A_\mathfrak{p}$ a pour seul idéal premier l'idéal $\mathfrak{p}A_\mathfrak{p}$. L'idéal $(\mathfrak{p}A_\mathfrak{p})S^{-1}B$ qu'induit ce dernier dans $S^{-1}B$ se décompose en produit d'idéaux premiers de $S^{-1}B$.

Théorème 1.5.7. — *Cette décomposition est la suivante :*

$$(\mathfrak{p}A_\mathfrak{p})S^{-1}B = \prod_{i=1}^{g} (\mathfrak{P}_i(S^{-1}B))^{e_i}$$

Pour $i = 1, \ldots, g$, $\mathfrak{P}_i(S^{-1}B)$ est un idéal premier de $S^{-1}B$, son indice de ramification et son degré résiduel dans l'extension d'anneaux $A_\mathfrak{p} \hookrightarrow S^{-1}B$ sont respectivement e_i et f_i ; c'est-à-dire, ils concident avec ceux de l'idéal $\mathfrak{P}_i$ dans l'extension $A \hookrightarrow B$.

Démonstration. — La primalité de l'idéal $\mathfrak{P}_i(S^{-1}B)$ (engendré par $\mathfrak{P}_i$ dans $S^{-1}B$, et qui vaut $S^{-1}\mathfrak{P}_i$) , $i = 1, \ldots, g$, résulte de la proposition 1.1.1. La décomposition annoncée s'obtient par la suite d'égalités

$$(\mathfrak{p}A_\mathfrak{p})S^{-1}B = \mathfrak{p}(S^{-1}B) = S^{-1}(\mathfrak{p}B) = S^{-1}\left(\prod_{i=1}^{g} \mathfrak{P}_i^{e_i}\right) = \prod_{i=1}^{g} (\mathfrak{P}_i(S^{-1}B))^{e_i}$$

L'énoncé sur les indices de ramification en découle. Quant à celui sur les degrés résiduels, il se déduit de $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq A/\mathfrak{p}$ et $S^{-1}B/\mathfrak{P}_i(S^{-1}B) \simeq B/\mathfrak{P}_i$, $i = 1, \ldots, g$. Pour le deuxième isomorphisme, on procède comme au §1.2.2.3 pour montrer que $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq A/\mathfrak{p}$. L'argument montre aussi que $B/\mathfrak{P}_i \simeq B_{\mathfrak{P}_i}/\mathfrak{P}_i B_{\mathfrak{P}_i}$ et aussi que $B_{\mathfrak{P}_i}/\mathfrak{P}_i B_{\mathfrak{P}_i} = S^{-1}B/\mathfrak{P}_i(S^{-1}B)$, $i = 1, \ldots, g$. □

Remarque 1.5.8. — En raison des théorèmes 1.5.6 et 1.5.7, il est usuel de confondre les points de vue d'idéaux (dans un anneau de Dedekind donné ou dans l'anneau de valuation de la place donnée ou dans son complété), de places et de plongements dans la terminologie. Ainsi, on dit indifféremment qu'un idéal premier ou que la place correspondante est ramifiée, et on peut ne pas préciser s'ils le sont dans l'extension de départ ou dans l'extension obtenue par localisation ou celle obtenue après complétion. On parle de la même façon du corps résiduel d'un idéal premier ou de la place associée.

1.5.2.6. Exemple d'extension non ramifiée. — On suppose que K est le corps des fractions d'un anneau de valuation discrète A, d'idéal de valuation $\mathcal{M}$ et de corps résiduel k. On se donne une extension E/K séparable de degré d.

Soit $\mathcal{P}$ un idéal maximal de l'anneau A'_E. Il est nécessairement au-dessus de l'idéal $\mathcal{M}$. On note $\overline{E}/k$ l'extension résiduelle correspondante.

Proposition 1.5.9. — *Les énoncés suivants sont équivalents :*
(i) *$\mathcal{P}$ est le seul idéal premier au-dessus de $\mathcal{M}$ et il est non ramifié,*
(ii) *L'idéal $\mathcal{M}$ est inerte dans l'extension E/K et l'extension résiduelle $\overline{E}/k$ est séparable,*
(iii) *L'extension résiduelle $\overline{E}/k$ est séparable et de degré $d = [E : K]$,*
(iv) *Il existe un élément $y \in A'_E$ dont la classe $\overline{y}$ modulo $\mathcal{P}$ est un élément primitif séparable de l'extension résiduelle $\overline{E}/k$,*
(v) *Il existe un polynôme unitaire $f \in A[Y]$ de degré d tel que E soit le corps de rupture de f (sur K) et le polynôme $\overline{f}$ obtenu par réduction modulo $\mathcal{M}$ soit irréductible dans $k[Y]$ et séparable*[8] .
(vi) *A'_E est un anneau de valuation discrète dont le corps résiduel est une extension séparable de degré d de k.*

On a alors de plus que si f est comme dans (v) *(ou plus généralement comme dans la démonstration), l'anneau A'_E est isomorphe à l'anneau $B_f = A[Y]/\langle f \rangle$ via la correspondance envoyant Y sur une racine y de f dans E. De façon équivalente on a $A'_E = A \oplus Ay \oplus \cdots Ay^{d-1}$.*

[8] On dit ici qu'un polynôme est *séparable* s'il n'a que des racines distinctes dans tout corps (de façon équivalente, dans un corps) où il est totalement décomposé.

Définition 1.5.10. — Une extension séparable E/K du corps des fractions d'un anneau de valuation discrète est dite non ramifiée si l'idéal de valuation est non ramifié dans E/K. Elle est dite non ramifiée résiduellement maximale si elle vérifie les énoncés de la proposition 1.5.9.

Par exemple, d'après la proposition 1.5.9, si $f \in A[X]$ est un polynôme tel que le polynôme $\overline{f}$ obtenu par réduction modulo $\mathcal{M}$ est irréductible dans $k[X]$ et séparable, alors le corps $K[X]/\langle f\rangle$ est une extension de K non ramifiée résiduellement maximale. Réciproquement, si E/K est une extension finie non ramifiée résiduellement maximale, alors il existe un élément primitif y de E/K entier sur A dont le polynôme minimal $f \in A[X]$ a la propriété que $\overline{f}$ est irréductible dans $k[X]$ et séparable. On donne dans le corollaire 1.5.15 des énoncés analogues pour les extensions non ramifiées.

Dans le cas où A est un anneau de valuation discrète complet, il n'existe qu'un seul idéal premier de A'_E au-dessus de $\mathcal{M}$ (théorèmes 1.3.15 (f) et 1.5.5). La condition (i) est réduite à "$\mathcal{P}$ non ramifié" et une extension E/K non ramifiée est nécessairement non ramifiée résiduellement maximale.

Démonstration de la proposition 1.5.9. — L'équivalence entre (i), (ii) et (iii) résulte des définitions et de la formule $\sum_{i=1}^{g} e_i f_i = d$ du théorème 1.5.3.

(iii) $\Rightarrow$ (iv) L'extension $\overline{E}/k$ étant séparable admet un élément primitif $\overline{y}$ (théorème 1.3.10), lequel est de degré $[\overline{E} : k] = d$ sur k et est séparable. Choisissons un élément $y \in A'_E$ dont la classe modulo l'idéal $\mathcal{P}$ vaut $\overline{y}$ et notons f le polynôme minimal de y sur K ; comme y est entier sur A et que A est intégralement clos, $f \in A[Y]$ (corollaire 1.3.11). De $f(y) = 0$ (dans A'_E), il découle que $\overline{f}(\overline{y}) = 0$ (modulo l'idéal $\mathcal{P}$). De la suite d'égalités et d'inégalités

$$d = [\overline{E} : k] = [k(\overline{y}) : k] \leq \deg(\overline{f}) = \deg(f) = [K(y) : K] \leq [E : K] = d$$

on déduit que les nombres écrits sont égaux. En particulier $[k(\overline{y}) : k] = d$.

(iv) $\Rightarrow$ (v) Notons f le polynôme minimal de y sur K. Comme ci-dessus, $f \in A[X]$ et découle de $f(y) = 0$ que $\overline{f}(\overline{y}) = 0$. Comme on suppose $[k(\overline{y}) : k] = d$, $\overline{f}$ est le polynôme minimal de $\overline{y}$ sur k ; il est donc irréductible sur k et séparable.

(v) $\Rightarrow$ (vi) D'après le corollaire 1.2.8, l'anneau $B_f = A[Y]/\langle f\rangle$ est un anneau de valuation discrète et c'est la fermeture intégrale de A dans $K[Y]/\langle f\rangle$. Le K-isomorphisme $K[Y]/\langle f\rangle \to E$ qui envoie Y sur y induit par restriction un isomorphisme entre les fermetures intégrales de A dans $K[Y]/\langle f\rangle$ et dans E, c'est-à-dire entre B_f et A'_E. Comme $B_f/\mathcal{M}B_f \simeq k[X]/\langle\overline{f}\rangle$, la séparabilité de l'extension résiduelle résulte de celle du polynôme $\overline{f}$.

(vi) ⇒ (i) L'anneau A'_E étant local, l'idéal $\mathcal{P}$ est le seul idéal maximal de A'_E. Comme l'extension résiduelle est supposée de degré d, la formule $\sum_{i=1}^{g} e_i f_i = d$ du théorème 1.5.3 donne que l'indice de ramification associé vaut 1. Comme l'extension est aussi supposée séparable, $\mathcal{P}$ est bien non ramifié. □

Corollaire 1.5.11. — *Soient E/K une extension finie du corps des fractions K d'un anneau de Dedekind A et $\mathfrak{p}$ un idéal premier non nul de A inerte et non ramifié dans E/K. Alors il existe un élément primitif $y \in A'_E$ de l'extension E/K dont le polynôme minimal soit irréductible et séparable modulo $\mathfrak{p}$.*

Démonstration. — Il suffit d'appliquer la proposition 1.5.9 à l'anneau de valuation discrète $A_{\mathfrak{p}}$ obtenu en localisant A par $\mathfrak{p}$ et à son idéal de valuation $\mathfrak{p}A_{\mathfrak{p}}$, qui, d'après le le théorème 1.5.7 est inerte et non ramifié dans l'extension E/K si $\mathfrak{p}$ l'est supposé comme idéal de A. □

Corollaire 1.5.12. — *Soient A un anneau de valuation discrète de corps résiduel k et de corps des fractions K. Soit ε/k une extension finie séparable de degré d. Alors il existe une extension E/K non ramifiée de degré d dont l'extension résiduelle soit isomorphe à ε/k.*

Démonstration. — L'extension ε/k étant séparable admet un élément primitif β. Soit $\varphi \in k[Y]$ le polynôme minimal de β sur k. Soit $f \in A[Y]$ un polynôme unitaire dont la réduction modulo l'idéal de valuation de A soit égal à φ. Posons $E = K[Y]/\langle f \rangle$. D'après la proposition 1.5.9, l'extension E/K est non ramifiée, et l'extension résiduelle associée est isomorphe à ε/k. □

1.5.3. Discriminant et ramification. — Les hypothèses sont celles du §1.5.2 : A est un anneau de Dedekind, $K = \mathrm{Frac}(A)$, E/K est une extension séparable de degré d et $B = A'_E$.

Définition 1.5.13. — On appelle idéal discriminant de B sur A l'idéal noté $\mathcal{D}_{B/A}$ engendré par les discriminants $\Delta(x_1, \ldots, x_d)$ (définition 1.3.13) des bases $(x_1, \ldots, x_d)$ de E sur K contenues dans B.

Si $(x_1, \ldots, x_d)$ est une base de E sur K contenue dans B, alors $\Delta(x_1, \ldots, x_d)$ est un élément de A non nul (corollaire 1.3.11 et théorème 1.3.12). L'idéal discriminant $\mathcal{D}_{B/A}$ est donc un idéal entier de A non nul.

Quand B est un A-module libre (par exemple si A est principal), l'idéal discriminant $\mathcal{D}_{B/A}$ coincide avec l'idéal $\mathcal{D}_{B/A}$ du §1.3.5.2 engendré par le discriminant $\Delta(e_1, \ldots, e_d)$ de toute base $(e_1, \ldots, e_d)$ de B sur A car pour toute base $(x_1, \ldots, x_n)$ de E sur K contenue dans B, on a $\Delta(x_1, \ldots, x_n) =$

$\det(a_{ij})^2\Delta(e_1,\dots,e_d)$, où $(a_{ij})_{i,j}$ est la matrice des coordonnées des x_i dans la base $(e_1,\dots,e_d)$.

Théorème 1.5.14. — *Un idéal premier $\mathfrak{p}$ de A se ramifie dans B si et seulement s'il contient l'idéal discriminant $\mathcal{D}_{B/A}$. Les idéaux premiers de A qui se ramifient dans B sont en nombre fini.*

Démonstration. — Notons $\varepsilon = B/\mathfrak{p}B$ et $\kappa = A/\mathfrak{p}$. D'après le théorème 1.5.3, l'anneau ε est isomorphe à l'anneau produit $\prod_{i=1}^g B/\mathfrak{P}_i^{e_i}$. Nous allons montrer tout d'abord que la condition "$\mathfrak{p}$ ramifié" équivaut à la nullité de l'idéal discriminant (au sens du §1.3.5.2) de la κ-algèbre ε.

Supposons que les indices de ramification $e_1,\dots,e_g$ vaillent 1. Alors ε est isomorphe au produit $Q = \prod_{i=1}^g Q_i$ des corps $Q_i = B/\mathfrak{P}_i$. On vérifie que

$$\mathcal{D}_{Q/\kappa} = \prod_{i=1}^n \mathcal{D}_{Q_i/\kappa}$$

Pour cela on se ramène par récurrence au cas $n = 2$. A partir d'une κ-base $(x_1,\dots,x_r)$ de Q_1 et d'une κ-base $(y_1,\dots,y_s)$ de Q_2, on forme la κ-base $(x_1,\dots,x_r,y_1,\dots,y_s)$ de $Q_1\times Q_2$. De $x_iy_j = 0$, il résulte que le déterminant $\Delta(x_1,\dots,x_r,y_1,\dots,y_s)$ à calculer est un déterminant à 4 blocs dont les blocs non diagonaux sont nuls et donc qu'il est égal au produit des deux déterminants des blocs diagonaux, c'est-à-dire $\Delta(x_1,\dots,x_r)\Delta(y_1,\dots,y_s)$. Si maintenant $\mathfrak{p}$ est non ramifié, alors en plus de ce qui précède, les extensions résiduelles Q_i/κ sont séparables (voir définition 1.5.2). On a donc $\mathcal{D}_{Q_i/\kappa} \neq \{0\}$ (§1.3.5.2), $i = 1,\dots,n$. D'où $\mathcal{D}_{Q/\kappa} = \mathcal{D}_{\varepsilon/\kappa} \neq \{0\}$.

Inversement, supposons $\mathfrak{p}$ ramifié. Si un indice de ramification e_i est ≥ 2, alors il existe dans ε un élément nilpotent $x \neq 0$. La κ-algèbre ε est de dimension d (théorème 1.5.3). Formons une κ-base $\{x_1,\dots,x_d\}$ de ε avec $x_1 = x$. La nilpotence de x_1 entraîne celle des endomorphismes de multiplication par chacun des éléments x_1x_i, $i = 1,\dots,d$. Ainsi la trace de ces endomorphismes est nulle et il y a une ligne de 0 dans le déterminant de la matrice $(\mathrm{Tr}_{\varepsilon/\kappa}(x_ix_j))_{i,j}$. D'où $\Delta(x_1,\dots,x_n) = 0$ et $\mathcal{D}_{\varepsilon/\kappa} = \{0\}$. Si $e_1 = \cdots = e_g = 1$, alors "$\mathfrak{p}$ ramifié" signifie qu'il existe $i \in \{1,\dots,g\}$ tel que l'extension résiduelle Q_i/κ soit inséparable. Notons Q_i^{s}/κ l'extension séparable maximale contenue dans Q_i. Complétons une Q_i^{s}-base $\{x_1,\dots,x_r\}$ de Q_i en une κ-base $\{x_1,\dots,x_r\}\cup\{y_1,\dots,y_s\}$ de Q_i^{s}. Comme $Q_i^{\mathrm{s}} \neq Q_i$, au moins un des x_i, disons x_1, n'est pas dans Q_i^{s}. Les éléments x_1x_i qui ne sont pas dans Q_i^{s}, sont inséparables (par maximalité de Q_i^{s}) et les éléments x_1y_j ($j = 1,\dots,s$) le sont également (car sinon $x_1 \in Q_i^{\mathrm{s}}$). Tous ces éléments sont donc de trace nulle

(leurs polynômes minimaux sur κ sont de la forme $f(X^{p^m})$ avec $m \geq 1$ (corollaire 1.3.9) et ont donc un terme linéaire nul). Quant aux éléments $x_1 x_i$ qui sont dans Q_i^{s}, leur trace, relative à Q_i/κ est un multiple de $[Q_i : \kappa(x_1 x_i)]$ et donc aussi de $[Q_i : Q_i^{\mathrm{s}}]$, qui est nul puisque la caractéristique $p > 0$ de κ divise $[Q_i : Q_i^{\mathrm{s}}]$ (corollaire 1.3.9). On obtient finalement comme ci-dessus une ligne de 0 dans le déterminant qui définit le discriminant $\mathcal{D}_{Q_i/\kappa}$. Joint à la formule pour $\mathcal{D}_{Q/\kappa}$ établie plus haut, cela conduit à $\mathcal{D}_{\varepsilon/\kappa} = \{0\}$.

Pour la suite, on va, comme dans la preuve du théorème 1.5.3, localiser A pour se ramener au cas où c'est un anneau principal. De façon précise, soit $S = A \setminus \mathfrak{p}$. L'anneau $A_{\mathfrak{p}}$ est un anneau de valuation discrète, l'anneau $B' = S^{-1}B$ est la clôture intégrale de $A_{\mathfrak{p}}$ dans E, B' est un $A_{\mathfrak{p}}$-module libre de rang $d = [E : K]$, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = A/\mathfrak{p}$ et $B'/\mathfrak{p}B' = B/\mathfrak{p}B$.

Fixons une base $(e_1, \ldots, e_d)$ de B' sur $A_{\mathfrak{p}}$. L'étape suivante est de montrer que la condition $\mathcal{D}_{\varepsilon/\kappa} \neq \{0\}$ équivaut à $\Delta(e_1, \ldots, e_d) \notin \mathfrak{p}A_{\mathfrak{p}}$. On voit aisément que les classes $\bar{e}_1, \ldots, \bar{e}_d$ de $e_1, \ldots, e_d$ modulo $\mathfrak{p}B'$ constituent une base de $B'/\mathfrak{p}B'$ sur $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. D'autre part, la réduction modulo $\mathfrak{p}B'$ étant un homomorphisme d'anneaux, on a $\Delta(\bar{e}_1, \ldots, \bar{e}_d) = \overline{\Delta(e_1, \ldots, e_d)}$. L'équivalence souhaitée découle de ce que $\Delta(\bar{e}_1, \ldots, \bar{e}_d)$ est un générateur de l'idéal $\mathcal{D}_{\varepsilon/\kappa}$.

Finalement on va montrer que $\Delta(e_1, \ldots, e_d) \in \mathfrak{p}A_{\mathfrak{p}}$ si et seulement si $\mathfrak{p} \supset \mathcal{D}_{B/A}$. Soit $(x_1, \ldots, x_d)$ une base de E/K contenue dans B. On a $x_i = \sum_{i=1}^{d} a_{ij} e_j$ avec $a_{ij} \in A_{\mathfrak{p}}$. Un calcul déjà fait (§1.3.5.2) donne $\Delta(x_1, \ldots, x_d) = \det(a_{ij})^2 \, \Delta(e_1, \ldots, e_d)$. Si on suppose $\Delta(e_1, \ldots, e_d) \in \mathfrak{p}A_{\mathfrak{p}}$ on obtient alors $\Delta(x_1, \ldots, x_d) \in \mathfrak{p}A_{\mathfrak{p}} \cap A = \mathfrak{p}$ et donc $\mathfrak{p} \supset \mathcal{D}_{B/A}$. Pour la réciproque, écrivons $e_i = y_i/s$ avec $y_i \in B$ et $s \in S$, $i = 1, \ldots, d$. On obtient $\Delta(e_1, \ldots, e_d) = s^{-2d} \Delta(y_1, \ldots, y_d) \in \mathcal{D}_{B/A} A_{\mathfrak{p}}$ et donc $\Delta(e_1, \ldots, e_d) \in \mathfrak{p}A_{\mathfrak{p}}$ si on a supposé $\mathfrak{p} \supset \mathcal{D}_{B/A}$.

La seconde partie de l'énoncé, c'est-à-dire, la finitude des idéaux premiers de A ramifiés dans B, résulte de la première partie, et de la remarque 1.2.5. □

Corollaire 1.5.15. — *Soient A est un anneau de Dedekind, $K = \mathrm{Frac}(A)$, y un élément de $\overline{K}$ entier sur A et $\mathfrak{p}$ un idéal premier non nul de A. Soit $P \in A[Y]$ le polynôme minimal de y sur K. Si le polynôme obtenu par réduction modulo $\mathfrak{p}$ n'a que des racines simples (dans $\overline{A/\mathfrak{p}}$), alors l'extension $K(y)/K$ est non ramifiée au-dessus de $\mathfrak{p}$.*

Démonstration. — Sous l'hypothèse de l'énoncé, le discriminant Δ_P de P est non nul modulo $\mathfrak{p}$, ou, de façon équivalente $\Delta_P \notin \mathfrak{p}$. Or Δ_P est égal au signe près au discriminant $\Delta(1, y, \ldots, y^{d-1})$ de la base $(1, y, \ldots, y^{d-1})$ de $K(y)$ sur K (remarque 1.3.14) ; il est donc dans l'idéal discriminant de $\mathcal{D}_{B/A}$ de l'extension

$K(y)/K$ (ici $B = A'_{K(y)}$). On a donc $\mathcal{D}_{B/A} \not\subset \mathfrak{p}$, c'est-à-dire, $\mathfrak{p}$ est non ramifié dans l'extension $K(y)/K$, d'après le théoréme 1.5.14. □

Il existe une réciproque utile au corollaire 1.5.15.

Corollaire 1.5.16. — *Soient E/K une extension finie du corps des fractions K d'un anneau de Dedekind A et $\mathfrak{p}$ un idéal premier non nul de A non ramifié dans E/K. On suppose que le corps résiduel $A/\mathfrak{p}$ est infini. Alors il existe un élément primitif $y \in A'_E$ de l'extension E/K dont le polynôme minimal est séparable modulo $\mathfrak{p}$.*

Démonstration. — L'idéal $\mathfrak{p}$ étant non ramifié dans E/K, la décomposition de l'idéal $\mathfrak{p}A'_E$ dans A'_E est de la forme $\mathfrak{p}A'_E = \prod_{i=1}^{g} \mathfrak{P}_i$ où $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ sont des idéaux premiers non nuls distincts de A'_E. La non ramification de $\mathfrak{p}$ entraîne aussi que les extensions résiduelles correspondantes sont séparables. Notons $\overline{c_i}$ un élément primitif de l'extension résiduelle correspondant à $\mathfrak{P}_i$, $i = 1, \ldots, g$. Comme le corps $A/\mathfrak{p}$ est infini, on peut grâce au théorème 1.3.10 choisir $\overline{c_1}, \ldots, \overline{c_g}$ de façon qu'ils ne soient pas conjugués sur $A/\mathfrak{p}$. D'après le lemme chinois (lemme 1.1.6), il existe $y \in A'_E$ tel que la classe de y modulo $\mathfrak{P}_i$ soit $\overline{c_i}$ pour chaque $i = 1, \ldots, g$. Soit P le polynôme minimal de y sur K ; $P \in A[Y]$. Soit $\overline{P}$ le polynôme obtenu à partir de P par réduction modulo $\mathfrak{p}$. De $P(y) = 0$ découle que $\overline{P}(\overline{c_i}) = 0$, $i = 1, \ldots, g$. Il en résulte que $\overline{P}$ est divisible dans $A/\mathfrak{p}\,[Y]$ par chacun des polynômes minimaux $h_1, \ldots, h_g$ de $\overline{c_1}, \ldots, \overline{c_g}$, et donc par leur produit $h_1 \cdots h_g$ puisque $\overline{c_1}, \ldots, \overline{c_g}$ ne sont pas conjugués sur $A/\mathfrak{p}$. Si on note f_i le degré résiduel de $\mathfrak{P}_i$, $i = 1, \ldots, g$, on obtient

$$[E : K] = \sum_{i=1}^{g} f_i = \sum_{i=1}^{g} \deg(h_i) \leq \deg(\overline{P}) = \deg(P) = [K(y) : K] \leq [E : K]$$

et on peut conclure que $E = K(y)$ et que $\overline{P} = \prod_{i=1}^{g} h_i$. L'élément y satisfait la conclusion de l'énoncé. □

1.5.4. Groupes d'inertie et groupes de décomposition. — On se place dans la situation suivante : A est un anneau noethérien, intégralement clos, de corps des fractions K et B est la clôture intégrale de A dans E.

On suppose ici de plus que E/K est une extension galoisienne.

Soit $\mathcal{P}$ un idéal maximal de B. Le sous-groupe de $G = \mathrm{Gal}(E/K)$ formé des automorphismes σ tels que $\sigma(\mathcal{P}) = \mathcal{P}$ s'appelle le *groupe de décomposition* de $\mathcal{P}$ dans E/K et on le note $D_{\mathcal{P}}$. On a un homomorphisme naturel

$$\varepsilon : D_{\mathcal{P}} \to \mathrm{Aut}(\bar{E}/\bar{K})$$

Le noyau $\ker(\varepsilon)$ est appelé *groupe d'inertie* de $\mathcal{P}$ et noté $I_{\mathcal{P}}$.

1.5.4.1. Groupe de Galois d'une extension résiduelle. —

Proposition 1.5.17. — *L'extension résiduelle $\bar{E}/\bar{K}$ est normale et l'homomorphisme ε induit un isomorphisme de $D_{\mathcal{P}}/I_{\mathcal{P}}$ sur* $\mathrm{Aut}(\bar{E}/\bar{K})$.

Démonstration. — Soient $\bar{a} \in \bar{E}$ et $a \in B$ un représentant de $\bar{a}$. Considérons le polynôme $P(X) = \prod_{\sigma\in G}(X - \sigma(a))$; il est à coefficients dans A et unitaire. Le polynôme réduit $\bar{P}(X) \in \bar{K}[X]$ annule $\bar{a}$ et ses $\bar{K}$-conjugués. Or les racines de $\bar{P}$ sont les éléments $\overline{\sigma(a)}$ ($\sigma \in G$), qui sont dans $\bar{E}$. L'extension $\bar{E}/\bar{K}$ est donc normale.

Notons $\bar{E}^{\mathrm{s}}$ la plus grande extension séparable de $\bar{K}$ contenue dans $\bar{E}$ et montrons préalablement que $\mathrm{Aut}(\bar{E}/\bar{K}) \simeq \mathrm{Aut}(\bar{E}^{\mathrm{s}}/\bar{K})$. La restriction naturelle est surjective (§1.3.2) Voyons qu'elle est également injective. Pour x arbitraire dans $\bar{E}$, soit $m \geq 0$ le plus petit entier tel que $x^{p^m} \in \bar{E}^{\mathrm{s}}$ (corollaire 1.3.9). Soit $\sigma \in \mathrm{Aut}(\bar{E}/\bar{K})$ tel que $\sigma = \mathrm{Id}$ sur $\bar{E}^{\mathrm{s}}$. On a $\sigma(x^{p^m}) = x^{p^m}$ ce qui conduit à $(\sigma(x) - x)^{p^m} = 0$. D'où $\sigma = \mathrm{Id}$ sur $\bar{E}$.

Montrer que ε est surjective revient à montrer que $\varepsilon(D_{\mathcal{P}}) \simeq \mathrm{Aut}(\bar{E}^{s}/\bar{K})$. Soit $\bar{a} \neq \bar{0}$ un élément primitif de l'extension $\bar{E}^{\mathrm{s}}/\bar{K}$. D'après le corollaire 1.1.7 du lemme "chinois", il existe un représentant $a \in B$ de $\bar{a}$ tel que a appartienne à tous les idéaux maximaux $\sigma(\mathcal{P})$ pour $\sigma \notin D_{\mathcal{P}}$. Comme ci-dessus, posons $P(X) = \prod_{\sigma\in G}(X - \sigma(a))$. Si $\sigma \notin D_{\mathcal{P}}$, alors $a \in \sigma^{-1}(\mathcal{P})$ et donc $\sigma(a) \in \sigma(\sigma^{-1}(\mathcal{P}) \subset \mathcal{P}$. Les seules racines non nulles du polynôme réduit $\bar{P}(X) \in \bar{K}[X]$ sont donc les $\overline{\sigma(a)}$ où $\sigma \in D_{\mathcal{P}}$; en particulier, les $\bar{K}$-conjugués de $\bar{a}$ sont de la forme $\overline{\sigma(a)} = \varepsilon(\sigma)(\bar{a})$ avec $\sigma \in D_{\mathcal{P}}$. La primitivité de $\bar{a}$ permet de conclure que tout $\overline{K}$-automorphisme de $\bar{E}_{\mathrm{s}}$ est de la forme $\varepsilon(\sigma)$ avec $\sigma \in D_{\mathcal{P}}$. □

1.5.4.2. Propriétés galoisiennes. —

Proposition 1.5.18. — *Le groupe* $\mathrm{Gal}(E/K)$ *opère transitivement sur l'ensemble des idéaux maximaux de B au-dessus d'un idéal maximal $\mathfrak{p}$ de A donné. En conséquence, les groupes de décomposition (resp. les groupes d'inertie) au-dessus de $\mathfrak{p}$ sont conjugués dans* $\mathrm{Gal}(E/K)$.

Démonstration. — Soit $\mathcal{P}$ un idéal maximal de B au-dessus d'un idéal maximal $\mathfrak{p}$ de A. Supposons qu'il existe un idéal maximal $\mathcal{P}'$ de B au-dessus de $\mathfrak{p}$ et distinct des $\sigma(\mathcal{P})$, $\sigma \in \mathrm{Gal}(E/K)$. D'après le corollaire 1.1.7 du lemme "chinois", il existe $x \in \mathcal{P}'$ tel que $x \notin \sigma(\mathcal{P})$, pour tout $\sigma \in \mathrm{Gal}(E/K)$. Posons $a = \mathrm{N}_{E/K}(x)$. On a $a \in A$, et $a = \prod_{\sigma\in\mathrm{Gal}(E/K)} \sigma(x)$ d'où $a \in \mathcal{P}'$ et

$a \notin \mathcal{P}$ (sinon il existe $\sigma \in \mathrm{Gal}(E/K)$ tel que $\sigma(x) \in \mathcal{P}$). Cela est absurde puisque $\mathcal{P} \cap A = \mathcal{P}' \cap A$. La dernière affirmation de l'énoncé se vérifie sans difficultés. □

La proposition suivante est utile.

Proposition 1.5.19. — *Soient E/K et A comme ci-dessus, H un sous-groupe distingué de $\mathrm{Gal}(E/K)$ et L le sous-corps de E fixé par H. Si $\mathcal{Q}$ est un idéal premier non nul de A'_E, $\mathcal{P}$ sa restriction à A'_L, alors, si $\mathrm{Gal}(L/K)$ est identifié à $\mathrm{Gal}(L/K)/H$, on a $D_{\mathcal{P}} = D_{\mathcal{Q}}/H$ et $I_{\mathcal{P}} = I_{\mathcal{Q}}/H$.*

Démonstration. — Montrons que, pour $\sigma \in \mathrm{Gal}(E/K)$, on a $(\sigma|_L)(\mathcal{P}) = \mathcal{P}$ si et seulement s'il existe $h \in H$ tel que $h^{-1}\sigma(\mathcal{Q}) = \mathcal{Q}$ (cela donnera $D_{\mathcal{P}} = D_{\mathcal{Q}}/H$) et qu'alors, $\sigma|_L \in I_{\mathcal{P}}$ si et seulement s'il existe $h' \in H$ tel que $(h')^{-1}\sigma \in I_{\mathcal{Q}}$ (ce qui donnera $I_{\mathcal{P}} = I_{\mathcal{Q}}/H$).

Si $(\sigma|_L)(\mathcal{P}) = \mathcal{P}$, alors $\sigma(\mathcal{Q})$ et $\mathcal{Q}$ sont deux idéaux de A'_E au-dessus de l'idéal $\mathcal{P} \subset A'_L$. D'après la proposition 1.5.18, il existe $h \in H$ tel que $\sigma(\mathcal{Q}) = h(\mathcal{Q})$, c'est-à-dire $h^{-1}\sigma(\mathcal{Q}) = \mathcal{Q}$.

Pour la partie de l'énoncé sur l'inertie, on utilise les morphismes ε introduits au début du §1.5.4. Notons $\varepsilon_{E/K} : D_{\mathcal{Q}} \to \mathrm{Aut}(\bar{E}/\bar{K})$, $\varepsilon_{L/K} : D_{\mathcal{P}} \to \mathrm{Aut}(\bar{L}/\bar{K})$ et $\varepsilon_{E/L} : D_{\mathcal{Q},E/L} \to \mathrm{Aut}(\bar{E}/\bar{L})$ ceux qui correspondent aux trois situations $(E/K, \mathcal{Q})$, $(L/K, \mathcal{P})$ et $(E/L, \mathcal{Q})$.

Sous l'hypothèse $(\sigma|_L)(\mathcal{P}) = \mathcal{P}$, on peut, quitte à changer σ en $h^{-1}\sigma$ pour l'élément h ci-dessus, supposer que $\sigma \in D_{\mathcal{Q}}$. Si de plus $\sigma|_L \in I_{\mathcal{P}}$, alors $\varepsilon_{E/K}(\sigma) \in \mathrm{Aut}(\bar{E}/\bar{L})$ et est donc de la forme $\varepsilon_{E/L}(h')$ avec h' dans le sous-groupe $D_{\mathcal{Q},E/L} \subset H$. On a alors que $(h')^{-1}\sigma \in I_{\mathcal{Q}}$.

Réciproquement, si $h^{-1}\sigma(\mathcal{Q}) = \mathcal{Q}$ pour un élément $h \in H$, on a alors $(h^{-1}\sigma)|_L(\mathcal{P}) = \sigma|_L(\mathcal{P}) = \mathcal{P}$. Et si $(h')^{-1}\sigma \in I_{\mathcal{Q}}$ pour un élément $h' \in H$, alors $\varepsilon_{E/K}((h')^{-1}\sigma) = \mathrm{Id}_{\bar{E}}$. On vérifie que la restriction à L du membre de gauche vaut $\varepsilon_{L/K}(((h')^{-1}\sigma)|_L) = \varepsilon_{L/K}(\sigma|_L)$ pour conclure que $\varepsilon_{L/K}(\sigma|_L) = \mathrm{Id}_{\bar{L}}$, c'est-à-dire que $\sigma|_L \in I_{\mathcal{P}}$. □

1.5.4.3. Conséquences. —

Corollaire 1.5.20. — *Si A est un anneau de Dedekind, les indices de ramification (resp. les degrés résiduels) des idéaux premiers $\mathcal{P}$ de B au-dessus d'un idéal premier $\mathfrak{p}$ non nul de A sont tous égaux à un entier e (resp. un entier f). De plus le groupe de décomposition d'un idéal premier $\mathcal{P}$ au-dessus de $\mathfrak{p}$ est d'ordre ef et, si l'extension résiduelle est séparable, son groupe d'inertie est d'ordre e.*

Démonstration. — La première partie résulte immédiatement de la proposition 1.5.18. Si g est le nombre d'idéaux premiers distincts de B au-dessus de $\mathfrak{p}$, alors par la définition du groupe de décomposition $D_{\mathcal{P}}$, on a $[E:K] = g|D_{\mathcal{P}}|$. L'égalité $|D_{\mathcal{P}}| = ef$ résulte alors de $[E:K] = efg$ (théorème 1.5.3). Enfin, si l'extension résiduelle est séparable, par le théorème 1.5.17, on a $|D_{\mathcal{P}}| = |I_{\mathcal{P}}|f$. D'où $|I_{\mathcal{P}}| = e$. □

Le corollaire suivant complète le théorème 1.5.6.

Soient v une valuation discrète de K, $\widetilde{K}$ le complété de K, $\mathfrak{p}$ l'idéal de valuation de v et $\mathfrak{p}B = (\prod_{i=1}^{g} \mathcal{P}_i)^e$ la décomposition de l'idéal $\mathfrak{p}$ dans l'extension E/K. Notons $w_1, \ldots, w_g$ les prolongements de la valuation v à E et $(\widetilde{E}_1, \widetilde{w}_1), \ldots, (\widetilde{E}_g, \widetilde{w}_g)$ les complétés correspondants de E.

Corollaire 1.5.21. — *L'extension $\widetilde{E}_i/\widetilde{K}$ est galoisienne et son groupe de Galois est le groupe de décomposition $D_{\mathcal{P}_i}$ de l'idéal $\mathcal{P}_i$ ($i = 1, \ldots, g$).*

Démonstration. — Que l'extension $\widetilde{E}_i/\widetilde{K}$ soit galoisienne découle de ce que $\widetilde{E}_i$ est $\widetilde{K}$-isomorphe à $E\widetilde{K}$ (théorème 1.5.6). Tout élément $\sigma \in D_{\mathcal{P}_i}$ se prolonge par continuité en un $\widetilde{K}$-automorphisme de $\widetilde{E}_i$: on procède comme dans la preuve du théorème 1.5.6 (b)), juste voir ici que pour $\sigma \in D_{\mathcal{P}_i}$, les valuations $\widetilde{w}_i$ et $\widetilde{w}_i \circ \sigma$ coincident sur $\widetilde{E}_i$. On obtient un morphisme $D_{\mathcal{P}_i} \to \mathrm{Gal}(\widetilde{E}_i/\widetilde{K})$, qui est injectif. Comme les deux groupes ont même ordre, à savoir ef (théorème 1.5.6 et corollaire 1.5.20), c'est un isomorphisme. □

1.5.4.4. Idéaux premiers ramifiés. — On revient aux hypothèses du §1.5.4.

On dit que $\mathcal{P}$ est *ramifié* (dans l'extension E/K) si le groupe d'inertie $\mathcal{I}_{\mathcal{P}}$ n'est pas trivial. Dans le cas où A est un anneau de Dedekind et si l'extension résiduelle associée à $\mathcal{P}$ est séparable, cela est équivalent à la définition 1.5.2 (d'après le corollaire 1.5.20).

Proposition 1.5.22. — *Il existe un idéal non nul $\mathcal{R} \subset B$ tel que les idéaux premiers $\mathcal{P}$ de B ramifiés dans l'extension E/K sont exactement ceux qui contiennent $\mathcal{R}$.*

Démonstration. — Pour tout $\sigma \in G = \mathrm{Gal}(E/K)$, notons $\mathcal{R}_\sigma$ l'idéal de B engendré par $(\sigma - \mathrm{Id})(B)$ et posons $\mathcal{R} = \prod_{\sigma \neq 1} \mathcal{R}_\sigma$. Les K-sous-espaces vectoriels $\mathrm{Ker}(\sigma - \mathrm{Id}) \subset E$ (avec $\sigma \neq 1$) sont de réunion strictement contenue dans E. En effet, si K est fini, l'extension est cyclique et il existe un élément primitif de E/K, lequel n'est pas dans la réunion considérée. Si K est infini, E ne peut être réunion finie de sous-espaces propres. Il existe donc un élément $b \in K$,

qu'on peut supposer dans B tel que $\sigma(b) - b \neq 0$ pour tout $\sigma \in G$, $\sigma \neq 1$. Il en découle que l'idéal $\mathcal{R}$ est non nul.

Soit $\mathcal{P}$ un idéal premier de B ramifié. Par définition, il existe $\sigma \neq 1$ tel que $\sigma(x) - x \in \mathcal{P}$ pour tout $x \in B$, c'est-à-dire, $\mathcal{R}_\sigma \subset \mathcal{P}$. *A fortiori* $\mathcal{R} \subset \mathcal{P}$. Réciproquement, si $\mathcal{R} \subset \mathcal{P}$, alors, comme $\mathcal{P}$ est premier, il existe $\sigma \in G$, $\sigma \neq 1$ tel que $\mathcal{R}_\sigma \subset \mathcal{P}$, c'est-à-dire, $\mathcal{P}$ est ramifié. □

1.6. Relèvement dans les extensions intégrales

1.6.1. Relèvement des idéaux premiers. —

***Théorème 1.6.1* (going-up theorem).** — *Soit B un anneau entier sur un sous-anneau A.*
(a) *Si $\mathfrak{p}$ est un idéal premier de A, alors il existe un idéal premier $\mathcal{P}$ de B tel que $\mathcal{P} \cap A = \mathfrak{p}$.*
(b) *Soit $\mathcal{B}$ un idéal de B. Pour tout idéal premier $\mathfrak{p}$ de A tel que $\mathcal{B} \cap A \subset \mathfrak{p}$, il existe un idéal premier $\mathcal{P}$ de B tel que $\mathcal{B} \subset \mathcal{P}$ et $\mathcal{P} \cap A = \mathfrak{p}$.*
(c) *Si de plus B est un A-module de type fini, alors l'ensemble des idéaux premiers $\mathcal{P}$ de B au-dessus d'un idéal premier $\mathfrak{p}$ de A (i.e., tels que $\mathcal{P} \cap A = \mathfrak{p}$) est fini.*

Deux autres propriétés du relèvement des idéaux premiers dans une extension intégrale viendront compléter le théorème 1.6.1 (voir théorème 1.6.3).

En termes géométriques, le théorème correspond au cas affine (et donc local) de l'énoncé suivant : *Si $f : X \to Y$ est un morphisme fini entre deux schémas X et Y, alors f est surjectif, quasi-fini et fermé* [**Har77**, Ex.3.5 p.91].

Démonstration du théorème 1.6.1. — (a) Pour $\mathfrak{p}$ idéal premier de A, soit S la partie multiplicative $S = A \setminus \mathfrak{p}$. L'anneau $S^{-1}B$ est entier sur $S^{-1}A = A_\mathfrak{p}$. On a le diagramme commutatif suivant

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ A_\mathfrak{p} & \longrightarrow & S^{-1}B \end{array}$$

où les flèches sont les morphismes naturels. Soit $\mathcal{Q}$ un idéal maximal de $S^{-1}B$ (l'existence de $\mathcal{Q}$ est une conséquence standard du Lemme de Zorn). D'après le (b) du lemme 1.1.21, $\mathcal{Q} \cap A_\mathfrak{p}$ est un idéal maximal de l'anneau local A_p ; on a donc $\mathcal{Q} \cap A_\mathfrak{p} = S^{-1}\mathfrak{p}$. Posons $\mathcal{P} = j^{-1}(\mathcal{Q})$. Alors $\mathcal{P}$ est premier et on a : $\mathcal{P} \cap A = i^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$.

(b) La situation est résumée par le diagramme commutatif ci-dessous (où les flèches sont les morphismes naturels). L'anneau $B/\mathcal{B}$ est entier sur l'anneau $A/(\mathcal{B}\cap A)$. Soit $\mathfrak{p}$ un idéal premier de A tel que $\mathcal{B}\cap A\subset\mathfrak{p}$. L'image $r(\mathfrak{p})$ est un idéal premier de $A/(\mathcal{B}\cap A)$. D'après le (a), il existe un idéal premier $\overline{\mathcal{P}}$ de $B/\mathcal{B}$ tel que $\overline{\mathcal{P}}\cap(A/(\mathcal{B}\cap A))=r(\mathfrak{p})$. Soit $\mathcal{P}=s^{-1}(\overline{\mathcal{P}})$. C'est un idéal premier de B qui contient $\mathcal{B}$ et $\mathcal{P}\cap A=r^{-1}(r(\mathfrak{p}))=\mathfrak{p}$.

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle s} \\ A/(\mathcal{B}\cap A) & \longrightarrow & B/\mathcal{B} \end{array}$$

(c) Notons $\mathfrak{p}B$ l'idéal de B engendré par l'idéal premier $\mathfrak{p}$ donné de A. On a le diagramme commutatif suivant

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & B \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \beta} \\ A/\mathfrak{p} & \longrightarrow & B/\mathfrak{p}B \end{array}$$

où les flèches sont les morphismes naturels. Les idéaux premiers $\mathcal{P}$ de B tels que $\mathcal{P}\cap A=\mathfrak{p}$ sont parmi ceux qui contiennent l'idéal $\mathfrak{p}B$. Ces derniers sont en correspondance bijective avec les idéaux premiers de l'anneau quotient $B/\mathfrak{p}B$ (par l'application $\mathcal{P}\to\beta(\mathcal{P})=\mathcal{P}/\mathfrak{p}B$). De plus, si $\mathcal{P}\cap A=\mathfrak{p}$, alors $j^{-1}(\beta(\mathcal{P}))=\{0\}$. En effet, soient $a\in A$ tel que $\alpha(a)\in j^{-1}(\beta(\mathcal{P}))$, c'est-à-dire, $(j\circ\alpha)(a)=\beta(\pi)$ avec $\pi\in\mathcal{P}$. On a donc aussi $(\beta\circ i)(a)=\beta(\pi)$. D'où $i(a)=\pi+b$ avec $b\in\mathfrak{p}B$. En particulier $i(a)\in\mathcal{P}$, c'est-à-dire, $a\in i^{-1}(\mathcal{P})=\mathfrak{p}$ et donc $\alpha(a)=0$.

Il suffit donc de montrer qu'il n'y a qu'un nombre fini d'idéaux premiers $\overline{\mathcal{P}}$ de $B/\mathfrak{p}B$ tels que $j^{-1}(\overline{\mathcal{P}})=\{0\}$. Si on note k le corps des fractions de $A/\mathfrak{p}$, ces derniers idéaux correspondent à des idéaux premiers de l'anneau $B/\mathfrak{p}B\otimes_{A/\mathfrak{p}}k$. Pour le voir, le point essentiel est le suivant :

Notons $t : B/\mathfrak{p}B\to B/\mathfrak{p}B\otimes_{A/\mathfrak{p}}k$ l'application canonique. Si $\overline{\mathcal{P}}$ est un idéal premier de $B/\mathfrak{p}B$ tels que $j^{-1}(\overline{\mathcal{P}})=\{0\}$ et J un idéal quelconque de $B/\mathfrak{p}B$ et si les idéaux engendrés par $t(\overline{\mathcal{P}})$ et $t(J)$ dans $B/\mathfrak{p}B\otimes_{A/\mathfrak{p}}k$, notés respectivement $\overline{\mathcal{P}}^*$ et J^*, vérifient $J^*\subset\overline{\mathcal{P}}^*$, alors nécessairement $J\subset\overline{\mathcal{P}}$.

En effet, soit $x\in J$. La condition $J^*\subset\overline{\mathcal{P}}^*$ donne qu'il existe $d\in A/\mathfrak{p}$ tel que $j(d)x\in\overline{\mathcal{P}}$ et $d\neq 0$. Comme $\overline{\mathcal{P}}$ est premier et que $j(d)\notin\overline{\mathcal{P}}$ (puisque $j^{-1}(\overline{\mathcal{P}})=\{0\}$), nécessairement $x\in\overline{\mathcal{P}}$.

Cela montre en particulier que $\overline{\mathcal{P}}^*$ est un idéal propre de $B/\mathfrak{p}B \otimes_{A/\mathfrak{p}} k$; la condition $xy \in \overline{\mathcal{P}}^* \Rightarrow x \in \overline{\mathcal{P}}^*$ ou $y \in \overline{\mathcal{P}}^*$ est également immédiate. Le fait général ci-dessus montre aussi que la correspondance $\overline{\mathcal{P}} \to \overline{\mathcal{P}}^*$, qui envoie idéaux premiers de $B/\mathfrak{p}B$ tels que $j^{-1}(\overline{\mathcal{P}}) = \{0\}$ sur des idéaux premiers de $B/\mathfrak{p}B \otimes_{A/\mathfrak{p}} k$, est injective. Il suffit donc de montrer qu'il n'y a qu'un nombre fini d'idéaux premiers dans l'anneau $B/\mathfrak{p}B \otimes_{A/\mathfrak{p}} k$

L'anneau $C = B/\mathfrak{p}B \otimes_{A/\mathfrak{p}} k$ est un k-espace vectoriel de dimension finie. En particulier, c'est un anneau noethérien. D'après le théorème 1.1.11, l'idéal $\sqrt{0}$ de C peut s'écrire $\sqrt{0} = J_1 \cap \cdots \cap J_n$ avec $J_1, \ldots, J_n$ idéaux premiers de C. On en déduit que $C/\sqrt{0}$ s'injecte dans l'anneau produit

$$C/J_1 \times \cdots C/J_n$$

Cet anneau produit est un k-espace vectoriel de dimension finie. En conséquence, il est donc entier sur k et donc sur C. Les idéaux premiers distincts de C se relèvent en des idéaux premiers (forcément distincts) de l'anneau produit (par le (a)). Il suffit donc de montrer que cet anneau produit n'a qu'un nombre fini d'idéaux premiers. Vu la structure produit, il s'agit en fait de montrer que chacun des facteurs C/J_i n'a qu'un nombre fini d'idéaux premiers, $j = 1, \ldots, n$. Or l'anneau C/J_i, étant intègre et entier sur le corps k, est un corps (lemme 1.1.21) ; son seul idéal premier est l'idéal nul.

Pour conclure la preuve, il suffit de voir que l'ensemble des idéaux premiers d'un anneau C est en bijection avec l'ensemble des idéaux premiers de $C/\sqrt{0}$. Ce dernier point est facile à établir, une fois remarqué que le nil-radical $\sqrt{0}$ est inclus dans tout idéal premier de C.

□

1.6.2. Dimension d'une extension intégrale. —

Théorème 1.6.2. — *Soit B un anneau entier sur un sous-anneau A. Si la dimension de A est finie égale à d, la dimension de B est égale à d.*

Démonstration. — Considérons une suite strictement croissante

$$\mathcal{P}_0 \underset{\neq}{\subset} \mathcal{P}_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathcal{P}_d$$

d'idéaux premiers de A. D'après le théorème 1.6.1 (a), il existe un idéal premier $\mathcal{Q}_0$ de B tel que $\mathcal{Q}_0 \cap A = \mathcal{P}_0$.

Posons $\overline{A} = A/\mathcal{P}_0$ et $\overline{B} = B/\mathcal{Q}_0$; $\overline{A}$ est un sous-anneau de B sur lequel B est entier. On a le diagramme commutatif suivant

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ \overline{A} & \longrightarrow & \overline{B} \end{array}$$

où les flèches sont les morphismes naturels. D'après le théorème 1.6.1 (a), il existe un idéal premier $\overline{\mathcal{Q}_1}$ de $\overline{B}$ tel que $\overline{\mathcal{Q}_1} \cap \overline{A} = p(\mathcal{P}_1)$. Soit $\mathcal{Q}_1 = q^{-1}(\overline{\mathcal{Q}_1})$; $\mathcal{Q}_1$ est un idéal premier de B et $\mathcal{Q}_0 \subset \mathcal{Q}_1$. De plus $\mathcal{Q}_1 \cap A = p^{-1}(\overline{\mathcal{Q}_1} \cap \overline{A}) = p^{-1}(p(\mathcal{P}_1)) = \mathcal{P}_1$ (la dernière égalité provenant de $\mathcal{P}_0 \subset \mathcal{P}_1$.

Ce que prouve l'argument ci-dessus est énoncé plus généralement dans le théorème 1.6.3 (d). En itérant cet argument, on arrive à construire une suite, évidemment strictement croissante, d'idéaux premiers de B

$$\mathcal{Q}_0 \underset{\neq}{\subset} \mathcal{Q}_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathcal{Q}_\ell$$

de longueur $\ell = d$ et telle que $\mathcal{Q}_i \cap A = \mathcal{P}_i$, $i = o, \ldots, d$. Cela montre que la dimension de B est supérieure à d.

D'autre part, il ne peut exister une suite comme ci-dessus, strictement croissante d'idéaux premiers de B de longueur $\ell > d$. Sinon on aurait $\mathcal{Q}_i \cap A = \mathcal{Q}_{i+1} \cap A$ pour un indice $i \in \{1, \ldots, \ell-1\}$, ce qui contredirait le (b) du théorème 1.6.3 qui complète le théorème 1.6.1. □

***Théorème 1.6.3* (going-up theorem (suite))**. — *Soit B un anneau entier sur un sous-anneau A.*
(d) *Si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers de A tels que $\mathfrak{p} \subset \mathfrak{p}'$ et si $\mathcal{P}$ est un idéal premier de B tel que $\mathcal{P} \cap A = \mathfrak{p}$, alors il existe un idéal premier $\mathcal{P}'$ de B tel que $\mathcal{P} \subset \mathcal{P}'$ et $\mathcal{P}' \cap A = \mathfrak{p}'$.*
(e) *Si $\mathcal{P}$ et $\mathcal{P}'$ sont deux idéaux premiers de B tels que $\mathcal{P} \subset \mathcal{P}'$ et si $\mathcal{P} \cap A = \mathcal{P}' \cap A$, alors $\mathcal{P} = \mathcal{P}'$.*

Démonstration. — (e) Posons $\mathfrak{p} = \mathcal{P} \cap A = \mathcal{P}' \cap A$ et $S = A \setminus \mathfrak{p}$. L'anneau $A_\mathfrak{p} = S^{-1}A$ est local d'idéal maximal $S^{-1}\mathfrak{p}$. Par construction $S \cap \mathcal{P} = Q \cap \mathcal{P}' = \emptyset$; $S^{-1}\mathcal{P}$ et $S^{-1}\mathcal{P}'$ sont donc des idéaux premiers de l'anneau $S^{-1}B$. De $\mathfrak{p} \subset \mathcal{P} \subset \mathcal{P}' \subset B$ résultent $S^{-1}\mathfrak{p} \subset S^{-1}\mathcal{P} \subset S^{-1}\mathcal{P}' \subset S^{-1}B$ puis

$$S^{-1}\mathfrak{p} \subset S^{-1}\mathcal{P} \cap A_\mathfrak{p} \subset S^{-1}\mathcal{P}' \cap A_\mathfrak{p} \subset A_\mathfrak{p}$$

De plus, comme $\mathcal{P}' \neq B$ (c'est-à-dire $1 \notin \mathcal{P}'$), on a $S^{-1}\mathcal{P}' \cap A_\mathfrak{p} \neq A_\mathfrak{p}$. On déduit donc de la suite d'inclusions précédente que $S^{-1}p = S^{-1}\mathcal{P} \cap A_\mathfrak{p} = S^{-1}\mathcal{P}' \cap A_\mathfrak{p}$. Il découle alors du lemme 1.1.21 que $S^{-1}\mathcal{P}$ et $S^{-1}\mathcal{P}'$ sont des idéaux maximaux

de $S^{-1}B$. Comme $S^{-1}\mathcal{P} \subset S^{-1}\mathcal{P}'$, on a donc $S^{-1}\mathcal{P} = S^{-1}\mathcal{P}'$, ce qui entraîne $\mathcal{P} = \mathcal{P}'$. □

1.7. Nullstellensatz

1.7.1. Prolongement de morphismes. — L'énoncé suivant est une extension du théorème 1.3.4 au cas des extensions de type fini.

Théorème 1.7.1. — *Soient k un corps, B une k-algèbre de type fini, $A \subset B$ une sous-algèbre et $\varphi : A \to C$ un morphisme d'anneaux dans un corps algébriquement clos C. On suppose que*

(*) *il existe un idéal $\mathcal{P} \subset B$ tel que $\mathcal{P} \cap A = \ker(\varphi)$.*

Alors il existe un morphisme $\Phi : B \to C$ qui prolonge $\varphi : A \to C$.

L'hypothèse (*) est vérifiée notamment dans les deux cas suivants :

Cas particulier 1 : $A = k$. On a alors $\ker(\varphi) = \{0\}$. Comme on va le voir, ce cas particulier est suffisant pour établir le Nullstellensatz (théorème des zéros de Hilbert).

Cas particulier 2 : B est entier sur A. (*) résulte dans ce cas du fait que $\ker(\varphi)$ est un idéal premier de A et du théorème 1.6.1 (a) (going-up theorem).

Pour démontrer le théorème 1.7.1, on commence par le cas (2). Nous allons établir l'énoncé un peu plus général suivant où on se dispense notamment de l'hypothèse de type fini.

Lemme 1.7.2. — *Soient B un anneau entier sur un sous-anneau A et $\varphi : A \to C$ un morphisme d'anneaux dans un corps algébriquement clos C. Alors il existe un morphisme $\Phi : B \to C$ qui prolonge $\varphi : A \to C$.*

Démonstration. — Notons $\mathfrak{p} = \ker(\varphi)$ et $S = A \setminus \mathfrak{p}$. L'anneau $S^{-1}B$ est entier sur $S^{-1}A = A_{\mathfrak{p}}$. On a le diagramme commutatif suivant

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ A_{\mathfrak{p}} & \longrightarrow & S^{-1}B \end{array}$$

Le morphisme $\varphi : A \to C$ se prolonge de façon unique en morphisme $\varphi_{\mathfrak{p}} : A_{\mathfrak{p}} \to C$. D'après le théorème 1.6.1 (a), il existe un idéal premier $\mathcal{P} \subset S^{-1}B$ tel que $\mathcal{P} \cap A_{\mathfrak{p}} = \ker(\varphi_{\mathfrak{p}})$. Comme $\ker(\varphi_{\mathfrak{p}}) = \mathfrak{p}A_{\mathfrak{p}}$ est maximal, d'après le lemme 1.1.21, $\mathcal{P}$ l'est aussi.

Ainsi $S^{-1}B/\mathcal{P}$ est un corps et est une extension algébrique du corps $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. D'autre part le morphisme $\varphi_\mathfrak{p}$ induit par passage au quotient un morphisme $\overline{\varphi_\mathfrak{p}} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to C$. Le diagramme suivant résume la situation.

$$\begin{array}{ccccccc} B & \longrightarrow & S^{-1}B & \longrightarrow & S^{-1}B/\mathcal{P} & & \\ \uparrow & & \uparrow & & \uparrow & & \\ A & \longrightarrow & A_\mathfrak{p} & \longrightarrow & A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} & \xrightarrow{\overline{\varphi_\mathfrak{p}}} & C \end{array}$$

Le théorème 1.3.4 permet de prolonger $\overline{\varphi_\mathfrak{p}}$ à $S^{-1}B/\mathcal{P}$ et de conclure. □

Le lemme ci-dessous est un autre résultat intermédiaire de la preuve du theéorème 1.7.1.

Lemme 1.7.3. — *Soient k un corps, $\mathbf{T} = (T_1, \ldots, T_r)$ r indéterminées, $y_1, \ldots, y_n$ des éléments de $\overline{k(\mathbf{T})}$ et $\varphi : k \to C$ un morphisme à valeurs dans un corps algébriquement clos C. Il existe un polynôme $c(\mathbf{T}) \in k[\mathbf{T}]$ non nul tel que pour tout $\mathbf{t}_0 \in C^r$ pour lequel $c^\varphi(\mathbf{t}_0) \neq 0$[9], il existe un morphisme d'anneau $\varphi_{\mathbf{t}_0} : k[\mathbf{T}, y_1, \ldots, y_n] \to C$ égal à φ sur k et envoyant $\mathbf{T}$ sur $\mathbf{t}_0$.*

Démonstration. — Pour $i = 1, \ldots, n$, soit $a_i(\mathbf{t}) \in k[\mathbf{T}]$ non nul tel que $a_i(\mathbf{T})\, y_i$ soit entier sur $k[\mathbf{T}]$. Soient $c(\mathbf{T})$ le polynôme non nul $c(\mathbf{T}) = a_1(\mathbf{T}) \cdots a_n(\mathbf{T})$ et $\mathbf{t}_0 = (t_{01}, \ldots, t_{0r}) \in C^r$ tel que $c^\varphi(\mathbf{t}_0) \neq 0$. L'homomorphisme $k[\mathbf{T}] \to C$ égal à φ sur k et envoyant T_i sur t_{0i}, $i = 1, \ldots, n$, se prolonge (de façon unique) au localisé $k[\mathbf{T}]_\mathcal{K}$ de $k[\mathbf{T}]$ par son noyau $\mathcal{K}$. Par construction $a_1(\mathbf{T}), \ldots, a_n(\mathbf{T}) \notin \mathcal{K}$ et donc $k[\mathbf{T}, 1/a_1(\mathbf{T}), \ldots, 1/a_n(\mathbf{T})] \subset k[\mathbf{T}]_\mathcal{K}$. Ainsi la k-algèbre $k[\mathbf{T}, y_1, \ldots, y_n]$ est entière sur $k[\mathbf{T}]_\mathcal{K}$ et on peut invoquer le lemme 1.7.2 pour conclure. □

Preuve du théorème 1.7.1. — Soient $\mathfrak{p} = \ker(\varphi)$, $S = A \setminus \mathfrak{p}$ et $\mathcal{P}$ un idéal de B tel que $\mathcal{P} \cap A = \mathfrak{p}$. Comme $A/\mathfrak{p}$ est isomorphe à un sous-anneau de C, $A/\mathfrak{p}$ est intègre, $\mathfrak{p}$ est un idéal premier de A et $\mathfrak{p}A_\mathfrak{p}$ un idéal maximal de $A_\mathfrak{p}$. Comme $\mathcal{P} \cap A \subset \mathfrak{p}$, on a $\mathcal{P} \cap S = \emptyset$ et l'idéal $S^{-1}\mathcal{P}$ est un idéal propre de $S^{-1}B$. Soit $\mathcal{M}$ un idéal maximal de $S^{-1}B$ contenant $S^{-1}\mathcal{P}$. Comme $\mathfrak{p} \subset \mathcal{P}$, on a $\mathfrak{p}A_\mathfrak{p} \subset S^{-1}\mathcal{P} \subset \mathcal{M}$, d'où un morphisme $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to S^{-1}B/\mathcal{M}$, lequel est forcément injectif puisque $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ et $S^{-1}B/\mathcal{M}$ sont des corps. D'autre part $\mathfrak{p}A_\mathfrak{p}$ est le noyau du prolongement naturel $\varphi_\mathfrak{p} : A_\mathfrak{p} \to C$ de φ à $A_\mathfrak{p}$. Le passage au quotient fournit un morphisme $\overline{\varphi_\mathfrak{p}} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to C$. On a le diagramme

[9] Rappelons que c^φ désigne le polynôme obtenu en appliquant φ aux coefficients de c.

suivant, où on a noté $k_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ et $K_\mathcal{M} = S^{-1}B/\mathcal{M}$:

$$\begin{array}{ccccc} B & \longrightarrow & S^{-1}B & \longrightarrow & K_\mathcal{M} \\ \uparrow & & \uparrow & & \uparrow \\ A & \longrightarrow & A_\mathfrak{p} & \longrightarrow & k_\mathfrak{p} \xrightarrow{\overline{\varphi_\mathfrak{p}}} C \end{array}$$

Il suffit de prolonger $\overline{\varphi_\mathfrak{p}}$ à $K_\mathcal{M}$. Si l'extension $K_\mathcal{M}/k_\mathfrak{p}$ est algébrique, on applique le théorème 1.3.4. Supposons la transcendante. Soit $\mathbf{t} = \{t_1, \ldots, t_r\}$ une base de transcendance de $K_\mathcal{M}$ sur $k_\mathfrak{p}$. Si $x_1, \ldots, x_n$ sont des générateurs de la k-algèbre B et qu'on note $\bar{x}_1, \ldots, \bar{x}_n$ leurs images respectives dans $K_\mathcal{M} = S^{-1}B/\mathcal{M}$, on a $K_\mathcal{M} = k_\mathfrak{p}[\mathbf{t}, \bar{x}_1, \ldots, \bar{x}_n]$ (noter que $k \subset k_\mathfrak{p}$ puisque $k \cap \mathfrak{p} = \{0\}$) ; de plus, pour chaque $i = 1, \ldots, n$, $\bar{x}_i$ est algébrique sur $k_\mathfrak{p}(\mathbf{t})$. On est dans la situation du lemme 1.7.3 qui permet de conclure : plus précisément, si $c(\mathbf{t}) \in k_\mathfrak{p}[\mathbf{t}]$ est le polynôme non nul donné par cet énoncé, il existe $\mathbf{t}_0 \in C^r$ tel que $c^{\overline{\varphi_\mathfrak{p}}}(\mathbf{t}_0) \neq 0$ et tout tel choix de $\mathbf{t}_0$ permet de construire un morphisme d'anneau $\varphi_{\mathbf{t}_0} : k_\mathfrak{p}[\mathbf{t}, \bar{x}_1, \ldots, \bar{x}_n] \to C$ égal à φ sur $k_\mathfrak{p}$ et envoyant $\mathbf{t}$ sur $\mathbf{t}_0$. □

1.7.2. Théorèmes des zéros de Hilbert. — Les énoncés suivants sont des applications classiques du théorème 1.7.1.

Corollaire 1.7.4. — *Soient k un corps et B une k-algèbre de type fini. Si B est un corps, alors c'est une extension algébrique de k.*

Démonstration. — D'après le théorème 1.7.1 (cas particulier 1), l'inclusion $k \to \overline{k}$ se prolonge en un morphisme $B \to \overline{k}$. Si B est un corps, ce morphisme est injectif. □

Corollaire 1.7.5 **(Nullstellensatz faible)**. — *Soient k un corps algébriquement clos. Les idéaux maximaux de l'anneau de polynômes $k[T_1, \ldots, T_n]$ sont les idéaux du type $\langle T_1 - \alpha_1, \ldots, T_n - \alpha_n \rangle$ où $(\alpha_1, \ldots, \alpha_n) \in k^n$.*

Démonstration. — Un idéal du type indiqué $\langle T_1 - \alpha_1, \ldots, T_n - \alpha_n \rangle$ est maximal puisque c'est le noyau de l'homomorphisme surjectif $k[T_1, \ldots, T_n] \to k$ envoyant T_i sur α_i, $i = 1, \ldots, n$. Inversement, si $\mathcal{M} \subset k[T_1, \ldots, T_n]$ est un idéal maximal, le corollaire 1.7.4 fournit un isomorphisme entre $k[T_1, \ldots, T_n]/\mathcal{M}$ et k. Soient $\alpha_1, \ldots, \alpha_n$ les images respectives de $T_1, \ldots, T_n$ par cet isomorphisme. Par construction, on a $\langle T_1 - \alpha_1, \ldots, T_n - \alpha_n \rangle \subset \mathcal{M}$. Comme l'idéal de gauche est maximal, cette inclusion est une égalité. L'unicité du point $(\alpha_1, \ldots, \alpha_n)$ est claire. □

***Théorème 1.7.6* (Nullstellensatz).** — *Soient k un corps algébriquement clos et I un idéal de $k[T_1,\dots,T_n]$. Soit $Z(I)$ l'ensemble des points $(\alpha_1,\dots,\alpha_n) \in k^n$ tel que $f(\alpha_1,\dots,\alpha_n) = 0$ pour tout $f \in I$. Soit $F \in k[T_1,\dots,T_n]$ tel que $F(\alpha_1,\dots,\alpha_n) = 0$ pour tout $(\alpha_1,\dots,\alpha_n) \in Z(I)$. Alors il existe $m \in \mathbb{N}$ tel que $F^m \in I$, c'est-à-dire, $F \in \sqrt{I}$.*

Démonstration. — Soit $A = k[T_1,\dots,T_n]/I$ et $s : k[T_1,\dots,T_n] \to A$ la surjection canonique. Tout idéal maximal de A est de la forme $s(\mathcal{M})$ avec $\mathcal{M}$ idéal maximal de $k[T_1,\dots,T_n]$ contenant I. De plus, d'après le corollaire 1.7.5, il existe $(\alpha_1,\dots,\alpha_n) \in k^n$ tel que $\mathcal{M} = \langle T_1 - \alpha_1,\dots,T_n - \alpha_n\rangle$. Pour tout $f \in k[T_1,\dots,T_n]$, la condition $f \in \mathcal{M}$ est équivalente à $f(\alpha_1,\dots,\alpha_n) = 0$ (comme le montre par exemple la formule de Taylor). Ainsi l'inclusion $I \subset \mathcal{M}$ entraîne que $(\alpha_1,\dots,\alpha_n) \in Z(I)$ et l'hypothèse sur F donne alors que $F \in \mathcal{M}$. On obtient $s(F) \in s(\mathcal{M})$. Comme $s(\mathcal{M})$ est un idéal maximal arbitraire de A, on obtient que $s(F)$ est dans le niradical de A, ou de façon équivalente, que $F \in \sqrt{I}$, ce qui donne la conclusion désirée, *via* la proposition 1.1.10. □

1.7.3. Morphismes de spécialisation. — Soient k un corps, $\mathbf{T} = (T_1,\dots,T_r)$ r indéterminées, $y_1,\dots,y_n$ des éléments de $\overline{k(\mathbf{T})}$ et $\varphi : k \to C$ un k-morphisme à valeurs dans un corps algébriquement clos C.

Définition 1.7.7. — On appelle *morphisme de spécialisation* en $\mathbf{t}_0$ de $k[\mathbf{T}, y_1,\dots,y_n]$ tout morphisme $\varphi_{\mathbf{t}_0} : k[\mathbf{T}, y_1,\dots,y_n] \to C$ comme dans le lemme 1.7.3.

Dans la suite, il nous arrivera quand il n'y aura pas d'ambiguïté, de noter $y(\mathbf{t}_0)$ l'élément $\varphi_{\mathbf{t}_0}(y)$ (pour $y \in k[\mathbf{T}, y_1,\dots,y_n]$). On se rappellera cependant que $y(\mathbf{t}_0)$ dépend du prolongement $\varphi_{\mathbf{t}_0}$ (lequel n'est pas unique).

Considérons la situation particulière où $y_1,\dots,y_n$ sont les racines supposées simples d'un polynôme $P(\mathbf{T}, Y) \in k(\mathbf{T})[Y]$ non constant. On a

$$P(\mathbf{T}, Y) = c(\mathbf{T}) \prod_{i=1}^{n} (Y - y_i) \text{ avec } c(\mathbf{T}) \neq 0$$

Notons $\Delta(\mathbf{T})$ le discriminant de P par rapport à Y ; c'est un élément non nul de $k(\mathbf{T})$. Si en plus de la condition $c^{\varphi}(\mathbf{t}_0) \neq 0$ du lemme 1.7.3, on impose que $\Delta^{\varphi}(\mathbf{t}_0)$ soit défini et non nul, alors tout morphisme de spécialisation $\varphi_{\mathbf{t}_0}$ de $k[\mathbf{T}, y_1,\dots,y_n]$ en $\mathbf{t}_0$ induit une bijection entre $\{y_1,\dots,y_n\}$ et l'ensemble des racines de $P^{\varphi}(\mathbf{t}_0, Y)$. Quitte à composer $\varphi_{\mathbf{t}_0}$ par un $k(\mathbf{t})$-isomorphisme de $\overline{k(\mathbf{t})}$ on peut demander en outre à un morphisme de spécialisation d'envoyer y_1 sur n'importe quelle racine de $P^{\varphi}(\mathbf{t}_0, Y)$.

1.8. B-A-BA de la géométrie algébrique

1.8.1. Topologie de Zariski. —

1.8.1.1. L'espace affine $\mathbb{A}^n$. — Soient k un corps et $n \geq 1$ un entier. On définit l'espace affine $\mathbb{A}^n(k)$ comme l'ensemble des n-uplets $(a_1, \ldots, a_n)$ à composantes dans k. Etant donné un sous-ensemble $\mathcal{P} \subset k[X_1, \ldots, X_n]$, on note

$$Z(\mathcal{P}) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n(k) \mid P(a_1, \ldots, a_n) = 0 \text{ pour tout } P \in \mathcal{P}\}$$

On peut dans cette définition remplacer $\mathcal{P}$ par l'idéal engendré par $\mathcal{P}$ dans l'anneau $k[X_1, \ldots, X_n]$. Comme cet anneau est noethérien, on peut aussi trouver un sous-ensemble fini $\mathcal{P}_f \subset k[X_1, \ldots, X_n]$ tel que $Z(\mathcal{P}) = Z(\mathcal{P}_f)$.

Les ensembles de la forme $Z(\mathcal{P})$ sont appelés les *ensembles algébriques* de $\mathbb{A}^n(k)$. Si $\mathcal{P}$ ne consiste qu'en un seul polynôme non nul, $Z(\mathcal{P})$ est appelé une *hypersurface* de $\mathbb{A}^n(k)$. On vérifie sans peine que les ensembles algébriques sont les fermés d'une topologie sur $\mathbb{A}^n(k)$. Cette topologie est appelée la *topologie de Zariski*.

Remarque 1.8.1. — (a) Pour $n = 1$, les ensembles algébriques sont les parties finies de $\mathbb{A}^1(k)$ et l'ensemble $\mathbb{A}^1(k)$. Les ouverts de la topologie de Zariski de la droite affine $\mathbb{A}^1(k)$ sont les complémentaires de parties finies et l'ensemble vide.

(b) Les ensembles finis sont fermés pour la topologie de Zariski. En effet, tout singleton $\{(a_1, \ldots, a_n)\}$ s'écrit $Z(X_1 - a_1, \ldots, X_d - a_d)$. Cependant, la proposition 1.8.3 montre que, si k est infini, la topologie de Zariski n'est pas séparée. Cela n'est pas vrai si k fini : la topologie de Zariski sur $\mathbb{A}^n(k)$ est dans ce cas la topologie discrète.

Définition 1.8.2. — Un espace topologique non vide X est dit *irréductible* s'il satisfait les conditions équivalentes suivantes :
(i) Toute intersection de deux ouverts non vide est non vide.
(ii) Toute réunion de deux fermés propres de X est distincte de X.
(iii) Tout ouvert non vide est dense.
(iv) Tout fermé propre est d'intérieur vide.
(v) Tout ouvert est connexe.

Proposition 1.8.3. — *Si k est infini, l'espace affine $\mathbb{A}^n(k)$ est irréductible.*

Démonstration. — Si la condition (ii) n'était pas satisfaite, on pourrait trouver deux hypersurfaces $Z(P)$ et $Z(Q)$ avec $P, Q \in k[X_1, \ldots, X_n]$ non nuls tels que $\mathbb{A}^n(k) = Z(P) \cup Z(Q)$ (noter qu'un fermé propre est toujours inclus dans

une hypersurface). Mais alors on aurait $\mathbb{A}^n(k) = Z(PQ)$. Comme k est infini, cela entraîne classiquement que $PQ = 0$, ce qui contredit $P \neq 0$ et $Q \neq 0$. □

Définition 1.8.4. — Un sous-ensemble fermé et irréductible d'un espace affine $\mathbb{A}^n$ est appelé variété affine et un ouvert d'une variété affine une variété quasi-affine.

Définition 1.8.5. — Etant donné un espace topologique X, on appelle dimension de X le supremum (éventuellement infini) des longueurs d des chaînes

$$Z_0 \underset{\neq}{\subset} Z_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} Z_d$$

de sous-ensembles fermés et irrréductibles $Z_0, Z_1, \ldots Z_d$ de X.

La dimension de l'espace affine $\mathbb{A}^n$ est égale à n, qui est aussi la dimension de l'anneau $K[X_1, \ldots, X_n]$. Plus généralement, on a

Proposition 1.8.6. — *Si $Y \subset \mathbb{A}^n$ est une variété affine, alors sa dimension comme espace topologique est égale à celle de l'anneau $K[X_1, \ldots, X_n]/I(Y)$ quotient de $K[X_1, \ldots, X_n$ par l'idéal $I(Y) = \{f \in K[X_1, \ldots, X_n] \,|\, f(y) = 0$ pour tout $y \in Y\}$.*

Démonstration. — voir [**Har77**, chapter I]. □

1.8.1.2. La topologie des schémas affines. — Etant donné un anneau A, le *spectre* de A est défini ensemblistement comme l'ensemble, noté $\mathrm{Spec}(A)$ des idéaux premiers de A. Si $\mathfrak{a}$ est un idéal quelconque de A, on définit l'ensemble $Z(\mathfrak{a})$ comme l'ensemble des idéaux premiers $\mathfrak{p} \in \mathrm{Spec}(A)$ qui contiennent $\mathfrak{a}$. On vérifie facilement les assertions suivantes.

Proposition 1.8.7. — (a) *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A, on a alors $Z(\mathfrak{ab}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$.*[(10)]
(b) *Si $(\mathfrak{a}_i)_i$ est une famille d'idéaux de A, alors $Z(\sum_i \mathfrak{a}_i) = \bigcap_i Z(\mathfrak{a}_i)$.*
(c) *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A, $Z(\mathfrak{a}) \subset Z(\mathfrak{b})$ si et seulement si $\sqrt{\mathfrak{a}} \supset \sqrt{\mathfrak{b}}$.*

Il résulte de la proposition 1.8.7 que les ensembles $Z(\mathfrak{a})$, appelés *ensembles algébriques*, où $\mathfrak{a}$ décrit l'ensemble des idéaux de A, sont les fermés d'une topologie sur $\mathrm{Spec}(A)$. On l'appelle la topologie de Zariski.

Pour tout $I \in \mathrm{Spec}(A)$, l'adhérence $\overline{\{I\}}$ est l'ensemble $Z(I)$. Les idéaux maximaux de $\mathrm{Spec}(A)$ sont des fermés de $\mathrm{Spec}(A)$, appelés les *points fermés*.

(10) Cet énoncé est l'occasion de rappeler un fait standard qu'on utilisera de nombreuses fois : si un idéal premier contient un produit fini d'idéaux, alors il contient nécessairement l'un d'eux (par exemple [**Sam67**, §3. 3, lemme 2]).

Si A est intègre, l'idéal nul 0 est un idéal premier, appelé le *point générique* de $\mathrm{Spec}(A)$; il est dense dans $\mathrm{Spec}(A)$. En particulier $\mathrm{Spec}(A)$ est irréductible. Plus généralement, un fermé $Z(I)$ est irréductible si et seulement si $\sqrt{I}$ est un idéal premier de A.

Exemple 1.8.8. — (1) Pour $A = \mathbb{Z}$, $\mathrm{Spec}(A)$ est l'ensemble formé des idéaux premiers $p\mathbb{Z}$, où p est un nombre premier, et de l'idéal nul. Pour tout $n \in \mathbb{Z}$, le fermé $Z(n\mathbb{Z})$ correspond à l'ensemble des diviseurs premiers de n.

(2) Prenons $A = k[X_1, \ldots, X_n]$ avec k algébriquement clos. Le Nullstellensatz faible (corollaire 1.7.5) montre que les idéaux maximaux de A, sont les idéaux de la forme $\langle X_1 - a_1, \ldots, X_n - a_n\rangle$ avec $(a_1, \ldots, a_n) \in k^n$. Les points fermés de $\mathrm{Spec}(A)$ correspondent aux points usuels de $\mathbb{A}^n(k)$. De plus, dire qu'un idéal $\mathfrak{a}$ de A est contenu dans un tel idéal maximal $\langle X_1 - a_1, \ldots, X_n - a_n\rangle$ revient à dire que $f(a_1, \ldots, a_n) = 0$ pour tout $f \in \mathfrak{a}$. L'ensemble des points fermés dans $Z(\mathfrak{a})$ coincide donc avec la notion d'ensemble algébrique $Z(\mathfrak{a})$ dans l'espace affine $\mathbb{A}^n(k)$ défini plus haut. On note $\mathbb{A}^n_k$ le schéma affine $\mathrm{Spec}(k[X_1, \ldots, X_n])$ muni de la topologie de Zariski ; sa restriction aux points fermés est l'espace affine $\mathbb{A}^n(k)$. Il y a d'autres points dans $\mathbb{A}^n_k$ que ceux de $\mathbb{A}^n(k)$: il y a par exemple le point générique, les points correspondants à des idéaux principaux engendrés par des éléments $f \in k[X_1, \ldots, X_n]$ irréductibles, c'est-à-dire, les *hypersurfaces* irréductibles $f(x_1, \ldots, x_n) = 0$, etc.

Etant donné un sous-ensemble $S \subset \mathbb{A}^n(k)$, on introduit l'idéal $\mathcal{I}(S)$ comme l'ensemble de tous les polynômes $f \in k[X_1, \ldots, X_n]$ tels que $f(\mathbf{x}) = 0$ pour tout $\mathbf{x} \in S$. Le Nullstellensatz (théorème 1.7.6) se reformule alors comme suit : pour tout idéal $I \subset k[X_1, \ldots, X_n]$, on a $\mathcal{I}(Z(I)) = \sqrt{I}$.

(3) D'après la proposition 1.1.1, les idéaux premiers de A_{f^∞} sont en bijection avec les idéaux premiers de A ne contenant pas f ; autrement dit, $\mathrm{Spec}(A_{f^\infty})$ est en bijection avec l'ouvert de Zariski $\mathrm{Spec}(A) \setminus Z(Af)$. Si $A = k[X_1, \ldots, X_n]$ avec k algébriquement clos, les points fermés de $\mathrm{Spec}(A_{f^\infty})$ correspondent aux points fermés $(x_1, \ldots, x_n) \in \mathbb{A}^n_k$ tels que $f(x_1, \ldots, x_n) \neq 0$.

(4) La proposition 1.5.22 peut être reformulée ainsi : l'ensemble des idéaux premiers $\mathcal{P}$ de B ramifiés dans l'extension E/K est un fermé propre de Zariski $R = Z(\mathcal{R}) \subset \mathrm{Spec}(B)$ avec $\mathcal{R} \neq 0$.

Dans la suite, nous dirons parfois qu'une propriété $\mathcal{P}(x_1, \ldots, x_n)$ est vraie pour tout $(x_1, \ldots, x_n) \in \mathbb{A}^n(k)$ en dehors d'un fermé de Zariski. Cela signifie qu'il existe un fermé *propre*, qu'on peut prendre de la forme $Z(f)$ avec $f \in k[X_1, \ldots, X_n]$, $f \neq 0$, tel que la propriété est vraie pour tout $(x_1, \ldots, x_n) \in$

$\mathbb{A}^n(k)$ tel que $f(x_1,\dots,x_n)\neq 0$. Plus généralement, on parlera de propriété vraie pour tout idéal premier d'un anneau A sauf dans un fermé de Zariski.

1.8.2. k-points et points géométriques. — Supposons donnée une algèbre A de type fini sur un corps k parfait[(11)]. Elle est de la forme $k[T_1,\dots,T_r]/\mathcal{I}$ avec $\mathcal{I}$ idéal de $k[T_1,\dots,T_r]$. On note $V=\mathrm{Spec}(A)$ le spectre de A et, si A est intègre, $k(V)=\mathrm{Frac}(A)$ le *corps des fonctions* de V. Si $\mathcal{P}$ est un point de V, c'est-à-dire un idéal premier de A, le corps résiduel $\mathrm{Frac}(A/\mathcal{P})$ est appelé *corps de définition* de $\mathcal{P}$ sur k et noté $k(\mathcal{P})$. Si k' est une extension quelconque de k, on note $V(k')$ l'ensemble des points $\mathcal{P}$ de V tel que $k(\mathcal{P})\subset k'$; les points de $V(k')$ sont dits k'-rationnels. Les points fermés de $\mathrm{Spec}(A\otimes_k\overline{k})=V_{\overline{k}}$ sont appelés *points géométriques* (de $V_{\overline{k}}$).

On dit que A (ou $V=\mathrm{Spec}(A)$) est géométriquement intègre si $A\otimes_k\overline{k}$ est intègre. On dit alors que V est défini sur k. On a le résultat suivant [? ?].

Proposition 1.8.9. — *Les assertions suivantes sont équivalentes :*
(i) *A est géométriquement intègre,*
(ii) *$\mathcal{I}\otimes\overline{k}$ est un idéal premier de $\overline{k}[T_1,\dots,T_r]$,*
(iii) *$\mathrm{Frac}(A)=k(V)$ est une extension "régulière" de k (c'est-à-dire séparable et telle que $\overline{k}\cap k(V)=k$).*

Proposition 1.8.10. — *Si $\mathcal{P}$ est un point fermé de V, c'est-à-dire un idéal maximal de A, alors $k(\mathcal{P})$ est une extension algébrique de k. L'ensemble des points géométriques de $V_{\overline{k}}$ au-dessus de $\mathcal{P}$ est fini. Le groupe G_k opère sur l'ensemble de ces points. Il y a donc correspondance entre points fermés de V et ensembles de points géométriques k-conjugués sur $V_{\overline{k}}$.*

Démonstration. — L'anneau $A\otimes_k\overline{k}$ est entier sur A. D'après le théorème 1.6.1 (a), il existe un idéal maximal $\overline{\mathcal{P}}$ de $A\otimes_k\overline{k}$ au-dessus de $\mathcal{P}$ et on a alors $k(\mathcal{P})\subset\overline{k}(\overline{\mathcal{P}})$. Le point fermé $\overline{\mathcal{P}}$ est un idéal maximal de $A\otimes_k\overline{k}=k[T_1,\dots,T_r]/\mathcal{I}$. Par le Nullstellensatz faible (corollaire 1.7.5), un tel idéal est de la forme $<T_1-a_1,\dots,T_r-a_r>/\mathcal{I}$ avec $a_1,\dots,a_r\in\overline{k}$ (tels que $(a_1,\dots,a_r)\in Z(\mathcal{I})$). Cela donne $\overline{k}(\overline{\mathcal{P}})=\overline{k}$. Cette description donne aussi la finitude des $\tau(\overline{\mathcal{P}})$ où $\tau\in\mathrm{Gal}(\overline{k}/k)$. La dernière assertion résulte alors de la proposition 1.5.18, étendue au cas où l'extension galoisienne E/K n'est pas supposée finie ; on vérifiera que la preuve n'utilise pas cette hypothèse de finitude. □

(11) L'hypothèse "k parfait" sert ici à garantir que la clôture algébrique $\overline{k}$ de k est une extension séparable et donc galoisienne de k.

Si $\overline{\mathcal{P}}$ est un point fermé géométrique de V, son corps de définition sur $V_{\overline{k}}$ vaut $\overline{k}$. Son corps de définition sur V est défini (à k-conjugaison près) comme celui du point fermé $\overline{\mathcal{P}} \cap A$, c'est-à-dire, sa restriction sur V (si V est défini sur k). On le note abusivement $k(\overline{\mathcal{P}})$. Un point géométrique $\overline{\mathcal{P}}$ est dit k-rationnel sur V si $\overline{\mathcal{P}} \cap A$ est k-rationnel.

Ecrivons comme ci-dessus $A = k[T_1, \ldots, T_r]/\mathcal{I}$. Soient $f_1, \ldots, f_n \in k[T_1, \ldots, T_r]$ des générateurs de l'idéal $\mathcal{I}$.

Proposition 1.8.11. — (a) *Les points géométriques $\overline{\mathcal{P}} \in V_{\overline{k}}$ s'identifient aux idéaux $< T_1 - a_1, \ldots, T_r - a_r >$ contenant $\mathcal{I}$, c'est-à-dire aux r-uplets $\mathbf{a} = (a_1, \ldots, a_r) \in \overline{k}^r$ tels que $f_i(a_1, \ldots, a_r) = 0$, $i = 1, \ldots, n$. De plus, cette identification est $\mathrm{Gal}(\overline{k}/k)$-équivariante (c'est-à-dire, $\overline{\mathcal{P}}^\tau$ correspond à $\mathbf{a}^\tau$, pour $\tau \in \mathrm{Gal}(\overline{k}/k)$.*
(b) *Pour tout point géométrique $\overline{\mathcal{P}}$, on a $k(\overline{\mathcal{P}}) \simeq_k k(a_1, \ldots, a_r)$, $i = 1, \ldots, r$. En particulier, le corps $k(\overline{\mathcal{P}})$ est une extension de degré fini de k.*
(c) *Si $\mathcal{P}$ est un point fermé de V, le nombre de points géométriques au-dessus de $\mathcal{P}$ est égal au nombre de k-isomorphismes de $k(\mathcal{P})$ dans $\overline{k}$, c'est-à-dire, à $[k(\mathcal{P}) : k]$.*

Démonstration. — De façon générale, $\mathrm{Spec}(A)$ est en bijection avec le fermé de Zariski $Z(\mathcal{I})$. Sur le corps de base algébriquement clos $\overline{k}$, cela donne (a). Précisons que la correspondance est donnée par : $a_i = T_i(\overline{\mathcal{P}}) = (T_i \bmod(\mathcal{I})) \bmod(\overline{\mathcal{P}})$, $i = 1, \ldots, r$

(b) Notons $\mathcal{P} = \overline{\mathcal{P}} \cap A$ le point fermé de V au-dessous de $\overline{\mathcal{P}}$. Le morphisme de spécialisation $k[T_1, \ldots, T_r] \to \overline{k}$ envoyant T_i sur a_i, $i = 1, \ldots, r$ induit un morphisme $\mathrm{sp} : A \to \overline{k}$ dont le noyau est l'idéal maximal $\mathcal{P} = \overline{\mathcal{P}} \cap A$. Par définition, $A/\mathcal{P} = k(\mathcal{P})$. Ce corps est k-isomorphe à l'image du morphisme sp qui est engendrée par $a_1, \ldots, a_r$.

Le (c) est une conséquence du (a) et de la proposition ? ?. □

Exemple 1.8.12. — Pour $A = \mathbb{Q}[T]/(T^2 - 2)$, la variété $V = \mathrm{Spec}(A)$ consiste en un seul point o : A est un corps, l'idéal nul est le seul idéal maximal. Le corps de définition $\mathbb{Q}(o)$ est le corps A, qui est isomorphe à $\mathbb{Q}(\sqrt{2})$. Par contre, $A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \overline{\mathbb{Q}}(T)/(T^2 - 2)$ possède deux idéaux maximaux, engendrés par $T - \sqrt{2}$ et $T + \sqrt{2}$. Ils correspondent à deux points fermés o_+ et o_- de $V_{\overline{\mathbb{Q}}}$ au-dessus de o. Leur corps de définition, comme points de $V_{\overline{\mathbb{Q}}}$ est $\overline{\mathbb{Q}}$. Mais les corps $\mathbb{Q}(o_+)$ et $\mathbb{Q}(o_-)$ sont $\mathbb{Q}$-isomorphes à $\mathbb{Q}(o) \simeq \mathbb{Q}(\sqrt{2})$.

Soit a un point fermé de $V_{\overline{k}}$ (un point géométrique). Ce point est déterminé par sa restriction à $V_{k(a)}$. En effet, si, k' est une extension finie de k et $a_{k'}$

la restriction de a à $V_{k'}$, le nombre de points fermés de $V_{\overline{k}}$ au-dessus de $a_{k'}$ vaut $[k'(a) : k']$: ces points sont les k'-conjugués de a. En particulier, pour $k' = k(a)$, on obtient bien que a est le seul point de $V_{\overline{k}}$ au-dessus de sa restriction à $V_{k(a)}$. Le point a et sa restriction sur $V_{k(a)}$ sont $k(a)$-rationnels sur V. Notons aussi que la corps de définition de a, vu comme point de $V_{k(a)}$ et celui de sa restriction à V coincident : c'est le corps $k(a)$.

1.9. Spécialisation

Soient k un corps, $r \geq 1$ et $\mathbf{T} = (T_1, \ldots, T_r)$.

1.9.1. Théorème de spécialisation (par les extensions résiduelles). — Soient $N/k(\mathbf{T})$ une extension galoisienne finie et F un corps intermédiaire entre $k(\mathbf{T})$ et N. On note A'_F et A'_N les clôtures intégrales de $A = k[\mathbf{T}]$ dans F et N respectivement. L'anneau $A = k[\mathbf{T}]$ est noethérien, intégralement clos, de corps des fractions $k(\mathbf{T})$ et une k-algèbre de type fini.

Pour tout $\mathbf{t}_0 = (t_{01}, \ldots, t_{0r})$ point fermé rationnel de $\mathrm{Spec}(A) = \mathbb{A}^r_k$, considérons les extensions résiduelles dans les extensions $N/k(\mathbf{T})$ et $F/k(\mathbf{T})$. Ce sont des extensions de $k(\mathbf{t}_0) = k$. Ce sont les extensions

- $\bar{N}_{\mathcal{P}}/k$, notées aussi $k(\mathcal{P})/k$ pour l'extension $N/k(\mathbf{T})$

où $\mathcal{P}$ décrit les idéaux maximaux de A'_N au-dessus de $\mathbf{t}_0$, et

- $\bar{F}_{\mathcal{P}_F}/k$, notées aussi $k(\mathcal{P}_F)/k$, pour l'extension $F/k(\mathbf{T})$, où on a posé $\mathcal{P}_F = \mathcal{P} \cap A'_F$ et $\mathcal{P}$ varie comme ci-dessus.

Les extensions résiduelles $k(\mathcal{P})/k$ sont de même degré (mais pas les extensions $k(\mathcal{P}_F)/k$ en général). Le diagramme ci-dessous résume la situation.

$$\begin{array}{ccc}
\mathrm{Gal}(N/k(\mathbf{T})) & & \\
\left[\begin{array}{cc} \mathrm{Gal}(N/F) & \left[\begin{array}{c} N \\ \uparrow \\ F \end{array}\right. \\ & \uparrow \\ & k(\mathbf{T}) \end{array}\right. & \xrightarrow{\mathrm{mod}\ \mathcal{P}} \quad \begin{array}{c} k(\mathcal{P}) \\ \uparrow \\ k(\mathcal{P}_F) \\ \uparrow \\ k \end{array}
\end{array}$$

Soient y un élément primitif dans A'_N de l'extension $N/k(\mathbf{T})$ et z un élément primitif dans A'_F de l'extension $F/k(\mathbf{T})$. On note respectivement $P \in A[Y]$ et $p \in A[Y]$ les polynômes minimaux de y et z sur A.

Théorème 1.9.1. — *Les conclusions suivantes sont vraies pour tout* $\mathbf{t}_0 \in \mathbb{A}^r(k)$ *sauf dans un fermé propre de Zariski.*

(a) *L'extension résiduelle* $k(\mathcal{P})/k$ *est normale de groupe d'automorphismes isomorphe à un sous-groupe de* $\mathrm{Gal}(N/k(\mathbf{T}))$.
(b) *L'extension résiduelle* $k(\mathcal{P})/k(\mathcal{P}_F)$ *est normale de groupe d'automorphismes isomorphe à un sous-groupe de* $\mathrm{Gal}(N/F)$.
(c) $\begin{cases} [k(\mathcal{P}) : k] \leq [N : k(\mathbf{T})] \\ [k(\mathcal{P}_F) : k] \leq [F : k(\mathbf{T})] \\ k(\mathcal{P}) : k(\mathcal{P}_F)] \leq [N : F] \end{cases}$
(d) *Si* $P(\mathbf{t}_0, Y)$ *est irréductible dans* $k[Y]$*, on a*
- $p(\mathbf{t}_0, Y)$ *irréductible dans* $k[Y]$
- *l'extension* $k(\mathcal{P})/k$ *est galoisienne et* $\mathrm{Gal}(k(\mathcal{P})/k) = \mathrm{Gal}(N/k(\mathbf{T}))$
- *l'extension* $k(\mathcal{P})/k(\mathcal{P}_F)$ *est galoisienne et* $\mathrm{Gal}(k(\mathcal{P})/k(\mathcal{P}_F)) = \mathrm{Gal}(N/F)$.

Démonstration. — D'après le lemme 1.5.22, combiné au théorème 1.6.1, l'ensemble des $\mathbf{t_0} \in \mathbb{A}^r(k)$ tels que l'extension $N/k(\mathbf{T})$ est ramifiée au-dessus de $\mathbf{t_0}$ est un fermé propre de Zariski. Les énoncés (a) et (b) résultent alors immédiatement de la proposition 1.5.17.

Les inégalités dans (c) résultent de la proposition 1.5.1 : noter que l'anneau $k[\mathbf{T}]$ est intégralement clos et que, comme les extensions considérées sont séparables, le discriminant Δ intervenant dans la proposition 1.5.1 est non nul et donc le fermé de Zariski exceptionnel est un fermé propre de $\mathbb{A}^r$.

Pour montrer (d) notons $y(\mathcal{P})$ l'image de $y \in A'_N$ dans $k(\mathcal{P}) = \bar{N}_{\mathcal{P}} = A'_N/\mathcal{P}$. De $P(\mathbf{T}, y) = 0$, on déduit $P(\mathbf{t}_0, y(\mathcal{P})) = 0$. Supposons que $P(\mathbf{t}_0, Y)$ soit irréductible dans $k[Y]$. On obtient alors que l'extension résiduelle $k(\mathcal{P})/k$ est de degré $\geq D = \deg_Y(P) = [N : k(\mathbf{T})]$. Ce résultat, joint à (c), fournit $[k(\mathcal{P}) : k] = D$. Il résulte alors de la multiplicativité des degrés que les inégalités dans (c) sont nécessairement des égalités. Le discriminant $\Delta \in k(\mathbf{T})$ de $P(\mathbf{T}, Y)$ est non nul (car $y \in N$ est séparable). Supposons de plus que $\Delta(\mathbf{t}_0) \neq 0$ (ce qui exclut un fermé propre). Alors le polynôme $P(\mathbf{T}, y) = 0$ n'a que des racines simples (dans $\overline{k}$; l'extension $k(\mathcal{P})/k$, et donc aussi $k(\mathcal{P}_F)/k$, est séparable. On déduit alors du (a) que $\mathrm{Aut}(k(\mathcal{P})/k) = \mathrm{Gal}(N/k(\mathbf{T}))$ et $\mathrm{Aut}(k(\mathcal{P})/k(\mathcal{P}_F)) = \mathrm{Gal}(N/F)$. Les extensions résiduelles $k(\mathcal{P})/k$ et $k(\mathcal{P})/k(\mathcal{P}_F)$ sont donc galoisiennes de groupe $\mathrm{Gal}(N/k(\mathbf{T}))$ et $\mathrm{Gal}(N/F)$ respectivement.

Les éléments $1, z, \ldots, z^{d-1} \in A'_F$ constituent une base de l'extension $F/k(\mathbf{T})$. Notons $\Delta_z \in k[\mathbf{T}]$ le discriminant de cette base (qui est non nul). En utilisant la proposition 1.5.1, on obtient que pour $\mathbf{t}_0 \in \mathbb{A}^r(k)$ en dehors du fermé de Zariski $Z(\Delta_z)$, on a $k(\mathcal{P}_F) = k(z(\mathcal{P}_F))$ où $z(\mathcal{P}_F)$ est l'image dans $k(\mathcal{P}_F)$ de l'élément $z \in A'_F$. Son polynôme minimal sur k est de degré d et divise $p(\mathbf{t}_0, Y)$, qui est de degré d ; on a donc $p(\mathbf{t}_0, Y)$ irréductible. □

Remarque 1.9.2. — Si on ne suppose pas $P(\mathbf{t}_0, Y)$ irréductible dans $k[Y]$, la fin de la preuve donne plus généralement que pour $\mathbf{t}_0 \in \mathbb{A}^r(k) \setminus Z(\Delta)$, toute extension résiduelle au-dessus de $\mathbf{t}_0$ est k-conjuguée à une extension du type $k[Y]/(\pi)$ où π est un facteur irréductible de $p(\mathbf{t}_0, Y)$ dans $k[Y]$. On va voir plus bas que la réciproque est vraie (§1.9.3), de sorte que :

(*) *Pour $\mathbf{t}_0 \in \mathbb{A}^r(k)$ sauf dans un fermé propre de Zariski, les extensions résiduelles correspondent aux facteurs irréductibles de $p(\mathbf{t}_0, Y)$.*

On peut même préciser que *ce sont les idéaux maximaux $\mathcal{P}_F$ qui correspondent aux facteurs irréductibles de $p(\mathbf{t}_0, Y)$*. En effet, si $\mathcal{P}_1, \dots \mathcal{P}_f$ sont les idéaux maximaux de A'_F au-dessus de $\mathbf{t}_0$, alors $A'_F/\bigcap_{i=1}^f \mathcal{P}_i$ est un k-espace vectoriel, de dimension $\leq [F : k(\mathbf{T})]$ (k doit être compris ici comme $k[\mathbf{T}]/(\mathbf{T} - \mathbf{t}_0)$ et on utilise à nouveau $\Delta_z(\mathbf{t_0}) \neq 0$). Le lemme chinois (lemme 1.1.6) donne l'isomorphisme

$$A'_F/\bigcap_{i=1}^{f} \mathcal{P}_i \simeq \prod_{i=1}^{f} A'_F/\mathcal{P}_i$$

On déduit que la somme des degrés résiduels $[A'_F/\mathcal{P}_i : k]$, $i = 1, \dots, f$ est inférieure à $[F : k(\mathbf{T})]$[(12)]. D'après le fait (*), cette somme est nécessairement *égale* à $[F : k(\mathbf{T})]$.

Un cas particulier est le suivant. Pour tout $\mathbf{t}_0$ en dehors d'un fermé propre de Zariski de $\mathbb{A}^r(k)$, il y a équivalence entre

(i) *Il n'y a qu'un point fermé dans A'_F au-dessus de $\mathbf{t}_0$, et*

(ii) *$p(\mathbf{t}_0, Y)$ est irréductible dans $k[Y]$.*

1.9.2. Théorème de spécialisation (par les extensions spécialisées). — Soit $P(\mathbf{T}, Y) \in k(\mathbf{T})[Y]$ un polynôme irréductible dans $k(\mathbf{T})[Y]$ et tel que le corps de rupture $N/k(\mathbf{T})$ soit une extension galoisienne de $k(\mathbf{T})$. Notons $y_1, \dots, y_D$ les racines de P dans $\overline{k(\mathbf{t})}$. Pour $i = 1, \dots, D$, on peut écrire

$$y_i = \frac{a_i(\mathbf{T}, y_1)}{b_i(\mathbf{T})} \text{ où } a_i \in k[\mathbf{T}, Y] \text{ et } b_i \in k[\mathbf{T}]$$

On note G le groupe de Galois $\mathrm{Gal}(N/k(\mathbf{T}))$ et $\Delta(\mathbf{t})$ le discriminant de P par rapport à Y.

(12) Ce fait est vrai plus généralement si $k[\mathbf{T}]$ est remplacé par un anneau noethérien et intégralement clos : l'argument donné vaut dans ce cadre.

On se donne aussi un corps intermédiaire F entre $k(\mathbf{T})$ et E et un élément primitif

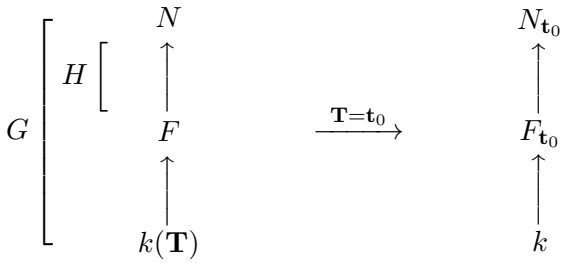
$$z = \frac{a(\mathbf{T}, y_1)}{b(\mathbf{T})} \text{ où } a \in k[\mathbf{T}, Y] \text{ et } b \in k[\mathbf{T}]$$

de l'extension $F/k(\mathbf{T})$. On notera $p \in k(\mathbf{T})[Y]$ le polynôme minimal de z sur $k(\mathbf{T})$. L'extension N/F est galoisienne ; on note H son groupe de Galois.

Soit $\mathbf{t}_0$ un élément de k^r pour lequel un morphisme de spécialisation $\varphi_{\mathbf{t}_0}$ est défini (voir §1.7.3). On suppose de plus que $\Delta(\mathbf{t}_0) \neq 0$, $b(\mathbf{t}_0) \neq 0$ et $b_i(\mathbf{t}_0) \neq 0$, $i = 1, \ldots, d$. On peut donc considérer les extensions "spécialisées"

$$\begin{cases} N_{\mathbf{t}_0} = k(y_1(\mathbf{t}_0), \ldots, y_d(\mathbf{t}_0)) = k(y_1(\mathbf{t}_0)) \\ F_{\mathbf{t}_0} = k(z(\mathbf{t}_0)) = k\left(\frac{a(\mathbf{t}_0, y_1(\mathbf{t}_0))}{b(\mathbf{t}_0)}\right) \end{cases}$$

Le diagramme suivant résume la situation.



Théorème 1.9.3. — *On suppose les conditions précédentes satisfaites ; en particulier* $\mathbf{t_0}$ *est un point quelconque dans* $\mathbb{A}^r(k)$ *en dehors d'un certain fermé propre de Zariski. On a alors :*
(a) *Le corps* $N_{\mathbf{t}_0}$ *est le corps de décomposition sur* k *du polynôme* $P(\mathbf{t}_0, Y)$ *; l'extension* $N_{\mathbf{t}_0}/k$ *est galoisienne de groupe de Galois un sous-groupe de* G.
(b) *L'extension* $N_{\mathbf{t}_0}/F_{\mathbf{t}_0}$ *est galoisienne de groupe de Galois un sous-groupe de* H.
(c) $[F_{\mathbf{t}_0} : k] \leq [F : k(\mathbf{T})]$
(d) *Si* $P(\mathbf{t}_0, Y)$ *est irréductible dans* $k[Y]$, *on a*
- $p(\mathbf{t}_0, Y)$ *irréductible dans* $k[Y]$
- $\mathrm{Gal}(N_{\mathbf{t}_0}/k) = G$
- $\mathrm{Gal}(N_{\mathbf{t}_0}/F_{\mathbf{t}_0}) = H$

Ce résultat doit être comparé au théorème 1.9.1. Nous examinerons plus précisément le lien au §1.9.3. Nous commençons par établir le lemme suivant, classique pour $r = 1$. Pour tout anneau intègre κ, on note $\kappa[[\mathbf{T} - \mathbf{t}_0]]$ l'anneau

des séries formelles

$$y(\mathbf{T}) = \sum_{n\geq 0} a_n(\mathbf{T} - \mathbf{t}_0)$$

en les r variables $T_1 - t_{01}, \ldots, T_r - t_{0r}$ (exemples 1.2.15) : les $a_n(\mathbf{T} - \mathbf{t}_0)$ sont des polynômes homogènes de degré n à coefficients dans κ, $(n \geq 0)$. On notera $\kappa((\mathbf{T} - \mathbf{t}_0))$ le corps des fractions de $\kappa((\mathbf{T} - \mathbf{t}_0))$. Remarquons aussi que le morphisme de spécialisation $\varphi_{\mathbf{t}_0} : \kappa[\mathbf{T}] \to \kappa$ s'étend de façon unique en un morphisme $\kappa[[\mathbf{T} - \mathbf{t}_0]] \to \kappa$: l'élément $y(\mathbf{T})$ ci-dessus est envoyé sur a_0.

Lemme 1.9.4. — *Pour tout $i = 1, \ldots, D$, il existe une unique série formelle $y_i(\mathbf{T}) = \sum_{n\geq 0} a_{i,n}(\mathbf{T} - \mathbf{t}_0) \in \overline{k}[[\mathbf{T} - \mathbf{t}_0]]$ telle que $P(\mathbf{T}, y_i(\mathbf{T})) = 0$ et $a_{i,o} = y_i(\mathbf{t}_0)$. Plus précisément, cette série formelle est à coefficients dans $k(y_i(\mathbf{t}_0))$.*

Démonstration. — Il s'agit d'un cas particulier du lemme de Hensel (théorème 1.2.17) : l'anneau $A = \kappa[[\mathbf{T} - \mathbf{t}_0]]$ a été défini comme le complété de $\kappa[\mathbf{T}]$ pour la métrique associée à l'idéal maximal I engendré par $T_1 - t_{01}, \ldots, T_r - t_{0r}$; il est donc hensélien. L'hypothèse de simplicité des racines modulo I est garantie par la condition $\Delta(\mathbf{t}_0) \neq 0$.

Une alternative est d'expliciter la méthode de Newton dans ce cas particulier. Fixons un indice $i \in \{1, \ldots, D\}$. Par changement de variable, on se ramène à la situation où $\mathbf{t}_0 = \mathbf{0} = (0, \ldots, 0)$ et $y_i(\mathbf{t}_0) = 0$. Pour tout entier $n > 0$, la partie homogène de degré n dans $P(\mathbf{T}, y_i(\mathbf{T}))$ est de la forme

$$p_1(\mathbf{0})a_{i,n}(\mathbf{T}) + r_n(\mathbf{T}, a_{i,n-1}(\mathbf{T}), \ldots, a_{i,1}(\mathbf{T}))$$

où $p_1(\mathbf{T})$ est le coefficient de Y dans le polynôme $P(\mathbf{T}, Y)$ et r_n est un polynôme à coefficients dans k. L'hypothèse $\Delta(\mathbf{t}_0)c(\mathbf{t_0}) \neq 0$ donne que $p_1(\mathbf{0}) \neq 0$. L'unicité de la série recherchée en découle aussitôt. Pour l'existence, on considère la série formelle dont les parties homogènes $a_{i,n}(\mathbf{T})$ sont définies par la formule de récurrence précédente ; cette série est limite dans l'espace métrique complet $k[[\mathbf{T}]]$ d'une suite de polynômes qui est de Cauchy. Par construction, cette série vérifie $P(\mathbf{T}, y_i(\mathbf{T})) = 0$. □

Démonstration du théorème 1.9.3. — Par définition, le corps $N_{\mathbf{t}_0}$ est le corps de décomposition du polynôme $P(\mathbf{t}_0, Y)$, lequel n'a que des racines distinctes ; $N_{\mathbf{t}_0}$ est donc une extension galoisienne de k. D'après le lemme 1.9.4, le corps N est peut être identifié (à $k(\mathbf{T})$-isomorphisme près) au sous-corps $k(\mathbf{T}, y_1(\mathbf{T}), \ldots, y_D(\mathbf{T}))$ du corps $\overline{k}((\mathbf{T} - \mathbf{t}_0))$. D'après ce lemme, on a même alors $k(\mathbf{T}, y_1(\mathbf{T}), \ldots, y_D(\mathbf{T})) \subset N_{\mathbf{t}_0}((\mathbf{T} - \mathbf{t}_0))$. On peut étendre tout élément $\tau \in \mathrm{Gal}(N_{\mathbf{t}_0}/k)$ en un $k(\mathbf{T})$-automorphisme de l'anneau $N_{\mathbf{t}_0}[[\mathbf{T} - \mathbf{t}_0]]$ (en faisant agir τ sur les coefficients des séries formelles) et donc aussi en un

$k(\mathbf{T})$-automorphisme $\tilde{\tau}$ du corps $N_{\mathbf{t}_0}((\mathbf{T}-\mathbf{t}_0))$. L'extension $N/k(\mathbf{T})$ étant galoisienne, $\tilde{\tau}$ laisse N invariant. La correspondance $\tau \to \tilde{\tau}$ définit un homomorphisme

$$s : \mathrm{Gal}(N_{\mathbf{t}_0}/k) \to \mathrm{Gal}(N/k(\mathbf{T}))$$

Cet homomorphisme est injectif. Cela prouve (a).

Pour montrer (b), il suffit de montrer que $s(\mathrm{Gal}(N_{\mathbf{t}_0}/F_{\mathbf{t}_0})) \subset H = \mathrm{Gal}(N/F)$. Soit $p_F(Y)$ le polynôme minimal de y_1 sur F : p_F est dans $k[\mathbf{T}, \gamma(\mathbf{T})^{-1}, z][Y]$, pour un certain $\gamma(\mathbf{T}) \in k[\mathbf{T}, z]$ non nul. Supposons $\gamma(\mathbf{t}_0) \neq 0$. L'image, notée $p_F(\mathbf{t}_0, Y)$, du polynôme $p_F(Y)$ par $\varphi_{\mathbf{t}_0}$ est alors dans $F_{\mathbf{t}_0}[Y]$, et on a $p_F(\mathbf{t}_0, y_1(\mathbf{t}_0)) = 0$. Considérons un élément τ quelconque dans $\mathrm{Gal}(N_{\mathbf{t}_0}/F_{\mathbf{t}_0})$. L'automorphisme τ envoie $y_1(\mathbf{t}_0)$ sur une racine $y_i(\mathbf{t}_0)$ du polynôme $p_F(\mathbf{t}_0, Y)$. Il en résulte que $\tilde{\tau}$ envoie y_1 sur une racine de $p_F(Y)$, c'est-à-dire un élément de N qui est F-conjugué à y_1 ; autrement dit $\tilde{\tau} = s(\tau) \in H$.

Il résulte de $p(\mathbf{T}, z) = 0$ que $p(\mathbf{t}_0, z(\mathbf{t}_0)) = 0$. L'assertion (c) en découle aussitôt.

Supposons maintenant $P(\mathbf{t}_0, Y)$ irréductible dans $k[Y]$. Il résulte de $P(\mathbf{t}_0, y_1(\mathbf{t}_0)) = 0$ et $N_{\mathbf{t}_0} = k(y_1(\mathbf{t}_0))$ que $[N_{\mathbf{t}_0} : k] = \deg_Y P = [N : k(\mathbf{T})]$. D'après (b) et (c), on a $[N_{\mathbf{t}_0} : F_{\mathbf{t}_0}] \leq [N : F]$ et $[F_{\mathbf{t}_0} : k] \leq [F : k(\mathbf{T})]$. Il résulte de la multiplicativité des degrés que ces inégalités sont nécessairement des égalités. Vu ce qu'on a déjà montré en (a) et (b), le reste de (d) découle immédiatement. □

Remarque 1.9.5. — A quelques modifications mineures près, le §1.9.1 et le §1.9.2 restent valables si $k[\mathbf{T}]$ est remplacé par un localisé $k[\mathbf{T}]_{\Delta^\infty}$ où $\Delta \in k[\mathbf{T}]$, $\Delta \neq 0$. Dans les énoncés sur $\mathbf{t}$, ce changement n'affecte qu'un fermé propre de Zariski puisque $\mathrm{Spec}(k[\mathbf{T}]_{\Delta^\infty})$ correspond à l'ouvert complémentaire dans $\mathbb{A}^r$ de $Z(\Delta)$.

1.9.3. Lien entre les deux aspects. — Le §1.9.2 peut paraître plus élémentaire. Le §1.9.1 est plus général car il permet de définir les extensions résiduelles pour tout $\mathbf{t}_0 \in \mathbb{A}^r(k)$ (et pas seulement pour tout point en dehors d'un fermé propre de Zariski). Quand les extensions sont galoisiennes, c'est pour tout $\mathbf{t}_0 \in \mathbb{A}^r(k)$ qu'on a une formule pour le groupe de Galois résiduel.

Le lien entre les extensions spécialisées et les extensions résiduelles ne peut se faire qu'en dehors d'un fermé de Zariski. Nous gardons les notations précédentes. Nous allons comparer extensions résiduelles et extensions spécialisées au niveau de l'extension $F/k(\mathbf{T})$.

Si $\varphi_{\mathbf{t}_0}$ est un morphisme de spécialisation au-dessus de $\mathbf{t}_0$, son noyau est un idéal maximal $\mathcal{P}$ au-dessus de $\mathbf{t}_0$. Réciproquement, si $\mathcal{P}$ est un idéal maximal de A'_F au-dessus de $\mathbf{t}_0$, le morphisme $A'_F \to A'_F/\mathcal{P}$ est un morphisme de spécialisation au-dessus de $\mathbf{t}_0$. Et il est clair que $z \ [\mathrm{mod}\ \mathcal{P}] = \varphi_{\mathbf{t}_0}(z) = z(\mathbf{t}_0)$.

De plus, on sait d'après la proposition 1.5.1, que, pour tout $\mathbf{t}_0 \in \mathbb{A}^r(k)$ en dehors d'un fermé de Zariski, l'extension résiduelle $\bar{F}_{\mathcal{P}}/k$ est engendrée par $z(\mathbf{t}_0)$. C'est-à-dire, $\bar{F}_{\mathcal{P}} = F_{\mathbf{t}_0}$. Conclusion : en dehors d'un fermé de Zariski, extensions résiduelles et extensions spécialisées coincident.

On peut aussi maintenant conclure la remarque 1.9.2 : pour presque tout $\mathbf{t}_0$, toute extension du type $k[Y]/(\pi)$ où π est un facteur irréductible de $p(\mathbf{t}_0, Y)$ dans $k[Y]$ est une extension résiduelle/spécialisée au-dessus de $\mathbf{t}_0$; on utilise ici le fait indiqué dans le §1.7.3 que $\varphi_{\mathbf{t}_0}(y_1)$ peut être n'importe quelle racine de $p(\mathbf{t}_0, Y)$.

CHAPITRE 2

INTRODUCTION À L'ARITHMÉTIQUE DES REVÊTEMENTS

2.1. Problème inverse de Galois

2.1.1. Enoncé du problème. — Le problème inverse de la théorie de Galois est l'étude de la conjecture suivante. On le note parfois **IGP** pour "Inverse Galois Problem".

***Conjecture 2.1.1* (IGP).** — *Tout groupe fini G est le groupe de Galois* $\mathrm{Gal}(E/\mathbb{Q})$ *d'une extension de corps $E/\mathbb{Q}$.*

Dans la suite, on dit qu'un groupe G est groupe de Galois sur un corps K s'il est le groupe de Galois d'une extension E/K, ou, de façon équivalente, s'il est quotient du groupe de Galois absolu G_K ou encore image d'un homomorphisme (continu) $\mathrm{G}_K \to G.$. Le problème inverse consiste à *réaliser* tous les groupes finis comme groupes de Galois sur $\mathbb{Q}$.

2.1.2. Groupes abéliens. — Le cas des groupes abéliens est classique. Sa démonstration utilise le lemme suivant.

Lemme 2.1.2. — *Pour tout entier $m \neq 0$, il existe une infinité de nombres premiers congrus à 1 modulo m.*

Il s'agit d'un cas particulier du théorème de Dirichlet. Ce cas particulier possède une démonstration élémentaire.

Démonstration. — On note ϕ_m le polynôme cyclotomique d'ordre m. Le résultat découle de l'observation suivante :

(*) si p est un diviseur premier d'une valeur $\phi_m(n)$ de ϕ_m en un entier n, alors ou bien p divise m ou bien $p \equiv 1\ [m]$.

En effet, si p divise $\phi_m(n)$, alors $n^m \equiv 1 \pmod{p}$ (car $T^m - 1 = \prod_{d/m} \phi_d(T)$). De plus, si $n^\mu \equiv 1 \pmod{p}$ pour un diviseur strict μ de m, alors n est une racine double de $T^m - 1$ modulo p. On a alors $m.n^{m-1} \equiv 0 \pmod{p}$ et donc $m \equiv 0 \pmod{p}$ ($n \equiv 0 \pmod{p}$ est interdit par $n^m \equiv 1 \pmod{p}$). On conclut que ou bien $m \equiv 0 \pmod{p}$ ou bien n est d'ordre m modulo p. Dans le second cas, on a alors, m divise $p - 1$.

A partir de (*), il est facile de construire une infinité de nombres premiers congrus à 1 modulo m. Si $p_1, \ldots, p_k$ le sont, alors les diviseurs premiers de $\phi_m(mp_1 \cdots p_k)$ sont congrus à 1 modulo m et sont distincts de $p_1, \ldots, p_k$. □

Théorème 2.1.3. — *Tout groupe fini abélien G est groupe de Galois sur $\mathbb{Q}$.*

Démonstration. — Tout groupe abélien est isomorphe à un produit

$$\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$$

(les m_i non nécessairement distincts). Grâce au lemme ci-dessus, on peut trouver r nombres premiers distincts $p_1, \ldots, p_r$ tels que $p_i \equiv 1 \ [m_i]$. Le produit ci-dessus est alors un quotient de

$$\frac{\mathbb{Z}}{(p_1 - 1)\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{(p_r - 1)\mathbb{Z}}$$

Il suffit donc de réaliser ce dernier groupe produit sur $\mathbb{Q}$. Or, ce groupe est le groupe de Galois de l'extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ pour $N = p_1 \cdots p_r$ et ζ_N une racine primitive N-ième de 1. En effet, on a

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times$$

□

2.1.3. Les groupes résolubles. — Le cas des groupes résolubles a été également été traité mais est beaucoup plus difficile.

Théorème 2.1.4 **(Shafarevitch)**. — *Tout groupe fini résoluble G est groupe de Galois sur $\mathbb{Q}$.*

La première démonstration de Shafarevitch comportait une erreur. Shafarevitch et ses étudiants ont expliqué comment la corriger. Certains sont restés sceptiques mais après plusieurs articles et livres, il semble qu'on dispose aujourd'hui d'une preuve complète. Dans son livre [**Ser92**], Serre mentionne l'énoncé de Shafarevitch mais ne donne la démonstration que du cas particulier suivant.

Théorème 2.1.5 **(Scholz-Reichardt)**. — *Tout groupe fini nilpotent d'ordre impair est groupe de Galois sur $\mathbb{Q}$.*

D'après le théorème de Feit-Thompson, tout groupe d'ordre impair est résoluble. Le théorème de Scholz-Reichardt résulte bien de l'énoncé de Safaravic. Pour démontrer le théorème de Scholz-Reichardt, on peut se ramener au cas d'un p-groupe avec $p \neq 2$. En effet, un groupe est nilpotent si et seulement s'il est le produit direct de ses sous-groupes de Sylow (qui sont distingués).

2.2. Théorème d'irréductibilité de Hilbert

Après les groupes résolubles, on peut essayer de s'attaquer au cas des groupes simples non abéliens. Dans ce cas, le problème est encore ouvert : on ne sait pas réaliser tous les groupes simples sur $\mathbb{Q}$. Un résultat très important des années 70 a été la classification des groupes finis simples. La liste comporte les groupes alternés A_n ($n \geq 5$), un certain nombre de familles de groupes géométriques sur un corps fini comme $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSU}_n(\mathbb{F}_q)$ etc. et une liste finie de 26 groupes appelés groupes *sporadiques*. On sait réaliser sur $\mathbb{Q}$ le groupe alterné, certains groupes géométriques sur certains corps $\mathbb{F}_q$, notamment sur les sous-corps premiers $\mathbb{F}_p$ et 25 des 26 groupes sporadiques.

La méthode utilisée pour les groupes simples diffère du cas résoluble. On cherche d'abord à réaliser les groupes sur $\mathbb{Q}(T)$. Comme nous allons le voir, on peut ensuite spécialiser l'indéterminée T. Cela résulte du théorème d'irréductibilité de Hilbert dont la forme la plus simple est le théorème 2.2.1 ci-dessous.

Cette section est une introduction au chapitre 5 où sera étudiée en détails la propriété de spécialisation de Hilbert.

2.2.1. Le théorème de Hilbert. —

Théorème 2.2.1 **(Hilbert)**. — *Soit $P(T,Y)$ un polynôme irréductible dans $\mathbb{Q}(T)[Y]$. Alors il existe une infinité d'éléments $t \in \mathbb{Q}$ tels que $P(t,Y)$ est irréductible dans $\mathbb{Q}[Y]$.*

Par exemple si $P(T,Y) = Y^2 - T$, $P(t,Y)$ est irréductible dans $k[Y]$ si et seulement si t n'est pas un carré dans k. Si $k = \mathbb{C}$, cela n'arrive jamais. Mais pour d'autres corps, $k = \mathbb{Q}$ par exemple, il existe "beaucoup" (une infinité) d'éléments non carrés. D'après le théorème d'irréductibilité de Hilbert (TIH), cela est vrai pour tout polynôme $P(T,Y)$ irréductible.

Plus généralement on envisage la situation suivante. Etant donnés un corps k, 3 entiers $n, r, s > 0$, $r + s$ variables $T_1, \ldots, T_r, Y_1, \ldots, Y_s$ et n polynômes $P_1, \ldots, P_n \in k(T_1, \ldots, T_r)[Y_1, \ldots, Y_s]$, supposés irréductibles dans

$k(T_1,\dots,T_r)[Y_1,\dots,Y_s]$, on pose

$$H_{P_1,\dots,P_n}=\left\{(t_1,\dots,t_r)\in k^r \;\middle|\; \begin{array}{c} P_i(t_1,\dots,t_r,Y_1,\dots,Y_s) \text{ irréductible} \\ \text{dans } k[Y_1,\dots,Y_s], i=1,\dots,n \end{array}\right\}$$

Les ensembles de la forme $H_{P_1,\dots,P_n}$ (avec $n,s>0$ quelconques) sont appelés *ensembles hilbertiens* ou *parties hilbertiennes* de k^r. Nous parlerons des variables $T_1,\dots,T_r$ qu'on spécialise comme des paramètres et des autres variables $Y_1,\dots,Y_s$ comme des indéterminées. Nous noterons parfois $\mathbf{T}$, $\mathbf{t}$ et $\mathbf{Y}$ pour $T_1,\dots,T_r$, $t_1,\dots,t_r$ et $Y_1,\dots,Y_s$ respectivement. Noter aussi que l'irréductibilité de P_i dans $k(\mathbf{T})[\mathbf{Y}]$ impose en particulier que $\deg_{\mathbf{Y}}(P_i)>0$, $i=1,\dots,r$.

Définition 2.2.2. — Un corps k est dit hilbertien si pour tout $r>0$, les parties hilbertiennes de k^r sont Zariski-denses.

De façon plus explicite, la condition est que toute partie hilbertienne contienne des points $(t_1,\dots,t_r)$ en dehors de toute hypersurface $Q(t_1,\dots,t_r)=0$ de k^r fixée à l'avance (avec $Q\neq 0$). Pour $r=1$, cela signifie simplement que les parties hilbertiennes sont infinies.

Remarque 2.2.3. — Dans [**Ser97**] et [**Ser92**], la propriété d'hilbertianité est définie un peu différemment à partir des parties *minces*. Un corps hilbertien est un corps k pour lequel k^r n'est pas mince pour tout $r>0$. L'équivalence des deux définitions correspond au fait que les parties minces sont les sous-ensembles de k^r contenus dans le complémentaire d'une partie hilbertienne.

Théorème 2.2.4 **(Hilbert)**. — *Le corps $\mathbb{Q}$ est un corps hilbertien.*

On donne ci-après la preuve du cas "1 paramètre, 1 variable" et en particulier du théorème 2.2.1 ; le cas général s'en déduit par des réductions classiques qui sont détaillées au §5.1 du chapitre 5. De $\mathbb{Q}$ hilbertien résulte que les corps de nombres le sont aussi et même, les extensions de type fini de $\mathbb{Q}$. Les corps algébriquement clos, les corps henséliens ne sont pas hilbertiens.

2.2.2. Réduction à la recherche de points sur des courbes algébriques. — Etant donnés N polynômes $Q_1,\dots,Q_N\in k(T)[Y]$ sans racine dans $k(T)$, on pose

$$V'_{Q_1,\dots,Q_N}=\left\{t\in k \;\middle|\; \begin{array}{c} Q_i(t,Y) \text{ n'a pas de} \\ \text{racine dans } k, i=1,\dots,N \end{array}\right\}$$

Autrement dit, si on note C_i la courbe affine $Q_i(t,y)=0$ et $C_i(k)$ l'ensemble de ses points k-rationnels, $i=1,\dots,N$, l'ensemble $V'_{Q_1,\dots,Q_N}$ est le

complémentaire dans k de la réunion des images $\mathrm{pr}_t(C_i(k))$ $(i = 1, \dots, N)$ par la projection $(t, y) \to t$.

Si $Q_1, \dots, Q_N$ sont irréductibles, on a $H_{Q_1,\dots,Q_N} \subset V'_{Q_1,\dots,Q_N}$: "être irréductible sur k" est plus fort que "ne pas avoir de racine dans k". La proposition suivante peut être vue comme une certaine réciproque.

Proposition 2.2.5. — *Etant donnés n polynômes irréductibles $P_1, \dots, P_n \in k(T)[Y]$, il existe N polynômes $Q_1, \dots, Q_N \in k[T, Y]$ sans racine dans $k(T)$ et unitaires (en Y) et un ensemble fini $F \subset k$ tels que*

$$V'_{Q_1,\dots,Q_N} \subset H_{P_1,\dots,P_n} \cup F$$

De plus, si on suppose les polynômes $P_1, \dots, P_n$ séparables en Y[(1)] (e.g. si k est de caractéristique 0), alors on peut demander aux polynômes $Q_1, \dots, Q_N$ d'être séparables et irréductibles dans $\overline{k}[T, Y]$ (quitte à grossir l'ensemble F).

Pour "irréductible dans $\overline{k}[T, Y]$" on dit "absolument irréductible".

Exemple 2.2.6. — Soit $P(T, Y) = Y^4 - T$. Les décompositions non triviales de $P(T, Y) \in \mathbb{Q}[T, Y]$ dans $\overline{\mathbb{Q}(T)}[Y]$ sont de la forme suivante :

$$\begin{aligned}
&(Y \pm \sqrt[4]{T})\, R\\
&(Y \pm i\sqrt[4]{T})\, R\\
&(Y - \sqrt[4]{T})(Y + \sqrt[4]{T})\, R = (Y^2 - \sqrt{T})\, R\\
&(Y - \sqrt[4]{T})(Y - i\sqrt[4]{T})\, R = (Y^2 - (1+i)\sqrt[4]{T}Y + i\sqrt{T})\, R\\
&(Y - \sqrt[4]{T})(Y + i\sqrt[4]{T})\, R = (Y^2 - (1-i)\sqrt[4]{T}Y - i\sqrt{T})\, R\\
&(Y - i\sqrt[4]{T})(Y + \sqrt[4]{T})\, R = (Y^2 + (1-i)\sqrt[4]{T}Y - i\sqrt{T})\, R\\
&(Y - i\sqrt[4]{T})(Y + i\sqrt[4]{T})\, R = (Y^2 + \sqrt{T})\, R\\
&(Y + \sqrt[4]{T})(Y + i\sqrt[4]{T})\, R = (Y^2 + (1+i)\sqrt[4]{T}Y + i\sqrt{T})\, R
\end{aligned}$$

où $R \in \overline{\mathbb{Q}(T)}[Y]$. Pour $t \in \mathbb{Q}$, une décomposition non triviale de $Y^4 - t$ est induite par l'une d'entre elles. Une telle décomposition n'existe pas si

$$\begin{cases} \sqrt[4]{t}, i\sqrt[4]{t} \notin \mathbb{Q} \\ \sqrt{t} \notin \mathbb{Q} \\ i\sqrt{t} \notin \mathbb{Q} \end{cases} \quad \text{c'est-à-dire, si} \quad \begin{cases} Q_1 = Y^4 - T \text{ n'a pas de racine dans } \mathbb{Q} \\ Q_2 = Y^2 - T \text{ n'a pas de racine dans } \mathbb{Q} \\ Q_3 = Y^2 + T \text{ n'a pas de racine dans } \mathbb{Q} \end{cases}$$

En conclusion, on a $V'_{Q_1,Q_2,Q_3} \subset H_P$.

(1) c'est-à-dire, n'ayant pas de racine multiple dans $\overline{k(T)}$.

Démonstration de la proposition 2.2.5. — Fixons $i \in \{1, \dots, n\}$ et posons $P = P_i$. On part d'une décomposition de $P(T, Y)$ dans $\overline{k(T)}[Y]$:

$$P(T, Y) = c(T) \prod_{i=1}^{d} (Y - y_i)$$

où $c(T) \in k(T)$ et $y_1, \dots, y_d \in \overline{k(T)}$.

Soit $t_0 \in K$ tel qu'un morphisme de spécialisation $\varphi_{t_0} : k[T, y_1, \dots, y_d] \to \overline{k}$ soit défini (§1.7.3). On a donc, dans $\overline{k}[Y]$

$$P(t_0, Y) = c(t_0) \prod_{i=1}^{d} (Y - y_i(t_0))$$

Supposons que $P(t_0, Y) = c(t_0) r(Y) s(Y)$ avec $r(Y), s(Y) \in k[Y]$ unitaires en Y et avec $\deg(r) > 0$ et $\deg(s) > 0$. En vertu de l'unicité de la décomposition en irréductibles dans $\overline{k}[Y]$, il existe nécessairement un sous-ensemble $I \subset \{1, \dots, d\}$ tel que $r(Y) = \prod_{i \in I} (Y - y_i(t_0))$ et $s(Y) = \prod_{i \notin I} (Y - y_i(t_0))$.

Considérons alors les polynômes

$$\begin{cases} R(Y) = \prod_{i \in I} (Y - y_i) \\ S(Y) = \prod_{i \notin I} (Y - y_i) \end{cases}$$

Le polynôme $P(T, Y) = c(T) R(Y) S(Y)$ étant irréductible dans $k(T)[Y]$, il existe nécessairement un coefficient γ de $R(Y)$ ou de $S(Y)$ qui n'appartient pas à $k(T)$. Par construction, ce coefficient γ est dans $k[T, y_1, \dots, y_d] \subset \overline{k(T)}$ et vérifie $\gamma(t_0) \in k$. Notons $Q(T, Y) \in k[T, Y]$ le polynôme minimal de γ sur $k(T)$. Par construction, $Q(T, Y)$ est irréductible dans $k(T)[Y]$ et $\deg_Y(Q) \geq 2$, donc $Q(T, Y)$ n'a pas de racine dans $k(T)$; d'autre part, $Q(t_0, Y)$ a une racine dans k (à savoir $\gamma(t_0)$). De plus, quitte à remplacer γ par $d(T)\gamma$ avec $d(T) \in k[T]$ convenable, on peut supposer que γ est entier sur $k[T]$ et donc que $Q(T, Y)$ est unitaire en Y.

Notons $\{Q_1, \dots, Q_N\}$ l'ensemble fini de tous les polynômes $Q(T, Y)$ obtenus comme précédemment, quand on fait varier I dans l'ensemble de tous les sous-ensembles propres (non vides) de $\{1, \dots, d\}$ (pour chaque sous-ensemble I, on choisit *un* coefficient $\gamma \in \overline{k(T)} \setminus k(T)$ d'un des deux facteurs de la décomposition $P(T, Y) = c(T) R(Y) S(Y)$ associée à I). Pour interdire la possibilité que $P(t_0, Y)$ soit réductible dans $k[Y]$, il suffit de choisir $t_0 \in k$ tel qu'aucun des polynômes $Q_i(t_0, Y)$ ait une racine dans k, c'est-à-dire, de le choisir dans $V'_{Q_1, \dots, Q_N}$ (et en dehors d'un certain ensemble fini).

Les polynômes $Q_1, \dots, Q_N$ peuvent être décrits en fonction de $P_1, \dots, P_n$. Ainsi les extensions associées de $k(T)$ sont toutes des sous-extensions du corps

de décomposition de $P_1 \cdots P_n$. En particulier si $P_1, \ldots, P_n$ sont séparables, alors les polynômes $Q_1, \ldots, Q_N$ ont la même propriété. La dernière partie de l'énoncé sur l'absolue irréductibilité résulte du lemme 2.2.7 ci-dessous. □

Lemme 2.2.7. — *Soit $Q(T,Y) \in k[T,Y]$ un polynôme séparable (en Y), irréductible mais pas absolument irréductible. Alors l'ensemble des points $(t_0, y_0) \in \mathbb{A}^2(k)$ tels que $Q(t_0, y_0) = 0$ est fini.*

Démonstration. — 1er argument, sous l'hypothèse "k de caractéristique 0". Soit $(t_0, y_0) \in \mathbb{A}^2(k)$ tel que $Q(t_0, y_0) = 0$. Soit $\Pi(T,Y)$ un facteur irréductible de $Q(T,Y)$ dans $\overline{k}[T,Y]$. Comme Q est irréductible sur k, on a $\Pi \notin k[T,Y]$. Il existe donc un coefficient γ du polynôme Π dans $\overline{k} \setminus k$. Le corps k étant parfait, ce coefficient γ est séparable sur k et il admet donc au moins un conjugué γ^τ distinct de γ ; en conséquence, Π^τ est distinct de Π (ici $\tau \in \mathrm{G}_K$ agit sur les coefficients dans $\overline{k}$ de Π). Ce polynôme Π^τ est alors un autre facteur irréductible de $Q(T,Y)$ dans $\overline{k}[T,Y]$. Le produit $\Pi(T,Y)\Pi^\tau(T,Y)$ divise donc $Q(T,Y)$. On en déduit que y_0 est une racine double de $Q(t_0,Y)$; l'élément t_0 est donc une racine du discriminant $\Delta(T) \in k[T]$ du polynôme Q par rapport à la variable Y. Comme Q est supposé séparable, ce discriminant est non nul et n'a qu'un nombre fini de racines.

2ème argument, dans le cas général. Le *corps des constantes* C_Q d'un polynôme $Q \in k(T)[Y]$ irréductible est défini (à k-isomorphisme près) de la façon suivante : on plonge le corps $R_Q = k(T)[Y]/(Q(T,Y))$ dans $\overline{k(T)}$ et on pose $C_Q = R_Q \cap \overline{k}$. Si $P(T,Y)$ est absolument irréductible, alors $C_P = k$ et la réciproque est vraie si $Q(T,Y)$ est séparable sur $K(T)$ (proposition 2.3.2).

Le polynôme Q étant non absolument irréductible et séparable, son corps des constantes contient strictement k. Soient $\alpha \in C_Q \setminus k$ et $M(Y) \in k[Y]$ son polynôme minimal sur k. Le polynôme $M(Y)$ a une racine dans le corps R_Q. Cela signifie qu'il existe $F(T,Y), R(T,Y) \in k(T)[Y]$ tel que

$$M(F(T,Y)) = R(T,Y)Q(T,Y)$$

Tout point $(t,y) \in \mathbb{A}^2(k)$ peut être substitué à (T,Y) sauf éventuellement ceux d'un nombre fini de droites $t = a$. Supposer qu'il existe une infinité de points $(t_0, y_0) \in k^2$ tels que $Q(t_0, y_0) = 0$ fournit une contradiction puisque qu'on aurait alors $M(F(t_0, y_0)) = 0$ pour une infinité de $(t_0, y_0) \in \mathbb{A}^2(k)$; en particulier, $M(Y)$ serait de degré 1, ce qui contredit $\alpha \notin k$. □

Remarque 2.2.8. — Le deuxième argument montre que si on ne suppose pas que les polynômes $P_1, \ldots, P_n$ sont séparables en Y, dans la proposition 2.2.5, on peut tout de même demander en plus aux polynômes $Q_1, \ldots, Q_N$ d'avoir

un corps des constantes égal à k (à défaut d'être absolument irréductibles). Cela est utilisé dans [**Dèb99b**].

2.2.3. La preuve de Hilbert-Dörge. —

Théorème 2.2.9. — *Pour toute partie hilbertienne H de $\mathbb{Q}$, il existe $\delta > 0$ tel que le nombre d'entiers dans $H^c \cap [1, B]$ est un $\mathrm{O}(B^{1-\delta})$ (où H^c désigne le complémentaire de H dans $\mathbb{Q}$ et B une variable réelle > 0). En conséquence, $\mathbb{Q}$ est un corps hilbertien.*

Remarque 2.2.10. — D'après le théorème des nombres premiers, le nombre de nombres premiers $\leq B$ est équivalent à $B/\log(B)$. Le théorème ci-dessus entraîne donc que toute partie hilbertienne de $\mathbb{Q}$ contient une infinité de nombres premiers. L'estimation du théorème n'est cependant pas la meilleure possible. On peut montrer que le nombre d'entiers dans $H^c \cap [0, B]$ est un $\mathrm{O}(\sqrt{B})$ ([**Lan83**], [**Dèb01**]).

Grâce à la proposition 2.2.5, il suffit de démontrer cet énoncé où H est remplacé par un ensemble du type

$$V'_P = \{t \in \mathbb{Q} | P(t, Y) \text{ n'a pas de racines dans } \mathbb{Q}\}$$

où $P(T, Y) \in \mathbb{Q}[T, Y]$ est absolument irréductible, unitaire en Y et sans racine dans $\mathbb{Q}(T)$. On peut aussi se ramener au cas d'un seul polynôme car si plusieurs polynômes P_i sont donnés, pour chacun desquels une valeur δ_i convient pour $H = V'_{P_i}$, alors le nombre $\min(\delta_i)$ convient pour l'intersection $\bigcap_i V'_{P_i}$.

Fixons un polynôme $P(T, Y)$ comme ci-dessus. Le théorème de Puiseux (théorème 3.1.1) va nous permettre une réduction supplémentaire.

Lemme 2.2.11. — *Il existe un entier $s \in [0, \deg_Y(P)]$, un entier $e > 0$, s séries de Laurent $\varphi_1(T), \ldots, \varphi_s(T)$ en $(1/T)^{1/e}$ et à coefficients dans $\mathbb{R}$ et un nombre réel τ tels que*
(a) *$\varphi_1, \ldots, \varphi_s$ convergent pour tout $t \in \mathbb{R}$ tel que $t > \tau$,*
(b) *pour tout $(t, x) \in \mathbb{R}^2$ tel que $P(t, x) = 0$ et $t > \tau$, il existe $i \in \{1, \ldots, s\}$ tel que $x = \varphi_i(t)$.*

On peut avoir $s = 0$. Dans ce cas la conclusion (b) entraîne que l'ensemble des nombres réels t tels que $P(t, Y)$ a une racine dans $\mathbb{R}$ est majoré.

Démonstration. — Le théorème 3.1.1 permet d'écrire chacune des racines $y = \varphi_i(T)$ de $P(T, Y)$ ($i = 1, \ldots, d = \deg_Y(P)$) comme une série de Puiseux formelle en $1/T$, c'est-à-dire, un élément de $\mathbb{C}(((1/T)^{1/e}))$, pour un entier e qui peut être choisi le même pour chaque racine.

Une telle série de Puiseux s'écrit $T^{n-1}\sum_{\ell=0}^{\infty} c_\ell\,(1/T)^{\frac{\ell}{e}}$ où $n \in \mathbb{Z}$ et $(c_\ell)_{\ell\geq 0}$ est une suite d'éléments de $\overline{\mathbb{Q}}$.

Lemme 2.2.12. — *La série entière $\mathcal{Y} = \sum_{\ell=0}^{\infty} c_\ell z^\ell$ a un rayon de convergence strictement positif.*

Démonstration. — Il est facile de construire à partir de P un polynôme $Q \in k(z)[Y]$ non nul tel que $Q(z,\mathcal{Y}) = 0$. La série $\mathcal{Y}$ est donc algébrique sur $k(z)$. De plus, le polynôme Q est totalement décomposé dans $\overline{\mathbb{Q}}((z))$ et donc l'extension $k(z,\mathcal{Y})/k(z)$ est non ramifiée au-dessus de $z = 0$. D'après le corollaire 1.5.16 (ou [**FJ04**, lemma 2.3.5]), l'extension $k(z,\mathcal{Y})/k(z)$ possède un élément primitif $\mathcal{Z}$ dont le polynôme minimal sur $k(z)$ est dans l'anneau localisé $k[z]_0[Y]$ et dont la réduction modulo l'idéal $\langle z\rangle$ est un polynôme (dans $k[Y]$) séparable. Il résulte du théorème des fonctions implicites que le rayon de convergence de $\mathcal{Z}$ est strictement positif. Mais alors il en de même de $\mathcal{Y}$ qui s'écrit comme un polynôme en $\mathcal{Z}$ à coefficients dans $k(z)$. □

En conséquence du lemme 2.2.12, il existe un nombre réel τ tel que $\varphi_1(T),\ldots,\varphi_s(T)$ définissent des fonctions analytiques définies sur $]\tau,+\infty[$. Pour $t \in]\tau,+\infty[$, les racines du polynôme $P(t,Y)$ dans $\mathbb{C}$ sont les nombres $\varphi_1(t),\ldots,\varphi_d(t)$.

Considérons un indice $i \in \{1,\ldots,d\}$ pour lequel la série de Puiseux $\varphi(T) = T^{n-1}\sum_{\ell=0}^{\infty} c_\ell\,(1/T)^{\frac{\ell}{e}}$ a des coefficients non réels. La différence $\varphi(T) - \varphi^c(T)$ (avec c la conjugaison complexe) est de la forme

$$\varphi(T) - \varphi^c(T) = T^{n-1}\left(\sum_{\ell=\ell_0}^{\infty} b_\ell\,(1/T)^{\frac{\ell}{e}}\right) \quad \text{avec } b_{l_0} \neq 0$$

Posons $\psi(T) = T^{1-n+\frac{l_0}{e}}(\varphi(T) - \varphi^c(T))$; c'est une série formelle en $(1/T)^{1/e}$ de terme constant $b_{l_0} \neq 0$. Comme $\psi(t)$ tend vers b_{l_0} quand t tend vers $+\infty$, on obtient que pour t suffisamment grand, $\psi(t) \neq 0$, c'est-à-dire $\varphi(t) - \varphi^c(t) \neq 0$ et donc $\varphi(t) \notin \mathbb{R}$. On obtient la conclusion souhaitée (quitte à augmenter le nombre réel τ). Les s séries de Laurent de l'énoncé sont celles parmi $\varphi_1(T),\ldots,\varphi_d(T)$ qui sont à coefficients réels. □

Pour établir le théorème 2.2.9, il reste à démontrer le lemme suivant.

Lemme 2.2.13. — *Soient e, n deux entiers > 0 et*

$$\varphi(t) = t^{n-1}\sum_{\ell=0}^{\infty} c_\ell\,(1/t)^{\frac{\ell}{e}}$$

une série de Laurent en $(1/t)^{1/e}$ *à coefficients* $c_\ell \in \mathbb{R}$ *convergeant pour tout* $t \in \mathbb{R}$ *supérieur à un nombre réel* τ. *Soit*

$$V_\varphi = \{t \in \mathbb{Z} | t > \tau \text{ et } \varphi(t) \in \mathbb{Z}\}$$

Alors il existe $\delta > 0$ *tel que le nombre d'entiers dans* $V_\varphi \cap [0, B]$ *est un* $\mathrm{O}(B^{1-\delta})$.

Démonstration. — Soient $t_0 < \cdots < t_n$ $(n+1)$ points dans V_φ. On va montrer qu'ils ne peuvent pas être trop proches. Notons $x_i = \varphi(t_i)$, $i = 0, \ldots, n$. Considérons le polynôme d'interpolation $F(T) \in \mathbb{R}[T]$ de degré n vérifiant $F(t_i) = x_i$, $i = 0, \ldots, n$. C'est-à-dire

$$F(T) = \sum_{i=0}^{n} x_i \left[\prod_{j \neq i} \frac{T - t_j}{t_i - t_j} \right]$$

La fonction $\varphi - F$ s'annule en $t_0, \ldots, t_n$. D'après le théorème de Rolle (appliqué n fois), il existe $\xi \in [t_0, t_n]$ tel que $\varphi^{(n)}(\xi) = F^{(n)}(\xi)$, c'est-à-dire

$$\varphi^{(n)}(\xi) = n! \sum_{i=0}^{n} \frac{x_i}{\prod_{j \neq i} t_i - t_j}$$

Ce nombre est un nombre rationnel dont un dénominateur est

$$\prod_{0 \leq i < j \leq n} |t_i - t_j| < (t_n - t_0)^{\frac{n(n+1)}{2}}$$

Notons aussi que le développement de $\varphi^{(n)}$ ne comporte que des puissances négatives de $1/t$. En conséquence on a $\varphi(t) \approx \gamma t^{-\mu}$ pour $t \to +\infty$ avec $\gamma \neq 0$ et $\mu > 0$; en particulier, pour t_0 suffisamment grand, $\varphi^{(n)}(\xi) \neq 0$. On obtient donc

$$1 \leq |\varphi^{(n)}(\xi)| (t_n - t_0)^{\frac{n(n+1)}{2}} \leq \gamma' t_0^{-\mu} (t_n - t_0)^{\frac{n(n+1)}{2}}$$

(pour un nombre réel $\gamma' \geq |\gamma|$). En posant $\alpha = \frac{2\mu}{n(n+1)}$, cela conduit à

$$t_n - t_0 \geq c t_0^{\alpha} \qquad (\text{avec } c > 0)$$

Conclusion : si t est un nombre réel suffisamment grand, l'intervalle $[t, t + ct^\alpha]$ contient au plus $n + 1$ points de l'ensemble V_φ. Pour obtenir l'estimation annoncée, on procède de la façon suivante. Soit $\kappa \in]0, 1[$. On coupe l'intervalle $[1, B]$ en $[1, B^\kappa]$ et $[B^\kappa, B]$, puis $[B^\kappa, B]$ en intervalles égaux de longueur $< cB^{\kappa\alpha}$. D'après ce qui précède, chacun des sous-intervalles de $[B^\kappa, B]$ contient au plus $n + 1$ éléments de V_φ. Donc l'intervalle $[1, B]$ contient au plus

$$B^\kappa + (n+1) \frac{B}{cB^{\kappa\alpha}} = \mathrm{O}(B^\kappa + B^{1-\kappa\alpha})$$

éléments de V_φ. Si on prend $\kappa = 1/(1+\alpha)$ (*i.e.* $\kappa = 1 - \kappa\alpha$), alors $0 < \kappa < 1$ et le nombre considéré ci-dessus est un $\mathrm{O}(B^\kappa)$. □

2.2.4. Spécialisation. — Le théorème d'irréductibilité de Hilbert est un résultat fondamental de géométrie arithmétique. Il permet de spécialiser des variables tout en conservant la structure algébrique.

Proposition 2.2.14. — *Soit k un corps hilbertien. Si un groupe fini G est groupe de Galois sur $k(T)$, alors G est groupe de Galois sur k.*

Ce résultat est une conséquence immédiate des théorèmes de spécialisation (théorème 1.9.1 ou théorème 1.9.2) du chapitre 1. Nous en redonnons ci-dessous une preuve directe.

Démonstration. — Soit $E_T/k(T)$ une extension galoisienne de groupe de Galois G. Soient $y(T) \in E_T$ un élément primitif, entier sur $k[T]$ et $P(T,Y) \in k[T,Y]$ le polynôme minimal unitaire de $y(T)$ sur $k(T)$. Le corps k étant supposé hilbertien, il existe une infinité de $t \in k$ tel que $P(t,Y)$ soit irréductible dans $k[Y]$. Pour ces t, notons $y(t) \in \overline{k}$ une racine du polynôme $P(t,Y)$ et $E_t = k(y(t))$ le corps de rupture. Nous allons montrer que sauf pour un nombre fini de t, l'extension E_t/k est galoisienne de groupe G.

L'extension $E_T/k(T)$ étant normale, toute racine de $P(T,Y)$ s'écrit $f_i(T, y(T))$ avec $f_i \in k(T)[Y]$, $i = 1, \ldots, d = \deg_Y(P)$; on a

$$P(T,Y) = \prod_{i=1}^{d} (Y - f_i(T, y(T)))$$

D'après le lemme 1.3.2, le morphisme $k[T] \to \overline{k}$ de spécialisation de T en t se prolonge en un morphisme $\sigma_t : k[T][y(T)] \to \overline{k}$ qui envoie $y(T)$ sur $y(t)$. Sauf pour un nombre fini de t (les racines des dénominateurs dans $k(T)$ des polynômes $f_i \in k(T)[Y]$), on peut appliquer le morphisme σ_t aux deux membres de l'identité précédente pour obtenir :

$$P(t,Y) = \prod_{i=1}^{d} (Y - f_i(t, y(t)))$$

Si on se limite de plus aux éléments $t \in k$ n'annulant pas le discriminant $\Delta(T) \in k[T]$ du polynôme (en Y) $P(T,Y)$ ($\Delta(T) \neq 0$ puisque l'extension $E/k(T)$ est séparable ; cette nouvelle restriction n'élimine qu'un nombre fini de t), on peut ajouter que les racines $f_1(t, y(t)), \ldots, f_d(t, y(t))$ sont distinctes. Pour les t considérés, l'extension E_t/k est galoisienne.

Il reste à voir que le groupe de Galois de ces extensions E_t/k est le groupe G. Les racines $y_1(t), \ldots, y_d(t)$ de $P(t, Y)$ sont simples. D'après le lemme de Hensel (théorème 1.2.17 ou lemme 1.9.4), pour tout $i = 1, \ldots, r$, il existe une unique série formelle $y_i(T) = \sum_{n \geq 0} a_{i,n}(T-t)^n$ telle que $P(T, y_i(T)) = 0$ et $a_{i,o} = y_i(t)$. Le corps E_T est $k(T)$-isomorphe et peut être identifié au sous-corps $k(T, y_1(T), \ldots, y_d(T))$ de $\overline{k}((T-t))$. De plus, pour $i = 1, \ldots, r$, les coefficients $a_{i,n}$ se déduisent tous rationnellement de $a_{i,o}$; ils sont dans $k(a_{i,o})$. L'extension E_t/k étant galoisienne, on a de plus $k(y_i(t)) = E_t$, $i = 1, \ldots, d$.

On peut étendre tout élément $\tau \in \mathrm{Gal}(E_t/k)$ en un $k(T)$-automorphisme $\tilde{\tau}$ de $E_t((T-t))$ en faisant agir τ sur les coefficients des séries formelles. L'extension $E_T/k(T)$ étant galoisienne, $\tilde{\tau}$ laisse E_T invariant. La correspondance $\tau \to \tilde{\tau}$ définit un homomorphisme

$$s : \mathrm{Gal}(E_t/k) \to \mathrm{Gal}(E_T/k(T))$$

Cet homomorphisme est clairement injectif. Comme les deux groupes ont même ordre, c'est un isomorphisme. □

Remarque 2.2.15. — Sauf pour un nombre fini de $t \in k$, tout $k(T)$-automorphisme τ de E_T induit par spécialisation un k-automorphisme τ_t de E_t : si $\tau(y_1(T)) = y_i(T)$, alors $\tau(y_1(t)) = y_i(t)$. Cela donne un homomorphisme

$$r : \mathrm{Gal}(E_T/k(T)) \to \mathrm{Gal}(E_t/k)$$

qui est surjectif. On a de plus $r \circ s = \mathrm{Id}$; s est une section de r.

2.3. Forme régulière du problème inverse de Galois

2.3.1. Extensions régulières. — Pour réaliser un groupe fini sur un corps hilbertien k, il suffit de le réaliser sur $k(T)$. Cette variable supplémentaire T donne un angle d'attaque géométrique au problème. En effet, nous verrons qu'une extension $E/k(T)$, si elle est *régulière*, correspond à un *revêtement algébrique* $X \to \mathbb{P}^1$ *défini sur* k.

Définition 2.3.1. — Etant donné un corps k, une extension séparable $E/k(T)$ est dite régulière (sur k) si k est algébriquement fermé dans E, c'est-à-dire si $E \cap \overline{k} = k$.

La définition d'"extension régulière E/k" associe habituellement à la condition $E \cap \overline{k} = k$ la séparabilité de l'extension E/k (au sens des extensions non nécessairement algébriques [**Lan78**, X,§6]). Nous ne l'indiquons pas dans notre

définition car nous supposons *a priori* la séparabilité de l'extension $E/k(T)$, qui est plus forte que la précédente[(2)].

Proposition 2.3.2. — *Soit $E/k(T)$ une extension séparable finie. Les propositions suivantes sont équivalentes.*

(i) *L'extension $E/k(T)$ est régulière.*

(ii) *Pour toute extension finie séparable F/k, $[EF : F(T)] = [E : k(T)]$.*

(iii) $[Ek^s : k^s(T)] = [E : k(T)]$.

(iv) $[E\overline{k} : \overline{k}(T)] = [E : k(T)]$.

(v) $[E\mathcal{K} : \mathcal{K}(T)] = [E : k(T)]$ *pour tout corps $\mathcal{K}$ sur lequel T est transcendant.*

Démonstration. — (i) $\Rightarrow$ (ii). On peut se contenter de démontrer le résultat pour les extensions galoisiennes F/k. Soit η un élément primitif d'une extension galoisienne F/k et $f(Y) \in k[Y]$ le polynôme minimal unitaire de η sur k. On a $[EF : F(T)] = [E : k(T)]$ si et seulement si $f(Y)$ est irréductible dans $E[Y]$. Supposons que $f(Y) = q(Y)r(Y)$ avec $q(Y), r(Y) \in E(Y)$ unitaires. Si $\eta_1, \ldots, \eta_r$ sont les racines de $f(Y)$ dans F, alors on a nécessairement, à des constantes multiplicatives près, $q(Y) = \prod_{i\in I}(Y - \eta_i)$ et $r(Y) = \prod_{i\in J}(Y - \eta_i)$ avec I et J constituant une partition de $\{1, \ldots, r\}$. Les polynômes sont à coefficients dans F et donc dans $E \cap F \subset E \cap \overline{k} = k$. Comme $f(Y)$ est irréductible dans $k[Y]$, on a $\deg(q) = 0$ ou $\deg(r) = 0$.

Pour la suite de la preuve, on note $y(T)$ un élément primitif de l'extension $E/k(T)$, entier sur $k[T]$, et $P(T, Y) \in k(T)[Y]$ le polynôme minimal unitaire de y sur $k(T)$; on a $P(T, Y) \in k[T, Y]$. Si $\mathcal{K}$ est un corps contenant k, en général $[E\mathcal{K} : \mathcal{K}(T)] \leq [E : k(T)]$ et on a $[E\mathcal{K} : \mathcal{K}(T)] = [E : k(T)]$ si et seulement si $P(T, Y)$ est irréductible dans $k(T)[Y]$.

(ii) $\Rightarrow$ (iii) : Si $P(T, Y)$ était réductible dans $k^{\mathrm{s}}(T)[Y]$, alors il serait réductible dans $F(T)[Y]$ pour F une extension finie séparable de k (puisqu'une décomposition $P(T, Y) = Q(T, Y)R(T, Y)$ ne fait intervenir qu'un nombre fini de coefficients). Cela contredirait la condition (ii).

(iii) $\Rightarrow$ (iv) : On peut supposer k de caractéristique $p > 0$. Notons $\widehat{E}/k(T)$ la clôture normale de $E/k(T)$; elle est séparable. De l'hypothèse résulte que le polynôme $P(T, Y)$ est irréductible sur le corps $k^{\mathrm{s}}(T)^{1/p^\infty}$ obtenu en adjoignant toutes les racines p^m-ièmes des éléments de $k^{\mathrm{s}}(T)$ pour m décrivant $\mathbb{N}$. En effet, les coefficients d'une factorisation $P = AB$ sur ce corps sont dans $\widehat{E} \cap k^{\mathrm{s}}(T)^{1/p^\infty}$

[(2)] La réciproque est fausse : l'extension $\mathbb{F}_p(T^{1/p})/\mathbb{F}_p$ est séparable (car $\mathbb{F}_p$ est parfait) mais l'extension $\mathbb{F}_p(T^{1/p})/\mathbb{F}_p(T)$ ne l'est pas.

qui est égal à $k^{\mathrm{s}}(T)$ puisque les éléments de $k^{\mathrm{s}}(T)^{1/p^\infty} \setminus k^{\mathrm{s}}(T)$ ne sont pas séparables[(3)] (et sont même purement inséparables) ; la factorisation est donc triviale. Ainsi $[Ek^{\mathrm{s}} : k^{\mathrm{s}}(T)] = [Ek^{\mathrm{s}}(T)^{1/p^\infty} : k^{\mathrm{s}}(T)^{1/p^\infty}]$. La conclusion résulte de $\overline{k}(T) \subset k^{\mathrm{s}}(T)^{1/p^\infty}$ qui découle de $\overline{k} = (k^{\mathrm{s}})^{1/p^\infty}$ [(4)].

(iv) $\Rightarrow$ (v) : Supposons que $P = AB$ avec $A, B \in \mathcal{K}(T)[Y]$ unitaires, où $\mathcal{K}$ est un corps contenant k. Comme $P \in k[T, Y]$, on a $A, B \in \mathcal{K}[T, Y]$[(5)]. On peut supposer que $\mathcal{K}$ est une extension de type fini de k. L'idée est ensuite de "spécialiser le corps $\mathcal{K}$ dans $\overline{k}$" afin d'obtenir une décomposition $P = A_0B_0$ avec $A_0, B_0 \in \overline{k}[T, Y]$. L'hypothèse (iv) entraînera alors que $\deg_Y(A_0) = \deg_Y(A) = 0$ ou $\deg_Y(B_0) = \deg_Y(B) = 0$.

Pour cette spécialisation, on invoque le théorème des zéros de Hilbert et plus précisément sa forme préparatoire donnée dans le théorème 1.7.1 : le morphisme $k \to \overline{k}$ se prolonge à l'anneau engendré par les coefficients dans $\mathcal{K}$ des polynômes A et B.

(iv) $\Rightarrow$ (i)[(6)] : Pour tout $\alpha \in \overline{k}$, on a

$$[Ek(\alpha) : k(\alpha, T)] = [E : k(T)]$$

(car on a *a priori* $[E\overline{k} : \overline{k}(T)] \leq [Ek(\alpha) : k(\alpha, T)] \leq [E : k(T)]$). Donc pour tout $\alpha \in E \cap \overline{k}$, on a $[E : k(\alpha, T)] = [E : k(T)]$, ce qui donne $\alpha \in k$. □

2.3.2. La forme régulière du problème inverse de Galois. — La conjecture suivante entraîne la conjecture initiale 2.1.1. On l'appelle la forme régulière du problème inverse de Galois, on la note parfois **RIGP** pour "Regular Inverse Galois Problem".

***Conjecture 2.3.3* (RIGP).** — *Etant donné un corps k quelconque, tout groupe fini G est le groupe de Galois d'une extension galoisienne régulière $E/k(T)$.*

Soient k un corps et $E/k(T)$ une extension galoisienne régulière de groupe G. Si $\mathcal{K}$ est une extension de k sur laquelle T est transcendant, les extensions

(3) Pour le voir, on montre que si α vérifie $\alpha^{p^n} = a \in k^{\mathrm{s}}(T)$ avec n minimal, alors son polynôme minimal sur $k^{\mathrm{s}}(T)$ est $Y^{p^n} - a$: *a priori* il divise celui-ci donc est de la forme $(Y - \alpha)^{p^m r}$ avec $m \leq n$ et $(p, r) = 1$ mais un tel polynôme n'est pas dans $k^{\mathrm{s}}(T)[Y]$ si $m < n$.
(4) Cette égalité est classique : d'après la preuve de la proposition 1.3.7, le polynôme minimal d'un élément $\alpha \in \overline{k}$ est de la forme $Q(X^{p^m})$ avec $Q \in k[X]$ séparable et donc $\alpha^{p^m} \in k^{\mathrm{s}}$.
(5) La raison est classique : les racines de A et B en Y sont entières sur $k[T] \subset \mathcal{K}[T]$; comme $\mathcal{K}[T]$ est intégralement clos, les coefficients de A et B, *a priori* dans $\mathcal{K}(T)$, sont dans $\mathcal{K}[T]$.
(6) L'argument qui suit ne fait pas intervenir l'hypothèse de séparabilité.

$E/k(T)$ et $Ek/k(T)$ sont de même degré (proposition 2.3.2) et en conséquence, leurs groupes de Galois sont isomorphes.

Si $\mathcal{K}$ est hilbertien, on peut spécialiser T dans $\mathcal{K}$ sans changer le groupe de Galois (proposition 2.2.14). On peut ainsi déduire de l'existence de l'extension galoisienne régulière $E/k(T)$ de groupe G que G est groupe de Galois sur tout corps $\mathcal{K}$ hilbertien contenant k sur lequel T est transcendant, par exemple sur tout corps de nombres si $k = \mathbb{Q}$.

Notons aussi que pour réaliser un groupe fini G de façon régulière sur k, il suffit de le réaliser comme groupe de Galois d'une extension $\overline{E}/\overline{k}(T)$ qui provienne par extension des scalaires de k à $\overline{k}$ d'une extension galoisienne régulière $E/k(T)$: le groupe de Galois reste le même sur k et sur $\overline{k}$.

On expliquera dans les chapitres suivants que :

- les extensions finies et séparables de $\overline{k}(T)$ correspondent aux *revêtements algébriques finis de* $\mathbb{P}^1$,

- celles de ces extensions qui proviennent par extension des scalaires de k à $\overline{k}$ d'une extension régulière $E/k(T)$ correspondent aux revêtements $f : X \to \mathbb{P}^1$ *qui peuvent être définis sur* k.

- celles de ces extensions qui proviennent par extension des scalaires de k à $\overline{k}$ d'une extension galoisienne régulière $E/k(T)$ correspondent aux revêtements $f : X \to \mathbb{P}^1$ *galoisiens définis sur* k *ainsi que leurs automorphismes.*

La conjecture **RIGP** se reformule donc comme suit. Son étude constitue l'approche moderne du problème inverse de Galois.

***Conjecture 2.3.4* (RIGP).** — *Etant donné un corps k quelconque, tout groupe fini G est le groupe d'automorphismes d'un revêtement galoisien $f : X \to \mathbb{P}^1$ défini sur k ainsi que ses automorphismes.*

2.3.3. Quotient et produit direct. —

Proposition 2.3.5. — *Soit k un corps. La propriété pour un groupe fini d'être réalisé comme groupe de Galois d'une extension galoisienne régulière $E/k(T)$ est stable par quotient. Si k est infini, elle l'est aussi par produit direct.*

La preuve utilise deux résultats classiques qui seront démontrés plus tard et que nous indiquons ci-dessous. On dit qu'une extension régulière $E/k(T)$ est non ramifiée au-dessus de $t_0 \in \mathbb{P}^1(\overline{k})$ ou que t_0 n'est pas un point de branchement de l'extension $E/k(T)$ s'il existe un $\overline{k}(T)$-homomorphisme (ou plongement) $\widehat{E\overline{k}} \to \overline{k}((T - t_0))$ de la clôture galoisienne $\widehat{E}/k(T)$ dans le corps

des séries formelles $\overline{k}((T-t_0))$, avec la convention que si $t_0=\infty$, $T-t_0$ doit être compris comme $1/T$. Les deux résultats en questions sont les suivants :

(a) l'ensemble des points de branchement est fini (voir §3.1.3.2),

(b) l'ensemble des points de branchement est non vide, sauf si $E=k(T)$.

Cela résulte de la formule de Riemann-Hurwitz [**Har77**, Corollary 2.4 p. 301] dont il résulte ici que, si $r\geq 0$ est le nombre de points de branchement, alors $2+(r-2)[E:k(T)]\geq 0$.

Démonstration de la proposition 2.3.5. — La partie de l'énoncé sur les quotients est claire. Considérons le produit $G_1\times G_2$ de deux groupes pour lesquels on a $G_i=\mathrm{Gal}(E_i/k(T))$ avec E_i/k régulière, $i=1,2$. Notons B_1 et B_2 leurs ensembles respectifs de points de branchement.

Supposons dans un premier temps que $B_1\cap B_2=\emptyset$. Les extensions $E_1/k(T)$ et $E_2/k(T)$ sont alors linéairement disjointes. En effet, l'intersection $E_1\cap E_2$ est une extension galoisienne de $k(T)$, régulière sur k et dont l'ensemble des points de branchement est vide. D'après l'assertion (b) ci-dessus, $E_1\cap E_2=k(T)$ comme annoncé. On en déduit aisément $\mathrm{Gal}(E_1E_2/k(T))\simeq G_1\times G_2$.

Si $B_1\cap B_2\neq\emptyset$ et si k est infini, alors en composant l'inclusion $k(T)\to E_2$ avec un isomorphisme $k(T)\to k(T)$ induit par une homographie $\chi(T)$ à coefficients dans k, on obtient une nouvelle extension $E_2'/k(T)$ dont on peut faire en sorte, grâce à l'assertion (a), que son ensemble de points de branchement, qui est l'image de B_2 par χ^{-1} soit disjoint de B_1. On est ainsi ramené au cas précédent. □

Remarque 2.3.6. — L'argument montre que pour k quelconque, la propriété pour un groupe fini d'être réalisé comme groupe de Galois d'une extension galoisienne régulière $E/k(T)$ avec la condition supplémentaire que l'ensemble des points de branchement est disjoint d'un ensemble fini quelconque donné à l'avance, est stable par produit direct.

2.3.4. Le cas des groupes abéliens. — La forme régulière du problème inverse de Galois est vraie pour les groupes abéliens. Plus précisément, on a le résultat suivant.

Théorème 2.3.7. — *Soit k un corps arbitraire et $D\subset\mathbb{P}^1(\overline{k})$ un ensemble fini. Pour tout groupe abélien fini G, il existe une extension galoisienne $E/k(T)$ de groupe G, régulière sur k et telle que $\overline{k}E$ se plonge dans $\overline{k}((T-t_0))$ pour tout $t_0\in D$ (c'est-à-dire, l'extension $E/k(T)$ n'est ramifiée au-dessus d'aucun point de D).*

Démonstration. — Grâce à la proposition 2.3.5, la remarque 2.3.6 et le théorème de structure des groupes abéliens finis, on peut se ramener au cas où G est un groupe cyclique d'ordre une puissance ℓ^m d'un nombre premier ℓ. On distingue alors deux cas suivant que la caractéristique p de k est égale à ℓ ou non. Dans le cas $\ell \neq p$, on construit une extension kummérienne de $\overline{k}(T)$ dont on montre que, pour les paramètres de la construction bien choisis, la descente à k est possible. Le principe est le même pour $\ell = p$ mais on utilise des extensions d'Artin-Schreier.

La construction est relativement élémentaire mais un peu technique. Le cas particulier où $\mathrm{card}(D) = 1$ est plus classique ; nous renvoyons à [**Völ96**, §11.4.3]. Pour le cas général, nous renvoyons à [**Dèb99c**]. □

On donnera au chapitre 4 une autre preuve valable en caractéristique 0 (voir théorème 4.2.7).

2.4. Théorème d'existence de Riemann

Au-delà des groupes abéliens, le problème reste très ouvert. On dispose cependant pour le cas général d'un résultat profond qui donne un point d'ancrage fort pour toute la théorie : le théorème d'existence de Riemann. Une conséquence fondamentale en théorie inverse de Galois est l'énoncé suivant.

Théorème 2.4.1. — *Tout groupe fini G est le groupe de Galois d'une extension $E/\mathbb{C}(T)$.*

Cela permet de voir le problème global comme un problème de descente : peut-on faire en sorte que certaines des extensions qui réalisent un groupe donné comme groupe de Galois sur $\mathbb{C}(T)$ soient définies sur $\mathbb{Q}$, c'est-à-dire, proviennent par extension des scalaires d'une extension galoisienne régulière $E/\mathbb{Q}(T)$? Dans l'affirmative, le théorème d'irréductibilité de Hilbert permet ensuite de réaliser le groupe en question sur $\mathbb{Q}$ lui-même.

Le théorème d'existence de Riemann lui-même est un résultat général de classification qui permet d'identifier les aspects algébrique, analytique et topologique de la notion de *revêtement*. En termes d'extensions de corps et de réalisation de groupes, on peut en donner la "forme pratique" suivante.

Théorème 2.4.2 **(Théorème d'existence de Riemann)**
Supposons donnés un groupe fini G et un entier $r > 0$ et r points distincts $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$. Alors il existe une correspondance bijective entre

- l'ensemble des extensions de corps $E/\mathbb{C}(T)$ galoisiennes de groupe G non ramifiées en dehors de $t_1, \ldots, t_r$, modulo les $\mathbb{C}(T)$-isomorphismes, et
- l'ensemble des r-uplets $(g_1, \ldots, g_r) \in G^r$ tels que $\langle g_1, \ldots, g_r \rangle = G$ et $g_1 \cdots g_r = 1$, modulo la conjugaison (composante par composante) par des éléments de G.

Le théorème 2.4.1 découle de cette première forme du théorème d'existence de Riemann : tout groupe fini G possède un r-uplet $(g_1, \ldots, g_r)$ comme ci-dessus, pourvu que r soit assez grand (plus précisément : strictement supérieur au rang de G).

La démonstration des théorèmes 2.4.1 et 2.4.2 sera un objectif des chapitres 7 et 8 ; ils seront finalement établis au §8.3.4.

2.5. Approche de Noether et autres perspectives

2.5.1. Le groupe symétrique et l'approche de Noether. —

2.5.1.1. Le groupe symétrique. — Le cas des groupes symétriques fut la motivation initiale de Hilbert en théorie inverse de Galois. On commence par le résultat classique suivant.

Théorème 2.5.1*. — Pour tout entier $d > 0$, le groupe symétrique est groupe de Galois sur le corps $\mathbb{Q}(T_1, \ldots, T_d)$ des fractions rationnelles à d indéterminées.*

Démonstration. — Soient k un corps et $Y_1, \ldots, Y_d$ d indéterminées. Notons $T_i = T_i(Y_1, \ldots, Y_d)$ les fonctions symétriques élémentaires de $Y_1, \ldots, Y_d$, c'est-à-dire les coefficients du polynôme

$$P = Y^d - T_1 Y^{d-1} + \cdots + (-1)^d T_d$$

dont les racines sont $Y_1, \ldots, Y_d$.

L'extension $k(T_1, \ldots, T_d)$ est une extension transcendante pure. En effet, soit F un polynôme à coefficients dans $\overline{k}$ tel que $F(T_1, \ldots, T_d) = 0$. Soient $\theta_1, \ldots, \theta_d$ des indéterminées algébriquement indépendantes et $\eta_1, \ldots, \eta_d$ des racines dans $\overline{k(\theta_1, \ldots, \theta_d)}$ du polynôme

$$Y^d - \theta_1 Y^{d-1} + \cdots + (-1)^d \theta_d$$

On a alors $T_i(\eta_1, \ldots, \eta_d) = \theta_i$, $i = 1, \ldots, d$ et donc $F(\theta_1, \ldots, \theta_d) = 0$, ce qui entraine $F = 0$.

L'extension

$$k(Y_1, \ldots, Y_d)/k(T_1, \ldots, T_d)$$

est une extension galoisienne car c'est le corps de décomposition sur $k(T_1, \ldots, T_d)$ du polynôme P. Chaque élément du groupe symétrique S_d induit un $k(T_1, \ldots, T_d)$-automorphisme de $k(Y_1, \ldots, Y_d)$. Le groupe S_d est donc un sous-groupe du groupe de Galois de l'extension ci-dessus. En particulier, Y_1 a au moins d conjugués sur $k(T_1, \ldots, T_d)$, à savoir $Y_1, \ldots, Y_d$. On déduit que le polynôme P est irréductible sur $k(T_1, \ldots, T_d)$ et que le groupe de Galois de l'extension $k(Y_1, \ldots, Y_d)/k(T_1, \ldots, T_d)$ (qui doit être d'ordre $\leq d!$) est le groupe S_d. □

Corollaire 2.5.2. — *Tout polynôme $F(Y_1, \ldots, Y_d)$ à coefficients dans k qui a la propriété que pour tout $\sigma \in S_d$, $F(Y_{\sigma(1)}, \ldots, Y_{\sigma(d)}) = F(Y_1, \ldots, Y_d)$ peut s'écrire comme fonction polynômiale des fonction symétriques élémentaires $T_1, \ldots, T_d$.*

Démonstration. — C'est une conséquence immédiate de la théorie de Galois : le sous-corps de $(Y_1, \ldots, Y_d)$ fixé par le groupe S_d est le corps $k(T_1, \ldots, T_d)$. □

Grâce au théorème d'irréductibilité de Hilbert (sous sa forme générale du théorème 2.2.4), il existe des spécialisations $t_1, \ldots, t_d \in \mathbb{Q}$ des indéterminées $T_1, \ldots, T_d$ telles que le polynôme $P(t_1, \ldots, t_r, Y)$ soit irréductible dans $\mathbb{Q}[Y]$ et que son corps de décomposition soit une extension galoisienne de $\mathbb{Q}$ de groupe S_d (appliquer le théorème 1.9.3 du chapitre 1 ou bien généraliser la preuve de la proposition 2.2.14). L'argument permet même de réaliser S_d comme groupe de Galois d'une extension régulière de $\mathbb{Q}(T)$. Il suffit de ne spécialiser que $d-1$ des variables $T_1, \ldots, T_d$.

2.5.1.2. L'approche de Noether. — Emmy Noether a essayé de généraliser l'exemple du groupe S_d de la manière suivante. Tout groupe fini G peut être vu comme un sous-groupe de S_d, *via* sa représentation régulière par exemple. Le groupe G a alors une action $G \to \mathrm{Aut}(\mathbb{Q}(Y_1, \ldots, Y_d))$ sur le corps $\mathbb{Q}(Y_1, \ldots, Y_d)$ des fractions rationnelles en d indéterminées. Notons $\mathbb{Q}(Y_1, \ldots, Y_d)^G$ le sous corps de $\mathbb{Q}(Y_1, \ldots, Y_d)$ des éléments laissés fixes par cette action. D'après la théorie de Galois, l'extension $\mathbb{Q}(Y_1, \ldots, Y_d)/\mathbb{Q}(Y_1, \ldots, Y_d)^G$ est une extension galoisienne de groupe de Galois G. Si le corps $\mathbb{Q}(Y_1, \ldots, Y_d)^G$ est une extension transcendante pure $\mathbb{Q}(T_1, \ldots, T_d)$, on peut, comme ci-dessus, spécialiser les indéterminées $T_1, \ldots, T_r$ dans $\mathbb{Q}$ et réaliser G comme groupe de Galois sur $\mathbb{Q}$.

Malheureusement, il existe des groupes pour lesquels le corps $\mathbb{Q}(Y_1, \ldots, Y_d)^G$ n'est pas une extension transcendante pure. Des exemples avec G cyclique ont été donnés par Swann. Il y a des travaux visant à étendre la propriété de spécialisation a des corps plus généraux que les extensions transcendantes

pures. Par exemple, Colliot-Hélène conjecture que cette propriété subsiste sur tout sous-corps d'une extension transcendante pure (de façon équivalente, sur le corps de fonctions de toute variété *unirationnelle*). *Via* l'approche de Noether, cette conjecture entraîne la conjecture 2.1.1, c'est-à-dire résoudrait le problème inverse de Galois.

2.5.2. Forme régulière forte. — Il existe une version forte de la forme régulière forte du problème inverse de Galois qui s'exprime en termes de *problèmes de plongement*. Un *problème de plongement (fini) pour un corps* K consiste en la donnée d'une suite exacte de groupes finis $1 \to N \to G \to H \to 1$ et d'une extension galoisienne E_H/K telle que $\mathrm{Gal}(E_H/K) = H$; le problème est de "plonger" la H-extension E_H/K dans une G-extension, c'est-à-dire de construire une extension E_G/E_H, galoisienne sur K, telle que $\mathrm{Gal}(E_G/K) = G$ et $\mathrm{Gal}(E_G/E_H) = N$.

D'après un théorème d'Iwasawa [**FJ04**, §24.8], si pour un corps K dénombrable, tout problème de plongement peut être résolu, alors le groupe de Galois absolu G_K est un groupe profini libre, c'est-à-dire libre dans la catégorie des groupes profinis. Ce n'est pas le cas par exemple pour $K = \mathbb{Q}$ puisque, au contraire de tout groupe pro-libre, le groupe $\mathrm{G}_{\mathbb{Q}}$ a des éléments de torsion (ceux induits par la conjugaison complexe). On conjecture cependant que, sur $\mathbb{Q}$ (ou plus généralement sur tout corps K *hilbertien*), il existe une solution à tout problème de plongement *scindé*, c'est-à-dire tel que l'épimorphisme $G \to H$ possède une section. Comme plus haut, on préfère la conjecture suivante qui ne dépend pas du corps de base.

***Conjecture 2.5.3* (RIGP+).** — *Etant donnés un corps k, tout problème de plongement scindé pour le corps $k(T)$ possède une solution régulière.*

"Solution régulière" signifie ici que la solution $E_G/k(T)$ vérifie $E_G \cap \overline{k} = E_H \cap \overline{k}$ (c'est-à-dire : les constantes dans l'extension solution E_G sont celles qui figurent déjà dans l'extension donnée E_H). La conjecture **RIGP** correspond au cas particulier de **RIGP+** où le groupe H est trivial. Une autre conséquence notable concerne le corps $\mathbb{Q}^{\mathrm{ab}}$ engendré par toutes les racines de l'unité.

***Conjecture 2.5.4* (Conjecture de Shafarevich).** — *Le groupe de Galois absolu $\mathrm{G}_{\mathbb{Q}^{\mathrm{ab}}}$ de $\mathbb{Q}^{\mathrm{ab}}$ est un groupe profini libre.*

On peut résumer l'argument comme suit. En appliquant la conjecture **RIGP+** à $k = \mathbb{Q}^{\mathrm{ab}}$, on obtient, par spécialisation de T (le corps $\mathbb{Q}^{\mathrm{ab}}$ est hilbertien d'après un résultat de Kuyk [**FJ04**, theorem 16.11.3]), que tout

problème de plongement scindé pour $\mathbb{Q}^{\mathrm{ab}}$ a une solution. Mais le fait que $\mathbb{Q}^{\mathrm{ab}}$ soit de *dimension cohomologique* ≤ 1. entraîne que la même conclusion est vraie, sans le mot "scindé". Le théorème d'Iwasawa, mentionné plus haut, permet de conclure l'argument. Pour plus de détails sur ces conjectures et leurs relations, nous renvoyons à l'article [**DD04**] où l'énoncé **RIGP+** est présenté comme la conjecture unifiante du domaine.

2.5.3. Problème de Beckmann-Black. — On peut, comme S. Beckmann et E. Black, s'interroger sur les arguments de spécialisation utilisés précédemment : pour réaliser un groupe G sur $\mathbb{Q}$, n'est-ce pas se limiter que se restreindre aux extensions de $\mathbb{Q}$ qui s'obtiennent par spécialisation d'une extension $E_T/\mathbb{Q}(T)$? La conjecture suivante, formulée par E. Black, répond par la négative. Ici encore, le corps de base est arbitraire.

Conjecture 2.5.5 **(Problème de Beckmann-Black)**
Etant donnés un corps k, un groupe fini G, une extension galoisienne E/k de groupe G, il existe une extension galoisienne régulière $E_T/k(T)$ de groupe G telle que l'extension résiduelle E_{t_0}/k en un point $t_0 \in \mathbb{P}^1(k)$ soit l'extension galoisienne E/k.

Cet énoncé précise l'énoncé **RIGP** : non seulement tout groupe fini G est *réalisable* sur $k(T)$, mais aussi toute extension galoisienne de k.

Pour aller un peu plus loin sur ces questions et pour une liste de références, nous renvoyons à [**Dèb01**].

CHAPITRE 3

REVÊTEMENTS ALGÉBRIQUES

Les revêtements algébriques de $\mathbb{P}^1$ ont de multiples descriptions. Nous privilégions le point de vue arithmétique en les introduisant comme extensions de corps. Nous revenons ensuite sur les équivalences avec les notions de revêtements au sens de la topologie et à celui de la géométrie algébrique.

3.1. Extensions régulières de $k(T)$

3.1.1. Les objets centraux. — Etant donnés un corps k et une indéterminée T, les objets au centre de notre étude sont les extensions finies régulières (définition 2.3.1) du corps $k(T)$. Les morphismes entre deux telles extensions $E/k(T)$ et $E'/k(T)$ sont les morphismes de corps $E \to E'$ dont la restriction à $k(T)$ est l'identité. Le groupe des automorphismes d'une extension $E/k(T)$ est noté $\mathrm{Aut}(E/k(T))$. Si l'extension est galoisienne, le groupe $\mathrm{Aut}(E/k(T))$ est le groupe de Galois $\mathrm{Gal}(E/k(T))$ de l'extension. De façon générale, l'extension séparable $E/k(T)$ possède une clôture galoisienne $\widehat{E}/k(T)$[(1)]. Son groupe de Galois $\mathrm{Gal}(\widehat{E}/k(T))$ agit transitivement sur les $d = [E : k(T)]$ $k(T)$-plongements de E dans une clôture séparable $k(T)^{\mathrm{s}}$ de $k(T)$ (ou, de façon équivalente, sur les d conjugués d'un élément primitif de $E/k(T)$). Moyennant une numérotation des $k(T)$-plongements $E \hookrightarrow k(T)^{\mathrm{s}}$, on obtient une action $\mathrm{Gal}(\widehat{E}/k(T)) \to S_d$.

3.1.2. Extensions de $\overline{k}((T))$. — On suppose ici k algébriquement clos et de caractéristique 0. Le but de ce paragraphe est de montrer le résultat suivant.

(1) qui n'est pas forcément régulière sur k : penser par exemple à $E = \mathbb{Q}(\sqrt[d]{T})$ $(d \geq 3)$.

***Théorème 3.1.1* (théorème de Puiseux).** — *La clôture algébrique du corps $k((T))$ est la réunion des corps $k((T^{1/d}))$, $d \geq 1$. En conséquence, les extensions finies $F/k((T))$ sont kummériennes ; plus précisément on a $F = k((T))(T^{1/d})$ où $d = [F : k((T))]$.*

Démonstration. — Il s'agit de montrer que toute extension galoisienne finie de $k((T))$ est une extension kummerienne de la forme $k((T))(T^{1/d})$ avec $d \geq 1$ (on voit facilement que $k((T))(T^{1/d}) = k((T^{1/d}))$). On en déduira aisément que c'est aussi le cas de toute extension finie (non nécessairement galoisienne).

Soit $E/k((T))$ une extension galoisienne de degré d et B la fermeture intégrale de $k[[T]]$ dans E ; c'est un anneau de valuation discrète (théorème 1.3.15). On note v la valuation T-adique sur $k((T))$, w son unique prolongement à E et π une uniformisante de w. On normalise w de telle sorte que $w(\pi) = 1$. Comme k est algébriquement clos, on a $f = 1$ et donc $e = d$, c'est-à-dire l'extension est totalement ramifiée. En particulier $w(T) = d$ et on a $k((T))(\pi) = E$: en effet, si $E_\pi = k((T))(\pi)$, on a $w(E) = w(E_\pi)$, or les indices $[w(E^\times) : w(k((T))^\times)]$ et $[w(E_\pi^\times) : w(k((T))^\times)]$ sont respectivement égaux à $[E : k((T))]$ et $[E_\pi : k((T))]$ (théorème 1.5.5). On a de plus $w(\pi) = 1$ et $w(a) \equiv 0 \pmod{d}$ si $a \in k[[T]]$.

1ère étape : utilisation des polynômes d'Eisenstein pour montrer que π est un générateur de la $k[[T]]$-algèbre B. Soit $f(X) \in k((T))[X]$ le polynôme minimal de π sur $k((T))$. Comme $k[[T]]$ est intégralement clos, $f(X) \in k[[T]][X]$. Ecrivons $f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ avec $a_i \in k[[T]]$ et $a_0 = 1$. Soit $r = \min_{0\leq i\leq d} w(a_i\pi^{d-i})$. Il résulte de $f(\pi) = 0$ qu'il existe deux entiers i, j avec $0 \leq i < j \leq d$ tels que $r = w(a_i\pi^{d-i}) = w(a_j\pi^{d-j})$. On en déduit $j - i = w(a_j/a_i) \equiv 0 \pmod{d}$ ce qui n'est possible que si $i = 0$, $j = d$ et donc $r = d$, $w(a_d) = d$ et $w(a_i) \geq i$ pour $i \geq 1$. On a ainsi $a_i \in \langle T\rangle$, $i > 0$ et $a_d \notin \langle T^2\rangle$; c'est-à-dire, $f(X)$ est ce qu'on appelle un polynôme d'Eisenstein.

Considérons l'anneau $B_f = k[[T]][X]/(f)$. D'après le lemme 1.1.8, B_f est un anneau local et son idéal maximal est l'idéal $\langle x, T\rangle$ où x est la classe de X modulo (f). On observe ensuite que $\langle x, T\rangle = \langle x, a_d\rangle = \langle x\rangle$ en utilisant successivement que a_d est une uniformisante de $k[[T]]$ (donc $T/a_d \in k[[T]]^\times$) et que $a_d = -x^d - a_1x^{d-1} - \cdots - a_{d-1}x$. Comme a_d n'est pas nilpotent, x ne l'est pas non plus. On peut donc conclure grâce au théorème 1.2.7 que B_f est un anneau de valuation discrète[(2)].

[(2)] Ce raisonnement redonne aussi le critère d'Eisenstein : de l'intégrité de l'anneau $B_f = k((T))[X]/(f)$ résulte que le polynôme $f(X)$ est irréductible dans $k((T))[X]$.

Du caractère intégralement clos découle que B_f est la clôture intégrale de $k[[T]]$ dans $E_f = \mathrm{Frac}(B_f) = k((T))[X]/(f)$. Comme E_f est $k((T))$-isomorphe à E *via* la correspondance $X \to \pi$, on peut conclure que cette correspondance induit un isomorphisme entre B_f et B (B est la clôture intégrale de $k[[T]]$ dans E), et donc que $1, \pi, \ldots, \pi^{d-1}$ constituent une $k[[T]]$-base de B.

2ème étape : utilisation des groupes de ramification supérieurs pour montrer que $\mathrm{Gal}(E/k((T)))$ *est cyclique.* Pour $i \geq -1$, on note $I_i \subset \mathrm{Gal}(E/k((T)))$ le sous-groupe des éléments s tels que $w(s(a) - a) \geq i + 1$ pour tout $a \in B$. On obtient ainsi une suite décroissante de sous-groupes distingués[(3)] de $\mathrm{Gal}(E/k((T)))$. On a $I_{-1} = \mathrm{Gal}(E/k((T)))$ et I_0 est le groupe d'inertie (qui est ici égal à $\mathrm{Gal}(E/k((T))))$. Comme B est engendré par π comme $k[[T]]$-algèbre, on a, pour $i \geq -1$, $s \in I_i$ si et seulement si $w(s(\pi) - \pi) \geq i + 1$: noter que pour $a \in B$, $w(s(a) - a) \geq i + 1$ équivaut à dire que les classes de a et de $s(a)$ sont égales dans l'anneau quotient $B/\langle \pi^{i+1} \rangle$. De plus, la condition $w(s(\pi) - \pi) \geq i + 1$ équivaut à $w(\frac{s(\pi)}{\pi} - 1) \geq 1$ ($i \geq -1$). En particulier $I_i = \{1\}$ pour tout i assez grand.

D'autre part, pour $i \geq 1$, l'application qui à $s \in I_i$ fait correspondre $s(\pi)/\pi$, définit par passage au quotient, un isomorphisme Θ_i du groupe I_i/I_{i+1} sur un sous-groupe du groupe $1 + \mathfrak{p}^i/1 + \mathfrak{p}^{i+1}$ où on a noté $\mathfrak{p} = \langle \pi \rangle$ ($i \geq -1$). Pour voir que Θ_i est un morphisme, on écrit, pour $s, t \in I_i$:

$$st(\pi)/\pi = s(\pi)/\pi \cdot t(\pi)/\pi \cdot s(u)/u \qquad \text{avec } u = t(\pi)/\pi$$

Comme $u \in B^\times$, on a $s(u) - u \in \mathfrak{p}^{i+1}$ et donc $s(u)/u - 1 \in \mathfrak{p}^{i+1}$, ce qui donne $st(\pi)/\pi \equiv s(\pi)/\pi \cdot t(\pi)/\pi$ modulo $\mathfrak{p}^{i+1}$. L'injectivité de Θ_i est facile.

On vérifie sans peine que, pour $i \geq 1$, la correspondance $x \to 1 + x$ induit un isomorphisme entre le groupe additif $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ et le groupe multiplicatif $1 + \mathfrak{p}^i/1 + \mathfrak{p}^{i+1}$. Le groupe $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ est isomorphe au groupe additif du corps résiduel $B/\mathfrak{p}$ de w, c'est-à-dire k. Mais comme k est de caractéristique 0, il n'a pas de sous-groupe fini non trivial. On peut ainsi conclure que les groupes I_i/I_{i+1} sont triviaux pour $i \geq 1$ et donc que les groupes I_i eux-mêmes sont triviaux pour $i \geq 1$ puisqu'on sait déjà qu'ils le sont pour i assez grand.

Pour $i = 0$, la même correspondance $s \to s(\pi)/\pi$ induit un isomorphisme entre I_0/I_1 et un sous-groupe de $B^\times/1 + \mathfrak{p}$[(4)], lequel est isomorphe au groupe

---

[(3)] Pour le caractère distingué, écrire $gsg^{-1}(a) - a = g(sg^{-1}(a) - g^{-1}(a))$ ($g \in \mathrm{Gal}(E/k((T)))$) et se rappeler que $w(g(x)) = w(x)$ ($x \in E$) (théorème 1.5.5).

[(4)] Pour voir que l'image de la correspondance est dans $B^\times$, noter que $w(s(\pi)) = w(\pi) = 1$.

multiplicatif du corps résiduel k. On peut donc conclure que I_0/I_1, c'est-à-dire $\mathrm{Gal}(E/k((T)))$, est isomorphe à un sous-groupe du groupe des racines de l'unité de k ; c'est donc un groupe cyclique d'ordre d.
(Pour une généralisation des arguments de cette étape, voir [**Ser62**, IV, §1-2]) ; les groupes I_i sont appelés les groupes de ramification supérieurs).

Conclusion : D'après ce qui précède, l'extension $E(T^{1/d})/k((T))$ est cyclique. D'autre part, les extensions $E/k((T))$ et $k((T^{1/d}))/k((T))$ en sont deux sous-extensions cycliques de degré d[(5)]. Comme un groupe cyclique n'a au plus qu'un sous-groupe cyclique d'ordre donné, la théorie de Galois permet de conclure que $E = k((T))(T^{1/d})$.

Si maintenant $F/k((T))$ est une extension finie, on a $F \subset k((T))(T^{1/d})$ pour un entier $d \geq 1$. Mais les sous-extensions de l'extension kummerienne $k((T))(T^{1/d})/k((T))$ sont kummeriennes, de la forme $k((T))(T^{1/m})/k((T))$ avec $m \mid d$. On a donc $E = k((T))(T^{1/m})$ et $m = [E : k((T))]$. □

Remarque 3.1.2. — Pour une utilisation ultérieure, nous notons que les morphismes $\Theta_i : I_i/I_{i+1} \to (1+\mathfrak{p}^i)/(1+\mathfrak{p}^{i+1})$ ($i \geq 0$, avec la convention que $1+\mathfrak{p}^i = B^\times$ pour $i = 0$), ne dépendent pas de l'uniformisante π. En effet, si $\pi' = u\pi$ est une autre uniformisante, c'est-à-dire, $u \in B^\times$, on a $s(\pi')/\pi' = s(\pi)/\pi \cdot s(u)/u$, et comme ci-dessus, on voit que $s(u)/u - 1 \in \mathfrak{p}^{i+1}$.

3.1.3. Extensions séparables de $\overline{k}(T)$. —

3.1.3.1. Points et places. — Dans ce premier paragraphe k est un corps quelconque et $E/k(T)$ une extension finie séparable.

Définition 3.1.3. — On appelle place de E (au-dessus de k) toute valuation discrète sur E et triviale sur k regardée modulo la relation d'équivalence identifiant deux valuations multiples l'une de l'autre par un nombre rationnel > 0, c'est-à-dire induisant la même topologie sur E (proposition 1.2.10). La place est dite k-rationnelle si son corps résiduel est k. On note $X_E(k)$ l'ensemble des places k-rationnelles de E, qu'on appelle aussi points k-rationnels de X_E.

Exemple 3.1.4. — D'après l'exemple 1.2.11, les places rationnelles de $k(T)$ correspondent aux valuations $(T-t_0)$-adiques décrites dans l'exemple 1.2.9 associées aux éléments $t_0 \in k$ et à $t_0 = \infty$. On a donc, ensemblistement, $X_{k(T)}(k) = \mathbb{P}^1(k)$.

(5) Pour voir que la seconde est de degré d, on peut par exemple invoquer le critère d'Eisenstein (redémontré plus haut) pour dire que le polynôme $X^d - T$ est irréductible dans $k((T))[X]$.

Les places de E peuvent ensuite être décrites comme suit, grâce au théorème 1.5.6. Pour $t_0 \in \mathbb{P}^1(k)$, on note $k[T]_{t_0}$ le localisé de l'anneau $k[T]$ en l'idéal $\langle T - t_0\rangle$ (pour $t_0 = \infty$, on convient que $k[T]_\infty = k[1/T]_{\langle 1/T\rangle}$) et $k((T - t_0))$ le corps des séries formelles en $T - t_0$ (pour $t_0 = \infty$, on prend $T - t_0 = 1/T$).

Proposition 3.1.5. — *Pour tout point/place $t_0 \in \mathbb{P}^1(K)$, les places de E au-dessus de t_0 correspondent*
- aux prolongements à E de la valuation $(T-t_0)$-adique sur $k(T)$, ou, de façon équivalente,
- aux $k(T)$-plongements de E dans une clôture séparable de $k((T-t_0))$, regardés modulo la $k((T - t_0))$-conjugaison, ou encore,
- aux idéaux premiers de la décomposition de l'idéal $\langle T-t_0\rangle$ de l'anneau $k[T]_{t_0}$ dans l'extension $E/k(T)$.

Si de plus k est algébriquement clos, alors les extensions résiduelles au-dessus d'un point $t_0 \in \mathbb{P}^1(k)$ sont triviales : les places de E au-dessus de t_0 sont k-rationnelles[(6)].

Cas d'un corps k algébriquement clos de caractéristique 0. Les indices de ramification $e_1, \dots, e_g$ correspondent aux degrés sur $k((T - t_0))$ des différents $k((T - t_0))$-plongements de $Ek((T - t_0))$ dans $\overline{k((T - t_0))}$. Vu la forme des extensions de $k((T - t_0))$ (théorème **??**), pour chaque $i = 1, \dots, g$, le corps $Ek((T - t_0))$ correspond *via* le plongement associé dans $\overline{k((T - t_0))}$ au corps $k(((T-t_0)^{1/e_i}))$ (le seul sous-corps de $\overline{k((T - t_0))}$ de degré e_i sur $k((T-t_0))$). Si $P(T, Y) \in k(T)[Y]$ est le polynôme minimal d'un élément primitif de l'extension $E/k(T)$, les indices de ramification $e_1, \dots, e_g$ sont alors les degrés des facteurs irréductibles de P dans $k((T - t_0))[Y]$, ou de façon équivalente, les ordres minimaux des racines $T^{1/e}$ nécessaires pour écrire les solutions de ces facteurs ; on les appelle les *exposants de Puiseux*.

Définition 3.1.6. — Etant donné $w \in X_E(k)$ et $f \in E$, le nombre $w(f)$ est appelé ordre de la fonction f au point w. On dit que w est un zéro de f si $w(f) > 0$ et un pôle de f si $w(f) < 0$.

L'exposant de Puiseux d'une place w correspond ainsi à l'ordre de la fonction $T - t_0$ au point w. Par exemple, si E est un corps de rupture de $P(T, Y) =$

(6) Cela reste vrai si k est séparablement clos et $t_0 \in \mathbb{P}^1(k)$ est non ramifié (au sens de la définition 3.1.7) ; en effet, par définition de "non ramifié", les extensions résiduelles au-dessus de t_0 sont séparables. Les places de E au-dessus de t_0 sont k-rationnelles.

$Y^2 - T^2(T+1)$, la fonction T a deux zéros simples sur $X_E(k)$; pour $P(T,Y) = Y^2 - T$, la fonction T a un zéro double.

3.1.3.2. Points non ramifiés et points de branchement. — On suppose que k est un corps séparablement clos (par exemple algébriquement clos) et $E/k(T)$ une extension finie régulière.

Définition 3.1.7. — Un point $t_0 \in \mathbb{P}^1(k)$ est dit non ramifié dans une extension finie régulière $E/k(T)$ si l'idéal $\langle T - t_0 \rangle$ (ou la place $T - t_0$-adique) est non ramifié dans l'extension $E/k(T)$ (au sens de la définition 1.5.2). Si t_0 est ramifié, on dit que c'est un point de branchement de l'extension $E/k(T)$.

Comme k est séparablement clos, les extensions résiduelles au-dessus d'un point non ramifié sont triviales (c'est-à-dire, les coefficients f_i valent 1). De façon équivalente à la définition 3.1.7, $t_0 \in \mathbb{P}^1(k)$ est non ramifié si tous les $k(T)$-plongements $E \to \overline{k((T-t_0))}$ sont à valeurs dans $k((T-t_0))$, c'est-à-dire, s'il existe un plongement de la clôture galoisienne $\widehat{E}$ dans $k((T-t_0))$. Si $P(T,Y) \in k(T)[Y]$ est le polynôme minimal d'un élément primitif de l'extension $E/k(T)$, la condition équivaut à demander que P soit totalement décomposé dans $k((T-t_0))$. En raison de la formule $\sum_i e_i f_i = [E : k(T)]$ (théorème 1.5.3), la non-ramification de t_0 équivaut aussi à l'existence de $d = [E : k(T)]$ places de E au-dessus du point t_0.

L'anneau $k[T]$ étant principal, la fermeture intégrale de $k[T]$ dans E est un k-module libre de rang d et l'idéal discriminant est engendré par le discriminant $\Delta(T) \in k[T]$ de toute $k[T]$-base. D'après le théorème 1.5.14, si $\Delta(T)$ est totalement décomposé dans k (par exemple si k est algébriquement clos), les points ramifiés $t_0 \in \mathbb{P}^1(k) \setminus \{\infty\}$ sont exactement les racines de $\Delta(T)$. En conséquence, si $P(T,Y) \in k(T)[Y]$ est le polynôme minimal d'un élément primitif y de $E/k(T)$ entier sur $k[T]$, ce sont des racines du discriminant $\Delta_P(T)$ de P par rapport à Y. En effet, d'après la remarque 1.3.14, $\Delta_P(T)$ est égal au signe près au discriminant $\Delta(1, y, \ldots, y^{d-1})$ de la base $(1, y, \ldots, y^{d-1})$ de E sur $k(T)$, et est donc un multiple dans $k[T]$ de $\Delta(T)$. En revanche il peut exister des racines de $\Delta_P(T)$ qui ne correspondent pas à des points de branchement. On sait par ailleurs que le discriminant est non nul (§1.3.5.2) ; il en résulte que l'ensemble des points de branchement est fini. Pour le point ∞, il faut "changer de carte", c'est-à-dire, faire le changement de variable $T \to 1/T$.

3.1.3.3. Groupes d'inertie des extensions de $k(T)$. — On suppose ici que k est un corps algébriquement clos de caractéristique 0 et que l'extension $E/k(T)$ est galoisienne.

Soit $t_0 \in \mathbb{P}^1(k)$. Notons $\mathcal{P}_1, \dots, \mathcal{P}_g$ les idéaux de la décomposition de l'idéal $\langle T - t_0 \rangle$ de l'anneau $k[T]_{t_0}$ dans l'extension $E/k(T)$, $w_1, \dots, w_g$ les places correspondantes de E au-dessus de t_0 et $\sigma_1, \dots, \sigma_g$ les $k(T)$-plongements correspondants $E \to \overline{k((T-t_0))}$, regardés modulo la $k((T-t_0))$-conjugaison (voir proposition 3.1.5). Comme l'extension $E/k(T)$ est galoisienne, tous les corps $\sigma_i(E)$ sont le même sous-corps, qu'on note E^ι, de $\overline{k((T-t_0))}$.

On sait que les idéaux $\mathcal{P}_1, \dots, \mathcal{P}_g$ sont conjugués par des éléments de $\mathrm{Gal}(E/k(T))$ et que, si $\widetilde{E}_i$ désigne le complété de E pour la place w_i, alors le groupe de décomposition $D_{\mathcal{P}_i}$ est le groupe de Galois de l'extension correspondante $\widetilde{E}_i/k((T-t_0))$ $(i = 1, \dots, g)$. *Via* l'identification de chaque $\widetilde{E}_i$ avec $E^\iota k((T-t_0))$, cette extension est, d'après le théorème de Puiseux (théorème 3.1.1), la même extension kummerienne $k(((T-t_0)^{1/e}))$ (avec e l'indice de ramification, qui ne dépend pas de i). Un générateur de $D_{\mathcal{P}_i}$ est donné par la correspondance

$$(T-t_0)^{1/e} \to \zeta_e (T-t_0)^{1/e}$$

où ζ_e est une racine primitive e-ième de l'unité[(7)]. Quant au groupe d'inertie $I_{\mathcal{P}_i}$, il est égal au groupe de décomposition puisque le degré résiduel vaut 1[(8)].

Lemme 3.1.8. — *Soient $\mathcal{P}$ un des idéaux $\mathcal{P}_1, \dots, \mathcal{P}_g$, π une uniformisante de la valuation $v_{\mathcal{P}}$ dans le complété $\widetilde{E}$ de E pour $v_{\mathcal{P}}$ et $\sigma \in \mathrm{Gal}(\widetilde{E}/k((T-t_0)))$. Alors $\sigma(\pi)/\pi$ est un élément de l'anneau de la valuation $v_{\mathcal{P}}$ congru modulo l'idéal de valuation (l'idéal $\langle \pi \rangle$) à une racine e-ième de l'unité ζ_σ qui ne dépend pas du générateur π.*

Via le plongement $\sigma_i : E \to E^\iota \subset k((T-t_0))$, cela revient à dire que $\sigma(\pi)/\pi$ est un élément de $k[[(T-t_0)^{1/e}]]$ congru modulo $\langle (T-t_0)^{1/e} \rangle$ à ζ_σ.

Démonstration. — Posons $\zeta_\sigma = \sigma((T-t_0)^{1/e})/(T-t_0)^{1/e}$; c'est une racine primitive e-ième de l'unité. On écrit $\pi = u(T-t_0)^{1/e}$; l'élément u est une unité de $k[[(T-t_0)^{1/e}]]$, c'est-à-dire une série formelle (en $(T-t_0)^{1/e}$) de terme constant non nul. On obtient que $\sigma(u)/u$ est une série formelle de terme constant égal à 1. Comme $\sigma(\pi)/\pi = \zeta_\sigma\, \sigma(u)/u$, on a bien la conclusion annoncée. □

Pour $e \geq 1$, on note μ_e le sous-groupe de $k^\times$ des racines e-ièmes de l'unité. Grâce à l'identification entre $I_{\mathcal{P}} \subset \mathrm{Gal}(E/k(T))$ et le groupe de Galois

(7) En écrivant une série $\sum_{n \geq n_0} a_n (T-t_0)^{n/e}$ dans la $k((T-t_0))$-base $1, \dots, (T-t_0)^{d-1/e}$, on vérifie que l'action du générateur ci-dessus consiste aussi à remplacer $(T-t_0)^{1/e}$ par $\zeta_e (T-t_0)^{1/e}$ dans le développement initial.

(8) On peut voir aussi directement que pour tout $x \in k[[(T-t_0)^{1/e}]]$, on a $\sigma(x) - x \in \mathcal{P}_i$ pour σ le générateur ci-dessus (et donc pour tout $\sigma \in D_{\mathcal{P}_i}$).

$\mathrm{Gal}(\widetilde{E}/k((T-t_0))$ fournie par le corollaire 1.5.21 et le lemme précédent, on définit une application

$$\Theta_{\mathcal{P}} : I_{\mathcal{P}} \to \mu_e$$

en posant $\Theta_{\mathcal{P}}(\sigma) = \sigma(\pi)/\pi$ modulo l'idéal $\langle\pi\rangle$ (pour π comme dans le lemme).

C'est un isomorphisme de groupe et c'est en fait l'isomorphisme $\Theta_0 : I_0/I_1 \to \Theta_0(I_0/I_1) \subset k^\times$ introduit dans la preuve du théorème de Puiseux (théorème 3.1.1) ; la démonstration du lemme précédent reprend de façon plus concrète des arguments utilisés à cette occasion.

On se fixe maintenant un système cohérent $(\zeta_n)_{n\geq 1}$ de racines de l'unité, c'est-à-dire, ζ_n est une racine primitive n-ième de l'unité et $\zeta_{nm}^n = \zeta_m$, pour tous $n, m \geq 1$. Si $k \subset \mathbb{C}$, on peut prendre $\zeta_n = e^{2i\pi/n}$ $(n \geq 1)$.

Définition 3.1.9. — On appelle générateur distingué du groupe d'inertie $I_{\mathcal{P}}$ l'élément $\sigma_{\mathcal{P}}$ défini par $\Theta_{\mathcal{P}}(\sigma_{\mathcal{P}}) = \zeta_e$.

Soient $\mathcal{P}'$ un autre des idéaux $\mathcal{P}_1, \ldots, \mathcal{P}_g$ et $\sigma_{\mathcal{P}'}$ son générateur distingué. Les groupes $\mathcal{P}$ et $\mathcal{P}'$ étant conjugués (sous $\mathrm{Gal}(E/k(T))$ et cycliques (d'ordre e), on a $\mathcal{P}' = \mathcal{P}^\tau$ et $\sigma_{\mathcal{P}'} = \tau\sigma_{\mathcal{P}}^a\tau^{-1}$ avec $\tau \in \mathrm{Gal}(E/k(T))$ et $a \in (\mathbb{Z}/e\mathbb{Z})^\times$. On calcule $\Theta_{\mathcal{P}'}(\sigma_{\mathcal{P}'})$ en utilisant le générateur $\tau(\pi)$ de l'idéal de valuation de la place associée à $\mathcal{P}'$:

$$\Theta_{\mathcal{P}'}(\sigma_{\mathcal{P}'}) = \Theta_{\mathcal{P}'}(\tau\sigma_{\mathcal{P}}\tau^{-1})^a = \left[\frac{\tau\sigma_{\mathcal{P}}\tau^{-1}(\tau(\pi))}{\tau(\pi)}\right]^a = \tau\left[\frac{\sigma_{\mathcal{P}}(\pi)}{\pi}\right]^a = \Theta_{\mathcal{P}}(\sigma_{\mathcal{P}})^a$$

la dernière égalité résultant du fait que τ fixe les éléments de k. Comme $\Theta_{\mathcal{P}}(\sigma_{\mathcal{P}}) = \Theta_{\mathcal{P}'}(\sigma_{\mathcal{P}'}) = \zeta_e$, on a $a \equiv 1 \ [\mathrm{mod}\ e]$ et donc $\sigma_{\mathcal{P}}$ et $\sigma_{\mathcal{P}'}$ sont conjugués dans $\mathrm{Gal}(E/k(T))$.

Définition 3.1.10. — La classe de conjugaison de $\sigma_{\mathcal{P}}$ dans $\mathrm{Gal}(E/k(T)$, qui ne dépend que t_0, est appelée la classe canonique d'inertie associée à t_0. Si $\{t_1, \ldots, t_r\}$ est l'ensemble des points de branchement de l'extension $E/k(T)$ et $C_1^{\mathrm{alg}}, \ldots, C_r^{\mathrm{alg}}$ les classes canoniques d'inertie associées, le r-uplet non ordonné[(9)] $\{C_1^{\mathrm{alg}}, \ldots, C_r^{\mathrm{alg}}\}$ est appelé l'invariant canonique de l'inertie.

3.1.3.4. Invariants d'une extension $E/\overline{k}(T)$. — Soient k un corps algébriquement clos et $E/k(T)$ une extension finie séparable. On note $\widehat{E}/k(T)$ sa clôture galoisienne. On associe alors à $E/k(T)$ les invariants suivants :

- *son degré* : $d = [E : k(T)]$,

[(9)] c'est-à-dire le r-uplet $(C_1^{\mathrm{alg}}, \ldots, C_r^{\mathrm{alg}})$ modulo l'action du groupe symétrique S_r, ce que l'on peut voir aussi comme diviseur formel : $C_1^{\mathrm{alg}} + \cdots + C_r^{\mathrm{alg}}$.

- *son groupe* : le groupe $\mathrm{Gal}(\widehat{E}/k(T))$, qui, *via* son action sur les $k(T)$-plongements de E dans une clôture séparable de $k(T)$, est plongé dans le groupe $\mathrm{Per}(\mathrm{Plg}(E, k(T)^{\mathrm{s}}))$ des permutations de ces plongements ; moyennant une numérotation des différents plongements, on peut voir $\mathrm{Gal}(\widehat{E}/k(T))$ comme plongé dans S_d,
- *son ensemble de points de branchement* $\mathbf{t} = \{t_1, \ldots, t_r\}$, qu'on peut aussi voir comme diviseur : $\mathbf{t} = t_1 + \cdots + t_r$,

et, *si k est de caractéristique* 0,

- *son invariant canonique de l'inertie* $\mathbf{C} = \{C_1^{\mathrm{alg}}, \ldots, C_r^{\mathrm{alg}}\}$, défini comme étant celui de la clôture galoisienne $\widehat{E}/k(T)$. On peut le voir aussi comme diviseur : $C_1^{\mathrm{alg}} + \cdots + C_r^{\mathrm{alg}}$. *Via* le plongement $\mathrm{Gal}(\widehat{E}/k(T)) \to S_d$, on peut aussi considérer le r-uplet non ordonné des classes correspondant aux C_i^{alg} dans le groupe S_d. Il n'est bien défini qu'à la conjugaison par des éléments de S_d près ; pour faire la distinction avec le premier, on parlera de celui-ci comme de l'*invariant canonique plongé* (dans S_d) et on le notera $\iota(\mathbf{C})$.

Ces données ont les propriétés d'invariance suivantes au sein d'une classe d'isomorphisme d'extensions finies séparables de $k(T)$.

Si $\chi : E \to E'$ est un $k(T)$-isomorphisme entre deux extensions $E/k(T)$ et $E'/k(T)$, alors $[E : k(T)] = [E' : k(T)] = d$ et χ se prolonge en un isomorphisme $\widehat{\chi}$ entre les clôtures galoisiennes $\widehat{E}/k(T)$ et $\widehat{E}'/k(T)$ (défini à un élément de $\mathrm{Gal}(\widehat{E}/E)$ près). L'isomorphisme $\widehat{\chi} : \widehat{E} \to \widehat{E}'$ induit un isomorphisme entre $\mathrm{Gal}(\widehat{E}/k(T))$ et $\mathrm{Gal}(\widehat{E}'/k(T))$ et un isomorphisme entre les actions $\mathrm{Gal}(\widehat{E}/k(T)) \to \mathrm{Per}(\mathrm{Plg}(E, k(T)^{\mathrm{s}}))$ et $\mathrm{Gal}(\widehat{E}'/k(T)) \to \mathrm{Per}(\mathrm{Plg}(E', k(T)^{\mathrm{s}}))$. Les deux extensions $E/k(T)$ et $E'/k(T)$ ont même ensemble de points de branchement. Si k est de caractéristique 0, l'isomorphisme entre les groupes de Galois envoie l'invariant canonique de l'inertie de $E/k(T)$ sur celui de $E'/k(T)$. Moyennant une numérotation des éléments de $\mathrm{Plg}(E, k(T)^{\mathrm{s}})$ et de $\mathrm{Plg}(E', k(T)^{\mathrm{s}})$, on a un isomorphisme entre les deux actions correspondantes $\mathrm{Gal}(\widehat{E}/k(T)) \to S_d$ et $\mathrm{Gal}(\widehat{E}/k(T)) \to S_d$. Cet isomorphisme envoie l'invariant canonique plongé de l'inertie de $E/k(T)$ sur celui de $E'/k(T)$.

De plus si une clôture séparable $k(T)^{\mathrm{s}}$ de $k(T)$ est fixée et les extensions séparables $E/k(T)$ sont vues au sein de $k(T)^{\mathrm{s}}$, alors on a $\widehat{E} = \widehat{E}'$ et $\mathrm{Gal}(\widehat{E}/k(T)) = \mathrm{Gal}(\widehat{E}'/k(T))$.

Si l'extension $E/k(T)$ est galoisienne, on a $d = |\mathrm{Gal}(\widehat{E}/k(T))|$ et l'action $\mathrm{Gal}(\widehat{E}/k(T)) \to S_d$ est l'action par translation (à gauche ou à droite), qu'on appelle souvent la représentation régulière de $\mathrm{Gal}(\widehat{E}/k(T))$.

Remarque 3.1.11. — Dans la suite nous nous placerons parfois dans la situation où k est seulement supposé séparablement clos. Nous ne considérerons alors que des extensions régulières $E/k(T)$ dont "les invariants sur k sont les mêmes que sur $\overline{k}$". C'est-à-dire nous supposerons que
- la clôture galoisienne $\widehat{E}/k(T)$ de $E/k(T)$ est régulière sur k. En conséquence les groupes de Galois $\mathrm{Gal}(\widehat{E}/k(T))$ et $\mathrm{Gal}(\widehat{E}\overline{k}/\overline{k}(T))$ sont isomorphes ainsi que leurs représentations dans S_d,
- les points de branchement de l'extension $E\overline{k}/\overline{k}(T)$ sont dans $\mathbb{P}^1(k)$ et les extensions résiduelles correspondantes dans l'extension $E/k(T)$ sont séparables (et donc triviales) ; les points de branchement sont alors les mêmes sur k et $\overline{k}$.
Ces hypothèses sont satisfaites si k est un corps parfait.

3.1.3.5. Action des automorphismes de k. — Soient k un corps algébriquement clos et $E/k(T)$ une extension finie séparable. Soient $\tau \in \mathrm{Aut}(k)$ et $\tilde{\tau}$ un prolongement fixé de τ à une clôture algébrique $\overline{k(T)}$ de $k(T)$. Considérons l'extension $E^{\tilde{\tau}}/k(T)$ et sa clôture galoisienne $\widehat{E^{\tilde{\tau}}}/k(T)$ dans $\overline{k(T)}$.

Proposition 3.1.12. — (a) *On a $[E : k(T)] = [E^{\tilde{\tau}} : k(T)]$ et $\widehat{E^{\tilde{\tau}}} = \widehat{E}^{\tilde{\tau}}$.*
(b) *La correspondance $\sigma \to \tilde{\tau}\sigma\tilde{\tau}^{-1}$ établit un isomorphisme entre les groupes de Galois, notés G et $G^{\tilde{\tau}}$ de $\widehat{E}/k(T)$ et $\widehat{E}^{\tilde{\tau}}/k(T)$, et même un isomorphisme entre les deux actions de groupe $G \to S_d$ et $G^{\tilde{\tau}} \to S_d$.*

Soit $t_0 \in \mathbb{P}^1(k)$ et $\mathcal{P}$ un des idéaux premiers de la décomposition de l'idéal $\langle T - t_0\rangle \subset k[T]_{t_0}$ dans l'extension $E/k(T)$.
(c) *$\mathcal{P}^{\tilde{\tau}}$ est un idéal premier de la décomposition l'idéal $\langle T - t_0^{\tilde{\tau}}\rangle \subset k[T]_{t_0^{\tilde{\tau}}}$ dans l'extension $E^{\tilde{\tau}}/k(T)$.*
(d) *La correspondance $\sigma \to \tilde{\tau}\sigma\tilde{\tau}^{-1}$ établit un isomorphisme entre les groupes d'inertie $I_{\mathcal{P}}$ et $I_{\mathcal{P}^{\tilde{\tau}}}$. En particulier, l'indice de ramification e est le même pour $\mathcal{P}$ et $\mathcal{P}^{\tilde{\tau}}$.*
(e) *Si k est de caractéristique 0, le diagramme*

$$\begin{array}{ccc} I_{\mathcal{P}} & \xrightarrow{\Theta_{\mathcal{P}}} & \mu_e \\ {\scriptstyle \tilde{\tau}.\tilde{\tau}^{-1}}\downarrow & & \downarrow{\scriptstyle .^{\tau}} \\ I_{\mathcal{P}^{\tilde{\tau}}} & \xrightarrow[\Theta_{\mathcal{P}^{\tilde{\tau}}}]{} & \mu_e \end{array}$$

est commutatif. C'est-à-dire, pour tout $\sigma \in I_{\mathcal{P}}$, on a $\Theta_{\mathcal{P}^{\tilde{\tau}}}(\sigma^{\tilde{\tau}}) = \Theta_{\mathcal{P}}(\sigma)^{\tau}$.

Démonstration. — (a), (b), (c) et (d) sont immédiats et laissés en exercice. Montrons (e). Soit $\sigma \in I_{\mathcal{P}}$. L'élément $\Theta_{\mathcal{P}}(\sigma) \in \mu_e$ est défini par la condition

$\sigma(\pi) - \Theta_{\mathcal{P}}(\sigma)\pi \in \langle \pi^2 \rangle$, où π est un générateur de l'idéal $\mathcal{P}$. Cela entraîne que $\sigma(\pi)^{\tilde{\tau}} - \Theta_{\mathcal{P}}(\sigma)^{\tau}\pi^{\tilde{\tau}} \in \langle (\pi^{\tilde{\tau}})^2 \rangle$, c'est-à-dire $\sigma^{\tilde{\tau}}(\pi^{\tilde{\tau}}) - \Theta_{\mathcal{P}}(\sigma)^{\tau}\pi^{\tilde{\tau}} \in \langle (\pi^{\tilde{\tau}})^2 \rangle$. Comme $\pi^{\tilde{\tau}}$ est un générateur de $\mathcal{P}^{\tilde{\tau}}$, cela signifie que $\Theta_{\mathcal{P}^{\tilde{\tau}}}(\sigma^{\tilde{\tau}}) = \Theta_{\mathcal{P}}(\sigma)^{\tau}$. (On peut aussi montrer (e) en reprenant le calcul fait après la définition 3.1.9). □

L'action des automorphismes de k sur les racines de l'unité est donnée par le caractère cyclotomique χ : pour tout $n \geq 1$ et $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\chi(\tau)$ est l'élément de $(\mathbb{Z}/n\mathbb{Z})^{\times}$ tel que $\zeta_n^{\tau} = \zeta_n^{\chi(\tau)}$. On précise parfois "modulo n" pour indiquer la référence à l'entier n. On peut voir la collection cohérente de tous les caractères cyclotomiques modulo n ($n \geq 1$) comme un morphisme de $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ ou même de $\mathrm{G}_{\mathbb{Q}}$ vers le groupe, noté $\widehat{\mathbb{Z}}^{\times}$, limite projective de tous les groupes $(\mathbb{Z}/n\mathbb{Z})^{\times}$ ($n \geq 1$).

Corollaire 3.1.13. — *Sous les hypothèses du paragraphe, si $G \to S_d$, $\mathbf{t} = \{t_1, \ldots, t_r\}$ (et $\mathbf{C} = \{C_1, \ldots, C_r\}$ si k est de caractéristique 0) sont les invariants de l'extension $E/k(T)$, alors les invariants de l'extension $E^{\tilde{\tau}}/k(T)$ sont les suivants :*

- groupe et son action : ils sont isomorphes à G et à $G \to S_d$. Si on identifie $\mathrm{Gal}(E^{\tilde{\tau}}/k(T))$ à G (via la correspondance $\sigma \to \tilde{\tau}\sigma\tilde{\tau}^{-1}$), l'action associée à l'extension conjuguée est égale à $G \to S_d$ à la conjugaison près par un élément $\omega \in \mathrm{Nor}_{S_d}(G)$.

- points de branchement : leur ensemble est $\mathbf{t}^{\tau} = \{t_1^{\tau}, \ldots, t_r^{\tau}\}$,

et si k est de caractéristique 0 :

- invariant canonique de l'inertie : c'est le r-ruplet non ordonné $\mathbf{C}^{1/\chi(\tau)} = \{C_1^{1/\chi(\tau)}, \ldots, C_r^{1/\chi(\tau)}\}$, où $1/\chi(\tau)$ désigne l'inverse de $\chi(\tau)$ dans $(\mathbb{Z}/e\mathbb{Z})^{\times}$.

De plus, il y a compatibilité de l'action de $\tilde{\tau}$ sur les points de branchement et sur les classes canoniques d'inertie : la classe canonique d'inertie associée à t_i^{τ} dans l'extension $E^{\tilde{\tau}}/k(T)$ est la classe $C_i^{1/\chi(\tau)}$. En d'autres termes

- l'ensemble $\{(t_1, C_1), \ldots, (t_r, C_r)\}$ est transformé par l'action de τ en l'ensemble $\{(t_1^{\tau}, C_1^{1/\chi(\tau)}), \ldots, (t_r^{\tau}, C_r^{1/\chi(\tau)})\}$.

Démonstration. — Ces conclusions découlent de la proposition 3.1.12. Pour le dernier point, voir que pour tout indice $i = 1, \ldots, r$, si $\mathcal{P}$ est un idéal premier de la décomposition de l'idéal $\langle T - t_i \rangle \subset k[T]_{t_i}$ et $\sigma_{\mathcal{P}}$ un générateur distingué du groupe d'inertie $I_{\mathcal{P}}$, alors $\Theta_{\mathcal{P}}(\sigma_{\mathcal{P}}) = \zeta_e$ entraîne $\Theta_{\mathcal{P}^{\tilde{\tau}}}(\sigma_{\mathcal{P}}^{\tilde{\tau}}) = \zeta_e^{\chi(\tau)}$. L'élément $(\sigma_{\mathcal{P}}^{1/\chi(\tau)})^{\tilde{\tau}}$ est donc le générateur distingué du groupe d'inertie $I_{\mathcal{P}^{\tilde{\tau}}}$. La classe canonique d'inertie associée est donc $C_i^{1/\chi(\tau)}$ (*via* l'identification par la conjugaison par $\tilde{\tau}$). □

3.1.4. Extensions régulières de $k(T)$. — On revient au cas où k est un corps quelconque et $E/k(T)$ une extension régulière de degré d.

3.1.4.1. Invariants de l'extension $E/k(T)$. — Ce sont ceux de l'extension $E\overline{k}/\overline{k}(T)$.

3.1.4.2. Corps de définition des points non ramifiés. —

Définition 3.1.14. — Pour tout point $w \in X_{E\overline{k}}(\overline{k})$, c'est-à-dire, pour toute place w de E (triviale sur k), on appelle corps de définition du point w le corps résiduel de la restriction de w à E. Le point w est dit k-rationnel si son corps de définition est égal à k.

Pour $t_0 \in \mathbb{P}^1(\overline{k})$, le corps de définition de t_0 est le corps $k(t_0)$.

Soit w une place non ramifiée de $E\overline{k}$ au-dessus d'un point t_0 k-rationnel. La place w correspond à un plongement $\sigma : E \to \overline{k}((T - t_0))$. Il existe alors une plus petite extension $k(w)/k$ tel que le plongement soit à valeurs dans $k(w)((T - t_0))$. Ce corps est le corps de définition du point w.

Considérons en effet un élément primitif $y(T)$ de l'extension $E/k(T)$, entier sur $A = k[T]$ (ou $A = k[1/T]$ si $t_0 = \infty$). *Via* le plongement σ, $y(T)$ s'écrit comme série formelle en $T - t_0$. Notons $k_{y(T)}$ le corps engendré sur k par les coefficients de cette série. Si $\Delta(T) \in k[T]$ est le discriminant de la base $\{1, y(T), \ldots, y(T)^{d-1}\}$, on a, par le théorème 1.3.15,

$$\Delta(T)A'_E \subset A \oplus \cdots \oplus Ay^{d-1} \subset k_{y(T)}[[T - t_0]]$$

On déduit d'une part que $E \subset k_{y(T)}((T - t_0))$ donc que $k(w) = k_{y(T)}$, d'autre part, que ce corps est aussi le corps résiduel de la restriction à E de w.

Si l'extension $k(w)/k$ est séparable, par exemple si k est un corps parfait, le corps $k(w)$ est une extension finie de degré $\leq d$. Cela résulte de la proposition 1.5.1. On peut aussi le voir en observant que les séries formelles obtenues à partir de $y(T)$ en appliquant aux coefficients les différents k-plongements $k(w) \to \overline{k}$ sont autant de conjugués de $y(T)$ sur $k(T)$.

Soit $P(T, Y) \in k[T, Y]$ le polynôme minimal de $y(T)$. Le terme constant $y(t_0)$ de la série est alors une racine du polynôme $P(t_0, Y)$. Si c'en est une racine simple (par exemple si t_0 n'est pas une racine du discriminant $\Delta_P(T)$ de P en Y), alors le lemme de Hensel (théorème 1.9.4) montre que le corps $k(w)$ est le corps $k(y(t_0))$.

3.1.4.3. Descente du corps de définition d'une extension $E/k(T)$. —

Définition 3.1.15. — Soient F/k une extension de corps et $E/F(T)$ une extension finie régulière. On dit que l'extension $E/F(T)$ est définie sur k s'il

existe une extension finie $E_k/k(T)$ régulière telle que E_kF et E soient $F(T)$-isomorphes. Si $E/F(T)$ est une extension galoisienne, elle est dite définie sur k comme G-extension s'il existe une extension finie $E_k/k(T)$ galoisienne et régulière telle que E_kF et E soient $F(T)$-isomorphes. On dit alors de k que c'est un corps de définition et de l'extension $E_k/k(T)$ que c'est un k-modèle (comme G-extension dans le second cas) de l'extension $E/F(T)$.

Si l'extension $E/F(T)$ est définie sur k, il en de même de toute extension $E'/F(T)$ qui lui est $F(T)$-conjuguée (comme simple extension ou comme G-extension). Pareillement les corps de définition, les modèles sont les mêmes au sein d'une classe d'isomorphisme sur $F(T)$ d'extensions $E/F(T)$.

Remarque 3.1.16. — L'extension galoisienne $\overline{\mathbb{Q}}(T^{1/d})/\overline{\mathbb{Q}}(T)$ ($d \geq 1$) est définie sur $\mathbb{Q}$: l'extension $\mathbb{Q}(T^{1/d})/\mathbb{Q}(T)$ en est un $\mathbb{Q}$-modèle. Mais ce n'en est pas un modèle comme G-extension puisque $\mathbb{Q}(T^{1/d})/\mathbb{Q}(T)$ n'est pas galoisienne. L'extension galoisienne $\overline{\mathbb{Q}}(T^{1/d})/\overline{\mathbb{Q}}(T)$ n'est en fait pas définie sur $\mathbb{Q}$ comme G-extension car par exemple la condition (d) du corollaire 3.1.18 n'est pas satisfaite. Pour distinguer les deux situations de la définition, on dit qu'une extension galoisienne $E/F(T)$ qui est définie sur k qu'elle l'est comme simple extension.

Dans la suite on suppose que F/k est une extension galoisienne. Un cas important, appelé *question de la descente absolue*, est celui où F est la clôture séparable k^{s} de k.

La descente du corps de définition d'une extension $E/F(T)$ de F à k n'est pas toujours possible. Une condition nécessaire est donnée par l'énoncé ci-dessous. Pour $\tau \in \mathrm{Gal}(F/k)$, on note $\tilde{\tau}$ un prolongement de τ à une clôture algébrique de $F(T)$.

Proposition 3.1.17. — (a) *Si une extension finie $E/F(T)$ séparable et régulière est définie sur k (comme simple extension), alors pour tout $\tau \in \mathrm{Gal}(F/k)$, il existe un $F(T)$-isomorphisme $\chi_\tau : E \to E^{\tilde{\tau}}$.*

(b) *Si une extension finie $E/F(T)$ galoisienne et régulière est définie sur k comme G-extension, alors pour tout $\tau \in \mathrm{Gal}(F/k)$, $E^{\tilde{\tau}} = E$ et il existe $\chi_\tau \in \mathrm{Gal}(E/F(T))$ tel que*

(*) *Pour tout $\sigma \in \mathrm{Gal}(E/F(T))$, on a $\tilde{\tau}\,\sigma\,\tilde{\tau}^{-1} = \chi_\tau\,\sigma\,\chi_\tau^{-1}$.*

On dit alors que k est le corps des modules de l'extension $E/F(T)$ relativement à l'extension F/k, comme simple extension dans le cas (a) *et comme G-extension dans le cas* (b).

On vérifie que les conditions obtenues ne dépendent pas des prolongements choisis $\tilde{\tau}$ des automorphismes τ.

La condition obtenue dans (a) revient à dire que l'extension $E/F(T)$ est isomorphe à chacune des extensions conjuguées $E^{\tilde{\tau}}/F(T)$. Pour la condition obtenue dans (b), on dira que l'extension $E/F(T)$ est isomorphe à chacune des extensions conjuguées $E^{\tilde{\tau}}/F(T)$ *comme G-extension.*

On peut formaliser la notion de G-extension de la façon suivante. Etant donné un groupe fini G et un corps F, une G-extension de $F(T)$ de groupe G (ou G-extension) consiste en la donnée d'une extension galoisienne régulière $E/F(T)$ et d'un isomorphisme $u : G \to \mathrm{Gal}(E/F(T))$. Un morphisme entre deux G-extensions $(E/F(T), u)$ et $(E'/F(T), u')$ est un $F(T)$-morphisme $\chi : E \to E'$ tel que pour tout $g \in G$, on a $\chi\, u(g)\, \chi^{-1} = u'(g)$.

Pour $\tau \in \mathrm{Gal}(F/k)$, on définit la G-extension conjuguée par $\tilde{\tau}$ de $(E/F(T), u)$ par le couple $(E^{\tilde{\tau}}/F(T), u^{\tilde{\tau}})$ où $u^{\tilde{\tau}} : G \to \mathrm{Gal}(E^{\tilde{\tau}}/F(T))$ est l'isomorphisme défini par $u^{\tilde{\tau}}(g) = \tilde{\tau}\, u(g)\, \tilde{\tau}^{-1}$ $(g \in G)$. La condition dans (b) correspond à dire que la G-extension $E/F(T)$[(10)] est isomorphe à chacune des G-extensions conjuguées $E^{\tilde{\tau}}/F(T)$.

Démonstration de la proposition 3.1.17. — Supposons $E/F(T)$ définie sur k comme simple extension. Soit $P(T, Y) \in k(T)[Y]$ le polynôme minimal d'un élément primitif d'un k-modèle $E_k/k(T)$. L'extension $E/F(T)$ est $F(T)$-isomorphe à l'extension $E_0 = F(T)[Y]/\langle P(T, Y)\rangle$ de $F(T)$. Pour tout $\tau \in \mathrm{Gal}(F/k)$, on prolonge τ à E_0 en envoyant T sur T et Y sur Y ; on fixe ensuite un prolongement $\tilde{\tau}$ de ce premier prolongement à $\overline{E_0}$. Les conditions annoncées dans la proposition 3.1.17 sont réalisées pour E_0 avec $\chi_\tau = \mathrm{Id}$.

En effet on a $E_0^{\tilde{\tau}} = E_0$, ce qui prouve (a). Pour le (b), supposons que $E_0/F(T)$ soit définie sur k comme G-extension. Si $\sigma \in \mathrm{Gal}(E_0/F(T))$, en utilisant que le corps $E_{0k} = k(T)[Y]/\langle P(T, Y)$ est extension galoisienne de $k(T)$, on peut écrire $\sigma(Y + \langle P\rangle) = R_\sigma(Y + \langle P\rangle)$ avec $R_\sigma \in k(T)[Y]$. On a

$$(*)\quad \tilde{\tau}\,\sigma\,\tilde{\tau}^{-1}(Y + \langle P\rangle) = \tilde{\tau}\,(R_\sigma(T, Y + \langle P\rangle)) = R_\sigma(T, Y + \langle P\rangle) = \sigma(Y + \langle P\rangle)$$

ce qui entraîne bien que $\tilde{\tau}\,\sigma\,\tilde{\tau}^{-1} = \sigma$.

Revenons à l'extension $E/F(T)$. Par construction, il existe un isomorphisme $\varphi : E_0 \to E$. Considérons le prolongement $\tilde{\tau}_E : E \to E$ de τ défini par $\tilde{\tau}_E = \varphi\,\tilde{\tau}\,\varphi^{-1}$ et prolongeons ensuite τ_E à $\overline{E}$ (de manière arbitraire). Vérifions d'abord que les conditions de la proposition 3.1.17 sont satisfaites pour ce prolongement $\tilde{\tau}_E$.

(10) Dans la pratique, on omet fréquemment la référence à l'isomorphisme u dans la notation.

On note $\varphi^{\tilde{\tau}_E} : E_0 \to E^{\tilde{\tau}_E}$ l'isomorphisme conjugué par $\tilde{\tau}_E$, qui est défini par $\varphi^{\tilde{\tau}_E}(x^{\tilde{\tau}}) = (\varphi(x))^{\tilde{\tau}_E}$ $(x \in E_0)$. Le morphisme $\chi_\tau = \varphi^{\tilde{\tau}_E} \circ \varphi^{-1}$ est un $F(T)$-isomorphisme entre E et $E^{\tilde{\tau}_E}$.

Supposons que $E/F(T)$ soit définie sur k comme G-extension. On a $E^{\tilde{\tau}_E} = E$ et pour tout $\sigma \in \mathrm{Gal}(E/F(T))$,

$$\begin{aligned}\tilde{\tau}_E\,\sigma\,(\tilde{\tau}_E)^{-1} &= (\varphi\,\tilde{\tau}\,\varphi^{-1})\,\sigma\,(\varphi\,\tilde{\tau}^{-1}\,\varphi^{-1})\\ &= \varphi\,\tilde{\tau}\,(\varphi^{-1}\,\sigma\,\varphi)\,\tilde{\tau}^{-1}\,\varphi^{-1}\\ &= \varphi\,(\varphi^{-1}\,\sigma\,\varphi)\,\varphi^{-1} \quad \text{(d'après (*))}\\ &= \sigma\end{aligned}$$

Si $\tilde{\tau}$ est un prolongement donné de τ à $\overline{k(T)}$, alors $\tilde{\tau}\tilde{\tau}_E^{-1}$ est l'identité sur $F(T)$. Sa restriction à $E^{\tilde{\tau}_E}$ est un $F(T)$-isomorphisme sur $E^{\tilde{\tau}}$. Cela donne (a), et, dans le cas où $E/F(T)$ est définie sur k comme G-extension, cela explique la présence du $F(T)$-automorphisme χ_τ dans la condition (b). □

3.1.4.4. Branch cycle lemma. — Si deux extensions $E/F(T)$ et $E'/F(T)$ sont conjuguées sur $F(T)$, elles le sont *a fortiori* sur $\overline{k}$. Le corollaire 3.1.13 fournit donc les conditions nécessaires suivantes pour qu'une extension $E/F(T)$ soit définie sur k.

Nous supposerons cependant toujours l'hypothèse suivante satisfaite :

(**) La clôture galoisienne $\widehat{E}/F(T)$ de l'extension $E/F(T)$ est régulière.

Cette hypothèse garantit que le groupe de l'extension $E/F(T)$ reste le même après extension des scalaires de F à $\overline{k}$. Cette hypothèse n'est pas restrictive dans la situation absolue où $F = k^{\mathrm{s}}$. En effet, il résulte de la séparabilité de $\widehat{E}/F(T)$ que $\widehat{E} \cap \overline{F}$ est une extension séparable de F et donc est égale à F dans le cas $F = k^{\mathrm{s}}$.

Corollaire 3.1.18. — *Soient $G \to S_d$, $\mathbf{t} = \{t_1, \ldots, t_r\}$, et $\mathbf{C} = \{C_1, \ldots, C_r\}$ pour k de caractéristique 0, les invariants d'une extension régulière $E/F(T)$.*

• *Si $E/F(T)$ est définie sur k, on a :*

(a) $\mathbf{t}^\tau = \mathbf{t}$ *pour tout* $\tau \in \mathrm{Gal}(F/k)$,

(b) $\iota(\mathbf{C})^{\chi(\tau)} = \iota(\mathbf{C})$, *pour tout* $\tau \in \mathrm{Gal}(F/k)$ *(pour k de caractéristique 0).*

(c) *plus précisément : pour tout* $\tau \in \mathrm{Gal}(F/k)$

$$\{(t_1^\tau, \iota(C_1)^{1/\chi(\tau)}), \ldots, (t_r^\tau, \iota(C_r)^{1/\chi(\tau)})\} = \{(t_1, \iota(C_1)), \ldots, (t_r, \iota(C_r))\}$$

• *Si $E/F(T)$ est galoisienne et définie sur k comme G-extension, on a en plus (pour k de caractéristique 0) :*

(d) $\mathbf{C}^{\chi(\tau)} = \mathbf{C}$, *pour tout* $\tau \in \mathrm{Gal}(F/k)$.

(e) *plus précisément : pour tout* $\tau \in \mathrm{Gal}(F/k)$,

$$\{(t_1^\tau, C_1^{1/\chi(\tau)}), \ldots, (t_r^\tau, C_r^{1/\chi(\tau)})\} = \{(t_1, C_1)), \ldots, (t_r, C_r)\}$$

Démonstration. — Ces conclusions découlent du corollaire 3.1.13 et la proposition 3.1.17. Noter que la condition (a) de la proposition 3.1.17 entraîne que les invariants canoniques de l'inertie de $\widehat{E}/k(T)$ et $\widehat{E}^{\tilde{\tau}}/k(T)$ sont égaux, après identification des groupes de Galois $\mathrm{Gal}(\widehat{E}^{\tilde{\tau}}/k(T))$ et $\mathrm{Gal}(\widehat{E}/k(T))$ *via* la conjugaison par $\tilde{\tau}$. Cela entraîne $\iota(\mathbf{C})^{\chi(\tau)} = \iota(\mathbf{C})$, ou, de façon plus explicite :

$$\{C_1^{\chi(\tau)}, \ldots, C_r^{\chi(\tau)}\} = \{C_1^{\omega_\tau}, \ldots, C_r^{\omega_\tau}\}$$

pour un élément $\omega_\tau \in \mathrm{Nor}_{S_d}(G)$. Si $E/F(T)$ est galoisienne et définie sur k comme G-extension, alors d'après la condition (b) de la proposition 3.1.17, la conjugaison par $\tilde{\tau}$ coincide avec une conjugaison dans $\mathrm{Gal}(E/k(T))$. On obtient ainsi la condition $\mathbf{C}^{\chi(\tau)} = \mathbf{C}$ ($\tau \in \mathrm{Gal}(F/k)$). □

Le corollaire 3.1.18 est connu sous le nom de "branch cycle lemma". Le résultat suivant en est une conséquence classique.

Proposition 3.1.19. — *Si* $E/\mathbb{Q}(T)$ *est une extension galoisienne régulière de groupe* $\mathbb{Z}/p^m\mathbb{Z}$ *avec* p *premier et* $m \geq 1$*, il y a au moins* $\varphi(p^m) = p^m - p^{m-1}$ *points de branchement totalement ramifiés (c'est-à-dire, d'indice de ramification égal à* p^m*). En conséquence, le groupe* $\mathbb{Z}_p$ *des entiers p-adiques n'est pas le groupe de Galois d'une extension régulière galoisienne de* $\mathbb{Q}(T)$*.*

Démonstration. — Soit $\mathbf{t} = \{t_1, \ldots, t_r\}$ l'ensemble des points de branchement de l'extension $E/\mathbb{Q}(T)$. Le groupe G étant abélien, les classes canoniques d'inertie associées sont réduites à un élément, que nous notons g_i, $i = 1, \ldots, r$. Ces éléments engendrent G : en effet, si $H = \langle g_1, \ldots, g_r \rangle$, alors d'après la proposition 1.5.19, l'extension $E^H/\mathbb{Q}(T)$ n'est ramifiée en aucun point de $\mathbb{P}^1(\overline{\mathbb{Q}})$, elle est donc triviale (voir §2.3.3 énoncé (b)), d'où $H = G$. Par conséquent, il existe nécessairement un g_j d'ordre p^m ; comme $p^m = [E : \mathbb{Q}(T)]$, le point de branchement correspondant est totalement ramifié. Comme l'image du caractère cyclotomique χ modulo p^m est $(\mathbb{Z}/p^m\mathbb{Z})^\times$, l'ensemble des éléments $g_j^{\chi(\tau)}$ où τ décrit $\mathrm{G}_\mathbb{Q}$ est de cardinal $\varphi(p^m)$. D'après le corollaire 3.1.18, tous ces éléments sont des classes canoniques d'inertie de l'extension $E/k(T)$, qui correspondent à autant de points de branchement totalement ramifiés.

Supposons qu'il existe une extension galoisienne régulière de groupe $\mathbb{Z}_p$. Pour tout entier $m \geq 1$, notons $E_m/\mathbb{Q}(T)$ l'extension intermédiaire de groupe de Galois $\mathbb{Z}/p^m\mathbb{Z}$. En raison de la multiplicativité des indices de ramification, un point de branchement totalement ramifié d'une extension $E_m/\mathbb{Q}(T)$ ($m \geq$

1) est aussi un point de branchement de l'extension $E_1/\mathbb{Q}(T)$. D'après ce qui précède, l'extension $E_1/\mathbb{Q}(T)$ devrait en avoir au moins $p^m - p^{m-1}$ pour tout $m \geq 1$, ce qui contredit la finitude de l'ensemble des points de branchement. □

3.2. Représentations du groupe fondamental

Le corps k est *a priori* un corps arbitraire.

3.2.1. Groupe fondamental. — Soit $r \geq 1$ un entier. Le sous-ensemble ouvert de $(\mathbb{P}^1)^r$ (resp. de $\mathbb{P}^r$) des r-uplets $(t_1, \ldots, t_r)$ (resp. des r-uplets non ordonnés $\{t_1, \ldots, t_r\}$) dont les coordonnées sont deux à deux distinctes est noté U^r (resp. U_r). Etant donné $\mathbf{t} = \{t_1, \ldots, t_r\} \in U_r(k)$[11], on définit le *$k$-groupe fondamental* de $\mathbb{P}^1 \setminus \{\mathbf{t}\}$ de la façon suivante.

Fixons une clôture séparable $k(T)^{\mathrm{s}}$ of $k(T)$. Soit $\Omega_{\mathbf{t}} \subset k(T)^{\mathrm{s}}$ l'extension algébrique séparable maximale de $k^{\mathrm{s}}(T)$ non ramifiée au-dessus de $\mathbb{P}^1 \setminus \mathbf{t}$, c'est-à-dire, la réunion de toutes les extensions finies séparables $E/k^{\mathrm{s}}(T)$ non ramifiées au-dessus de chaque point de $\mathbb{P}^1 \setminus \mathbf{t}$. L'extension $\Omega_{\mathbf{t}}/k^{\mathrm{s}}(T)$ est galoisienne ; par définition son groupe de Galois est le k^{s}-groupe fondamental de $\mathbb{P}^1 \setminus \mathbf{t}$ et est noté $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$. Comme $\mathbf{t} \in U_r(k)$, l'extension $\Omega_{\mathbf{t}}/k(T)$ est également galoisienne ; par définition son groupe de Galois est le k-groupe fondamental de $\mathbb{P}^1 \setminus \mathbf{t}$ et est noté $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_k$ (ou simplement $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ quand la référence à k est claire). On parle parfois du groupe $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$ comme du groupe fondamental *géométrique*. Le diagramme suivant résume la situation

$$\begin{array}{ccc} & & \Omega_{\mathbf{t}} \\ & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} & \uparrow \\ \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) & & k^{\mathrm{s}}(T) \\ & \mathrm{G}_k & \uparrow \\ & & k(T) \end{array}$$

et la théorie de Galois fournit la suite exacte

$$1 \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to \mathrm{G}_k \to 1$$

[11] $U_r(k)$ désigne l'ensemble des k-points de U_r, c'est-à-dire, des points $\mathbf{t} \in U_r$ dont les coordonnées sont les solutions d'un polynôme séparable $p(T) \in k(T)$, ou, de façon équivalente, dont les coordonnées sont dans k^{s} et vérifient $\mathbf{t}^\tau = \mathbf{t}$ pour tout $\tau \in \mathrm{G}_k$.

Le groupe fondamental est à l'origine une notion topologique. On parle donc parfois des groupes définis ici comme des groupes fondamentaux algébriques. Comme le point de vue algébrique est celui que nous mettons en avant, nous omettrons le terme "algébrique". Nous ferons le lien avec le groupe fondamental topologique à la section 3.4.

Théorème 3.2.1. — *La suite exacte ci-dessus est scindée.*
À tout point rationnel $t_0 \in \mathbb{P}^1(k) \setminus \{\mathbf{t}\}$ non ramifié est associée une section $s_{t_0} : G_k \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$, correspondant au plongement des extensions finies séparables $E/k^s(T)$ dans le corps $k^s((T-t_0))$.
Si k est de caractéristique 0, on peut également associer une section $s_{t_0} : G_k \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ à un point $t_0 \in \mathbb{P}^1(k)$ ramifié, qui correspond au plongement du corps $\Omega_{\mathbf{t}}$ dans le corps $\bigcup_{n\geq 1} \overline{k}((T-t_0)^{1/n}$ des séries de Puiseux à coefficients dans $\overline{k}$.
La section s_{t_0} est bien définie à un élément de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$ près.

Démonstration. — Supposons $t_0 \in \mathbb{P}^1(k) \setminus \{\mathbf{t}\}$. Pour tout $\tau \in \mathrm{G}_k$, notons $\tilde{\tau}$ le prolongement naturel de τ au corps $k^{\mathrm{s}}((T-t_0))$. Grâce au lemme ci-dessous, on dispose d'un plongement $i : \Omega_{\mathbf{t}} \hookrightarrow k^{\mathrm{s}}((T-t_0))$. L'homomorphisme

$$s_{t_0} : \begin{cases} \mathrm{G}_k & \to & \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \\ \tau & \longmapsto & s_{t_0}(\tau) = \ i^{-1} \circ \tilde{\tau} \circ i \end{cases}$$

est alors une section de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to \mathrm{G}_k$.

On procède similairement dans le cas où k est de caractéristique 0 et $t_0 \in \mathbb{P}^1(k)$ est un point de branchement mais en utilisant le corps $\bigcup_{n\geq 1} \overline{k}((T-t_0)^{1/n}$ à la place du corps $\overline{k}((T-t_0))$; le théorème de Puiseux remplace le lemme 3.2.2.

Pour terminer la preuve, il reste à traiter le cas où k est de caractéristique $p > 0$ et $\mathbb{P}^1(k) \subset \mathbf{t}$. Mais alors k est un corps fini $\mathbb{F}_q$ et G_k est un groupe "procyclique" isomorphe à $\widehat{\mathbb{Z}}$; il est engendré par le Frobenius, c'est-à-dire, le $\mathbb{F}_q$-automorphisme de $\overline{\mathbb{F}_q}$ envoyant tout élément $x \in \overline{\mathbb{F}_q}$ sur x^q. Cet automorphisme se relève en un élément de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ pour fournir la section désirée. □

Lemme 3.2.2. — *Pour tout point k-rationnel $t_0 \in \mathbb{P}^1(k) \setminus \{\mathbf{t}\}$, il existe un plongement $\Omega_{\mathbf{t}} \subset k^s((T-t_0))$.*

Démonstration. — Notons $\mathfrak{F}$ l'ensemble des couples (E, i_E) où $E \subset \Omega_{\mathbf{t}}$ est une extension séparable de $k^{\mathrm{s}}(T)$ non ramifiée en dehors de $t_1, \ldots, t_r$ et $i_E : E \hookrightarrow k^{\mathrm{s}}((T-t_0))$ est un $k^{\mathrm{s}}(T)$- plongement. On munit $\mathfrak{F}$ de la relation d'ordre : $(E, i_E) < (F, i_F)$ si $E \subset F$ et i_F prolonge i_E.

L'ensemble ordonné $(\mathfrak{F}, <)$ est un ensemble inductif non vide. D'après le lemme de Zorn, il existe un élément maximal (E_∞, i_∞). On a nécessairement $E_\infty = \Omega_{\mathbf{t}}$. En effet, sinon il existe $x \in \Omega_{\mathbf{t}}$ tel que $x \notin E_\infty$. Mais grâce au lemme 1.3.2 on peut prolonger l'homomorphisme i_∞ sur le corps $E_\infty(x)$: en effet le polynôme minimal de x sur E_∞ divise le polynôme minimal de x sur $k^{\mathrm{s}}(T)$, lequel a toutes ses racines dans $k^{\mathrm{s}}((T - t_0))$ puisque, par définition de $\Omega_{\mathbf{t}}$, l'extension $k^{\mathrm{s}}(T, x)/k^{\mathrm{s}}(T)$ est non ramifiée au-dessus de t_0 (§3.1.3.2). Cela contredit la maximalité de (E_∞, i_∞). □

3.2.2. Dictionnaire "extensions/représentations du π_1". — On fixe $\mathbf{t} = (t_1, \ldots, t_r) \in U_r(k)$ et une clôture séparable $k(T)^{\mathrm{s}}$ de $k(T)$.

Nous expliquons ci-dessous comment une extension finie séparable de $k(T)$ non ramifiée au-dessus de $\mathbb{P}^1 \setminus \mathbf{t}$ peut être vue comment une représentation transitive continue du groupe $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ de degré fini.

Dans la suite, nous disons simplement "extension $E/k(T)$" pour une extension finie séparable régulière $E/k(T)$, et, suivant le contexte, "simple extension" ou "G-extension".

3.2.2.1. Simples extensions. — À une simple extension $E/k(T)$ de degré d et de points de branchement contenus dans $\mathbf{t}$ correspond une représentation continue[(12)] transitive

$$\psi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$$

telle que la restriction à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$ reste transitive. Réciproquement à une telle représentation peut être associée une extension $E/k(T)$ comme ci-dessus. Ces correspondances, que nous détaillons ci-dessous ne sont pas canoniques. Mais elles induisent des correspondances bijectives canoniques entre les classes d'isomorphisme. Plus précisément, deux extensions $E/k(T)$ et $E'/k(T)$ sont isomorphes si et seulement si les représentations associées ψ et ψ' sont conjuguées par un élément $\varphi \in S_d$, c'est-à-dire

$$\psi'(x) = \varphi\psi(x)\varphi^{-1} \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$$

Via cette correspondance, le groupe de l'extension $E/k(T)$ est le groupe image $G = \psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}})$.

Correspondances. Par la théorie de Galois, la clôture galoisienne $\widehat{E}/k(T)$ de l'extension $E/k(T)$ correspond à un quotient continu du groupe fondamental $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$, ou, de façon équivalente, à un morphisme continu surjectif $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$ où $G = \mathrm{Gal}(\widehat{E}/k(T))$. A son tour, l'extension $E/k(T)$ correspond à

(12) c'est-à-dire, de noyau fermé pour la topologie de Krull.

un sous-groupe H de G. Numérotons les classes à gauche de G modulo H de 1 à d de telle manière que H corresponde à 1. L'action de G par translation à gauche sur ces classes fournit une représentation fidèle $i : G \to S_d$, qui correspond à l'action de G sur les d conjugués d'un élément primitif de $E/k(T)$. L'homomorphisme composé $\psi = i \circ \phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$ est la représentation désirée. Sa restriction à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$ est transitive du fait de la régularité de l'extension $E/k(T)$. La représentation ψ est bien définie 'a la conjugaison par un élément de S_d fixant 1 près.

Réciproquement, supposons donnée une représentation $\psi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$ de restriction transitive à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$. Notons en abrégé π_1 pour $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$, $\overline{\pi}_1$ pour $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$ et $\pi_1(1)$ pour le stabilisateur de 1 dans la représentation $\psi : \pi_1 \to S_d$. Considérons le sous-corps $E = \Omega_{\mathbf{t}}^{\pi_1(1)}$ de $\Omega_{\mathbf{t}}$ fixé par $\pi_1(1)$. L'extension $E/k(T)$ est régulière : d'une part $Ek^s = \Omega_{\mathbf{t}}^{\pi_1(1)}\Omega_{\mathbf{t}}^{\overline{\pi}_1} = \Omega_{\mathbf{t}}^{\pi_1(1)\cap\overline{\pi}_1}$(13) et d'autre part(14)

$$\begin{cases} [E : k(T)] & = [\pi_1 : \pi_1(1)] = d \\ [Ek^s : k^s(T)] & = [\overline{\pi}_1 : \pi_1(1) \cap \overline{\pi}_1] = d \end{cases}$$

3.2.2.2. G-extensions. — À une G-extension $E/k(T)$ de groupe G de points de branchement contenus dans $\mathbf{t}$ correspond un épimorphisme continu

$$\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$$

tel que $\phi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}) = G$. Réciproquement à un tel épimorphisme peut être associée une G-extension comme ci-dessus. Ces correspondances, détaillées ci-dessous, ne sont pas canoniques mais induisent des correspondances bijectives canoniques entre les classes d'isomorphisme. Deux G-extensions $E/k(T)$ et $E'/k(T)$ sont isomorphes si et seulement si les épimorphismes associés ϕ et ϕ' sont conjugués par un élément $\varphi \in G$, c'est-à-dire

$$\phi'(x) = \varphi\phi(x)\varphi^{-1} \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$$

(13) Pour la deuxième égalité, on a en général, $K^{G_1\cap G_2} = K^{G_1}K^{G_2}$ dès que $K^{G_1}/K^{G_1G_2}$ est galoisien, pour K un corps et G_1, G_2 deux sous-groupes d'un groupe G d'automorphismes de K. En effet, la restriction $\mathrm{Gal}(K^{G_1}K^{G_2}/K^{G_2}) \to \mathrm{Gal}(K^{G_1}/K^{G_1G_2})$ est un isomorphisme : l'injectivité est claire, le sous-corps fixé par son image est $K^{G_1} \cap K^{G_2}$, or, de façon immédiate, on a $K^{G_1} \cap K^{G_2} = K^{G_1G_2}$). On en déduit la suite d'isomorphismes $\mathrm{Gal}(K^{G_1\cap G_2}/K^{G_2}) \simeq G_2/(G_1 \cap G_2) \simeq G_1G_2/G_1 \simeq \mathrm{Gal}(K^{G_1}/K^{G_1G_2}) \simeq \mathrm{Gal}(K^{G_1}K^{G_2}/K^{G_2})$, qui fournit la conclusion désirée.

(14) Pour la seconde ligne, noter que $\pi_1(1) \cap \overline{\pi}_1$ est le stabilisateur de 1 de la restriction de $\psi : \pi_1 \to S_d$ à $\overline{\pi}_1$, laquelle est supposée transitive.

Correspondances. Une G-extension $E/k(T)$ de groupe G correspond à un sous-groupe ouvert normal bien défini $H \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$. Le groupe quotient $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})/H$ peut être canoniquement identifié au groupe de Galois $\mathrm{Gal}(E/k(T))$. En composant la surjection naturelle $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})/H$ avec l'isomorphisme donné $\mathrm{Gal}(E/k(T)) \to G$, on obtient l'épimorphisme désiré $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$. On a $\phi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}) = G$ car l'extension galoisienne $E/k(T)$ est régulière.

Réciproquement, soit $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$ un épimorphisme continu tel que $\phi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}) = G$. Considérons le sous-corps $E = \Omega_{\mathbf{t}}^{\ker(\phi)} \subset \Omega_{\mathbf{t}}$ fixé par le sous-groupe normal $\ker(\phi) \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$. L'extension $E/k(T)$ est galoisienne, de groupe $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})/\ker(\phi)$ et on montre comme pour les simples extensions qu'elle est régulière. L'isomorphisme $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})/\ker(\phi) \to G$ munit l'extension $E/k(T)$ d'une structure de G-extension.

3.2.2.3. Simple extension induite par une G-extension. — Si une G-extension $E/k(T)$ correspond à l'épimorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$, la simple extension associée $E/k(T)$ (c'est-à-dire, dépourvue de l'isomorphisme $\mathrm{Gal}(E/k(T)) \to G$) correspond à la représentation $\psi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$ obtenue en composant ϕ avec la représentation régulière à gauche $G \to S_d$ (où $d = |G|$).

3.2.2.4. G-extension associée à une simple extension. — Soit $\psi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$ la représentation de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ associée à une simple extension $E/k(T)$ de degré d. Soit $G = \psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t}))$. L'épimorphisme induit $\psi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$ correspond à la clôture galoisienne $\widehat{E}/k(T)$ de l'extension $E/k(T)$: le noyau $\ker(\psi)$ est le plus grand sous-groupe distingué de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ contenu dans le fixateur de 1 dans la représentation ψ. L'extension $\widehat{E}/k(T)$ ne correspond pas nécessairement à une G-extension (sur k). C'est le cas si et seulement si $\psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})) = \psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}) = G$, ce qui revient à dire que l'extension $\widehat{E}/k(T)$ est régulière sur k. En général on a $\psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})) \supset \psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s})$. Le groupe $\psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s})$ est appelé le groupe de Galois géométrique et $\psi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t}) = G$ le groupe de Galois arithmétique de l'extension $E/k(T)$.

3.2.2.5. Action des automorphismes de k. — Soient $\tau \in \mathrm{G}_k$ et $\tilde{\tau} \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ un prolongement fixé de τ à $\Omega_{\mathbf{t}}$.

Soit $E/k^s(T)$ une simple extension (resp. une G-extension) correspondant à la représentation $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to S_d$ (resp. à l'épimorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to G$). Considérons la représentation $\phi^{\tilde{\tau}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to S_d$ (resp. l'épimorphisme $\phi^{\tilde{\tau}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to G$) défini par

$$\phi^{\tilde{\tau}}(x) = \phi(x^{\tilde{\tau}^{-1}}) \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$$

L'homomorphisme $\phi^{\tilde{\tau}}$ correspond à une simple extension (resp. à une G-extension) qui est isomorphe à la simple extension (resp. à la G-extension) $E^{\tilde{\tau}}/k^{\mathrm{s}}(T)$: il suffit d'observer qu'on a $\ker(\phi^{\tilde{\tau}}) = \ker(\phi)^{\tilde{\tau}}$ et une relation similaire entre les fixateurs de 1 des représentations ϕ et $\phi^{\tilde{\tau}}$.

3.2.2.6. Action de Galois sur les fibres non ramifiées. — Etant donnés une extension finie séparable $E/k(T)$ et un point $t_0 \in \mathbb{P}^1(k)$, on appelle fibre au-dessus de t_0 l'ensemble des points/places de l'extension $Ek^{\mathrm{s}}/k^{\mathrm{s}}$ au-dessus de t_0. Comme t_0 est k-rationnel, la fibre au-dessus de t_0 est invariante par l'action de tout élément $\tau \in \mathrm{G}_k$[15]. Pour t_0 non ramifié, la section s_{t_0} utilisée ci-dessous est celle qui a été introduite pour le théorème 3.2.1.

Proposition 3.2.3. — *Soient $E/k(T)$ une simple extension et $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to S_d$ la représentation associée. Soit $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$. Alors pour tout $\tau \in \mathrm{G}_k$, la permutation $\phi(s_{t_0}(\tau))$ est conjuguée dans S_d à la permutation ω_τ induite par l'action de τ sur la fibre au-dessus de t_0.*

Démonstration. — De façon générale, pour $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$, la permutation $\phi(x)$ correspond à l'action de x sur les différents plongements de $E/k(T)$ dans une clôture galoisienne $\widehat{E}/k(T)$. Pour $x = s_{t_0}(\tau)$ avec $\tau \in \mathrm{G}_k$, $\widehat{E}$ peut être plongé dans $k^{\mathrm{s}}((T - t_0))$ et l'action est alors celle de τ sur les différents $k(T)$-plongements de E dans $k^{\mathrm{s}}((T - t_0))$ (théorème 3.2.1), lesquels correspondent à la fibre au-dessus de t_0 (théorème 3.1.5). □

Voici une application de la proposition 3.2.3.

Proposition 3.2.4. — *Soient $E/k(T)$ une extension régulière galoisienne de groupe de Galois abélien G. Soit $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$. Alors il existe une extension régulière galoisienne $\widetilde{E}/k(T)$ de groupe G tel que $\widetilde{E} \subset k((T - t_0))$.*

En d'autres termes, la condition supplémentaire satisfaite par $\widetilde{E}/k(T)$ revient à dire que tous les points/places de la fibre au-dessus de t_0 sont k-rationnels (voir 3.1.4.2).

Démonstration. — Soit $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$ la représentation associée à $E/k(T)$. Notons $p : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to \mathrm{G}_k$ la restriction naturelle et $s_{t_0} : \mathrm{G}_k \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ la section associée au point t_0. Considérons l'application $\widetilde{\phi} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to G$ définie par :

$$\widetilde{\phi}(x) = \phi(x) \cdot (\phi \circ s_{t_0} \circ p(x))^{-1} \quad (x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}))$$

[15] Cette action n'est bien définie qu'à conjugaison près.

L'application $\widetilde{\phi}$ est un homomorphisme de groupes (car G est abélien) de groupe image égal à G. De plus ϕ et $\widetilde{\phi}$ coincident sur $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$. L'épimorphisme $\widetilde{\phi}$ définit donc une G-extension $\widetilde{E}/k(T)$ de groupe G vérifiant $Ek^{\mathrm{s}} = \widetilde{E}k^{\mathrm{s}}$. On a de plus $\widetilde{\phi} \circ s_{t_0} = (\phi \circ s_{t_0}) \cdot (\phi \circ s_{t_0})^{-1} = 1$. La proposition 3.2.4 fournit alors la condition supplémentaire annoncée. □

3.3. Revêtements algébriques

Le corps de base k est arbitraire *a priori*.

3.3.1. Courbes affines et corps de fonctions. — Soient $P \in k[T, Y]$ un polynôme absolument irréductible tel que $\deg_Y(P) \geq 1$ et $C \subset \mathbb{A}^2$ la courbe affine d'équation $P(t, y) = 0$. Pour tout corps $\mathcal{K} \supset k$, on note $\mathcal{K}(C)$ le corps de fonctions de C sur $\mathcal{K}$ et $C(\mathcal{K})$ l'ensemble des points $\mathcal{K}$-rationnels sur C, c'est-à-dire

$$\begin{cases} \mathcal{K}(C) = \mathrm{Frac}\,(\mathcal{K}[T, Y]/(P(T, Y))) \\ C(\mathcal{K}) = \{(t, y) \in \mathcal{K} \times \mathcal{K} \mid P(t, y) = 0\} \end{cases}$$

Si $\partial P/\partial Y \neq 0$, l'extension $k(C)/k(T)$ est séparable, de degré $d = \deg_Y(P)$ et régulière sur k.

Réciproquement, si $E/k(T)$ est une extension finie séparable régulière, le choix d'un élément primitif permet de définir une courbe affine C comme ci-dessus dont le corps des fonctions est $k(T)$-isomorphe à E.

Un point $(t_0, y_0) \in C(\overline{k})$ est *régulier* ou *non-singulier* si $P'_T(t_0, y_0) \neq 0$ ou $P'_Y(t_0, y_0) \neq 0$. Dans ce cas, l'*anneau local* au point (t_0, y_0)

$$\mathcal{O}_{(t_0,y_0)} = \{f = \frac{a}{b} \in \overline{\mathbb{Q}}(C) | b(t_0, y_0) \neq 0\}$$

est un anneau de valuation discrète : il suffit de voir que l'idéal maximal est principal (théorème 1.2.7), or celui-ci est engendré par $(T - t_0)$ ou $(Y - y_0)$ suivant que $P'_Y(t_0, y_0) \neq 0$ ou $P'_T(t_0, y_0) \neq 0$. La valuation correspondante, notée $\mathrm{ord}_{(t_0,y_0)}$ est appelée *ordre* au point (t_0, y_0). On dit que $f \in \overline{k}(C)$ a un *zéro* en (t_0, y_0) si $\mathrm{ord}_{(t_0,y_0)}(f) > 0$ et qu'elle a un *pôle* en (t_0, y_0) si $\mathrm{ord}_{(t_0,y_0)}(f) < 0$.

3.3.2. Courbes projectives lisses. —

3.3.2.1. Généralités. — D'une façon analogue à la définition des espaces affines, on définit les espaces projectifs $\mathbb{P}^n$ et la topologie de Zariski sur ces espaces ; la différence est qu'on utilise des polynômes homogènes. Les sous-ensembles fermés et irréductibles des espaces projectifs sont appelés les variétés

projectives, et les ouverts des variétés projectives les variétés quasi-projectives. Voir [**Har77**, chapter I, §2].

Une variété sur k est définie comme étant soit une variété quasi-affine, soit une variété quasi-projective. On définit ensuite la notion de fonction régulière en un point P d'une variété Y : c'est une fonction $f : Y \to k$ qui au voisinage de P s'écrit comme une fraction rationnelle (de polynômes homogènes de même degré dans le cas projectif) sans pôle dans le voisinage en question. On note $\mathcal{O}(Y)$ l'anneau des fonctions régulières sur Y (c'est-à-dire, en tout point de Y). On peut ensuite définir la notion de morphisme entre deux variétés X et Y : c'est une application continue $\varphi : X \to Y$ telle que pour tout ouvert $V \subset Y$ et toute fonction régulière $f : V \to k$, la fonction $f \circ \varphi : \varphi^{-1}(V) \to k$ est régulière.

On appelle fonction rationnelle sur une variété Y la donnée (U, f) d'un ouvert $U \subset Y$ et d'une fonction f régulière sur U modulo l'équivalence qui identifie deux tels couples (U, f) et (V, g) si $f = g$ sur $U \cap V$. L'ensemble des fonctions rationnelles sur une variété Y constitue un corps appelé corps des fonctions de Y. Etant donné un point P d'une variété Y, on appelle anneau local en P, l'anneau noté $\mathcal{O}_{Y,P}$ des classes de couples (U, f) comme ci-dessus mais avec la condition supplémentaire que $P \in U$; c'est effectivement un anneau local. Voir [**Har77**, chapter I, §3].

On appelle application rationnelle entre deux variétés X et Y la donnée (U, f) d'un ouvert $U \subset X$ et d'un morphisme $f : U \to Y$ modulo l'équivalence qui identifie deux couples (U, f) et (V, g) si $f = g$ sur $U \cap V$. L'application rationnelle (U, f) est dite dominante si $f(U)$ est dense dans Y. Voir [**Har77**, chapter I, §4]

On a une notion générale de dimension pour une variété : comme espace topologique irréductible. On appelle courbe toute variété de dimension 1.

On suppose désormais k algébriquement clos.

3.3.2.2. Birationalité. — Toute application rationnelle dominante $f : X \to Y$ induit un morphisme $f^* : k(Y) \to k(X)$ envoyant $\varphi \in k(Y)$ sur $\varphi \circ f \in k(X)$. La correspondance $f \to f^*$ induit une équivalence de catégories entre la catégorie des variétés et des applications rationnelles dominantes, et celle des extensions de type fini de k et des morphismes de corps ([**Har77**, theorem 4.4]. En particulier, on a le résultat suivant ([**Har77**, corollaire 4.5]).

Théorème 3.3.1. — *Pour deux variétés X et Y, les assertions suivantes sont équivalentes :*

(a) *X et Y sont birationnellement équivalentes (c'est-à-dire, il existe une application rationnelle $f : X \to Y$ qui a une application inverse $Y \to X$ rationnelle).*
(b) *Il existe deux ouverts $U \subset X$ et $V \subset Y$ tels que U et V soient isomorphes.*
(c) *Les corps de fonctions rationnelles $k(X)$ et $k(Y)$ sont k-isomorphes.*

3.3.2.3. Non-singularité. — Soit Y une variété et $P \in Y$. Notons $\mathcal{O}_{Y,P}$ l'anneau local en P et $\mathfrak{M}$ son idéal maximal. Le corps résiduel de $\mathcal{O}_{Y,P}$ est égal à k et son corps des fractions est le corps $k(Y)$. Un point $P \in Y$ est dit régulier ou non singulier si l'anneau $\mathcal{O}_{Y,P}$ est régulier au sens de la définition 1.1.4, c'est-à-dire si $\mathfrak{M}/\mathfrak{M}^2$ est un k-espace vectoriel de dimension $\dim(\mathcal{O}_{Y,P})$, laquelle vaut aussi $\dim(Y)$[16]. Une variété est dite lisse si tous ses points sont non-singuliers. Voir [**Har77**, chapter I,§5].

Si Y est une courbe et P un point non-singulier sur Y, alors l'anneau local en P est un anneau local régulier intègre de dimension 1, et donc un anneau de valuation discrète (théorème 1.2.7).

Les notions introduites étendent celles du §3.3.1. Pour l'équivalence entre les deux notions de non-singularité, voir [**Har77**, theorem 5.1] ; si P est un point non singulier sur la variété Y, la valuation de l'anneau local $\mathcal{O}_{Y,P}$ généralise la valuation $\mathrm{ord}_{(t_0,y_0)}$ du §3.3.1.

3.3.3. Modèle projectif lisse d'une courbe. — Pour cette sous-section, nous suivons [**Har77**, chapter I, §6] ; nous y renvoyons pour les détails.

On suppose k algébriquement clos.

Supposons donnée une extension finie séparable $E/k(T)$ et considérons l'ensemble $X_E(k)$ de toutes les places de E (définition 3.1.3). On munit $X_E(k)$ de la topologie pour laquelle les fermés sont les ensembles finis et l'ensemble $X_E(k)$. Si $U \subset X_E(k)$ est un ouvert, définissons l'anneau des fonctions régulières sur U comme étant l'anneau intersection $\mathcal{O}(U) = \bigcap_{P \in U} R_P$ de tous les anneaux de valuation R_P des places $P \in U$; un élément $f \in \mathcal{O}(U)$ définit une fonction sur U en prenant pour $P \in U$ $f(P)$ égal à la classe de f dans le corps résiduel de R_P, lequel est le corps k [**Har77**, corollaire 6.6]. On appelle courbe abstraite non singulière la donnée de l'espace topologique $X_E(k)$ et des anneaux $\mathcal{O}(U)$ de fonctions régulières sur tout ouvert $U \subset X_E(k)$.

[16] Pour l'égalité $\dim(\mathcal{O}_{Y,P}) = \dim(Y)$, voir que $\dim(Y) = \dim(U)$ pour tout ouvert $U \subset Y$ [**Har77**, proposition 1.10], et que, pour un ouvert affine $U \ni P$ (c'est-à-dire, isomorphe à une variété affine), on a $\dim(\mathcal{O}_{U,P}) = \dim(U)$ [**Har77**, theorem 3.2] et que les anneaux locaux $\mathcal{O}_{U,P}$ et $\mathcal{O}_{Y,P}$ sont isomorphes. La dimension de Y est également égale au degré de transcendance du corps de fonctions $k(Y)$ [**Har77**, theorem 3.2].

On étend ensuite la notion de morphisme $\varphi : X \to Y$ au cas où X et Y sont soit une courbe abstraite non-singulère soit une variété ; la définition est identique à celle donnée au §3.3.2 : c'est une application continue $\varphi : X \to Y$ telle que pour tout ouvert $V \subset Y$ et toute fonction régulière $f : V \to k$, la fonction $f \circ \varphi : \varphi^{-1}(V) \to k$ est régulière.

On vérifie ensuite que si C est une courbe non-singulière, alors elle est isomorphe à une courbe abstraite non singulière [**Har77**, proposition 6.7]. Le résultat principal est le suivant [**Har77**, theorem 6.9].

Théorème 3.3.2. — *La courbe abstraite non singulière $X_E(k)$ est isomorphe à une courbe projective lisse.*

La courbe $X_E(k)$ est appelée le modèle projectif lisse du corps de fonctions E ; par exemple, on a $X_{k(T)} = \mathbb{P}^1$.

Pour les courbes, on a ainsi ce résultat de classification [**Har77**, corollaire 6.11].

Corollaire 3.3.3. — *Toute courbe est birationnellement équivalente à une courbe projective lisse.*

En particulier, la courbe affine $C : P(t, y) = 0$ du §3.3.1 est birationnellement équivalente au modèle projectif $X_{k(C)}$ de son corps de fonctions. Notons C' l'ensemble de ses points non-singuliers. Il existe un ouvert $U \subset C'$ et un morphisme injectif $U \to X_{k(C)}$. En vertu du résultat suivant [**Har77**, proposition 6.8], il peut être prolongé à C' tout entier, qui peut être ainsi identifié à un ouvert de la courbe projective lisse $X_{k(C)}$. L'ensemble $X_{k(C)} \setminus C'$ est un ensemble fini qui correspond aux *points à l'infini* de C et aux points obtenus par désingularisation des points singuliers de C.

Théorème 3.3.4. — *Soient X une courbe abstraite non singulière, $P \in X$, Y une variété projective et $\varphi : X \setminus \{P\} \to Y$ un morphisme. Alors il existe un unique morphisme $\overline{\varphi} : X \to Y$ qui prolonge φ.*

Le résultat suivant est une forme catégorique du théorème 3.3.2 [**Har77**, corollary 6.12].

Théorème 3.3.5. — *Les catégories suivantes sont équivalentes :*
(a) *courbes projectives lisses, et morphismes non constants*[17]

[17] Pour un morphisme ou une application rationnelle $f : X \to Y$ à valeurs dans une courbe Y, être dominant équivaut à être non constant : l'image $f(Y)$ ne peut être finie de cardinal > 1 à cause de l'irréductibilité de X.

(b) *courbes quasi-projectives et applications rationnelles non constantes,*
(c) *corps de fonctions de dimension* 1 *(c'est-à-dire, extension de type fini de* k *de degré de transcendance* 1*), et* k*-morphismes.*

3.3.4. Revêtements algébriques. —

Définition 3.3.6. — On appelle revêtement algébrique de courbes tout morphisme non constant $X \to Y$ entre deux courbes projectives lisses tel que l'extension associée $k(X)/k(Y)$ des corps de fonctions soit séparable et finie.

On peut voir de façon équivalente un revêtement algébrique de courbes comme une extension séparable finie de deux corps de fonctions d'une variable. En particulier, les extensions séparables finies $E/k(T)$ correspondent à des revêtements algébriques de $\mathbb{P}^1$.

Les notions introduites pour les extensions finies séparables s'étendent telles quelles aux revêtements algébriques. Par exemple, un revêtement $X \to \mathbb{P}^1$ est dit ramifié au-dessus de $t_0 \in \mathbb{P}^1$ si c'est le cas de l'extension $k(X)/k(T)$. *Idem* pour "être défini sur un sous-corps $k' \subset k$", etc.

On peut relire les paragraphes §3.1.3.1 et §3.1.3.2 avec un point de vue plus géométrique. Etant donnée une extension finie séparable $E/k(T)$ et un point $t_0 \in \mathbb{P}^1(k)$, les places de E au-dessus de la place t_0 correspondent aux points P_i de la courbe projective lisse X_E au-dessus du point t_0 dans le revêtement $\varphi : X_E \to \mathbb{P}^1$; leur ensemble $\varphi^{-1}(t_0)$ est appelé la fibre du revêtement au-dessus de t_0. Le point t_0 est un point de branchement si et seulement si la fibre $\varphi^{-1}(t_0)$ a strictement moins de d éléments, où $d = [E : k(T)] = \deg_Y(P)$ est le degré du revêtement.

Si $P(T, Y)$ est le polynôme minimal d'un élément primitif de l'extension $E/k(T)$ et C la courbe affine d'équation $P(t, y) = 0$, alors la restriction de φ à l'ouvert $C' \subset C$ des points non-singuliers correspond à la première projection $(t, y) \to t$. Le revêtement $\varphi : X_E \to \mathbb{P}^1$ peut être vu comme un prolongement projectif de la fonction $T \in k(C)$. Les indices de ramification e_i au-dessus de t_0 sont les ordres de la fonction $\varphi - t_0$ en les points P_i correspondants dans la fibre $\varphi^{-1}(t_0)$.

3.4. Revêtements topologiques

Cette section est pure topologie. Nous rappelons deux points fondamentaux de la théorie du groupe fondamental : la structure du groupe fondamental de la sphère de Riemann privée de quelques points et la correspondance entre

revêtements topologiques et représentation du groupe fondamental. Nous nous limitons aux énoncés et renvoyons aux chapitres 7 et 8 pour les détails.

3.4.1. Groupe fondamental de la sphère de Riemann privée de quelques points. — Etant donné un espace toplogique X et un point-base $t_0 \in X$, le groupe fondamental de X avec t_0 pour point-base sera noté $\pi_1^{\mathrm{top}}(X, x_0)$, pour le distinguer du groupe fondamental algébrique introduit précédemment.

Théorème 3.4.1. — *Soient $r \geq 0$ un entier, $t_0, t_1, \ldots, t_r$ $r+1$ points sur la sphère de Riemann $\mathbb{P}^1(\mathbb{C})$. Le groupe fondamental $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}, t_0)$ est isomorphe au groupe libre à r générateurs $\gamma_1, \ldots, \gamma_r$ modulo la relation $\gamma_1 \cdots \gamma_r = 1$.*

On peut préciser comment réaliser cet isomorphisme : on peut prendre pour $\gamma_1, \ldots, \gamma_r$ des lacets "tournant une fois dans le sens direct" autour de $t_1, \ldots, t_r$ respectivement et satisfaisant quelques conditions techniques comme ne se croisant pas mutuellement, etc. On appelle bouquet la donnée de tels lacets $\gamma_1, \ldots, \gamma_r$.

3.4.2. Revêtements et groupe fondamental. —

Définition 3.4.2. — Soit B un espace topologique et $f : X \to B$ une application continue. Les assertions suivantes sont équivalentes :

(a) Pour tout $b \in B$, il existe un voisinage U de b, un espace discret non vide D et un homéomorphisme $\Phi : f^{-1}(U) \to U \times D$ tel que $p_1 \circ \Phi$ coincide avec f, où $p_1 : U \times D \to U$ est la première projection.

(b) Pour tout $b \in B$, il existe un voisinage U de b et une famille $(V_d)_{d \in D}$ paramétrée par un ensemble D non vide vérifiant

(i) Les ensembles V_d sont des ouverts de X deux à deux disjoints.

(ii) $f^{-1}(U) = \bigcup_{d \in D} V_d$.

(iii) Pour tout $d \in D$, f induit un homéomorphisme $f_d : V_d \to U$.

Une application $f : X \to B$ ayant ces propriétés est appelée revêtement topologique de B. Il est dit fini si l'ensemble D est fini, et le cardinal de B est alors appelé le degré du revêtement.

On a une notion de morphisme de revêtements topologiques. Si $f : X \to B$ et $f' : X' \to B$ sont deux revêtements, alors un morphisme entre ces deux revêtements est une application continue $\chi : X \to X'$ telle que $f' \circ \chi = f$. Les

notions de d'isomorphisme, d'endomorphisme, d'automorphisme sont définies de façon habituelle.

Fixons un espace topologique B connexe par arcs, localement connexe par arcs et localement simplement connexe (par exemple $B = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$) et $t_0 \in B$. La *monodromie* permet d'associer à tout revêtement connexe $f : X \to B$ de degré d une représentation transitive $\phi : \pi_1^{\text{top}}(B, t_0) \to S_d$. Plus précisément, étant donnée une classe d'homotopie $[\gamma] \in \pi_1^{\text{top}}(B, t_0)$ et un point $x \in f^{-1}(t_0)$, il existe un unique relèvement de γ à un chemin sur X commençant en x. Ce chemin se termine en un point $y \in f^{-1}(t_0)$. On a construit de cette façon une permutation de la fibre $f^{-1}(t_0)$, qui, après numérotation de cette fibre, donne l'élément $\phi([\gamma]) \in S_d$. Le *groupe de monodromie* est le sous-groupe de S_d de toutes les permutations obtenues de cette façon, c'est-à-dire le groupe $\phi(\pi_1^{\text{top}}(\mathcal{B}, t_0))$.

Théorème 3.4.3. — *Soit B un espace topologique connexe par arcs, localement connexe par arcs et localement simplement connexe (par exemple $B = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$). Soit $t_0 \in B$. La monodromie établit une bijection entre*
- l'ensemble des revêtements connexes de degré d $f : X \to B$ modulo l'isomorphie des revêtements, et,
- l'ensemble des représentations transitives $\phi : \pi_1^{\text{top}}(B, t_0) \to S_d$ modulo l'isomorphie des représentations de $\pi_1^{\text{top}}(B, t_0)$ (c'est-à-dire la conjugaison par les éléments de S_d).

On a le dictionnaire suivant entre revêtements de B et représentations de $\pi_1^{\text{top}}(B, t_0)$:

- $\deg(f) \overset{\text{déf}}{=} \text{card}\left(f^{-1}(t_0)\right) = d$,
- groupe de monodromie $\mathrm{G}(f) \simeq G \overset{\text{def}}{=} \phi(\pi_1^{\text{top}}(B, t_0))$,
- groupe d'automorphismes $\mathrm{Aut}(f) \simeq \mathrm{Cen}_{S_d}(G)$,
- f revêtement galoisien (c'est-à-dire $|\mathrm{Aut}(f)| = d$) si et seulement si $|\mathrm{Cen}_{S_d}(G)| = d$ si et seulement si l'action de $\mathrm{Aut}(f)$ sur $f^{-1}(t_0)$, ou, de façon équivalente, de $\mathrm{Cen}_{S_d}(G)$, sur $\{1, \ldots, d\}$ est transitive (et libre) et alors on a

$$\begin{array}{ccc} \mathrm{Aut}(f) & \simeq & \mathrm{Cen}_{S_d}(G) \\ | \wr \text{ anti} & & | \wr \text{ anti} \\ \mathrm{G}(f) & \simeq & G \qquad (= \mathrm{Nor}_G(G(1))/G(1)\ ) \end{array}$$

(où $G(1) \subset G$ est le fixateur de 1 dans la représentation $G \to S_d$).

3.4.3. Revêtements de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$. — En combinant le théorème 3.4.1 et le théorème 3.4.3, on obtient que le choix d'un bouquet $\gamma_1, \ldots, \gamma_r$ pour $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$ détermine une correspondance bijective entre
- l'ensemble des revêtements connexes de degré d de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$ modulo l'isomorphie des revêtements, et
- l'ensemble des r-uplets transitifs $(g_1, \ldots, g_r) \in (S_d)^r$ tels que $g_1 \cdots g_r = 1$ modulo la conjugaison (composante par composante) par des éléments de S_d.

Cela fournit en particulier le résultat suivant.

Corollaire 3.4.4. — *Pour tout groupe fini G, si r est un entier $> \mathrm{rg}(G)$ et $t_1, \ldots, t_r$ sont r points distincts dans $\mathbb{P}^1(\mathbb{C})$, alors G est groupe de monodromie et groupe d'automorphismes d'un revêtement topologique galoisien de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$.*

Démonstration. — L'action par translation à gauche de G sur lui-même fournit un plongement $G \to S_d$ (la représentation régulière de G). Si $r > \mathrm{rg}(G)$, il existe un r-uplet $(g_1, \ldots, g_r)$ dont les composantes engendrent G et sont de produit égal à 1. Le centralisateur $\mathrm{Cen}_{S_d}(G)$ est anti-isomorphe à G ; la correspondance est donnée par l'action par translation *à droite* par les éléments de G. Il s'agit d'une action transitive (et libre). D'après les correspondances ci-dessus, ces données permettent de construire un revêtement comme dans l'énoncé. □

Comme pour les revêtements algébriques, on a un invariant lié à la ramification pour les revêtements topologiques de $B = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$. On appelle *cycles de ramification* les permutations $g_1, \ldots, g_r$ de la fibre $f^{-1}(t_0)$ induites par monodromie le long des générateurs $\gamma_1, \ldots, \gamma_r$ d'un bouquet fixé pour $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$, c'est-à-dire, $g_i = \phi(\gamma_i)$, $i = 1, \ldots, r$. Ces cycles dépendent du bouquet $\gamma_1, \ldots, \gamma_r$ mais on peut voir que leurs classes de conjugaison n'en dépendent pas ; on les note $C_1^{\mathrm{top}}, \ldots, C_r^{\mathrm{top}}$.

On peut définir les classes C_i^{top} de façon plus intrinsèque. Il existe, dans le groupe $\pi_1^{\mathrm{top}}(\mathcal{B}, t_0)$, une classe de conjugaison des lacets "tournant une fois autour de t_i dans le sens direct". Si $D_i \subset B$ est un petit disque autour de t_i, le plongement $D_i \setminus \{t_i\} \to B = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$ fournit un homomorphisme $\pi_1^{\mathrm{top}}(D_i \setminus \{t_i\}) \to \pi_1^{\mathrm{top}}(B)$. La classe "tourner une fois autour de t_i dans le sens direct" est la classe de conjugaison de l'image du générateur (orienté) du groupe monogène $\pi_1^{\mathrm{top}}(D_i \setminus \{t_i\})$. La classe C_i^{top} est alors l'image de cette classe par la représentation $\phi : \pi_1^{\mathrm{top}}(B) \to S_d$.

On appellera *type de ramification* le r-uplet $\mathbf{C}^{\mathrm{top}} = (C_1^{\mathrm{top}}, \ldots, C_r^{\mathrm{top}})$.

Si on voit la représentation de monodromie comme un morphisme $\phi : \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}) \to \mathrm{Per}(f^{-1}(t_0))$ à valeurs dans l'ensemble des permutations de la fibre au-dessus de t_0, les classes $C_1^{\mathrm{top}}, \ldots, C_r^{\mathrm{top}}$ sont des classes de conjugaison dans le groupe image $\phi(\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}))$. Si on choisit une numérotation des points de la fibre, la représentation n'est plus définie qu'à la conjugaison par des éléments de S_d et les classes $C_1^{\mathrm{top}}, \ldots, C_r^{\mathrm{top}}$ sont des classes de conjugaison dans S_d ; pour distinguer les deux cas, on parle dans le second de type de ramification plongé.

3.5. Théorème d'existence de Riemann

Le théorème d'existence de Riemann est un résultat d'identification des notions de revêtement algébrique et de revêtement topologique. Il établit que tout revêtement toplogique de la sphère de Riemann privée de r points provient d'un revêtement algébrique de $\mathbb{P}^1$.

La preuve se fait en plusieurs étapes. Partant d'un revêtement topologique $f : X \to \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$, on montre d'abord comment prolonger f au-dessus des points manquants $t_1, \ldots, t_r$ pour obtenir un "revêtement analytique ramifié" $\overline{f} : \overline{X} \to \mathbb{P}^1(\mathbb{C})$ de surfaces de Riemann. Ce problème de prolongement est un problème local, au voisinage de chaque point t_i. L'ingrédient principal est que le groupe fondamental du disque unité privé de l'origine est isomorphe à $\mathbb{Z}$ et que ses revêtements connexes de degré d correspondent aux applications $z \to z^{1/d}$, lesquelles se prolongent continument de façon unique en envoyant 0 sur 0.

L'étape suivante est d'établir l'origine algébrique du revêtement $\overline{f} : \overline{X} \to \mathbb{P}^1(\mathbb{C})$: on montre que l'extension correspondante $\mathcal{M}(\overline{X})/\mathcal{M}(\mathbb{P}^1(\mathbb{C}))$ des corps des fonctions méromorphes sur $\overline{X}$ et sur $\mathbb{P}^1(\mathbb{C})$) est une extension finie ; la conclusion vient du fait que le corps $\mathcal{M}(\mathbb{P}^1(\mathbb{C}))$ est une extension transcendante pure de $\mathbb{C}$ de degré de transcendance 1, c'est-à-dire, est isomorphe au corps $\mathbb{C}(T)$.

Pour boucler la boucle, il reste à expliquer comment on retrouve le revêtement topologique de départ à partir de l'extension $\mathcal{M}(\overline{X})/\mathbb{C}(T)$: on considère le morphisme $X_{\mathcal{M}(\overline{X})} \to \mathbb{P}^1(\mathbb{C})$ auquel on retire les fibres au-dessus des points de branchement. Pour les détails, nous renvoyons au chapitre 8.

Les différentes étapes de la construction sont fonctorielles, c'est-à-dire, s'étendent aux morphismes entre les objets considérés. Le théorème d'existence de Riemann est un résultat d'équivalence de catégories.

Théorème 3.5.1 **(Théorème d'existence de Riemann)**
Etant donné $\mathbf{t} = \{t_1, \dots, t_r\} \subset \mathbb{P}^1(\mathbb{C})$*, les catégories suivantes sont équivalentes :*

- [(au sein de la catégorie des) Corps de fonctions d'une variable sur $\mathbb{C}$]
Extensions finies de $\mathbb{C}(T)$ *non ramifiées en dehors de* $\mathbf{t}$
& $\mathbb{C}(T)$*-isomorphismes de corps*

- [Courbes projectives lisses sur $\mathbb{C}$]
Revêtements algébriques finis de $\mathbb{P}^1$ *non ramifiés en dehors de* $\mathbf{t}$
& morphismes de revêtements algébriques

- [Surfaces de Riemann connexes compactes]
Revêtements analytiques de $\mathbb{P}^1(\mathbb{C})$ *non ramifiés en dehors de* $\mathbf{t}$
& morphismes de revêtements analytiques

- [Espaces topologiques connexes]
Revêtements topologiques finis de $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$
& morphismes de revêtements topologiques

- [Représentations transitives de groupes fondamentaux]
Représentations transitives de $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t})$ *dans un groupe symétrique*
& applications compatibles entre ensemble finis

- [r-uplets d'éléments d'un groupe fini]
r-uplets de permutations de produit égal à 1 *et engendrant un sous-groupe transitif*
& applications compatibles entre ensemble finis

On obtient en particulier la forme pratique du théorème d'existence de Riemann que nous avons énoncée au chapitre 2 (théorème 2.4.2) qui permet de résoudre le problème inverse de Galois sur $\mathbb{C}(T)$. Le revêtement topologique galoisien de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_r\}$ construit dans la preuve du corollaire 3.4.4 est en fait algébrique, c'est-à-dire, provient d'une extension galoisienne de groupe le groupe G qui était donné au départ.

Ce revêtement peut-il être défini sur un corps plus petit, idéalement sur le corps $\mathbb{Q}$? C'est ce genre de questions que nous étudierons au chapitre suivant.

Via les équivalences de catégories du théorème 3.5.1, les invariants habituels se correspondent : degré, groupe d'automorphisme, etc. On peut ajouter ceci. Comme au §3.1.3.3 on se fixe un système cohérent $(\zeta_n)_{n\geq 1}$ de racines de l'unité.

Proposition 3.5.2. — *Soient* $E/\mathbb{C}(T)$ *une extension de degré* d *et* $f : X \to \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_r\}$ *le revêtement topologique associé. Alors via l'isomorphisme*

entre le groupe de Galois $\mathrm{Gal}(\widehat{E}/\mathbb{C}(T))$ *et le groupe de monodromie* $\mathrm{G}(f)$*, les classes de conjugaison* C_i^{top} *et* C_i^{alg} *se correspondent l'une à l'autre,* $i = 1, \ldots, r$*. Autrement dit, invariant canonique de l'inertie et type de ramification se correspondent.*

Démonstration. — Précisons l'isomorphisme $\mathrm{G}(f) \simeq \mathrm{Gal}(\widehat{E}/\mathbb{C}(T))$. Un cycle de ramification $\phi(\gamma)$ associé à un lacet $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\})$ agit sur les points de la fibre $f^{-1}(t_0)$ *via* la propriété de *relèvement des chemins*. A ces éléments $\phi_{t_0}(\gamma) \in G(f)$ correspondent, dans l'isomorphisme ci-dessus, des éléments de $\mathrm{Gal}(\widehat{\mathbb{C}(X)}/\mathbb{C}(T))$ qui agissent sur les *fonctions* dans $\widehat{\mathbb{C}(X)}$, par *prolongement analytique*. Pour $\gamma = \gamma_i$ un chemin "tournant une fois" autour de t_i, les éléments qu'on obtient sont bien, à conjugaison près, ceux de C_i^{top} et C_i^{alg} respectivement, $i = 1, \ldots, r$. □

Le théorème d'existence de Riemann permet également d'exprimer le groupe fondamental algébrique de $\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}$ sur $\mathbb{C}$, et plus généralement sur tout corps algébriquement clos $\overline{k}$ de caractéristique 0, en fonction de son groupe fondamental topologique. On suppose fixés une clôture algébrique de $\overline{k}(T)$ et un point-base $t_0 \notin \{t_1, \ldots, t_r\}$. Voir [**Ser92**] pour plus de détails.

Théorème 3.5.3. — *Pour tout bouquet* $(\gamma_1, \ldots, \gamma_r)$ *pour* $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$*, il existe un morphisme* $i : \pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}, t_0) \to \pi_1^{\mathrm{alg}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\})_{\overline{k}}$ *ayant les propriétés suivantes :*
(a) *pour tout sous-groupe normal ouvert* $N \subset \pi_1^{\mathrm{alg}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\})_{\overline{k}}$*, le morphisme induit par* i *modulo* N *:* $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}, t_0) \to \pi_1^{\mathrm{alg}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\})_{\overline{k}}/N$ *envoie la classe d'homotopie* $[\gamma_i]$ *sur un générateur distingué d'un groupe d'inertie au-dessus de* t_i *de l'extension galoisienne finie de* $k(T)$ *associée à* N *au-dessus de* t_i*,* $i = 1, \ldots, r$*.*
(b) *le morphisme* i *s'étend*[(18)] *en un isomorphisme entre le complété profini du groupe* $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}, t_0)$ *et le groupe* $\pi_1^{\mathrm{alg}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\})_{\overline{k}}$*.*

Remarque 3.5.4 **(Généralisation en dimension supérieure)**

Plutôt que des revêtement de courbes, on peut considérer des revêtements de variétés de dimension supérieure. Une partie de ce qui précède peut être étendu à ce contexte plus large. Plus précisément, si k un corps et B une variété projective non-singulière définie sur k et géométriquement irréductible

(18) Le morphisme naturel du groupe $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}, t_0)$ dans son complété est injectif (voir [**Ser92**]).

(c'est-à-dire, irréductible après extension des scalaires à $\overline{k}$), on peut s'intéresser aux objets suivants (voir [**DD97**] pour plus de détails) :

Extensions finies séparables $E/k(B)$ et régulières sur k. Le corps des fonctions $k(B)$ remplace le corps $k(T)$. Il y a aussi une notion d'hypersurface ramifiée qui généralise la notion de point de branchement. On définit le diviseur de branchement D comme la somme formelle des hypersurfaces ramifiées.

Représentations du groupe fondamental $\pi_1(B\backslash D)$. La définition de ce groupe fondamental et le dictionnaire "extensions/représentations" sont analogues à ceux vus en dimension 1.

Revêtements algébriques. Un revêtement algébrique de B sur k est un morphisme algébrique $f : X \to B$, fini, génériquement non-ramifié et défini sur k avec X une variété normale et géométriquement irréductible. À ce revêtement $f : X \to B$ est associée l'extension de corps de fonctions $k(X)/k(B)$. C'est une extension finie séparable avec $k(X)/k$ régulière. Le foncteur "corps des fonctions" fournit une équivalence de catégories entre la catégorie des k-revêtements algébriques de B et celle des extensions finies séparables et régulières de $k(B)$. Le foncteur inverse est donné par le procédé de normalisation : étant donné $E/k(B)$ comme ci-dessus, on considère, pour tout ouvert affine $U = \mathrm{Spec}(R)$ de B, la clôture intégrale $\widetilde{R}$ de R in E ; les morphismes associés $\mathrm{Spec}(\widetilde{R}) \to \mathrm{Spec}(R)$ se recollent pour fournir le revêtement f cherché.

En revanche, l'équivalence avec le point de vue topologique ne s'étend pas de façon aussi simple qu'en dimension 1. Il existe cependant des résultats d'équivalence entre les points de vue analytique et algébrique en géométrie, qu'on appelle résultats de type GAGA (voir [**Ser92**, §6] pour une présentation des résultats dans le contexte des revêtements).

CHAPITRE 4

THÉORIE INVERSE DE GALOIS

Dans une première section, nous mettons en place le contexte algébrique dans lequel nous allons traiter le problème. La section 4.2 est consacrée au théorème de rigidité. Ce résultat, qui donne des conditions suffisantes pour qu'un groupe soit groupe de Galois sur $\mathbb{Q}(T)$, a permis des avancées marquantes ces trente dernières années. La section 4.2.3 traite le cas des groupes abéliens. La section 4.3 concerne la descente sur $\mathbb{R}$. Dans la section 4.4, nous nous intéressons à la descente sur le corps des modules : dans quels cas ce corps, le plus petit corps de définition possible, est-il effectivement un corps de définition ?

4.1. Critère de descente du corps de définition

On se donne un corps k arbitraire et une clôture algébrique $\overline{k}$.

4.1.1. Position du problème. — Nous continuons de privilégier le point de vue arithmétique ; les objets au centre de notre étude sont les extensions finies régulières de $k(T)$ (pour un corps k). Comme au chapitre 3, nous disons simplement "extension $E/k(T)$". De façon équivalente, on peut dans ce qui suit voir les objets centraux comme des revêtements $X \to \mathbb{P}^1$ définis sur k.

La question de la descente se pose à la fois pour les simples extensions et pour les G-extensions. Nous allons traiter les deux situations simultanément. Nous utiliserons le mot "(G-)extension" pour désigner soit une simple extension soit une G-extension.

Les (G-)extensions considérées sont *a priori* définies sur une extension galoisienne F de k (par exemple $F = k^{\mathrm{s}} \subset \overline{k}$) et on suppose que leurs invariants sont identiques sur k^{s} et sur $\overline{k}$ (voir remarque 3.1.11).

La proposition 3.1.17 et son corollaire 3.1.18 fournissent des conditions nécessaires pour qu'une (G-)extension soit définie sur k. En particulier, l'ensemble $\mathbf{t} = \{t_1, \dots, t_r\}$ des points de branchement vérifie : $\mathbf{t}^\tau = \mathbf{t}$ pour tout $\tau \in \mathrm{Gal}(F/k)$. Dans la suite, nous supposons donné $\mathbf{t} = \{t_1, \dots, t_r\} \in U_r(k)$.

On sait depuis le chapitre 3 que, pour tout corps $\mathcal{K}$ tel que $K \subset \mathcal{K} \subset K^{\mathrm{s}}$, les simples extensions $E/\mathcal{K}(T)$ de degré d et non ramifiées en dehors de $\mathbf{t}$ correspondent aux représentations transitives $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathcal{K}} \to S_d$ de restriction à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K^{\mathrm{s}}}$ demeurant transitive et que les G-extensions $E/\mathcal{K}(T)$ de groupe de Galois G et non ramifiées en dehors de $\mathbf{t}$ correspondent au épimorphismes continus $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathcal{K}} \to G$ de restriction à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K^{\mathrm{s}}}$ demeurant surjective. Notons

$$\mathcal{R} = \begin{cases} G & \text{pour une G-extension} \\ S_d & \text{pour une simple extension} \end{cases}$$

Dans les deux cas, une (G-)extension $E/\mathcal{K}(T)$ correspond à un homomorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathcal{K}} \to \mathcal{R}$ et deux (G-)extensions sont isomorphes si et seulement si les homomorphismes associés sont conjugués par un élément de $\mathcal{R}$.

Nous verrons toujours $\mathcal{R}$ comme un sous-groupe de S_d où d est le degré de l'extension : dans le cas d'une simple extension, un plongement $\mathcal{R} \hookrightarrow S_d$ est donné par définition ; dans le cas d'une G-extension, on plonge $\mathcal{R} = G$ dans S_d *via* la représentation régulière de G.

Grâce aux correspondances du §3.2.2, on peut poser la question de la descente du corps de définition en termes de prolongement d'homomorphismes.

Théorème 4.1.1. — *Soit $E/F(T)$ une (G-)extension comme ci-dessus, non ramifiée en dehors de $\mathbf{t}$. Elle est définie sur k si et seulement si l'homomorphisme associé $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F \to \mathcal{R}$ se prolonge en un homomorphisme $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_k \to \mathcal{R}$.*

4.1.2. Le critère pour la descente absolue. — On suppose ici que $F = k^{\mathrm{s}}$. D'après le théorème 3.2.1, la suite exacte

$$1 \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}) \to \mathrm{G}_k \to 1$$

est scindée. On note $s : \mathrm{G}_k \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_k$ une section. Le groupe fondamental $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$ est alors isomorphe au produit semi-direct $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \times^s \mathrm{G}_k$. Une condition nécessaire et suffisante pour qu'un homomorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \to \mathcal{R}$ se prolonge au produit semi-direct $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \times^s \mathrm{G}_k$ est que le prolongement sur G_k soit compatible avec l'action de G_k sur $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$ induite par s. Plus précisément, on obtient l'énoncé suivant.

Théorème 4.1.2. — *Soient $E/k^s(T)$ une (G-)extension non ramifiée en dehors de $\mathbf{t}$ et $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to \mathcal{R}$ l'homomorphisme associé. La (G-)extension est définie sur k si et seulement si il existe un homomorphisme $\varphi : \mathrm{G}_k \to \mathcal{R}$ tel que, pour tout $\tau \in \mathrm{G}_k$ et tout $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$, on ait*

$$\phi(x^{s(\tau)}) = \varphi(\tau)\phi(x)\varphi(\tau)^{-1}$$

Supposons maintenant k de caractéristique 0. Fixons un point-base $t_0 \notin \mathbf{t}$ et $(\gamma_1, \ldots, \gamma_r)$ un bouquet pour $\mathbb{P}^1(\mathbb{C}) \setminus \{\mathbf{t}\}$ basé en t_0. Notons x_i la classe d'homotopie de γ_i vue dans $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{k}}$ et posons $\phi(x_i) = g_i$, $i = 1, \ldots, r$ et fixons $\tau \in \mathrm{G}_k$. La condition précédente est équivalente à

$$\phi(x_i^{s(\tau)}) = \varphi(\tau)\, g_i\, \varphi(\tau)^{-1},\ i = 1, \ldots, r$$

Les éléments $x_1^{s(\tau)}, \ldots, x_r^{s(\tau)}$ engendrent le groupe $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{k}}$ et vérifient $x_1^{s(\tau)} \cdots x_r^{s(\tau)} = 1$. Pour un homomorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s} \to \mathcal{R}$ donné *a priori*, on a donc

(*) $\phi(x_1^{s(\tau)}), \ldots, \phi(x_r^{s(\tau)})$ engendrent le groupe $G = \phi(\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{k}})$, et

(**) $\phi(x_1^{s(\tau)}) \cdots \phi(x_r^{s(\tau)}) = 1$

Le théorème 3.5.3 combiné au corollaire 3.1.13 donne un autre renseignement. Notons C_i la classe canonique d'inertie associée à t_i, c'est-à-dire, la classe de conjugaison dans G de g_i, $i = 1, \ldots, r$. On a alors

(***) L'élément $\phi(x_i^{s(\tau)})$, qui est un générateur distingué d'un groupe d'inertie au-dessus de t_i de l'extension conjuguée par τ^{-1} de $E/F(T)$[(1)], est dans la classe $C_j^{\chi(\tau)}$, où $t_j = t_i^{\tau}$ et χ est le caractère cyclotomique modulo $|G|$, $i = 1, \ldots, r$. Si C_i est une classe plongée, l'affirmation reste vraie à la conjugaison près par un élément de $\mathrm{Nor}_{S_d}(G)$.

Remarque 4.1.3. — Si le morphisme $\varphi : \mathrm{G}_k \to \mathcal{R}$ du théorème 4.1.2 existe, il est nécessairement à valeurs dans le normalisateur de G dans $\mathcal{R}$. Dans la suite, nous posons

$$N = \mathrm{Nor}_{\mathcal{R}}(G) = \begin{cases} G & \text{pour une G-extension} \\ \mathrm{Nor}_{S_d}(G) & \text{pour une simple extension} \end{cases}$$

$$C = \mathrm{Cen}_{\mathcal{R}}(G) = \begin{cases} Z(G) & \text{pour une G-extension} \\ \mathrm{Cen}_{S_d}(G) & \text{pour une simple extension} \end{cases}$$

Pour tout $\tau \in \mathrm{G}_k$, la condition du théorème 4.1.2 détermine l'élément $\phi(\tau) \in G$ (quand il existe) à un élément du groupe C près. Si $C = \{1\}$, l'élément $\phi(\tau)$,

(1) D'après la formule du §3.2.2.5.

s'il existe, est unique et l'application correspondante $\tau \to \phi(\tau)$ est automatiquement un morphisme de groupes.

4.2. Rigidité

4.2.1. Le théorème de rigidité. — Le théorème 4.2.2 ci-dessous est un résultat marquant de la théorie. Plusieurs mathématiciens y ont contribué, de façon indépendante, notamment Belyi, Fried, Matzat, Shih, Thompson. Sa conclusion est que, sous certaines hypothèses, un groupe G est groupe de Galois sur $\mathbb{Q}(T)$. Le contexte de cette section est celui des G-extensions.

Plus précisément, on se donne un groupe G et des éléments $g_1, \ldots, g_r$ de G engendrant G et de produit $g_1 \cdots g_r = 1$. Pour $i = 1, \ldots r$, on note C_i la classe de conjugaison de g_i dans G. Une des hypothèses du théorème 4.2.2 est que les classes $C_1, \ldots, C_r$ sont rationnelles.

Définition 4.2.1. — La classe de conjugaison C d'un élément g d'un groupe G est dite rationnelle si $g^a \in C$ pour tout entier a premier à l'ordre de g. (De façon évidente, cette propriété ne dépend pas de l'élément $g \in C$).

Par exemple, toutes les classes de conjugaison du groupe symétrique S_d sont rationnelles.

Considérons l'ensemble

$$\mathrm{sni}(C_1, \ldots, C_r) = \left\{ (g'_1, \ldots, g'_r) \in G \middle| \begin{cases} (i)\ g'_1, \ldots, g'_r \text{ engendrent } G \\ (ii)\ g'_1 \cdots g'_r = 1 \\ (iii)\ g'_i \in C_i, i = 1, \ldots, r \end{cases} \right\}$$

Il y a une action naturelle du groupe G sur l'ensemble $\mathrm{sni}(C_1, \ldots, C_r)$: on fait opérer chaque élément $g \in G$ par conjugaison sur chacune des composantes d'un élément de $\mathrm{sni}(C_1, \ldots, C_r)$.

Théorème 4.2.2. — *Si les trois hypothèses suivantes sont satisfaites,*

(H$_1$) $Z(G) = 1$

(H$_2$) *Les classes $C_1, \ldots, C_r$ sont rationnelles.*

(H$_3$) $\mathrm{sni}(C_1, \ldots, C_r) \neq \emptyset$ *et l'action de G sur cet ensemble est transitive,*

alors pour tout r-uplet $\mathbf{t} = \{t_1, \ldots, t_r\}$ de points dans $\mathbb{P}^1(\mathbb{Q})$, il existe une extension galoisienne régulière $E/\mathbb{Q}(T)$ de groupe G, de points de branchement $t_1, \ldots, t_r$ et d'invariant canonique de l'inertie le r-uplet $(C_1, \ldots, C_r)$.

Démonstration. — Soient $t_0, t_1, \ldots, t_r$ $r+1$ points distincts dans $\mathbb{P}^1(\mathbb{Q})$ et $(\gamma_1, \ldots, \gamma_r)$ un bouquet pour $\mathbb{P}^1(\mathbb{C}) \setminus \{\mathbf{t}\}$ basé en t_0 (où $\mathbf{t} = \{t_1, \ldots, t_r\}$).

Soit $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{\mathbb{Q}}} \to G$ l'homomorphisme qui envoie la classe d'homotopie $x_i = [\gamma_i]$ sur g_i, $i = 1, \ldots, r$. Il résulte des conditions (*), (**) et (***) du §4.1.2 et de l'hypothèse (H_2) que, pour tout $\tau \in G_{\mathbb{Q}}$ le r-uplet $(\phi(x_1^\tau), \ldots, \phi(x_r^\tau))$ est un élément de $\mathrm{sni}(C_1, \ldots, C_r)$. D'après l'hypothèse ($H_3$), il existe ϕ_τ tel que

$$(\phi(x_1^\tau), \ldots, \phi(x_r^\tau)) = \phi_\tau \cdot (g_1, \ldots, g_r) \cdot \phi_\tau^{-1}$$

Posons $\phi(\tau) = \phi_\tau$, $\tau \in G_{\mathbb{Q}}$. La condition du théorème 4.1.2 est satisfaite. De plus, d'après l'hypothèse (H_1) et la remarque 4.1.3, la correspondance $\tau \to \phi_\tau$ est un homomorphisme de groupes. □

Remarque 4.2.3. — L'hypothèse (H_2) est nécessaire : d'après la condition (***), la rationalité de C_i résulte de celle de t_i, $i = 1, \ldots, r$.

Si $k = \mathbb{Q}^{ab}$ on n'a pas besoin de l'hypothèse (H_2).

Théorème 4.2.4. — *Sous les l'hypothèses (H_1) et (H_3), on a la conclusion du théorème 4.2.2 avec $\mathbb{Q}^{ab}$ à la place de $\mathbb{Q}$. C'est-à-dire, pour tout r-uplet $\mathbf{t} = \{t_1, \ldots, t_r\}$ de points dans $\mathbb{P}^1(\mathbb{Q}^{ab})$, il existe une extension galoisienne régulière $E/\mathbb{Q}^{ab}(T)$ de groupe G, de points de ramification $t_1, \ldots, t_r$ et d'invariant canonique de l'inertie le r-uplet $(C_1, \ldots, C_r)$.*

Démonstration. — La démonstration est identique à celle du théorème 4.2.2. Il faut juste remarquer que le caractère cyclotomique est trivial sur G_k pour $k = \mathbb{Q}^{\mathrm{ab}}$. Par conséquent, si $t_1, \ldots, t_r$ sont choisis dans $\mathbb{P}^1(\mathbb{Q}^{ab})$, la condition (***) donne que pour tout $\tau \in G_k$ et $i = 1, \ldots, r$, l'élément $\phi(x_i^{s(\tau)})$ est dans la classe C_i, sans qu'il soit besoin de faire appel à l'hypothèse (H_2). □

Remarque 4.2.5. — L'hypothèse (H_1) n'est en fait pas nécessaire non plus. Elle assure dans la preuve du théorème 4.2.2 que la correspondance $\tau \to \phi_\tau$ est un homomorphisme de groupes. A la place, on peut invoquer la *projectivité* du groupe $G_{\mathbb{Q}^{\mathrm{ab}}}$ dont une conséquence est la suivante. La correspondance $\tau \to \phi_\tau$ peut ne pas être un homomorphisme de groupes, mais on peut changer ϕ_τ en $\phi_\tau \zeta_\tau$ avec $\zeta_\tau \in Z(G)$ de telle sorte que la correspondance $\tau \to \phi_\tau \zeta_\tau$ en soit un.

C'est l'hypothèse (H_3) qu'on appelle plus spécifiquement condition de rigidité. Il s'agit d'une hypothèse assez contraignante et est principalement vérifiée dans la pratique pour $r \leq 3$. Elle est cependant satisfaite par de nombreux groupes simples : beaucoup de résultats obtenus ces trente dernières années sur la réalisation sur $\mathbb{Q}(T)$ de groupes simples l'ont été grâce au théorème 4.2.2 ou ses variantes.

4.2.2. Exemples. —

4.2.2.1. Le groupe symétrique S_n. — On prend $G = S_n$, $r = 3$ et

$$\begin{cases} g_1 & = (n \ \dots \ 1) \\ g_2 & = (1 \ \dots \ n-1) \\ g_3 & = (n \ n-1) \end{cases}$$

Leurs classes de conjugaison sont respectivement la classe C_1 des n-cycles, la classe C_2 des $(n-1)$-cycles et la classe C_3 des 2-cycles. Comme toute classe de conjugaison de S_n, elles sont rationnelles. Si $n > 2$, le groupe S_n est de centre trivial. Il reste à vérifier l'hypothèse (H_3) de rigidité.

Il s'agit de voir que tout triplet $(g_1', g_2', g_3') \in \mathrm{sni}(C_1, C_2, C_3)$ est égal à (g_1, g_2, g_3) modulo l'action de S_d. Par conjugaison par un élément $g \in S_n$, on peut transformer g_1' en g_1. Il existe ensuite une certaine puissance g_1^a du n-cycle $g_1 = (n \ \dots \ 1)$ telle que

$$\begin{cases} (g_1^a g)\, g_1'\, (g_1^a g)^{-1} & = (n \ \dots \ 1) \\ (g_1^a g)\, g_2'\, (g_1^a g)^{-1} & \text{fixe } n \end{cases}$$

Posons $\tilde{g}_i = (g_1^a g)\ g_i'(g_1^a g)^{-1}$, $i = 1, \dots, 3$. Comme n doit être fixé par le produit $\tilde{g}_1\tilde{g}_2\tilde{g}_3 = 1$, on obtient nécessairement $\tilde{g}_3 = (n\ n-1)$ et donc

$$(\tilde{g}_1, \tilde{g}_2, \tilde{g}_3) = (g_1, g_2, g_3)$$

ce qui démontre (H_3). Les hypothèses et la conclusion du théorème 4.2.2 sont vraies pour le groupe symétrique S_n si $n \geq 3$.

4.2.2.2. Le groupe $\mathrm{PSL}_2(\mathbb{F}_p)$. — On prend pour G le groupe $\mathrm{PSL}_2(\mathbb{F}_p)$, c'est-à-dire le groupe $\mathrm{SL}_2(\mathbb{F}_p)$ modulo $\{\pm\mathrm{Id}\}$. Il est de centre trivial. Le cas $p = 2$ pour lequel on a

$$\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = S_3$$

est particulier et peut être traité à part. Nous supposerons $p \neq 2$.

Il y a dans $\mathrm{PSL}_2(\mathbb{F}_p)$ *une classe d'éléments d'ordre* 2*, notée* $2A$ *:* On résout $X^2 = \pm 1$ dans $\mathrm{SL}_2(\mathbb{F}_p)$. L'équation $X^2 = 1$ donne X diagonalisable et donc $X \in \{\pm\mathrm{Id}\}$ et donc triviale dans $\mathrm{PSL}_2(\mathbb{F}_p)$. Toute matrice X telle que $X^2 = -1$ est semblable à la matrice suivante (matrice de l'endomorphisme associé u dans une base $\{u(x), x\}$) :

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Il y a dans $\mathrm{PSL}_2(\mathbb{F}_p)$ *une classe d'éléments d'ordre* 3*, notée* $3A$ *:* On résout $X^3 = 1$ dans $\mathrm{SL}_2(\mathbb{F}_p)$ (le cas $X^3 = -1$ s'y ramène en changeant X en $-X$). Le nombre 1 ne peut être valeur propre de X si $X \neq \mathrm{Id}$ dans $\mathrm{SL}_2(\mathbb{F}_p)$. Le polynôme minimal de X est donc un diviseur de $T^2 + T + 1$. La matrice X est

semblable à la matrice suivante (matrice de l'endomorphisme associé u dans une base $\{x, u(x)\}$) :

$$\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

Il y a dans $\mathrm{PSL}_2(\mathbb{F}_p)$ *deux classes d'éléments d'ordre* p*, notées* pA *et* pB *:* On résout $X^p = 1$ soit $(X-1)^p = 0$ dans $\mathrm{SL}_2(\mathbb{F}_p)$ (le cas $X^p = -1$ s'y ramène en changeant X en $-X$). Les solutions de cette équation sont semblables à :

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \quad (\text{avec } a \in \mathbb{F}_p)$$

Pour $\alpha \in \mathbb{F}_p$, le changement de base $\{e, f\} \to \{\alpha e, f/\alpha\}$ (lequel correspond à un élément dans $\mathrm{SL}_2(\mathbb{F}_p)$) change la matrice en la matrice

$$\begin{bmatrix} 1 & a/\alpha^2 \\ 0 & 1 \end{bmatrix}$$

Les deux classes de similitude pA et pB sont celles des matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ et } \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$$

où u n'est pas un carré dans $\mathbb{F}_p$.

Lemme 4.2.6. — (a) *Le triplet* $(2A, pA, pB)$ *vérifie* (H_3) *si* $\left(\frac{2}{p}\right) = -1$.

(b) *Le triplet* $(3A, pA, pB)$ *vérifie* (H_3) *si* $\left(\frac{3}{p}\right) = -1$.

Démonstration. — (a) On vérifie que le triplet

$$g_1 = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix} \qquad g_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad g_3 = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}$$

est dans l'ensemble $\mathrm{sni}(2A, pA, pB)$. Vérifions l'hypothèse (H_3). Soit $(u, v, w) \in \mathrm{sni}(2A, pA, pB)$. On peut relever u, v, w en des éléments $\tilde{u}, \tilde{v}, \tilde{w} \in \mathrm{SL}_2(\mathbb{F}_p)$ d'ordres respectifs 4, p et p et tels que $\tilde{u}\tilde{v}\tilde{w} = \pm 1$. Soient e et f deux vecteurs propres de $\tilde{v}$ et $\tilde{w}$ respectivement. Ils ne sont pas liés, sinon ils seraient laissés fixes ou changés en leurs opposés par $\tilde{u}$. En prenant pour base le couple $(\alpha e, f/\alpha)$ pour α bien choisi (voir ci-dessus), on se ramène au cas où

$$\tilde{v} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \tilde{w} = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$$

Comme $\tilde{v}\tilde{w}$ est d'ordre 4, on obtient que $\mathrm{Tr}(\tilde{v}\tilde{w}) = 0$[(2)] d'où $\lambda = -2$. On procède de façon analogue pour (b) en utilisant les matrices :

$$g_1 = \begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \qquad g_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad g_3 = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}$$

□

Les classes $2A$, $3A$ sont rationnelles mais pas les classes pA et pB : l'élévation à une puissance première à p laisse invariant l'ensemble $\{pA, pB\}$ mais peut permuter les deux classes. On doit raffiner un peu le théorème 4.2.2.

Soit H le sous-groupe des éléments $\tau \in \mathrm{G}_{\mathbb{Q}}$ tels que $\zeta^{\tau} = \zeta^{a}$ avec a carré dans $\mathbb{F}_p$, c'est-à-dire, tels que $\chi(\tau)$ modulo p est un carré dans $\mathbb{F}_p$. C'est un sous-groupe d'indice 2 de $\mathrm{G}_{\mathbb{Q}}$. Notons $\mathbb{Q}(\sqrt{D})$ ($D \in \mathbb{Z}$) le sous-corps laissé fixe par H. Considérons un triplet (t_1, t_2, t_3) de points distincts de $\mathbb{P}^1(\overline{\mathbb{Q}})$ vérifiant

$$\begin{cases} t_1 \in \mathbb{P}^1(\mathbb{Q}) \\ t_2 \text{ et } t_3 \text{ sont conjugués dans } \mathbb{Q}(\sqrt{D}) \end{cases}$$

Montrons comme dans la preuve du théorème 4.2.2 que l'homomorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{\mathbb{Q}}} \to G$ (où $G = \mathrm{PSL}_2(\mathbb{F}_p)$) envoyant x_i sur g_i, $i = 1, 2, 3$ (où g_1, g_2, g_3) sont les éléments donnés dans la preuve du lemme 4.2.6 ((a) ou (b))) se prolonge à $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})$. La seule différence est dans la vérification du fait que pour tout $\tau \in \mathrm{G}_{\mathbb{Q}}$, $\phi(x_i^{s(\tau)})$ est conjugué à g_i, $i = 2, 3$.

Soit $\tau \in \mathrm{G}_{\mathbb{Q}}$. Si τ fixe $\mathbb{Q}(\sqrt{D})$ c'est-à-dire $\tau \in H$, alors $t_i^{\tau} = t_i$, $i = 2, 3$, $(pA)^{\chi(\tau)} = pA$ et $(pB)^{\chi(\tau)} = pB$. La propriété (***) des $\phi(x_i^{s(\tau)})$ donne la conclusion désirée. Si τ ne fixe pas $\mathbb{Q}(\sqrt{D})$, c'est-à-dire $\tau \notin H$, alors $t_1^{\tau} = t_2$ et $(pA)^{\chi(\tau)} = pB$. La propriété (***) donne encore la conclusion désirée.

On obtient en définitive que pour tout triplet ordonné (t_1, t_2, t_3) choisi comme ci-dessus, il existe une extension galoisienne régulière $E/\mathbb{Q}(T)$ de groupe $\mathrm{PSL}_2(\mathbb{F}_p)$, de points de branchement t_1, t_2, t_3 dans les cas suivants :

$$\left(\frac{2}{p}\right) = -1 \text{ ou } \left(\frac{3}{p}\right) = -1$$

Ces résultats ont été établis par Shih par une méthode un peu différente. Le résultat est vrai également pour les premiers p tels que $\left(\frac{7}{p}\right) = -1$ ou $\left(\frac{5}{p}\right) = -1$. La plupart des autres cas restent ouverts.

(2) en notant que $\mathrm{Tr}(\tilde{v}\tilde{w})$ est la somme de deux racines de 1 d'ordre 4 de produit égal à 1.

4.2.2.3. Le Monstre. — On peut montrer de façon générale que le nombre d'orbites de l'action de G sur l'ensemble $\mathrm{sni}(C_1, \ldots, C_r)$ s'écrit en fonction des ordres et des valeurs des caractères du groupe sur les classes de conjugaison $C_1, \ldots, C_r$. La condition de rigidité (H_3) peut donc se vérifier à partir de la table de caractères du groupe.

En utilisant cette méthode (et la classification des groupes simples), on a pu trouver un triplet de classes de conjugaison vérifiant la propriété de rigidité (H_3) pour le groupe de Fisher-Griess M et le réaliser ainsi sur $\mathbb{Q}(T)$.

Le groupe de Fisher-Griess M, connu comme le "Monstre", est le plus grand des groupes sporadiques simples. Il est d'ordre

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

4.2.3. Les groupes abéliens. — Nous donnons une seconde méthode pour réaliser les groupes abéliens comme groupes de Galois sur $\mathbb{Q}(T)$ de façon régulière (la première est donnée au §2.3.4). La méthode, qui suit la méthode de la rigidité et donc repose sur le théorème d'existence de Riemann, ne s'étend pas en caractéristique positive, contrairement à la première méthode pour laquelle le corps de base est quelconque. On obtient l'énoncé suivant, qui est la version en caractéristique 0 du théorème 2.3.7.

Théorème 4.2.7. — *Soit k un corps de caractéristique 0 et $D \subset \mathbb{P}^1(\overline{k})$ un ensemble fini. Pour tout groupe abélien fini G, il existe une extension galoisienne $E/k(T)$ de groupe G, régulière sur k et non ramifiée au-dessus de chaque point de D.*

Démonstration. — Observons d'abord que comme k est infini, il sera facile de satisfaire la condition de ramification "$E/k(T)$ non ramifiée au-dessus de chaque point de D" une fois construite $E/k(T)$ vérifiant le reste : on peut en effet toujours garantir en composant avec une homographie χ à coefficients dans k que les points de branchement sont en dehors d'un ensemble fini donné.

On peut également supposer que $k = \mathbb{Q}$ (ce cas implique les autres) et on sait qu'on peut restreindre le problème au cas des groupes cycliques.

Fixons un entier $n \geq 1$ et prenons $G = \mathbb{Z}/n\mathbb{Z}$. On se donne *a priori* $r+1$ points distincts $t_0, t_1, \ldots, t_r$ dans $\mathbb{P}^1(\mathbb{Q})$, un bouquet $(\gamma_1, \ldots, \gamma_r)$ pour $\mathbb{P}^1(\mathbb{C}) \setminus \{\mathbf{t}\}$ basé en t_0 (où $\mathbf{t} = \{t_1, \ldots, t_r\}$), un système générateur $\{g_1, \ldots, g_r\}$ de G tel que $g_1 \cdots g_r = 1$ et on considère l'homomorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{\mathbb{Q}}} \to G$ qui envoie la classe d'homotopie $x_i = [\gamma_i]$ sur g_i, $i = 1, \ldots, r$.

L'abélianité de G fait que la condition (***) donne ici que, si $t_i^\tau = t_j$, $\phi(x_i^{s(\tau)})$ est non seulement conjugué mais égal à $\chi(\tau)g_j$ [(3)]. La stratégie consiste à choisir les paramètres $t_1, \ldots, t_r$ et $g_1, \ldots, g_r$ de telle sorte que, pour tout $\tau \in \mathrm{G}_{\mathbb{Q}}$,

$$\{(t_1^{(\tau^{-1})}, \chi(\tau)g_1), \ldots, (t_r^{(\tau^{-1})}, \chi(\tau)g_r)\} = \{(t_1, g_1), \ldots, (t_r, g_r)\}$$

Supposons cela réalisé. On a alors $\phi(x_i^{s(\tau)})$ égal à $\phi(x_i)$, $i = 1, \ldots, r$, et donc $\phi(x^{s(\tau)})$ égal à $\phi(x)$, pour tout $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{\mathbb{Q}}}$ et tout $\tau \in \mathrm{G}_{\mathbb{Q}}$. La condition de descente à $\mathbb{Q}$ du théorème 4.1.2 est satisfaite pour $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ le morphisme constant égal à 1. La proposition 3.2.3 indique d'autre part que la fibre du revêtement au-dessus du point t_0 est constituée de points $\mathbb{Q}$-rationnels.

Pour réaliser la condition ci-dessus, pour $n > 2$, on fixe une numérotation $g_1, \ldots, g_r$ du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$, une racine primitive de l'unité ζ d'ordre n, et on pose $t_i = \zeta^{g_i^{-1}}$, $i = 1, \ldots, r$. Pour $n = 2$, on prend $g_1 = g_2 = 1$ et on choisit deux points distincts t_1 et t_2 dans $\mathbb{P}^1(\mathbb{Q})$. Dans les deux cas, la vérification de la condition est immédiate. □

4.3. Descente sur $\mathbb{R}$

La descente de $\mathbb{C}$ à $\mathbb{R}$ du corps de définition des revêtements est un problème classique. Voir notamment [**Hur91**], [**KN71**] et [**FD90**].

4.3.1. La situation sur $\mathbb{R}$. — Le cas $k = \mathbb{R}$ est particulier. Le groupe $\mathrm{G}_{\mathbb{R}}$ est le groupe à deux éléments engendré par la conjugaison complexe c. De plus, l'action de c sur le groupe fondamental algébrique provient de l'action continue de c sur le groupe fondamental topologique.

De façon plus précise, fixons un ensemble $\mathbf{t} \in U_r(\mathbb{R})$: cet ensemble est constitué de r_1 points réels $t_1, \ldots, t_{r_1}$ et de r_2 paires $\{z_i, z_i^c\}$ de points complexes conjugués, $i = 1, \ldots, r_2$. Fixons un point $t_0 \in \mathbb{P}^1(\mathbb{R}) \setminus \mathbf{t}$. Si $f : X \to \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ est un revêtement topologique et $T : \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0) \to \mathrm{Per}(f^{-1}(t_0))$ sa représentation de monodromie, la monodromie du revêtement conjugué $f^c : X^c \to \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$, défini par $f^c(x^c) = f(x)^c$ $(x \in X)$, est représentée par le morphisme $T^c : \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0) \to \mathrm{Per}((f^c)^{-1}(t_0))$ donné par

$$T^c([\gamma]) = c \circ T([\gamma^c]) \circ c \quad ([\gamma] \in \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0))$$

Supposons désormais que le revêtement topologique provienne d'un revêtement algébrique $f : X \to \mathbb{P}^1$, non ramifié en dehors de $\mathbf{t}$. Si $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}} \to S_d$

(3) Noter la notation additive dans le groupe abélien $\mathbb{Z}/n\mathbb{Z}$.

est la représentation associée, alors le revêtement algébrique conjugué f^c est représenté par $\phi^c : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}} \to S_d$ donné par

$$\phi^c(x) = \phi(x^{s_{t_0}(c)}) \quad (x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}})$$

(où $s_{t_0} : \mathrm{G}_{\mathbb{R}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{R}}$ est la section introduite au §3.2.1). On sait aussi qu'une classe homotopie $[\gamma]$ agissant par monodromie correspond à l'élément $[\gamma] \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}}$ agissant par prolongement analytique (moyennant le plongement des corps de fonctions dans $\mathbb{C}((T - t_0))$). Les deux formules ci-dessus étant cohérentes au sein de la famille des revêtements algébriques de $\mathbb{P}^1$ non ramifiés en dehors de $\mathbf{t}$, on peut conclure que

(*) l'action de c sur les classes d'homotopie peut-être identifiée à la conjugaison par $s_{t_0}(c)$: pour $[\gamma] \in \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$, on a $[\gamma^c] = [\gamma]^{s_{t_0}(c)}$ dans $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}}$.

En particulier l'isomorphisme $\widehat{\pi}_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0) \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}}$ entre le complété profini du groupe fondamental topologique et le groupe fondamental algébrique sur $\mathbb{C}$ (théorème 3.5.3) s'étend en un isomorphisme $\widehat{\pi}_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0) \times^s \{1, c\} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{R}}$. Dans la suite on note $s_{t_0}(c) = c$ quand il n'y a pas d'ambiguïté.

4.3.2. Formules de Hurwitz. —

***Théorème 4.3.1* (formules de Hurwitz).** — *Etant donné $\mathbf{t} \in U_r(\mathbb{R})$ avec r_1 et r_2 comme ci-dessus, on peut choisir $t_0 \in \mathbb{P}^1(\mathbb{R}) \setminus \mathbf{t}$ et trouver un bouquet $x_1, \ldots, x_r$ de $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \mathbf{t}, t_0)$ tels que l'action de la conjugaison complexe c soit donnée par les formules suivantes :*

$$\begin{cases} (cx_1 \cdots x_i)^2 = 1, \ i = 1, \ldots, r_1 \\ x_{r+1-i} = c(x_{r_1+i})^{-1}c, \ i = 1, \ldots, r_2 \end{cases}$$

dans $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t_0)_{\mathbb{R}}$, ou dans $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \mathbf{t}, t_0) \times^s \{1, c\}$.

Démonstration. — L'idée générale est que ces formules sont topologiques et que l'action de la conjugaison complexe sur les chemins fermés basés en t_0 peut être explicitée. Nous donnons ci-dessous une construction naturelle qui conduit aux formules de l'énoncé. Il n'y a pas de difficulté majeure, si ce n'est la technicité de la présentation. Pour simplifier, nous nous limitons au cas où $t_1, \ldots, t_r \in \mathbb{R}$ et disons comment traiter le cas général en fin de preuve. On suppose $t_1 < t_2 < \cdots < t_{r-1} < t_r$ et on choisit $t_0 > t_r$ (plus exactement on doit dire que $t_1, \ldots, t_r, t_0$ sont dans cet ordre sur la droite projective réelle).

Pour tout $i = 1, \ldots, r$, on choisit $a_i \in]t_i, t_{i+1}[$ si $i \neq r$, $a_r = a_0 = t_0$ et on note u_i le chemin de $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ composé d'un segment joignant $(a_i, 0)$ à $(a_i, 1)$ puis d'un segment joignant $(a_i, 1)$ à $(a_{i-1}, 1)$ et d'un segment joignant $(a_{i-1}, 1)$

à $(a_{i-1}, 0)$. On définit ensuite le chemin fermé rectangulaire $\rho_i = u_i\ (u_i^c)^{-1}$, $i = 1, \ldots, r$, où, d'une manière générale, on désigne par γ^{-1} le chemin inverse d'un chemin γ. On définit enfin r chemins fermés $\gamma_1, \ldots, \gamma_r$ de $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ basés en t_0 par les formules suivantes :

$$\begin{cases} \gamma_r & = \rho_r \\ \gamma_{r-1} & = u_r \rho_{r-1} (u_r)^{-1} \\ \gamma_{r-2} & = u_r u_{r-1} \rho_{r-2} (u_r u_{r-1})^{-1} \\ & \vdots \\ \gamma_2 & = (u_r \cdots u_3) \rho_2 (u_r \cdots u_3)^{-1} \\ \gamma_1 & = (u_r \cdots u_2) \rho_1 (u_r \cdots u_2)^{-1} \end{cases}$$

Les classes d'homotopie $[\gamma_1], \ldots, [\gamma_r]$ sont des générateurs du groupe $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$ modulo l'unique relation $[\gamma_1] \cdots [\gamma_r] = 1$.

Les classes d'homotopie des chemins $\gamma_1^c, \gamma_2^c, \ldots, \gamma_{r-1}^c, \gamma_r^c$ sont données par les formules suivantes :

$$\begin{cases} [\gamma_r^c] & = [\gamma_r]^{-1} \\ [\gamma_{r-1}^c] & = [\gamma_r]^{-1} [\gamma_{r-1}]^{-1} [\gamma_r] \\ [\gamma_{r-2}^c] & = [\gamma_{r-1}\gamma_r]^{-1} [\gamma_{r-2}]^{-1} [\gamma_{r-1}\gamma_r]. \\ & \vdots \\ [\gamma_2^c] & = [\gamma_3 \cdots \gamma_r]^{-1} [\gamma_2]^{-1} [\gamma_3 \cdots \gamma_r] \\ [\gamma_1^c] & = [\gamma_2 \cdots \gamma_r]^{-1} [\gamma_1]^{-1} [\gamma_2 \cdots \gamma_r] \end{cases}$$

En effet, la définition de ρ_i donne $[\rho_i^c] = [\rho_i]^{-1}$, $i = 1, \ldots, r$. Pour $i = r$, on obtient la première formule $[\gamma_r^c] = [\gamma_r]^{-1}$. Pour la deuxième, on écrit

$$\begin{aligned} \gamma_{r-1}^c & = u_r^c \rho_{r-1}^c (u_r^c)^{-1} \\ & = (u_r^c (u_r)^{-1})\ (u_r \rho_{r-1}^{-1} (u_r)^{-1})\ (u_r (u_r^c)^{-1}) \\ & = \rho_r\ \gamma_{r-1}^{-1}\ \rho_r^{-1} \\ & = \gamma_r\ \gamma_{r-1}^{-1}\ \gamma_r^{-1} \end{aligned}$$

Passons au cas général ; soit $i < r$ un indice quelconque.

$$\begin{aligned} \gamma_i^c & = (u_r \cdots u_{i+1})^c\ \rho_i^c\ ((u_r \cdots u_{i+1})^c)^{-1} \\ & = (u_r \cdots u_{i+1})^c (u_r \cdots u_{i+1})^{-1}\ (u_r \cdots u_{i+1}) \rho_i^{-1} (u_r \cdots u_{i+1})^{-1}\ (u_r \cdots u_{i+1})\, ((u_r \cdots u_{i+1})^c)^{-1} \\ & = (u_r \cdots u_{i+1})^c (u_r \cdots u_{i+1})^{-1}\ \gamma_i^{-1}\ (u_r \cdots u_{i+1})\, ((u_r \cdots u_{i+1})^c)^{-1} \end{aligned}$$

Mais on a $\left[(u_r \cdots u_{i+1})\, ((u_r \cdots u_{i+1})^c)^{-1}\right] = [\gamma_{i+1} \cdots \gamma_r]$ d'où la formule

$$[\gamma_i^c] = [\gamma_{i+1} \cdots \gamma_r]^{-1} [\gamma_i]^{-1} [\gamma_{i+1} \cdots \gamma_r]$$

On déduit ensuite que, pour tout $i = 1, \ldots, r$, on a

$$[\gamma_i^c \gamma_{i+1}^c \cdots \gamma_r^c] = [\gamma_i \cdots \gamma_r]^{-1}$$

ce qui, pour $x_i = [\gamma_i]$, $i = 1, \ldots, r$, correspond aux formules de l'énoncé. La formule précédente se démontre par récurrence descendante. C'est clair pour $i = r$. Si elle est vraie pour $i + 1$, alors on a

$$\begin{aligned}[\gamma_i^c \gamma_{i+1}^c \cdots \gamma_r^c] &= [\gamma_i^c]\ [\gamma_{i+1} \cdots \gamma_r]^{-1} \\ &= [\gamma_{i+1} \cdots \gamma_r]^{-1}\ [\gamma_i]^{-1}\ [\gamma_{i+1} \cdots \gamma_r]\ [\gamma_{i+1} \cdots \gamma_r]^{-1} \\ &= [\gamma_i \cdots \gamma_r]^{-1}\end{aligned}$$

Dans le cas général, les points de branchement sont constitués de r_1 points réels et r_2 paires de points complexes conjugués. On construit les chemins associés $\gamma_1, \ldots, \gamma_r$ de la façon suivante. Pour les points réels, on construit les chemins comme ci-dessus. Pour chaque paire (z_i, z_i^c) où z_i est celui des deux points dans le demi-plan supérieur, on construit un chemin γ_i tournant une fois autour de z_i dans le sens trigonométrique et on prend le chemin $(\gamma^c)^{-1}$ comme chemin associé au point z_i^c. On peut faire cela en sorte que les conditions techniques du théorème 3.4.1 soient satisfaites et donc que les classes d'homotopie correspondantes $[\gamma_1], \ldots, [\gamma_r]$ engendrent le groupe $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t})$ avec l'unique relation $[\gamma_1], \ldots, [\gamma_r] = 1$. On vérifie ensuite que l'action de la conjugaison complexe sur $\gamma_1, \ldots, \gamma_r$ correspond aux formules annoncées. □

4.3.3. Solution du problème inverse de Galois sur $\mathbb{R}(T)$. — Dans ce paragraphe, nous démontrons le résultat suivant.

Théorème 4.3.2. — *Tout groupe fini G est groupe de Galois d'une extension galoisienne régulière de $\mathbb{R}(T)$.*

Démonstration. — Les notations étant celles du §4.3.2, on se place dans la situation où aucun point de ramification n'est réel, c'est-à-dire $r_1 = 0$. Le groupe G étant fixé, on fixe r_2 éléments $g_1, \ldots, g_{r_2}$ engendrant G. On pose $r = 2r_2$ et on fixe r_2 paires $\{z_i, z_i^c\}$ de complexes conjugués. On note $\mathbf{t} = (t_1, \ldots, t_r)$ le r-uplet $(z_1, \ldots, z_{r_2}, z_{r_2}^c, \ldots, z_1^c)$ et $C_1, \ldots, C_r$ les classes de conjugaison respectives des éléments

$$g_{r_2}^{-1}, \ldots, g_1^{-1}, g_1, \ldots, g_{r_2}$$

Considérons alors l'épimorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}} \to G$ qui envoie les générateurs $x_1, \ldots, x_{r_2}, x_{r_2+1}, \ldots, x_r$ respectivement sur les éléments précédents, c'est-à-dire

$$\begin{cases} \phi(x_i) = g_{r_2+1-i}^{-1}, & i = 1, \ldots, r_2 \\ \phi(x_i) = g_{i-r_2}, & i = r_2 + 1, \ldots, r \end{cases}$$

En utilisant les formules de Hurwitz, on obtient, pour $i = 1, \ldots, r_2$,

$$\begin{aligned} \phi(x_i^c) &= \phi(x_{r+1-i}^{-1}) \\ &= g_{(r+1-i)-r_2}^{-1} \\ &= g_{r_2+1-i}^{-1} \\ &= \phi(x_i) \end{aligned}$$

Le calcul est analogue pour $i = r_2+1, \ldots, r$. La condition du théorème 4.1.2 est donc satisfaite pour l'homomorphisme $\varphi : \mathrm{G}_{\mathbb{R}} \to G$ égal à l'homomorphisme trivial ; le G-revêtement associé à l'épimorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{C}} \to G$ est défini sur $\mathbb{R}$. En particulier, le groupe G est groupe de Galois d'une extension galoisienne régulière de $\mathbb{R}(T)$. La proposition 3.2.3 indique d'autre part que la fibre du revêtement au-dessus du point t_0 est constituée de points réels. □

4.3.4. Revêtements à points de ramification réels. — L'objet de ce paragraphe est de démontrer le résultat suivant.

Théorème 4.3.3. — *Un groupe fini G est groupe de Galois d'une extension galoisienne régulière de $\mathbb{R}(T)$ avec points de ramification réels si et seulement si G peut être engendré par r éléments d'ordre ≤ 2.*

Démonstration. — On est cette fois dans la situation où il n'y a que des points de ramification réels, c'est-à-dire $r = r_1$. L'existence d'une extension galoisienne régulière de $\mathbb{R}(T)$ non ramifiée en dehors d'un sous-ensemble $\mathbf{t} = \{t_1, \ldots, t_r\} \subset U_r(\mathbb{R})$ équivaut, une fois fixé $t_0 \in \mathbb{P}^1(\mathbb{R}) \setminus \mathbf{t}$, à celle d'un épimorphisme $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\mathbb{R}} \to G$. Notons $x_1, \ldots, x_r$ un bouquet comme dans le théorème 4.3.1 et notons $g_i = \phi(x_i), i = 1, \ldots r$ et $g_0 = \phi(c)$. En utilisant les formules de Hurwitz, on obtient,

$$(g_0 g_1 \cdots g_i)^2 = 1, \quad i = 0, 1, \ldots, r-1$$

Les éléments $g_0 g_1 \cdots g_i$, $i = 0, 1, \ldots, r-1$ sont les r générateurs de G d'ordre ≤ 2 de l'énoncé. □

Le théorème 4.3.3 fournit une condition nécessaire pour qu'un groupe G puisse être réalisé comme groupe de Galois sur $\mathbb{Q}(T)$ avec points de ramification réels, et en particulier, pour que le théorème 4.2.2 de rigidité puisse être appliqué : le groupe G doit pouvoir être engendré par des involutions. D'après une conséquence classique du théorème de Feit-Thompson, c'est le cas de tous les groupes simples non abéliens.

4.4. Corps des modules et corps de définition

Comme au §3.1.4.3, fixons une extension galoisienne F/k et une (G-)extension $E/F(T)$. Considérons le sous-groupe $M(E)$ (resp. $M_G(E)$) de $\mathrm{Gal}(F/k)$ de tous les éléments τ tels que les simples extensions (resp. les G-extensions) $E/k(T)$ et $E^\tau/k(T)$[(4)] soient isomorphes. Pour traiter simultanément les deux situations nous notons $M_{(G)}(E)$ pour $M(E)$ ou $M_G(E)$ suivant que $E/F(T)$ est une simple extension ou une G-extension. Comme dans la proposition 3.1.17, on dit du sous-corps $F^{M_{(G)}(E)} \subset F$ fixé par $M_{(G)}(E)$ que c'est le corps des modules de la (G-)extension $E/F(T)$ relativement à l'extension F/k.

Proposition 4.4.1. — *Le corps des modules est une extension finie de k contenue dans tout corps de définition de $E/F(T)$ contenant k.*

Ainsi le corps des modules est le plus petit corps de définition si c'est un corps de définition, mais ce n'est pas nécessairement le cas en général.

Démonstration. — Si $\mathcal{K}$ est un corps de définition, on a $\mathrm{Gal}(F/\mathcal{K}) \subset M_{(G)}(E)$ (proposition 3.1.17), d'où la seconde partie de l'affirmation. Notons $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F \to \mathcal{R}$ la représentation associée à la (G-)extension considérée $E/F(T)$ où $\mathcal{R}$ est soit le groupe S_d ($d = [E : F(T)]$) soit le groupe G de l'extension suivant que $E/F(T)$ est une simple extension ou une G-extension (notation introduite au §4.1). Le groupe $N = \mathrm{Nor}_{\mathcal{R}}(G)$ agit par conjugaison sur l'ensemble G^r (composante par composante) ; soit $(G^r)^{\mathrm{inn}}$ le quotient de G^r par cette action. Pour $(x_1, \ldots, x_r)$ un bouquet pour $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ (basé en un point $t_0 \in \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$), considérons l'application

$$\begin{cases} \mathrm{Gal}(F/k) & \to & (G^r)^{\mathrm{inn}} \\ \tau & \to & (\phi(x_1), \ldots, \phi(x_r)) \end{cases}$$

L'ensemble quotient $\mathrm{Gal}(F/k)/M_{(G)}(E)$ est en bijection avec l'image de cette application. D'autre part, le cardinal de cet ensemble quotient est supérieur ou égal au degré sur k du corps des modules. □

Remarque 4.4.2. — (a) On utilise ci-dessus que, si k_m désigne le corps des modules, on a $M_{(G)}(E) \subset \mathrm{Gal}(F/k_m)$ et donc $\mathrm{Gal}(F/k)/M_{(G)}(E)$ est de cardinal $\geq [k_m : k]$. On a en fait égalité car le sous-groupe $M = M_{(G)}(E)$ est un sous-groupe fermé de $\mathrm{Gal}(F/k)$ pour la topologie de Krull, c'est-à-dire $M_{(G)}(E) = \mathrm{Gal}(F/k_m)$ ($\mathrm{Gal}(F/k_m)$ est *a priori* l'adhérence de $M_{(G)}(E)$). Pour voir l'inclusion non banale $M \supset \mathrm{Gal}(F/k_m)$, considérons $\sigma \in \mathrm{Gal}(F/k_m)$. Soit

(4) L'extension $E^\tau/k(T)$ dépend du choix d'un prolongement $\tilde{\tau}$ de τ mais la condition elle-même ne dépend que de τ.

F_0/k une sous-extension galoisienne finie de F/k telle que la (G-)extension $E/F(T)$ soit définie sur F_0. Le groupe de Galois $\mathrm{Gal}(F/F_0)$ est un sous-groupe normal d'indice fini de $\mathrm{Gal}(F/k)$. Donc $\sigma \cdot \mathrm{Gal}(F/F_0)$ est un voisinage ouvert de σ, ce qui donne $\sigma \cdot \mathrm{Gal}(F/F_0) \cap M \neq \emptyset$. Ainsi il existe $\widetilde{\sigma} \in M$ tel que $\sigma^{-1}\widetilde{\sigma} \in \mathrm{Gal}(F/F_0)$. Comme $E/F(T)$ est défini sur F_0 et que $\widetilde{\sigma} \in M$, les (G-)extensions $E^{\sigma}/F(T)$ et $E^{\widetilde{\sigma}}/F(T)$ sont isomorphes, à la (G)-extension $E/F(T)$. D'où $\sigma \in M$.

(b) La propriété suivante est également souvent utilisée. Si k_m est le corps des modules d'une (G-)extension $E/F(T)$ relativement à l'extension F/k et si k' est un corps intermédiaire entre k et F, alors le corps des modules de la (G-)extension $E/F(T)$ relativement à l'extension F/k' est le corps $k'k^m$. Il suffit de voir que le corps des modules cherché est le sous-corps de F fixé par $M_{(G)}(E) \cap \mathrm{Gal}(F/k')$ et que ce groupe est égal à $\mathrm{Gal}(F/k_m k')$.

Grâce au dictionnaire entre extensions de $k(T)$ et représentations du groupe fondamental fourni au §3.2.2, on obtient les caractérisations suivantes qui prolongent le théorème 4.1.2.

Proposition 4.4.3. — *Soit $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F \to \mathcal{R}$ la représentation associée à une (G-)extension $E/F(T)$.*

(a) *Un élément $\tau \in \mathrm{Gal}(F/k)$ appartient au sous-groupe $M_{(G)}(E)$ si et seulement, pour un prolongement $\tilde{\tau} \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F$ de τ[5], il existe φ_τ dans le groupe $N = \mathrm{Nor}_{\mathcal{R}}(G)$ tel que*

$$(*) \qquad \phi(x^{\tilde{\tau}}) = \varphi_\tau \, \phi(x) \, \varphi_\tau^{-1} \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F$$

Si $F = k^s$ (descente absolue) et $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$ est un point fixé, on a :

(b) *Un élément $\tau \in \mathrm{G}_k$ appartient au sous-groupe $M_{(G)}(E)$ si et seulement s'il existe $\varphi_\tau \in N = \mathrm{Nor}_{\mathcal{R}}(G)$ tel que*

$$(**) \qquad \phi(x^{s_{t_0}(\tau)}) = \varphi_\tau \, \phi(x) \, \varphi_\tau^{-1} \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^s}$$

(c) *Un corps $k \subset \mathcal{K} \subset F$ est un corps de définition de la (G-)extension $E/k^s(T)$ si et seulement si on peut trouver une famille $(\varphi_\tau)_{\tau \in \mathrm{G}_k}$ d'éléments $\varphi_\tau \in N$ satisfaisant (**) ci-dessus et telle que la correspondance $\tau \to \varphi_\tau$ soit un homomorphisme de groupes.*

En général, pour tous $\tau_1, \tau_2 \in \mathrm{G}_k$, l'expression

$$(\varphi_{\tau_1\tau_2})^{-1}\varphi_{\tau_1}\varphi_{\tau_2}$$

[5] Il est équivalent de dire "pour tout prolongement $\tilde{\tau} \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_F$ de τ".

appartient au groupe $C = \mathrm{Cen}_N(G)$. On obtient en particulier que si $C = \{1\}$, c'est-à-dire, $\mathrm{Cen}_{S_d}(G) = \{1\}$ pour une simple extension et $Z(G) = \{1\}$ pour une G-extension, le corps des modules est un corps de définition. Nous allons affiner ce critère dans la sous-section suivante.

4.4.1. Critère de descente sur le corps des modules. — Soient $E/k^{\mathrm{s}}(T)$ une (G-)extension, $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}} \to \mathcal{R}$ la représentation associée et $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$.

On suppose que k est le corps des modules, c'est-à-dire $\mathrm{G}_k = M_{(G)}(E)$. On conserve les notations du §4.4. Considérons l'application

$$\overline{\varphi} : \begin{cases} \mathrm{G}_k & \to & N/C \\ \tau & \to & \overline{\varphi}_\tau \end{cases}$$

qui envoie chaque élément $\tau \in \mathrm{G}_k$ sur la classe modulo C d'un élément $\varphi_\tau \in N$ vérifiant la condition (**) de la proposition 4.4.3. C'est un homomorphisme de groupes qui ne dépend pas du choix des éléments $\varphi_\tau \in N$ vérifiant (**). L'énoncé suivant est une reformulation du (c) de la proposition 4.4.3.

Proposition 4.4.4. — *Le corps des modules k est un corps de définition de la (G-)extension $E/k^s(T)$ si et seulement si le morphisme $\overline{\varphi} : \mathrm{G}_k \to N/C$ peut être relevé en un morphisme $\varphi : \mathrm{G}_k \to N$.*

Le relèvement est possible en particulier quand la suite exacte

$$1 \to C \to N \to N/C \to 1$$

est scindée. Cette condition est satisfaite dans chacun des cas suivants :

(*pour une simple extension*) :
- $\mathrm{Cen}_{S_d}(G) = \{1\}$ c'est-à-dire, la simple extension $E/k^{\mathrm{s}}(T)$ n'a pas d'automorphismes,
- l'extension $E/k^{\mathrm{s}}(T)$ est galoisienne,

[Dans ce cas, le plongement $\gamma : G \hookrightarrow S_d$ est la représentation régulière de G à gauche (c'est-à-dire $\gamma(g)(x) = g.x$ $(g, x \in G)$). Si on identifie G et $\gamma(G)$, le groupe $\mathrm{Nor}_{S_d}(G)$ est alors le produit semi-direct $C \times^s \mathrm{Aut}(G)$ de $\mathrm{Cen}_{S_d}G$ et de $\mathrm{Aut}(G)$. En effet, le groupe $\mathrm{Cen}_{S_d}(G)$ est l'image de la représentation régulière $\delta : G \hookrightarrow S_d$ de G à droite (c'est-à-dire $\delta(g)(x) = x.g$ $(g, x \in G)$). Pour chaque $\sigma \in S_d$, il existe un unique $c_\sigma \in \mathrm{Cen}_{S_d}(G)$ tel que $c_\sigma\sigma(1) = 1$. On

vérifie alors que $\sigma \in \mathrm{Nor}_{S_d}(G)$ si et seulement si $c_\sigma \sigma \in \mathrm{Aut}(G)$[(6)]. L'argument se conclut alors aisément.]

(*pour une G-extension*) :
- $Z(G) = \{1\}$.
- $Z(G) = G$ c'est-à-dire G est abélien.

De façon générale, l'existence d'un relèvement au morphisme $\overline{\varphi} : \mathrm{G}_k \to N/C$ est un problème cohomologique. Nous renvoyons à [**DD97**] pour une telle approche.

Remarque 4.4.5. — (a) Le résultat ci-dessus selon lequel le corps des modules d'une extension galoisienne $E/k^{\mathrm{s}}(T)$ est un corps de définition (comme simple extension) est connu sous le nom de théorème de Coombes et Harbater ; il est démontré dans [**CH85**]. La preuve se reinterprète de la façon suivante.

Partant d'une famille $(\varphi_\tau)_{\tau \in \mathrm{G}_k}$ d'éléments $\varphi_\tau \in \mathrm{Nor}_{S_d}(G)$ satisfaisant la condition (**) de la proposition 4.4.3, on peut, quitte à multiplier chaque φ_τ par un élément de $\mathrm{Cen}_{S_d}(G)$ (qui agit librement et transitivement), supposer que φ_τ fixe l'élément 1 ($\tau \in \mathrm{G}_k$). Cette condition détermine alors φ_τ et il en résulte que la correspondance $\tau \to \varphi_\tau$ est un morphisme de groupes. La simple extension est donc définie sur k et grâce à la proposition 3.2.3, on peut même ajouter qu'il existe un k-modèle pour lequel la fibre au-dessus de t_0 contient un point k-rationnel.

(b) Un autre cas intéressant où le relèvement du morphisme $\overline{\varphi} : \mathrm{G}_k \to N/C$ est possible est celui où le groupe de Galois absolu G_k est projectif. Cette condition est satisfaite notamment si k est fini ou si k est de dimension cohomologique ≤ 1. Les corps $\overline{\kappa}((T))$ avec κ de caractéristique 0, les corps $\mathbb{Q}_p^{\mathrm{ur}}$ (extension algébrique maximale non ramifiée de $\mathbb{Q}_p$), $\overline{\kappa}(T)$, $\mathbb{Q}^{\mathrm{ab}}$ sont des exemples classiques de corps de dimension cohomologique ≤ 1. Sur ces corps, le corps des modules d'une (G-)extension $E/k^{\mathrm{s}}(T)$ est un corps de définition.

Le résultat suivant est une autre conséquence de la proposition 4.4.3. Le noyau $\ker(\overline{\varphi})$ est le sous-groupe de G_k de tous les éléments $\tau \in G_k$ tels que

$$(***) \qquad \phi(x^{s_{t_0}(\tau)}) = \phi(x) \text{ pour tout } x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{k^{\mathrm{s}}}$$

Désignons le sous-corps $(k^{\mathrm{s}})^{\ker(\overline{\varphi})}$ fixé par $\ker(\overline{\varphi})$ par $R_{t_0}(E)$.

(6) voir que si $\sigma \in N$ et $\sigma(1) = 1$, alors $\sigma\gamma(g)\sigma^{-1} = \gamma(\sigma(g))$, ce qui, via l'identification de G et $\gamma(G)$, indique que $\sigma(g)$ est égal à $\sigma\gamma(g)\sigma^{-1}$ et définit un morphisme.

Corollaire 4.4.6. — *Le corps $R_{t_0}(E)$ est un corps de définition de la (G-)extension $E/k^s(T)$. De plus $[R_{t_0}(E) : k] \leq |N|/|C|$.*

4.5. Construction de revêtements sur les corps complets

CHAPITRE 5

LA PROPRIÉTÉ DE SPÉCIALISATION DE HILBERT

Pour une introduction au théorème d'irréductibilité de Hilbert, nous renvoyons au §2.2.1 du chapitre 2 que nous développons dans ce chapitre.

Rappelons la définition des parties hilbertiennes. Etant donnés un corps k, 3 entiers $n, r, s > 0$, $r + s$ variables $T_1, \ldots, T_r, Y_1, \ldots, Y_s$, et n polynômes $P_1, \ldots, P_n \in k(T_1, \ldots, T_r)[Y_1, \ldots, Y_s]$, supposés irréductibles dans $k(T_1, \ldots, T_r)[Y_1, \ldots, Y_s]$, on pose

$$H_{P_1,\ldots,P_n} = \left\{ (t_1, \ldots, t_r) \in k^r \;\middle|\; \begin{array}{c} P_i(t_1, \ldots, t_r, Y_1, \ldots, Y_s) \text{ irréductible} \\ \text{dans } k[Y_1, \ldots, Y_s], i = 1, \ldots, n \end{array} \right\}$$

Les ensembles de la forme $H_{P_1,\ldots,P_n}$ (avec $n, s > 0$ quelconques) sont appelés *ensembles hilbertiens* ou *parties hilbertiennes* de k^r. Rappelons aussi (définition 2.2.2) qu'un corps k est dit hilbertien si pour tout $r > 0$, les parties hilbertiennes de k^r sont Zariski-denses.

Le *théorème d'irréductibilité de Hilbert* est l'énoncé suivant, déjà donné au chapitre 2.

Théorème 2.2.4 — *Le corps $\mathbb{Q}$ est un corps hilbertien.*

Le cas $r = s = 1$ a déjà été démontré au chapitre 2. Le cas général s'en déduit *via* les réductions expliquées dans la suite du chapitre. Il en résultera aussi que toute extension de type fini de $\mathbb{Q}$, en particulier tout corps de nombres, est un corps hilbertien. Un autre exemple important est celui du corps $\kappa(x)$ où κ est un corps quelconque et x est une indéterminée (théorème 5.3.1).

Au contraire, les corps suivants ne sont pas hilbertiens : le corps $\mathbb{C}$ des nombres complexes, et plus généralement tout corps algébriquement clos, le

corps $\mathbb{R}$ des nombres réels (prendre $P_1(T,Y) = Y^2 - (1+T^2)$), les corps p-adiques $\mathbb{Q}_p$ (exercice (1) ci-dessous), les corps de séries formelles $\kappa((x))$ (exercice (2)). Un corps fini n'est jamais hilbertien : pour $P_1(T,Y) = Y^2 + TY + \prod_{a\in k}(T-a)$, $H_{P_1} = \emptyset$. Désormais, nous supposerons toujours que le corps étudié est infini.

Exemple 5.0.1. — (1) Soit k un corps pour lequel il existe un entier $d > 1$ tel que $(k^\times)/(k^\times)^d$ est fini (par exemple $\mathbb{Q}_p$, $\overline{\kappa}((x))$). Alors k n'est pas hilbertien.

Démonstration. — Considérer les polynômes $P_i(T,Y) = Y^d - a_i^{-1}T$, $i = 1,\dots,n$ où n est l'ordre de $(k^\times)/(k^\times)^d$ et $a_1,\dots,a_n$ sont des représentants de $k^\times$ modulo $(k^\times)^d$.) □

(2) Un corps k hensélien pour une valuation v (par exemple $\mathbb{Q}_p$, $\kappa((x))$) n'est pas hilbertien[(1)].

Démonstration. — Le corps k est le corps des fractions d'un anneau A hensélien pour une valuation v. Considérons le polynôme $P(T,Y) = Y^2 - mT - 1$ où m est choisi dans l'idéal de valuation $\mathcal{M}$ de A et où Y^2 est remplacé par Y^3 si k est de caractéristique 2. D'après la propriété de Hensel (§1.2.2.7), ce polynôme vérifie que pour tout t dans l'anneau de valuation de k, $P(t,Y)$ a une racine dans k : en effet, le polynôme réduit $Y^2 - 1$ modulo I a deux racines simples. Si $t \in k$ n'est pas dans l'anneau de valuation, alors $t/(t+1)$ l'est (puisque $v(t+1) = v(t)$). D'après le raisonnement précédent, le polynôme $Y^2 - (mt/(t+1)) - 1$ a une racine dans k. Conclusion : la partie hilbertienne associée aux deux polynômes $Y^2 - mT - 1$ et $Y^2 - (mT/(T+1)) - 1$ est vide. □

5.1. Réductions générales

5.1.1. Réduction à $k[\mathbf{T}][\mathbf{Y}]$. — Dans la définition des parties hilbertiennes, on peut se restreindre aux parties hilbertiennes $H_{P_1,\dots,P_n}$ où les polynômes $P_1,\dots,P_n$ sont dans $k[T_1,\dots,T_r][Y_1,\dots Y_s]$, sont irréductibles dans cet anneau, et ne sont pas dans $k[T_1,\dots,T_r]$. En effet, supposons donnés $P_1,\dots,P_n$ irréductibles dans $k(\mathbf{T})[\mathbf{Y}]$. Pour $i = 1,\dots,n$, notons $c_i(\mathbf{T}) \in k[\mathbf{T}]$ le polynôme, défini à constante non nulle dans k près, tel que c_iP_i est irréductible

(1) Noter cependant que le corps $k_0((X_1,\dots,X_n))$ des séries formelles à coefficients dans un corps k_0 et en les n variables $(X_1,\dots,X_n)$ est hensélien au sens général de la définition 1.2.18 mais est hilbertien d'après un théorème de Weissauer (voir théorème 5.4.5).

dans $k[\mathbf{T},\mathbf{Y}]$, et posons $P_i' = c_i P_i$. On vérifie aisément que

$$H_{P_1',\dots,P_n'} \subset H_{P_1,\dots,P_n} \cup \bigcup_{i=1}^{n}(\{c_i(\mathbf{t})=0\}\cup\{c_i(\mathbf{t})=\infty\})$$

Il suffit donc que $H_{P_1',\dots,P_n'}$ soit Zariski-dense pour que $H_{P_1,\dots,P_n}$ le soit.

5.1.2. "Zariski" dense vs. "non vide". — On peut aussi remplacer "Zariski-dense" par "non vide" en se restreignant de plus aux parties hilbertiennes $H_{P_1,\dots,P_n}$ où les polynômes $P_1,\dots,P_n$ sont dans $k[\mathbf{T}][\mathbf{Y}]$ (au lieu de $k(\mathbf{T})[\mathbf{Y}]$). En effet, supposons $P_1,\dots,P_n$ donnés *a priori* dans $k(T_1,\dots,T_r)[Y_1,\dots Y_s]$ et notons $D(\mathbf{T})$ un dénominateur commun de $P_1,\dots,P_n$, *i.e.*, $D(\mathbf{T})P_i(\mathbf{T},\mathbf{Y}) \in k[\mathbf{T}][\mathbf{Y}]$. Soit $Q(t_1,\dots,t_r)=0$ une hypersurface de k^r avec $Q\in k[\mathbf{T}]$ non nul. On pose $P_i' = D^2QP_i$, $i=1,\dots,n$. On vérifie alors aisément que

$$H_{P_1',\dots,P_n'} = H_{P_1,\dots,P_n}\cap\{Q(\mathbf{t})\neq 0\}\cap\{D(\mathbf{t})\neq 0\}$$

On a multiplié par D^2 (et non D) pour assurer que si $t\in H_{P_1',\dots,P_n'}$, alors $D(t)\neq 0$ (penser à $P_1=(Y^2-T+1)/T$ et $D=T$).

Remarque 5.1.1. — Nous allons donner d'autres réductions dans la suite de cette section. Nous verrons alors que les réductions 5.1.1 et 5.1.2 peuvent être combinées. C'est-à-dire, pour montrer qu'un corps k est hilbertien, il suffit de montrer que les parties hilbertiennes $H_{P_1,\dots,P_n}$ où les polynômes $P_1,\dots,P_n$ sont irréductibles dans $k[\mathbf{T},\mathbf{Y}]$ et ne sont pas dans $k[\mathbf{T}]$, sont non vides. Voir remarque 5.1.9.

Etant donnés 3 entiers $n,r,s>0$, nous notons $\mathcal{H}(n,r,s)$ la propriété

($\mathcal{H}(n,r,s)$) *Pour tous* $P_1,\dots,P_n\in k[T_1,\dots,T_r][Y_1,\dots,Y_s]\backslash k[T_1,\dots,T_r]$, *irréductibles dans* $k[\mathbf{T}][\mathbf{Y}]$, *l'ensemble des points* $\mathbf{t}=(t_1,\dots,t_r)\in k^r$ *tels que* $P_i(\mathbf{t},\mathbf{Y})$ *est irréductible dans* $k[\mathbf{Y}]$, $i=1,\dots,n$, *est Zariski-dense.*

D'après le §5.1.1, un corps k est hilbertien si et seulement si $\mathcal{H}(n,r,s)$ est vraie pour tous entiers $n,r,s>0$. L'objet de ce paragraphe est d'établir d'autres réductions de la propriété d'hilbertianité. Nous obtiendrons qu'il suffit de démontrer $\mathcal{H}(1,1,1)$ pour montrer qu'un corps k est hilbertien.

5.1.3. Réduction $\mathcal{H}(n,1,s)(n,s>0)\Rightarrow\mathcal{H}(n,r,s)(n,r,s>0)$. — Soient $P_1,\dots,P_n$ comme dans $\mathcal{H}(n,r,s)$ et supposons qu'un corps k infini vérifie $\mathcal{H}(n,1,s)$ pour tous $n,s>0$. Comme $P_1,\dots,P_n$ sont irréductibles dans $k[T_1][T_2,\dots,T_r,Y_1,\dots,Y_s]$, d'après la condition $\mathcal{H}(n,1,r+s-1)$, il existe une

infinité de $t_1 \in k$ tels que, pour $i = 1, \ldots, n$, $P_i(t_1, T_2, \ldots, T_r, Y_1, \ldots, Y_s)$ est irréductible dans $k[T_2, \ldots, T_r, Y_1, \ldots, Y_s]$ et n'appartient pas à $k[T_2, \ldots, T_r]$ (noter que cette seconde condition peut n'être pas satisfaite que pour un nombre fini de $t \in k$ [(2)]; notons I_1 l'ensemble des $t_1 \in k$ convenables. D'après la condition $\mathcal{H}(n, 1, r+s-2)$, on peut ensuite déduire que l'ensemble I_2 des $t_2 \in k$ tels que $P_i(t_1, t_2, T_3 \ldots, T_r, Y_1, \ldots, Y_s)$ est irréductible dans $k[T_3, \ldots, T_r, Y_1, \ldots, Y_s]$ et n'appartient pas à $k[T_3, \ldots, T_r]$, $i = 1, \ldots, n$, est infini. On construit ainsi par récurrence r sous-ensembles infinis $I_1, \ldots, I_r$ de k vérifiant : pour tous $\mathbf{t} = (t_1, \ldots, t_r) \in I_1 \times \cdots \times I_r$, $P_i(\mathbf{t}, \mathbf{Y})$ est irréductible dans $k[\mathbf{Y}]$, $i = 1, \ldots, n$. Autrement dit $I_1 \times \cdots \times I_r \subset H_{P_1,\ldots,P_r}$. De plus, l'ensemble $I_1 \times \cdots \times I_r$ est Zariski-dense.

5.1.4. Réduction $\mathcal{H}(n, 1, 1)(n > 0) \Rightarrow \mathcal{H}(n, 1, s)(n, s > 0)$. — Considérons d'abord la situation d'*un* polynôme $P(T, Y_1, \ldots, Y_s) \in k[T, \mathbf{Y}]$ irréductible dans $k(T)[\mathbf{Y}]$. On utilise la *transformation de Kronecker*. Soit a un entier tel que $a > \deg_{Y_j}(P)$, $j = 1, \ldots, s$. Pour tout polynôme $Q \in k[T, \mathbf{Y}]$ on note $\mathrm{Kr}(Q)$ le polynôme

$$\mathrm{Kr}(Q) = Q(T, Y, Y^a, \ldots, Y^{a^{s-1}})$$

La transformation $P \to \mathrm{Kr}(P)$ est une bijection entre les ensembles

$$\{Q \in k[T, Y_1, \ldots, Y_s] | \deg_{Y_i}(Q) < a\} \text{ et } \{q \in k[T, Y] | \deg_Y(q) \leq a^s - 1\}$$

Cela résulte de la forme et de l'unicité de l'écriture en base a de tout entier positif inférieur à $a^s - 1$. On a d'autre part, pour tous polynômes $A, B \in k[T, \mathbf{Y}]$,

$$\mathrm{Kr}(AB) = \mathrm{Kr}(A)\mathrm{Kr}(B)$$

Soit $\mathrm{Kr}(P) = qr$ une factorisation non triviale de $\mathrm{Kr}(P)$ dans $K(T)[Y]$: $q, r \in K(T)[Y]$, $\deg_Y(q) > 0$ et $\deg_Y(r) > 0$. Comme $\deg(q) \leq a^s - 1$ et $\deg(r) \leq a^s - 1$, q et r s'écrivent $q = \mathrm{Kr}(Q)$ et $r = \mathrm{Kr}(R)$, avec $Q, R \in k(T)[\mathbf{Y}]$ tels que $\deg_{Y_i}(Q) < a$ et $\deg_{Y_i}(R) < a$ $(i = 1, \ldots, s)$, et $\deg_{\mathbf{Y}}(Q), \deg_{\mathbf{Y}}(R) > 0$. La factorisation de $\mathrm{Kr}(P)$ se réécrit $\mathrm{Kr}(P) = \mathrm{Kr}(Q)\mathrm{Kr}(R) = \mathrm{Kr}(QR)$. Si comme nous le supposons, P est irréductible dans $K(T)[\mathbf{Y}]$ (ce qui interdit $P = QR$), cela conduit à la condition suivante :

(*) il existe au moins un indice $i = 1, \ldots, s$ tel que $\deg_{Y_i}(QR) \geq a$.

---

(2) Plus précisément, si $c(T_1, T_2, \ldots, T_r) \in k[T_2, \ldots, T_r][T_1]$ est le coefficient (non nul) d'un monôme de P_i de degré strictement positif en Y, alors pour tout $t_1 \in k$ sauf un nombre fini, $c(t_1, T_2, \ldots, T_r) \neq 0$ et donc $P_i(t_1, T_2, \ldots, T_r, Y_1, \ldots, Y_s) \notin k[T_2, \ldots, T_r]$.

Soit $\mathrm{Kr}(P) = \prod_{i=1}^{m} \Pi_i(T, Y)$ une décomposition de $\mathrm{Kr}(P)$ en irréductibles de $K(T)[Y]$. Les factorisations de $\mathrm{Kr}(P)$ correspondent aux partitions de l'ensemble $\{1, \ldots, m\}$. D'après ce qui précède, à chaque factorisation non triviale, c'est-à-dire, à chaque sous-ensemble non vide $I \underset{\neq}{\subset} \{1, \ldots, m\}$, correspond une factorisation $\mathrm{Kr}(P) = \mathrm{Kr}(Q)\mathrm{Kr}(R)$ vérifiant la condition (*). Soit $c_I(T) \in K(T)$ le coefficient non nul d'un monôme du polynôme QR de degré $\geq a$ par rapport à l'une des indéterminées $Y_1, \ldots, Y_s$.

Nous allons montrer que

(**) pour tout $t_0 \in K$ tel que $\Pi_i(t_0, Y)$ est irréductible dans $K[Y]$, $i = 1, \ldots, m$ et tel que $c_I(t_0)$ défini et non nul pour tout sous-ensemble non vide $I \underset{\neq}{\subset} \{1, \ldots, m\}$, alors $P(t_0, \mathbf{Y})$ est irréductible dans $K[\mathbf{Y}]$.

Soit t_0 comme ci-dessus. En faisant $T = t_0$ dans la décomposition de $\mathrm{Kr}(P)$, on obtient la décomposition $\mathrm{Kr}(P(t_0, \mathbf{Y})) = \prod_{i=1}^{m} \Pi_i(t_0, \mathbf{Y})$ de $\mathrm{Kr}(P(t_0, \mathbf{Y}))$ en irréductibles de $K[\mathbf{Y}]$. De plus, à cause de la seconde partie de la condition (**), toute factorisation non triviale de $\mathrm{Kr}(P(t_0, \mathbf{Y}))$ est de la forme $\mathrm{Kr}(P(t_0, \mathbf{Y})) = \mathrm{Kr}(q)\mathrm{Kr}(r)$ avec $q, r \in K[\mathbf{Y}]$ vérifiant la condition (*). Or si on a $P(t_0, \mathbf{Y}) = q(\mathbf{Y})r(\mathbf{Y})$ ($q, r \in K[\mathbf{Y}]$ nécessairement de degré $< a$ en chacune des indéterminées Y_i), la factorisation $\mathrm{Kr}(P(t_0, \mathbf{Y})) = \mathrm{Kr}(q)\mathrm{Kr}(r)$ qu'on en déduit ne satisfait pas la condition (*). Une telle factorisation $P(t_0, \mathbf{Y}) = q(\mathbf{Y})r(\mathbf{Y})$ est donc nécessairement triviale, c'est-à-dire, $P(t_0, \mathbf{Y})$ est irréductible dans $K[\mathbf{Y}]$.

Conclusion : on a montré que $H_{\Pi_1, \ldots, \Pi_m} \subset H_P \cup F$ où F est un ensemble fini. Si au lieu d'un polynôme P, on considère n polynômes $P_1, \ldots, P_n \in k[T, \mathbf{Y}]$ comme dans $\mathcal{H}(n, 1, s)$, on choisit un entier a tel que $a > \deg_{Y_j}(P)$, $j = 1, \ldots, s$, $i = 1, \ldots, n$. D'après ce qui précède, si $\Pi_{ij}(T, Y)$ ($j = 1, \ldots, m_i$) sont les facteurs irréductibles d'une décomposition de $\mathrm{Kr}(P_i)$ dans $K(T)[Y]$, on a

$$H_{\Pi_{11} \ldots \Pi_{1m_1} \ldots \Pi_{n1} \ldots \Pi_{nm_n}} \subset H_{P_1, \ldots, P_n} \cup F$$

où F est un ensemble fini.

Remarque 5.1.2. — Dans la propriété $\mathcal{H}(n, 1, 1)$ ($n > 0$) à laquelle nous venons de réduire la propriété $\mathcal{H}(n, r, s)$ ($n, r, s > 0$), on peut sans perte de généralité supposer que les polynômes $P_1, \ldots, P_n$ sont unitaires en Y (en plus des conditions de $\mathcal{H}(n, 1, 1)$). En effet, si $P_i(T, Y) = a_{io}(T)Y^d + a_{i1}(T)Y^{d-1} + \cdots + a_{id}(T)$ avec $a_{io}(T) \neq 0$, on pose $\tilde{P}_i(T, Y) = Y^d + a_{i1}(T)Y^{d-1} + a_{i2}(T)a_{io}(T)Y^{d-2} \cdots + a_{id}(T)(a_{io}(T))^{d-1}$; c'est-à-dire, si $y_i \in \overline{k(T)}$ est une racine de $P_i(T, Y)$, alors $\tilde{P}_i(T, Y)$ est le polynôme minimal

sur $k(T)$ de $a_{io}(T)y_i$, $i = 1, \ldots, n$. Si $t \in k$ est tel que $\tilde{P}_i(t, Y)$ est irréductible dans $k[Y]$, alors ou bien $P_i(t, Y)$ l'est également ou bien $a_{io}(t) = 0$: si y_{it} est une racine de $\tilde{P}_i(t, Y)$ et $a_{io}(t) \neq 0$, $P_i(t, Y)$ est le polynôme minimal de $y_{it}/a_{io}(t)$. En conclusion, on a donc $H_{\tilde{P}_1,\ldots,\tilde{P}_n} \subset H_{P_1,\ldots,P_n} \cup Z$ où Z est un fermé de Zariski propre.

5.1.5. Première réduction à l'hypothèse d'absolue irréductibilité. — Dans le (b) du lemme 5.1.3 ci-dessous, nous disons qu'un polynôme $f \in A[Y_1, \ldots, Y_s]$ à coefficients dans un anneau intègre A est *normalisé* en $\mathbf{Y} = (Y_1, \ldots, Y_s)$ si le coefficient du monôme de plus haut degré pour l'ordre lexicographique (ascendant de 1 à s par exemple) vaut 1. Pour la situation $s = 1$ (à laquelle nous sous sommes ramenés au §5.1.4), "normalisé" signifie simplement "unitaire". On vérifie aisément que dans un produit $f_1 f_2$ de deux polynômes $f_1, f_2 \in A[Y_1, \ldots, Y_s]$, le monôme de plus haut degré est le produit des monômes de plus haut degré de f_1 et de f_2. En particulier, $f_1 f_2$ est normalisé si f_1 et f_2 le sont.

Lemme 5.1.3. — (a) *Soient ℓ/k une extension de corps avec $k \neq \ell$ et $P(T)$ un polynôme dans $\ell[T] \setminus k[T]$. Alors le nombre d'éléments $t \in k$ tels que $P(t) \in k$ est inférieur ou égal à* $\deg(P)$.

(b) *Soit $P \in k[T, Y_1, \ldots, Y_s]$ un polynôme irréductible dans $k(T)[\mathbf{Y}]$. Soit*

$$P(T, \mathbf{Y}) = a_n(T)\ \Pi_1(T, \mathbf{Y}) \cdots \Pi_r(T, \mathbf{Y})$$

une factorisation de $P(T, \mathbf{Y})$ dans $\overline{k}[T, \mathbf{Y}]$, avec $a_n(T) \in k[T]$ et $\Pi_1, \ldots, \Pi_r$ normalisés en $\mathbf{Y}$. Soit ℓ une extension de k contenant les coefficients de $\Pi_1, \ldots, \Pi_r$. Pour tout $t \in k$ sauf éventuellement un nombre fini, si $\Pi_i(t, \mathbf{Y})$ est irréductible dans $\ell[\mathbf{Y}]$, $i = 1, \ldots, r$, alors $P(t, \mathbf{Y})$ est irréductible dans $k[Y]$.

Démonstration. — (a) Soient $t_1, \ldots, t_m$ m éléments de k tels que $P(t_i) \in k$, $i = 1, \ldots, m$. Les $(\deg_Y(P) + 1)$ coefficients de P sont solution d'un système linéaire de m équations à coefficients dans k. Nécessairement $m < \deg_Y(P)+1$; sinon les formules de Cramer permettent d'écrire les coefficients de P comme éléments de k. (Un autre argument, essentiellement équivalent, consiste à utiliser les formules d'interpolation de Lagrange).

(b) Soit $t \in k$ tel que $\Pi_i(t, \mathbf{Y})$ est irréductible dans $\ell[\mathbf{Y}]$, $i = 1, \ldots, r$ et $a_n(t) \neq 0$. Supposons que $P(t, \mathbf{Y}) = a_n(t)Q(\mathbf{Y})R(\mathbf{Y})$ avec $Q(\mathbf{Y}), R(\mathbf{Y}) \in k[\mathbf{Y}]$ normalisés en $\mathbf{Y}$. En vertu de l'unicité de la décomposition en irréductibles dans $\ell[\mathbf{Y}]$, il existe nécessairement un sous-ensemble $I \subset \{1, \ldots, r\}$ tel que $Q(\mathbf{Y}) = \prod_{i \in I} \Pi_i(t, \mathbf{Y})$ et $R(\mathbf{Y}) = \prod_{i \notin I} \Pi_i(t, \mathbf{Y})$. On peut alors déduire

du (a) que, si t n'est pas dans un certain ensemble fini exceptionnel F (dépendant des Π_i), les deux polynômes $\mathcal{Q}(T,\mathbf{Y}) = \prod_{i\in I}\Pi_i(T,\mathbf{Y})$ et $\mathcal{R}(T,\mathbf{Y}) = \prod_{i\notin I}\Pi_i(T,\mathbf{Y})$ sont dans $k[T,\mathbf{Y}]$: on applique (a) à chacun des coefficients dans $\ell(T)$ des polynômes (en $\mathbf{Y}$) $\mathcal{Q}(T,\mathbf{Y})$ et $\mathcal{R}(T,\mathbf{Y})$. De l'irréductibilité de $P(T,\mathbf{Y})$ dans $k(T)[\mathbf{Y}]$, on peut alors conclure que, pour $t\notin F$, on a $I=\emptyset$ ou $I=\{1,\dots,n\}$. (On vérifie facilement que le nombre de t exceptionnels est $<\deg(P)(\deg(P)+1)^s 2^{\deg(P)}$ ($<\deg(P)2^{\deg(P)}$ pour $s=1$) [?]). □

Rappelons qu'un polynôme à coefficients dans un corps k est dit *absolument irréductible* s'il est irrédutible sur $\overline{k}$. D'après le lemme 5.1.3, pour montrer que k est hilbertien, il suffit de montrer que, pour toute extension finie ℓ/k, les parties hilbertiennes $H_{P_1,\dots,P_n}$ de ℓ avec $P_i\in\ell[T,\mathbf{Y}]\setminus\ell[T]$ *absolument irréductibles*, $i=1,\dots,n$, contiennent une infinité d'éléments de k.

5.1.6. Utilisation du théorème de Bertini. — Nous faisons le lien entre le théorème d'irréductibilité de Hilbert et le théorème de Bertini dont nous rappelons l'énoncé ci-dessous. Tous deux sont des résultats de spécialisation.

5.1.6.1. Enoncé du théorème de Bertini. — Le résultat ci-dessous est attribué suivant les formes et le contexte à Bertini, Bertini-Noether, Ostrowski, etc. Sa démonstration repose sur des faits "géométriques" généraux, la théorie de l'élimination essentiellement. Dans [**Har77**] c'est le théorème 8.18 du chapitre II mais il se place seulement dans un contexte géométrique. Dans [**FJ04**] c'est la proposition 9.4.3 ; là c'est le bon énoncé mais la preuve utilise la théorie des langages. Des preuves élémentaires sont données dans [**Sch00**] et dans [**Sch76**] (dans ce dernier c'et le cas $A=\mathbb{Z}$, attribué à Ostrowski du théorème 5.1.4 qui est traité.

On se donne un anneau intègre A, on note K son corps des fractions et $\overline{K}$ une clôture algébrique de K. Le théorème de Bertini concerne l'*absolue irréductibilité* des polynômes, *i.e.*, l'irréductibilité sur $\overline{K}$.

Théorème 5.1.4. — *Soit $f(Y_1,\dots,Y_m)\in A[Y_1,\dots,Y_m]$ un polynôme absolument irréductible. Il existe un élément $c\in A$ non nul tel que si $\varphi: A\to k$ est un morphisme d'anneau dans un corps k tel que $\varphi(c)\neq 0$, alors le polynôme $f^\varphi\in k[Y_1,\dots,Y_m]$ (obtenu en appliquant φ au coefficients de f) est absolument irréductible. En particulier, il existe un idéal non nul $\mathcal{A}$ de A tel que pour tout idéal premier $\mathcal{P}$ tel que $\mathcal{A}\not\subset\mathcal{P}$, la réduction modulo $\mathcal{P}$ de f est absolument irréductible (i.e., irréductible dans $\overline{A/\mathcal{P}}[Y_1,\dots,Y_m]$).*

Autrement dit, pour $\mathcal{P}$ en dehors d'un fermé de Zariski de $\mathrm{Spec}(A)$, il y a conservation de l'absolue irréductibilité de f modulo l'idéal premier $\mathcal{P}$.

5.1.6.2. Propriété de spécialisation avec $s \geq 2$. — Considérons un polynôme $P \in k[T_1, \ldots, T_r, Y_1, \ldots Y_s]$ et supposons le irréductible dans $\overline{k(\mathbf{T})}[\mathbf{Y}]$. On peut alors appliquer le théorème de Bertini avec $A = k[\mathbf{T}]$. On obtient qu'il existe une hypersurface $h(t_1, \ldots, t_r) = 0$ de k^r, avec $h \in k[T_1, \ldots, T_r]$ non nul, telle que, pour tout $\mathbf{t} = (t_1, \ldots, t_r)$ n'appartenant pas à l'hypersurface, $P(\mathbf{t}, \mathbf{Y})$ est irréductible dans $k[\mathbf{Y}]$.

Sous les hypothèses considérées, la conclusion est meilleure que celle du théorème d'irréductibilité de Hilbert : la partie hilbertienne H_P est ouverte et pas seulement dense pour la topologie de Zariski ; pour $r = 1$, cela revient à comparer "complémentaire d'une partie finie" et "infini". En particulier, la conclusion obtenue par Bertini s'étend directement au cas de plusieurs polynômes. De plus, il n'y a aucune hypothèse sur le corps k dans le théorème de Bertini.

Il faut cependant noter que l'hypothèse "P irréductible dans $\overline{k(\mathbf{T})}[\mathbf{Y}]$" est plus forte que l'hypothèse "P irréductible dans $k(\mathbf{T})[\mathbf{Y}]$" du théorème de Hilbert . En particulier, elle ne peut pas être satisfaite pour $s = 1$. Or ce cas, où il n'y a qu'une indéterminée, est le cas essentiel du théorème de Hilbert. Pour pouvoir appliquer le théorème de Bertini dans l'esprit du théorème de Hilbert, il faut qu'après spécialisation, il subsiste au moins 2 indéterminées. Une application typique du théorème de Bertini qu'on peut garder à l'esprit concerne les surfaces $f(t, x, y) = 0$: si f est irréductible dans $\overline{k(T)}[X, Y]$, les sections par les plans $t = t_0$ sont des courbes irréductibles sauf un nombre fini d'entre elles. Ajoutons que même avec $s > 1$, il y a des cas où le théorème de Bertini ne s'applique pas (et où le théorème de Hilbert s'applique) : prendre par exemple $P = Y_1^2 - TY_2^2$.

Il faut comprendre le théorème de Bertini comme un résultat géométrique et le théorème d'irréductibilité de Hilbert comme un résultat arithmétique.

5.1.6.3. Retour sur la réduction $\mathcal{H}(n, 1, 1)(n > 0) \Rightarrow \mathcal{H}(n, 1, s)(n, s > 0)$. — Pour se ramener au cas d'une indéterminée dans le théorème d'irréductibilité de Hilbert, on peut préférer la démarche suivante, qui utilise le théorème de Bertini. En comparaison avec la transformation de Kronecker, utilisée dans le §5.1.4, cette seconde méthode est plus géométrique et plus économique en le degré (relatif à Y) des polynômes.

Soient $P_1, \ldots, P_n \in k[T, Y_1, \ldots, Y_s]$ comme dans $\mathcal{H}(n, 1, s)$. On commence par utiliser le lemme 5.1.3 qui permet de supposer $P_1, \ldots, P_n$ absolument irréductibles. Puis on utilise la proposition suivante [**FJ04**, proposition 10.5.4].

Proposition 5.1.5. — *Si $P_1, \ldots, P_n$ sont comme ci-dessus absolument irréductibles et si $W_1, Z_1, \ldots, W_s, Z_s$ sont $2s$ nouvelles indéterminées, alors les polynômes $P_i(T, W_1Y + Z_1, \ldots, W_sY + Z_s) \in k(W_1, \ldots, W_s, Z_1, \ldots, Z_s)[T, Y]$ sont absolument irréductibles, $i = 1, \ldots, n$.*

Grâce au théorème de Bertini, on obtient qu'il existe un polynôme non nul $h \in k[W_1, \ldots, W_s, Z_1, \ldots, Z_s]$ tel que, pour tout $(w_1, \ldots, w_s, z_1, \ldots, z_s) \in k$ vérifiant $h(w_1, \ldots, w_s, z_1, \ldots, z_s) \neq 0$, le polynôme $P_i(T, w_1Y + z_1, \ldots, w_sY + z_s) \in k[T, Y]$ est absolument irréductible, $i = 1, \ldots, n$.

Pour conclure, on note que si $t \in k$ est tel que $P_i(t, w_1Y + z_1, \ldots, w_sY + z_s)$ est irréductible dans $k[Y]$, alors $P_i(t, Y_1, \ldots, Y_s)$ est irréductible dans $k[Y_1, \ldots, Y_s]$, $i = 1, \ldots, n$, sauf peut-être pour certains choix des points $(w_1, \ldots, w_s, z_1, \ldots, z_s)$ dans un fermé de Zariski de k^{2s}.

L'intérêt de s'être ramené au cas de polynômes en une indéterminée est de pouvoir utiliser la théorie des extensions algébriques de corps. En effet, tout polynôme P irréductible dans $k(\mathbf{T})[Y]$ définit une extension finie $E_{\mathbf{T}}/k(\mathbf{T})$.

5.1.7. Réduction $\mathcal{H}(1, 1, 1) \Rightarrow \mathcal{H}(n, 1, 1)(n > 0)$. —

Proposition 5.1.6. — *Soient $P_1, \ldots, P_n \in k(T)[Y]$ n polynômes irréductible séparables en Y. Alors il existe un polynôme irréductible $P \in k[T, Y]$, séparable et unitaire en Y tel que $H_P \subset H_{P_1,\ldots,P_n}$. On peut même demander en plus que l'extension de $k(T)$ déterminée par le polynôme P soit galoisienne.*

Démonstration. — Dans une clôture algébrique $\overline{k(T)}$, soit F_i le corps engendré sur $k(T)$ par une racine y_i de $P_i(T, y_i) = 0$, $i = 1, \ldots, n$. Le compositum $F_1 \cdots F_n$ est une extension séparable de $k(T)$. Soit $E/k(T)$ sa clôture galoisienne. Cette extension possède des éléments primitifs. Soit z un élément primitif qui soit de plus entier sur $k[T]$. Soit $P(T, Y)$ le polynôme minimal de z sur $k(T)$. D'après le théorème de spécialisation du chapitre 1 (théorème 1.9.1 ou théorème 1.9.3), le polynôme P répond au problème. □

Remarque 5.1.7. — L'énoncé et sa preuve restent valables si la variable T est remplacée par un r-uplet $\mathbf{T}$ de variables.

5.1.8. Corps séparablement hilbertiens. — Un corps k est dit séparablement hilbertien si pour tous polynômes $P_1, \dots, P_n \in k(T)[Y]$ irréductibles et *séparables* en Y[3] , la partie hilbertienne $H_{P_1,\dots,P_n}$ est infinie. D'après la proposition 5.1.6, il suffit que la propriété soit vraie dans le cas d'un polynôme (*i.e.* $n = 1$). En caractéristique 0, les deux notions de corps hilbertien et de corps séparablement hilbertien sont équivalentes. Pour la caractéristique $p > 0$, on a le résultat suivant, dû à Uchida.

Théorème 5.1.8. — *Un corps k de caractéristique $p > 0$ est hilbertien si et seulement si il est séparablement hilbertien et si l'ensemble k^p (puissances p-ièmes) est distinct de k.*

Un corps de caractéristique p vérifiant $k^p \neq k$ sera dit *imparfait*.

Démonstration. — ($\Rightarrow$) : Un corps hilbertien est séparablement hilbertien. Et il est aussi nécessairement imparfait : en effet si k est parfait, *i.e.*, si $k^p = k$, alors l'ensemble hilbertien H_{Y^p-T} est vide.
($\Leftarrow$) : voir [**FJ04**, proposition 12.4.3]. □

Le corps $\mathbb{F}_p(x)$ avec x une indéterminée est un exemple de corps hilbertien de caractéristique $p > 0$. Le corps fini $\mathbb{F}_p$ n'est ni séparablement hilbertien ni imparfait (il est fini). Le corps $\mathbb{F}_p((x))$, où x est une indéterminée est imparfait et non séparablement hilbertien (c'est un corps hensélien). Le corps $\varinjlim_n \mathbb{F}_p(x^{1/p^n})$ est infini, parfait donc non-hilbertien (bien que chaque corps $\mathbb{F}_p(x^{1/p^n})$ soit hilbertien). Le théorème 5.4.4 montre qu'il est séparablement hilbertien.

Dans l'étude des corps hilbertiens, on peut se restreindre aux corps imparfaits ou de caractéristique 0 ; et il suffit alors de se limiter aux parties hilbertiennes $H_{P_1,\dots,P_n}$ avec $P_1, \dots, P_n \in k(T)[Y]$ irréductibles et séparables en Y.

5.1.9. Réduction à la recherche de points sur des courbes algébriques. — Nous rappelons la réduction déjà expliquée au §2.2.2 du chapitre 2. Etant donnés N polynômes $Q_1, \dots, Q_N \in k(T)[Y]$ sans racine dans $k(T)$, on pose

$$V'_{Q_1,\dots,Q_N} = \left\{ t \in k \;\middle|\; \begin{array}{c} Q_i(t, Y) \text{ n'a pas de} \\ \text{racine dans } k, i = 1, \dots, N \end{array} \right\}$$

L'énoncé suivant a été démontré au chapitre 2.

[3] c'est-à-dire, n'ayant pas de racine multiple dans $\overline{k(T)}$.

Proposition 2.2.5 — *Etant donnés n polynômes irréductibles $P_1, \dots, P_n \in k(T)[Y]$, il existe N polynômes $Q_1, \dots, Q_N \in k[T,Y]$ sans racine dans $k(T)$ et unitaires (en Y) et un ensemble fini $F \subset k$ tels que*

$$V'_{Q_1,\dots,Q_N} \subset H_{P_1,\dots,P_n} \cup F$$

De plus, si on suppose les polynômes $P_1, \dots, P_n$ séparables en Y (e.g. si k est de caractéristique 0), alors on peut demander aux polynômes $Q_1, \dots, Q_N$ d'être séparables et absolument irréductibles (quitte à grossir l'ensemble F).

5.1.10. Conclusion. — Nous récapitulons les réductions faites.

5.1.10.1. Réduction de la propriété de Hilbert. — Un corps k doit être imparfait ou de caractéristique 0 pour être hilbertien. Dans ce cas, pour montrer que k est hilbertien, il suffit de prouver l'un des deux énoncés suivants.

Enoncé 1 — *Etant donnés N polynômes $Q_1(T,Y), \dots, Q_N(T,Y) \in k[T,Y]$ absolument irréductibles, séparables, unitaires en Y et tels que $\deg_Y(Q_i) \geq 2$, $i = 1, \dots, N$, il existe une infinité de $t \in K$ tels que $Q_i(t,Y)$ n'a pas de racine dans k, $i = 1, \dots, N$. C'est-à-dire, l'ensemble $V'_{Q_1,\dots,Q_N}$ est infini.*

Enoncé 2 — *Etant donné un polynôme $P(T,Y) \in k[T,Y]$ irréductible, séparable, unitaire en Y et tel que l'extension algébrique associée de $k(T)$ soit galoisienne, il existe une infinité de $t \in K$ tels que $P(t,Y)$ est irréductible dans $k[Y]$. C'est-à-dire, l'ensemble H_P est infini.*

Remarque 5.1.9. — Dans les énoncés 1 et 2, on peut remplacer "infini" par "non vide" (cela clôt en particulier la remarque 5.1.1). En effet, supposons l'énoncé 2 vrai avec "non vide" et supposons que, pour un polynôme $P(T,Y) = Y^d + a_1(T)Y^{d-1} + \cdots + a_d(T)$ comme dans cet énoncé, H_P soit un ensemble fini $\{t_1, \dots, t_n\}$. Posons $p(T) = (T - t_1) \cdots (T - t_n)$ et considérons le polynôme $\tilde{P}(T,Y) = Y^d + a_1(T)p(T)Y^{d-1} + \cdots + p(T)^d a_d(T)$. La suite reprend un argument déjà utilisé. Le polynôme $\tilde{P}(T,Y)$ est irréductible dans $k(T)[Y]$, séparable et unitaire en Y et l'extension algébrique associée de $k(T)$ est galoisienne : en effet, si y est une racine de $P(T,Y)$ dans $\overline{k(T)}$, $\tilde{P}(T,Y)$ est le polynôme minimal sur $k(T)$ de $p(T)y$. D'après l'hypothèse, il existe $t \in K$ tel que $\tilde{P}(t,Y)$ est irréductible sur k. Cela entraîne que $P(t,Y)$ est irréductible sur k : si y_t est une racine de $\tilde{P}(t,Y)$, $P(t,Y)$ est le polynôme minimal de $y_t/p(t)$. Et cet élément t ne peut être aucun des t_i ($i = 1, \dots, n$) puisque $\tilde{P}(t_i,Y) = Y^d$. Contradiction. L'argument est similaire pour l'énoncé 1.

5.1.10.2. Autres variantes. — Dans [**DH99**], on introduit plusieurs variantes de la propriété de Hilbert dont celles de corps *mordellien*, de corps G-*hilbertien*, de corps RG-*hilbertien*. Un corps mordellien est un corps qui vérifie l'énoncé 1 mais avec $n = 1$. Un corps hilbertien est automatiquement mordellien mais la réciproque est fausse : il existe des corps mordelliens qui ne sont pas hilbertiens [**DH99**]. Un corps G-hilbertien est un corps qui vérifie l'énoncé 2 : cette notion est donc équivalente à celle de corps hilbertien. Un corps RG-hilbertien est un corps qui vérifie l'énoncé 2 avec la condition supplémentaire que le polynôme P est absolument irréductible. Il s'agit d'une notion plus faible que l'hilbertianité : il existe des corps RG-hilbertiens qui ne sont pas hilbertiens [**FV92**] [**DH99**].

La variante suivante est introduite dans [**Dèb99b**]. Un corps k est dit *cyclhilbertien* si les parties hilbertiennes $H_{P_1,\dots,P_n}$ avec $P_1, \dots, P_n$ de la forme $Y^e - aT$ ($e \geq 1$ entier et $a \in k$, $a \neq 0$) sont infinies. Il s'agit là aussi d'une notion plus faible que l'hilbertianité : il est montré dans l'article précité que le corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques totalement réels est un corps cyclhilbertien mais non hilbertien.

On sait aussi qu'on affaiblit strictement la propriété d'hilbertianité si on ne retient dans l'énoncé 1 que les polynômes Q_i tels que la courbe $Q_i(t, y) = 0$ soit de genre inférieur ou égal à un entier g. Cela a été montré par Corvaja-Zannier [**CZ98**] pour $g = 0$ et pour g quelconque par Fried-Jarden [**FJ88**].

Dans une veine similaire, on peut mentionner le *problème de Hilbert-Siegel* (résolu par Fried [**Fri99**], généralisé par Müller [**MÖ2**], voir aussi [**Dèb99a**]). Il s'agit de déterminer les polynômes $h(Y) \in \mathbb{Q}[Y]$ tels que $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} \setminus h(\mathbb{Q})$. On supposera h indécomposable (dans le cas contraire $h(Y) = h_1(h_2(Y))$ avec $h_1, h_2 \in \mathbb{Q}[Y]$ de degré ≥ 2, et $h(Y) - t$ est réductible pour tout t de la forme $t = h_1(z)$, $z \in \mathbb{Q}$). On a le résultat suivant.

Théorème 5.1.10. — (a) *Les seuls polynômes indécomposables $h(Y) \in \mathbb{Q}[Y]$ pour lesquels $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} \setminus h(\mathbb{Q})$ sont de degré* 5.

(b) *De plus, le cas* $\deg(h) = 5$ *est réellement exceptionnel : il existe des polynômes indécomposables $h(Y) \in \mathbb{Q}[Y]$ (de degré* 5*) pour lesquels $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} \setminus h(\mathbb{Q})$* [**DF99**].

5.2. Extensions algébriques d'un corps hilbertien

5.2.1. Extensions finies. — Le résultat principal est le suivant.

Théorème 5.2.1. — *Soit ℓ/k une extension finie. Alors, si k est hilbertien, alors ℓ est hilbertien.*

Nous allons démontrer le théorème dans le cas où ℓ/k est une extension séparable. Pour obtenir le cas général, il reste à traiter le cas des extensions purement inséparables. Pour cela, nous renvoyons à [**FJ04**, proposition 12.3.5]. Pour ℓ/k séparable, nous allons montrer l'énoncé plus précis suivant :

Théorème 5.2.1 (addendum) *Si $P \in \ell[T,Y] \setminus \ell[T]$ est irréductible alors il existe $p \in k[T,Y] \setminus k[T]$ irréductible tel que $H_p \subset H_P$ (où H_p et H_P sont a priori définis comme des sous-ensembles de k et ℓ respectivement). En conséquence, toute partie hilbertienne de ℓ avec $s = 1$ contient une partie hilbertienne de k (à un fermé de Zariski près).*

Démonstration. — Sans restreindre la généralité, on peut supposer P unitaire en Y (remarque 5.1.2). Soient $\widehat{\ell}$ la clôture galoisienne de l'extension ℓ/k et G son groupe de Galois. On pose aussi $H = \mathrm{Gal}(\widehat{\ell}/\ell)$ et on se donne un ensemble Σ de représentants des classes à gauche de G modulo le sous-groupe H. Etant donné P comme ci-dessus, on pose $p(T,Y) = \prod_{\sigma\in\Sigma} P^\sigma(T,Y)$. La conclusion désirée résulte des trois points suivants.

• $p(T,Y) \in k[T,Y]$: on vérifie en effet que le polynôme $p(T,Y)$ est invariant par tout k-automorphisme $\tau \in G$.

• pour tout $t_0 \in k$ tel que $p(t_0,Y)$ est irréductible dans $k[Y]$, $P(t_0,Y)$ est irréductible dans $\ell[Y]$: si $Q(Y) \in \ell[Y]$ est un diviseur non trivial de $P(t_0,Y)$, alors le polynôme $q(Y) = \prod_{\sigma\in\Sigma} Q^\sigma(Y)$ est un diviseur non trivial de $p(t_0,Y)$ dans $k[Y]$.

• le polynôme $p(T,Y)$ n'est pas dans $k[T]$ et est irréductible dans $k[T,Y]$. La première affirmation est facile. Pour l'irréductibilité on procède en deux temps :

1er cas : sous l'hypothèse que les polynômes $P^\sigma(T,Y)$ ($\sigma \in \Sigma$) sont premiers deux à deux dans $\overline{k}[T,Y]$. Supposons que $p(T,Y) = q(T,Y)r(T,Y)$ avec $q, r \in k[T,Y]$. Le polynôme $P(T,Y)$, irréductible dans $\ell[T,Y]$, divise l'un des deux facteurs, disons $q(T,Y)$ dans $\ell[T,Y]$. Donc $P(T,Y)$ divise aussi $q(T,Y)$, dans $\overline{k}[T,Y]$; il en est de même des polynômes $P^\sigma(T,Y)$ ($\sigma \in \Sigma$). Sous l'hypothèse de ce premier cas, on en déduit que $\prod_{\sigma\in\Sigma} P^\sigma(T,Y) = p(T,Y)$ divise $q(T,Y)$ dans $\overline{k}[T,Y]$. Les deux polynômes en question étant dans $k[T,Y]$, la divisibilité

$p(T,Y) \mid q(T,Y)$ a lieu dans $k[T,Y]$. La factorisation initiale de $p(T,Y)$ est donc triviale.

Cas général : on se ramène au premier cas en utilisant le lemme ci-dessous. □

Lemme 5.2.2. — *Soient comme ci-dessus une extension finie séparable ℓ/k et un polynôme $P(T,Y) \in \ell[T,Y] \setminus \ell[T]$ unitaire en Y. Alors il existe $c(T) \in \ell[T]$ tel que les polynômes $P(T, Y+c(T))^\sigma$ ($\sigma \in \Sigma$) sont premiers deux à deux dans $\overline{k}[T,Y]$.*

(Pour conclure la preuve du théorème 5.2.1 (cas séparable) noter que, pour $t_0 \in k$ et $c(T) \in \ell[T]$, l'irréductibilité dans $\ell[Y]$ de $P(t_0, Y+c(t_0))$ équivaut à celle de $P(t_0,Y)$).

Démonstration. — Soit θ un élément primitif de l'extension ℓ/k. Donnons nous un ensemble $\tilde{\Sigma} = \{\sigma_0, \dots, \sigma_{d-1}\}$ de représentants des classes à gauche de $\mathrm{Gal}(\overline{k(T)}/k(T))$ modulo le sous-groupe $\mathrm{Gal}(\overline{k(T)}/\ell(T))$ (où $d = [\ell : k]$) ; de façon équivalente, $\sigma_0, \dots, \sigma_{d-1}$ peuvent être définis comme des prolongements à $\overline{k(T)}$ des d $k(T)$-morphismes de $\ell(T)$ dans une clôture algébrique. On se donne aussi d éléments $t_0, t_1, \dots, t_{d-1}$ algébriquement indépendants sur $\overline{k(T)}$ et on pose

$$u_i = t_0 + \theta^{\sigma_i} t_1 + \cdots + (\theta^{\sigma_i})^{d-1} t_{d-1}, \qquad i = 0, 1, \dots, d-1$$

La transformation linéaire qui envoie $(t_0, \dots, t_{d-1})$ sur $(u_0, \dots, u_{d-1})$ est de déterminant $\prod_{i<j}(\theta^{\sigma_i} - \theta^{\sigma_j}) \neq 0$. On en déduit que $t_0, \dots, t_{d-1}$ s'expriment comme $\widehat{\ell}(T)$-combinaisons linéaires de $u_0, \dots, u_{d-1}$; ces derniers sont donc algébriquement indépendants sur $\overline{k(T)}$ (s'ils ne l'étaient pas, le corps $\overline{k(T)}(t_0, \dots, t_{d-1})$ serait inclus dans une extension de $\overline{k(T)}$ de degré de transcendance $< d$).

Considérons une factorisation

$$P(T,Y) = \prod_{h=1}^{m} (Y - y_h)$$

de $P(T,Y)$ dans $\overline{k(T)}[Y]$. Pour i, j distincts dans $\{0, \dots, d-1\}$ et h, h' quelconques dans $\{1, \dots, m\}$, on a $u_i - y_h^{\sigma_i} \neq u_j - y_{h'}^{\sigma_j}$. On a donc

$$\prod_{i<j} \prod_{h,h'} \left[(u_i - y_h^{\sigma_i}) - (u_j - y_{h'}^{\sigma_j}) \right] \neq 0$$

On peut exprimer cette quantité en fonction de $\mathbf{t} = (t_0, \dots, t_{d-1})$; notons la $H(\mathbf{t})$: on a *a priori* $H(\mathbf{t}) \in \overline{k(T)}[\mathbf{t}]$. Comme $H(\mathbf{t}) \neq 0$, il existe $\mathbf{a} =$

$(a_0, \dots, a_{d-1}) \in (k[T])^d$ tel que $H(\mathbf{a}) \neq 0$. Posons

$$c(T) = a_0 + \theta a_1 + \cdots + \theta^{d-1} a_{d-1}$$

On définit ainsi un élément de $\ell[T]$.

La spécialisation $\mathbf{t} \to \mathbf{a}$ envoie u_i sur $c(T)^{\sigma_i}$, $i = 0, \dots, d-1$. Il découle donc de $H(\mathbf{a}) \neq 0$ que $c(T)^{\sigma_i} - y_h^{\sigma_i} \neq c(T)^{\sigma_j} - y_{h'}^{\sigma_j}$, pour $i, j \in \{0, \dots, d-1\}$ distincts et $h, h' \in \{1, \dots, m\}$. Les éléments $c(T)^{\sigma_i} - y_h^{\sigma_i} \in \overline{k(T)}$ $(h = 1, \dots, m)$ sont les racines du polynôme $P(T, Y + c(T))^{\sigma_i}$, $i = 0, \dots, d-1$. On en déduit que les polynômes $P(T, Y + c(T))^{\sigma_i}$ $(i = 0, \dots, d-1)$ sont premiers deux à deux dans $\overline{k(T)}[Y]$; ils le sont donc aussi dans $\overline{k}(T)[Y]$. Dans l'anneau $\overline{k}[T, Y]$, ces polynômes, pris deux à deux, sont de pgcd dans $\overline{k}[T]$; comme ces polynômes sont unitaires, ce pgcd est forcément dans k. Cela montre bien, comme annoncé, que les polynômes $P(T, Y + c(T))^{\sigma_i}$ $(i = 0, \dots, d-1)$ sont premiers deux à deux dans $\overline{k}[T, Y]$. □

Remarque 5.2.3. — Il peut arriver que l'hypothèse du premier cas ne soit pas satisfaite, c'est-à-dire que les polynômes $P^\sigma(T, Y)$ $(\sigma \in \Sigma)$ ne soient pas premiers deux à deux dans $\overline{k}[T, Y]$. Voici un contre-exemple. Posons $\alpha = \sqrt[3]{2}$ et $j = e^{2i\pi/3}$ et prenons

$$P(T, Y) = Y^2 + \alpha Y T + \alpha^2 T^2 = (Y - j\alpha T)(Y - j^2 \alpha T)$$

Le polynôme $P(T, Y)$ est irréductible sur $\mathbb{Q}(\alpha)$. Ses autres conjugués sont

$$\begin{cases} P^{\sigma_1}(T, Y) = Y^2 + j\alpha Y T + j^2 \alpha^2 T^2 = (Y - j^2 \alpha T)(Y - \alpha T) \\ P^{\sigma_2}(T, Y) = Y^2 + j^2 \alpha Y T + j \alpha^2 T^2 = (Y - \alpha T)(Y - j\alpha T) \end{cases}$$

5.2.2. Extensions algébriques. — Nous donnons en complément, sans démonstration, des résultats sur les extensions algébriques de degré éventuellement infini des corps hilbertiens.

5.2.2.1. Théorèmes de Weissauer et de Haran. — L'énoncé suivant est dû à D. Haran [**FJ04**, theorem 13.8.3].

***Théorème 5.2.4* (Diamond Theorem)**. — *Soient k un corps hilbertien, K_1/k et K_2/k deux extensions galoisiennes de K. Soit K un corps intermédiaire entre k et le compositum K_1K_2 tel que K ne soit contenu ni dans K_1 ni dans K_2. Alors K est un corps hilbertien.*

Il contient en particulier le résultat antérieur de Weissauer [**FJ04**, theorem 13.9.3], ci-dessous. Le théorème 5.2.1 concernant les extensions finies séparables correspond au cas particulier $K = k$.

***Théorème 5.2.5* (Weissauer).** — *Soient k un corps hilbertien, K/k une extension galoisienne et L une extension finie propre séparable de K. Alors L est un corps hilbertien.*

Un exemple classique d'application est que, si $\mathbb{Q}^{\mathrm{tr}}$ désigne le corps des nombres algébriques *totalement réels* (*i.e.*, dont tous les conjugués sur $\mathbb{Q}$ sont réels), alors $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ est hilbertien.

Démonstration du théorème 5.2.5 à partir du théorème 5.2.4.

Si K/k est de de degré fini, l'énoncé résulte du théorème 5.2.1. Supposons le contraire. Soit alors M/k une extension galoisienne finie telle que $L \subset MK$. Le corps L n'est contenu ni dans M ni dans K. D'après le théorème 5.2.4, c'est un corps hilbertien. □

5.2.2.2. Extensions abéliennes. — Pour les extensions abéliennes, *i.e.*, les extensions galoisiennes de groupe de Galois abélien, on a le résultat suivant, dû à Kuyk [**FJ04**, §16.11].

Théorème 5.2.6. — *Soient k un corps hilbertien, K/k une extension abélienne (éventuellement de degré infini). Alors K est un corps hilbertien.*

En particulier, la *clôture abélienne* $\mathbb{Q}^{ab}$ de $\mathbb{Q}$, c'est-à-dire, le sous-corps de $\overline{\mathbb{Q}}$ fixé par le groupe dérivé de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (et dont on sait, d'après le théorème de Kronecker-Weber, que c'est le corps engendré sur $\mathbb{Q}$ par toutes les racines de l'unité), est un corps hilbertien. Une autre conséquence est que le corps engendré par les racines carrées de tous les nombres premiers est un corps hilbertien. Ce résultat se déduit aussi du théorème 5.2.5. En effet, le corps engendré par les racines carrées de tous les nombres premiers sauf un est une extension galoisienne de $\mathbb{Q}$ et le corps voulu en est une extension finie propre (pour voir que qu'elle est propre, regarder la ramification).

5.3. Extensions transcendantes pures

Le résultat visé dans cette section est le suivant.

Théorème 5.3.1. — *Si k est un corps quelconque et ω un élément transcendant sur k, alors le corps $k(\omega)$ est un corps hilbertien.*

Une conséquence immédiate est que le corps des fractions rationnelles $k(T_1, \ldots, T_n)$ ($n \geq 1$) à coefficients dans un corps k quelconque est un corps hilbertien. Il en résulte même que toute extension transcendante pure (de

degré de transcendance > 0 mais éventuellement infini) d'un corps quelconque est un corps hilbertien [4].

Nous ne démontrerons le théorème 5.3.1 que dans le cas où k est un corps infini (ce cas entraîne "$k(T_1, \ldots, T_n)$ hilbertien" pour $n \geq 2$ pour tout corps). Les corps $\mathbb{F}_q(T)$ sont des corps globaux, et plus généralement des corps avec une formule du produit. Weissauer a montré que ces corps étaient hilbertiens en général. Nous renvoyons à [**FJ04**, §13.4] pour le cas des corps globaux et à [**FJ04**, §15.3] pour le théorème plus général de Weissauer. Pour k corps infini, nous allons démontrer l'énoncé plus précis suivant.

Théoreme 5.3.1 (addendum) *Soit ω un élément transcendant sur un corps infini k. Soient H une partie hilbertienne de $k(\omega)$ et $m \geq 1$ un entier. Alors il existe un polynôme $\phi \in k[\omega, t]$ non nul tel que pour tout $(\omega_0, t_0) \in \mathbb{A}^2(k)$ tel que $\phi(\omega_0, t_0) \neq 0$ et pour tout $\lambda_0 \in k$ sauf un nombre fini, l'élément $t_0 + \lambda_0(\omega - \omega_0)^m \in k(\omega)$ est dans la partie hilbertienne H.*

Démonstration. — Le corps $k(\omega)$ est imparfait s'il est de caractéristique > 0. Grâce aux résultats de réduction (5.1.10.1), il suffit de démontrer cet énoncé où H est remplacé par un ensemble du type

$$V'_P = \{t \in k(\omega) | P(t, Y) \text{ n'a pas de racines dans } k(\omega)\}$$

où $P(T, Y) \in k(\omega)[T, Y]$ est absolument irréductible, séparable, unitaire en Y et sans racine dans $k(\omega)(T)$. Ici on se limite aussi à la situation d'un seul polynôme : voir la fin de la preuve. Enfin, on peut aussi supposer que $P(T, Y) \in k[\omega][T, Y]$.

Fixons un tel polynôme $P(T, Y)$. que nous nous notons $P(\omega, T, Y)$ pour faire apparaître la dépendance en la variable ω. Comme les polynômes $P(\omega, T, Y)$ et $P'_Y(\omega, T, Y)$ sont premiers entre eux dans $k(\omega, T)[Y]$, il existe $A(\omega, T, Y), B(\omega, T, Y) \in k[\omega, T, Y]$ et $\varphi(\omega, T) \in k[\omega, T]$, $\varphi \neq 0$, tels que

$$A(\omega, T, Y)P(\omega, T, Y) + B(\omega, T, Y)P'_Y(\omega, T, Y) = \varphi(\omega, T)$$

Fixons une clôture algébrique $\overline{k(\omega, T)}$ de $k(\omega, T)$ et considérons une racine $y \in \overline{k(\omega, T)}$ de l'équation $P(\omega, T, y) = 0$. Pour tout $(\omega_0, t_0) \in \mathbb{A}^2(k)$ tel que $\varphi(\omega_0, t_0) \neq 0$, chaque racine $y_0 \in \overline{k}$ de $P(\omega_0, t_0, Y)$ vérifie $P'_Y(\omega_0, t_0, y_0) \neq 0$ et donc est une racine simple de $P(\omega_0, t_0, Y)$. D'après le lemme 1.9.4, lui-même

[4] Utiliser la proposition 2.3.2 du chapitre 2 : si K/k est une extension transcendante pure (plus généralement si $K \cap \overline{k} = k$) et si $P(Y) \in k[Y]$ est irréductible, alors $P(Y)$ est irréductible sur K.

cas particulier du lemme de Hensel (théorème 1.2.17), la fonction algébrique $y = y(\omega, T)$ a un développement dans $k(y_0)[[T - t_0, \omega - \omega_0]]$ de la forme

$$y = \sum_{i\geq 0} \sum_{j\geq 0} c_{ij}(\omega - \omega_0)^i (T - t_0)^j$$

où les coefficients c_{ij} sont dans $k(y_0)$.

Notons U l'ouvert de Zariski de $\mathbb{A}^2$ défini par $\varphi(\omega, t) \neq 0$. Soient $(\omega_0, t_0) \in U(k)$, $m \geq 1$ un entier, $\lambda_0 \in k$ et $t = t(\omega) = t_0 + \lambda_0(\omega - \omega_0)^m$. Supposons que $P(\omega, t(\omega), Y)$ a une racine $y_t = y_t(\omega) \in k(\omega)$, soit

$$P(\omega, t(\omega), y_t(\omega)) = 0$$

Comme l'anneau $k[\omega]$ est intégralement clos et que P est unitaire en Y, nécessairement $y_t \in k[\omega]$. Mais alors, en substituant ω_0 à ω, on obtient, en posant $y_0 = y_t(\omega_0)$

$$P(\omega_0, t_0, y_0) = 0$$

Soit $y = y(\omega, t) \in k[[T - t_0, \omega - \omega_0]]$ un développement en séries formelles associé à $(\omega_0, t_0) \in U$. En y substituant $t(\omega)$ à t, on obtient un développement dans $k[[\omega - \omega_0]]$ de y_t [(5)]

$$y_t = \sum_{i\geq 0} \sum_{j\geq 0} c_{ij}\lambda_0^j (\omega - \omega_0)^{i+mj} = \sum_{v=0}^{\infty} c_v(\lambda_0)(\omega - \omega_0)^v$$

où $c_v(\lambda_0)$ est la valeur en λ_0 du polynôme (en la variable λ)

$$c_v(\lambda) = \sum_h c_{v-mh,h}\lambda^h$$

lequel ne dépend que de y, t_0 et ω_0 mais pas de λ_0.

Le degré δ_0 par rapport à la variable ω du polynôme $P(\omega, t(\omega), Y)$ dépend *a priori* de λ_0, t_0 et ω_0 mais peut être majoré par une constante Δ_0 ne dépendant que de P et m (à savoir le degré par rapport à la variable ω du même polynôme mais avec λ_0, t_0 et ω_0 remplacés par des variables). Comme il y a un nombre infini de coefficients c_{ij} non nuls (sinon $y = y(\omega, T)$ serait une racine dans $k(\omega, T)$ de $P(\omega, T, y) = 0$), il existe $v_0 > \Delta_0$ tel que $c_{v_0}(\lambda) \neq 0$. Choisissons $\lambda_0 \in k$ en dehors de l'ensemble fini des racines de $c_{v_0}(\lambda)$. Si comme nous ne supposons,

$$y_t(\omega) = \sum_{v=0}^{\infty} c_v(\lambda_0)(\omega - \omega_0)^v$$

[(5)] Le développement obtenu dans $k[[\omega - \omega_0]]$ est bien un développement de y_t car son terme constant vaut $y_0 = y_t(\omega_0)$ (et que y_0 est une racine simple de $P(\omega_0, t_0, Y)$.

est un polynôme, alors il a un pôle d'ordre $\geq v_0$ au point ∞. Or la fonction $y_t(\omega)$, parce qu'elle satisfait $P(\omega, t(\omega), y_t(\omega)) = 0$, ne peut avoir de pôle au point ∞ d'ordre $> \delta_0$; plus précisément l'ordre du pôle en ∞ est inférieur ou égal au degré en $1/\omega$ du coefficient dominant q_n (dans $k[1/\omega]$) de tout polynôme $Q \in k[1/\omega, Y]$ satisfaisant $Q(y_t(\omega)) = 0$ [(6)]. On obtient donc la contradiction cherchée.

On peut conclure que, pour tout $(\omega_0, t_0) \in U$, pour tout entier $m \geq 1$ et pour tout $\lambda_0 \in k$ sauf un nombre fini, on a $t(\omega) = t_0 + \lambda_0(\omega - \omega_0)^m \in V'_P$. Si plusieurs polynômes $P_1, \ldots, P_n$ (satisfaisant les mêmes hypothèses que P) sont donnés et que $U_1, \ldots, U_n$ sont les ouverts de Zariski associés comme ci-dessus, on a que pour tout $(\omega_0, t_0) \in \bigcap_{i=1}^n U_i$, pour tout entier $m \geq 1$ et pour tout $\lambda_0 \in k$ sauf un nombre fini, on a $t(\omega) = t_0 + \lambda_0(\omega - \omega_0)^m \in V'_{P_1,\ldots,P_n}$. □

5.4. Corps hilbertiens et non hilbertiens : récapitulatif

5.4.1. Corps hilbertiens. —

5.4.1.1. Propriétés de conservation par extension. — L'énoncé suivant récapitule les résultats obtenus. Les énoncés (a), (b) et (c) s'obtiennent en joignant les théorèmes 2.2.4, 5.2.1 et 5.3.1 ; (c) et (d) reprennent les théorèmes de Haran, Weissauer et Kuyk vus au §5.2.2 .

Théorème 5.4.1. — (a) *Toute extension de type fini d'un corps hilbertien est un corps hilbertien.*

(b) *Tout corps de type fini sur $\mathbb{Q}$ est un corps hilbertien.*

(c) *Toute extension transcendante (de degré de transcendance > 0) de type fini d'un corps quelconque est un corps hilbertien.*

(d) *Toute extension abélienne K d'un corps hilbertien k est un corps hilbertien.*

(e) *Soient k un corps hilbertien, K_1/k et K_2/k deux extensions galoisiennes de K. Soit K un corps intermédiaire entre k et le compositum K_1K_2 tel que K ne soit contenu ni dans K_1 ni dans K_2. Alors K est un corps hilbertien.*

Nous donnons en complément, sans démonstration, d'autres exemples de corps hilbertiens.

[(6)] Déduire de $Q(y_t(\omega)) = 0$ que, si $\mathrm{ord}_\infty(y_t) < 0$, alors $\mathrm{ord}_\infty(q_n y_t^n) \geq \mathrm{ord}_\infty(y_t^{n-1})$, ce qui donne $\mathrm{ord}_\infty(y_t) \leq -\mathrm{ord}_\infty(q_n) \leq \delta_0$.

5.4.1.2. Corps avec une formule du produit. — Soit K un corps. Une valeur absolue v sur K est dite *bien se comporter avec les extensions finies* si pour toute extension finie E/K, on a $[E : K] = \sum_{w/v}[E_w/K_v]$. Elle est dite *propre* si de plus, elle est non-triviale et si, dans le cas où K est de caractéristique 0, sa restriction à $\mathbb{Q}$ est soit triviale, soit la valeur absolue usuelle, soit la valeur absolue p-adique pour un nombre premier p (normalisée de telle sorte que $|p|_p = p^{-1}$).

Définition 5.4.2. — Supposons qu'il existe un ensemble M_K de valeurs absolues *propres* de K satisfaisant les propriétés suivantes :
(i) Deux valeurs absolues distinctes dans M_K sont non équivalentes (*i.e.*, induisent des topologies non équivalentes sur K, voir §1.2.2.4).
(ii) pour tout $x \in K$, on a $|x|_v = 1$ pour tout $v \in M_K$ sauf un nombre fini.
(iii) Il existe une famille $(d_v)_{v\in M_K}$ d'entiers $d_v > 0$ telle que pour tout $x \in K$, $x \neq 0$, on a $\prod_{v\in M_K} |x|_v^{d_v} = 1$.
On dit alors que K est un corps avec une *formule du produit*.

Exemple 5.4.3. — (1) Le corps $\mathbb{Q}$ est un corps avec une formule du produit pour $M_{\mathbb{Q}}$ l'ensemble de toutes les valeurs abolues $|\ |_p$ de $\mathbb{Q}$ $p = \infty$) (normalisées de façon usuelle). Pour tout $x \in \mathbb{Q}$, $x \neq 0$, on a $\prod_{p\in M_{\mathbb{Q}}} |x|_p = 1$.

(2) Le corps $k(T)$ avec k corps arbitraire est un autre exemple. Pour tout polynôme irréductible $P \in k[T]$, la valuation P-adique associée (§1.2.2.3) définit une valeur absolue qu'on normalise en posant $|P|_P = c^{-\deg(P)}$ où $c > 1$ est un nombre réel fixé. On définit aussi la valeur absolue *infinie* par $|f/g|_\infty = c^{\deg(f)-\deg(g)}$ $(f, g \in k[T])$. Notons $M_{k(T)}$ l'ensemble de ces valeurs absolues sur $k(T)$. Pour tout $x \in k(T)$, $x \neq 0$, on a $\prod_{v\in M_{k(T)}} |x|_v = 1$.

(3) On montre que toute extension finie d'un corps avec une formule du produit est un corps avec une formule du produit. En conséquence, les corps de nombres, les extensions transcendantes (de degré de transcendance > 0) de type fini d'un corps quelconque sont des corps avec une formule du produit. Voir [**Lan83**, chapter 2], [**FJ04**, §15.3] pour plus de détails.

Pour les corps avec une formule du produit, on a le résultat suivant, dû à Weissauer [**FJ04**, §15.3].

Théorème 5.4.4. — *Tout corps muni d'une formule du produit est un corps séparablement hilbertien.*

Ce résultat contient les énoncés (b) et (c) du théorème 5.4.1 sur les corps de type fini sur $\mathbb{Q}$ et les extensions transecendantes pures de type fini sur un corps.

Il redonne en particulier que tout corps global (*i.e.*, soit un corps de nombres, soit une extension de type fini d'un corps fini de degré de transcendance 1) est un corps hilbertien.

5.4.1.3. Corps de séries formelles.— Si k est un corps arbitraire, l'anneau $k[[X_1, \dots, X_n]]$ des séries formelles en les indéterminées $X_1, \dots, X_n$ et à coefficients dans k (§1.2.15) un anneau local intègre. Son corps des fractions, le corps des séries formelles, se note $k((X_1, \dots, X_n))$.

***Théorème 5.4.5* (Weissauer).** — *Si $n \geq 2$, le corps des séries formelles $k((X_1, \dots, X_n))$ est un corps hilbertien.*

Nous renvoyons à [**FJ04**, §15.4]. Rappelons que le corps $k((X))$ ($n = 1$) est un corps hensélien (pour la valuation discrète X-adique) et donc n'est pas hilbertien.

5.4.2. Corps non hilbertiens. — Les corps ci-dessous ne sont pas des corps hilbertiens.

• les corps algébriquement clos.

• le corps $\mathbb{R}$ des nombres réels et les corps $\mathbb{Q}_p$ des nombres p-adiques, et plus généralement les corps henséliens pour une valuation (exemple 5.0.1).

• le corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques totalement réels : pour $P(T, Y) = Y^2 - 1 - T^2$, on a $H_P = \emptyset$.

• pour tout nombre premier p, le corps $\mathbb{Q}^{\mathrm{t}p}$ des nombres algébriques totalement p-adiques, défini comme l'ensemble de tous les nombres algébriques dont tous les conjugués sont dans (une copie fixée de) $\mathbb{Q}_p$, ou de façon équivalente comme la plus grande extension galoisienne de $\mathbb{Q}$ contenue dans $\mathbb{Q}_p$. Pour $P(T, Y) = Y^2 - pT/(T+1) - 1$ si $p \neq 2$ et $P(T, Y) = Y^3 - 2T/(T+1) - 1$ si $p = 2$, on a $H_P = \emptyset$ (voir exemple 5.0.1).

• la clôture pythagoricienne d'un corps. Un corps k est dit *pythagoricien* si toute somme de deux carrés dans k est un carré dans k. L'intersection de toutes les extensions algébriques pythagoriciennes d'un corps k_0 est un corps pythagoricien appelé clôture pythagoricienne de k_0. Si $P(T, Y) = Y^2 - T^2 - 1$, alors $H_P = \emptyset$. On peut généraliser cela aux clôtures *p-fermattiennes* (remplacer 2 par p), qui ne sont pas non plus des corps hilbertiens [**Des01**].

• pour tout nombre premier p, tout corps k et tout polynôme $q(T) \in k[T] \setminus k$, le corps obtenu comme réunion dans $\overline{k}$ des corps k_n définis inductivement par : $k_0 = k$ et k_{n+1} est le corps engendré sur k_n par toutes les racines p-ièmes des éléments $q(t)$ où t décrit k_n. Pour $P(T, Y) = Y^p - q(T)$, on a $H_P = \emptyset$.

5.5. Application à la recherche de courbes elliptiques de rang élevé

L'application principale du théorème d'irréductibilité de Hilbert concerne la théorie de Galois. Grâce aux théorèmes de spécialisation du chapitre 1 (théorème 1.9.1 et 1.9.3), on sait que, si $N/k(\mathbf{T})$ est une extension galoisienne finie de groupe G et que k est un corps hilbertien, alors il existe un point $\mathbf{t}_0 \in \mathbb{A}^r(k)$ (il en existe en fait un ensemble Zariski-dense) tel que l'extension résiduelle (ou spécialisée) $N_{\mathbf{t}_0}/k$ est également galoisienne de groupe G.

Cet argument est un ingrédient fondamental de l'approche moderne du Problème Inverse de Galois. Nous renvoyons aux chapitres 2 et au chapitre 4 où cette application est développée. Nous allons donner d'autres applications du théorème d'irréductibilité de Hilbert :
- à la recherche de courbes elliptiques de rang élevé, dans cette section,
- à la géométrie, dans la section suivante,
- à la factorisation des polynômes, dans le chapitre suivante (§6.6).

5.5.1. Théorème de Mordell-Weil. — Pour cette sous-section, nous renvoyons à [**Sil86**] pour plus de détails.

Il y a diverses définitions de la notion de *courbe elliptique* sur un corps K. Nous partirons ici du *modèle de Weierstrass* : pour un corps K de caractéristique différente de 2 et 3 [(7)], une courbe elliptique E sur K peut être définie comme une courbe projective d'équation

$$y^2z = x^3 - g_2xz^2 - g_3z^3$$

où g_2, g_3 sont deux éléments de K tels que le polynôme $x^3 - g_2x - g_3$ a 3 racines distinctes, *i.e.*, $4g_2^3 - 27g_3^2 \neq 0$. Pour $z = 1$, on obtient une *équation affine* de la courbe elliptique : $E' : y^2 = x^3 - g_2x - g_3$. Pour $z = 0$, on obtient le seul point à l'infini de E : le point $(0, 1, 0)$, noté ∞. On a donc, ensemblistement,

$$E = \mathrm{Spec}(K[X, Y]/(y^2 - (x^3 - g_2x - g_3)) \cup \{\infty\}$$

La condition sur g_2, g_3 est équivalente à la lissité de la partie affine. Le point ∞ est également un point lisse de E : un ouvert affine contenant ∞ est d'équation $z = x^3 - g_2xz - g_3z^3$, avec $x(\infty) = z(\infty) = 0$. La courbe elliptique E est donc une *cubique projective lisse*; cela peut être une définition possible des courbes elliptiques : *via* des transformations élémentaires, on montre que toute cubique lisse projective a un modèle de Weierstrass comme ci-dessus (pour K de caractéristique $\neq 2, 3$).

(7) Pour les caractéristiques 2 et 3, il existe aussi des modèles de Weierstrass mais les équations sont plus compliquées (*cf.* [**Sil86**]).

Il existe une loi de groupe sur $E(K) = E'(K) \cup \{\infty\}$. Elle est définie de la façon suivante. Pour $a, b \in E'(K) \subset \mathbb{A}^2(K)$, il existe un unique troisième point $c(x, y) \in E(K)$ sur la droite passant par a et b ; le point $a + b$ est alors défini comme le point de coordonnées $(x, -y)$, *i.e.*, le symétrique de c par rapport à l'axe des x. Cette définition demande quelques ajustements : par exemple, quand $a = b$, par droite passant par a et b, il faut comprendre la tangente à a ; si la droite (ab) est parallèle à l'axe Oy et ne coupe pas $E'(K)$ en un troisième autre point, on prend $c = \infty$ et $a+b = \infty$, etc. Le point ∞ est l'élément neutre de cette loi et, pour tout point $a = (x, y) \in E'(K)$, l'élément symétrique est le point $-a = (x, -y)$. On note additivement cette loi, qui est commutative. Il existe des définitions plus intrinsèques de la loi.

On peut écrire explicitement les formules d'addition pour cette loi. Elles sont données par des fractions rationnelles en les coordonnées des points a et b à coefficients dans $Q(g_1, g_2)$ (où Q est le corps premier). On montre qu'elles définissent un morphisme algébrique $E \times E \to E$.

Muni de cette loi, l'ensemble $E(K)$ a une structure de groupe. Le théorème de Mordell-Weil qui donne la structure de ce groupe est un résultat central de la géométrie diophantienne. Voir par exemple [**Lan83**, chapter 6].

Théorème 5.5.1. — *Si K est un corps de type fini sur son corps premier, alors, $E(K)$ est un groupe abélien de type fini. C'est-à-dire, il existe r points $a_1, \dots, a_r \in E(K)$ linéairement indépendants sur $\mathbb{Z}$ tels que*

$$E(K) = \mathrm{Tor}(E(K)) + \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_r$$

où $\mathrm{Tor}(E(K))$ est le sous-groupe (fini) de torsion de $E(K)$.

L'entier $r \geq 0$ est appelé le *rang* de la courbe elliptique sur K et noté $\mathrm{rg}_K(E)$. Un problème classique est de demander s'il existe des courbes elliptiques sur $\mathbb{Q}$ de rang arbitrairement grand. Le record actuel ne dépasse pas 30.

Pour trouver des courbes elliptiques de rang élevé, la stratégie est de construire des courbes elliptiques sur le corps $\mathbb{Q}(X_1, \dots, X_N)$ et de *spécialiser* ensuite les indéterminées $X_1, \dots, X_N$ dans $\mathbb{Q}$. Nous allons montrer en utilisant le théorème d'irréductibilité de Hilbert qu'il existe des spécialisations pour lesquelles le rang ne chute pas.

5.5.2. Spécialisation. — Supposons donnée une courbe elliptique E sur un corps $K = k(X_1, \dots, X_N)$ avec k de type fini sur son corps premier (de caractéristique $\neq 2, 3$), *i.e.*, une cubique projective lisse d'équation

$$y^2 z = x^3 - g_2(\mathbf{X})xz^2 - g_3(\mathbf{X})z^3$$

avec $g_2(\mathbf{X}), g_3(\mathbf{X}) \in k(\mathbf{X})$. Notons U l'ouvert de $\mathbb{A}^r_k$ défini par les conditions : $g_2(\mathbf{x})$ et $g_3(\mathbf{x})$ sont définis, $4g_2(\mathbf{x})^3 - 27g_3(\mathbf{x})^2 \neq 0$ et les formules d'addition sur E se spécialisent en $\mathbf{x}$. Pour tout $\mathbf{x} \in U(k)$, l'équation $y^2z = x^3 - g_2(\mathbf{x})xz^2 - g_3(\mathbf{x})z^3$ définit une courbe elliptique $E_\mathbf{x}$ sur k et les formules d'addition sur $E_\mathbf{x}$ s'obtiennent par spécialisation à partir de celles sur E.

Posons $G = E(K)$ [resp. $G' = E'(K)$] et $G_\mathbf{x} = E_\mathbf{x}(k)$ [resp. $G'_\mathbf{x} = E'_\mathbf{x}(k)$]. Pour tout $a = (x, y) \in G'$ tel que les coordonnées affines $x, y \in K = k(X_1, \ldots, X_N)$ se spécialisent en $\mathbf{x}$, *i.e.*, dont $\mathbf{x}$ n'est pas un pôle, le point spécialisé $a(\mathbf{x})$ est un point de $G'_\mathbf{x}$. De plus, les formules d'addition (telles que données dans [**Sil86**, pp.58-59] par exemple) donnent que

(*) *si les coordonnées de $a, b \in G'$ se spécialisent en $\mathbf{x}$ et si $a(\mathbf{x}) \neq \pm b(\mathbf{x})$, alors $(a+b)(\mathbf{x}) = a(\mathbf{x}) + b(\mathbf{x})$. D'autre part, si $2a \neq \infty$ et si les coordonnées de $2a$ se spécialisent en $\mathbf{x}$, alors $(2a)(\mathbf{x}) = 2a(\mathbf{x})$. Si $2a = \infty$ alors $2a(\mathbf{x}) = \infty$; plus généralement, si $ka = \infty$, alors $ka(\mathbf{x}) = \infty$.*

Expliquons comment définir un *morphisme de spécialisation*

$$\varphi_\mathbf{x} : G \to G_\mathbf{x}$$

On écrit une décomposition du groupe abélien de type fini G en somme de sous-groupes monogènes et on choisit un générateur de chacun des facteurs. Quitte à retirer à U un autre fermé propre de Zariski, on peut supposer que les coordonnées affines de ces générateurs $g_1, \ldots, g_N \in G'$ se spécialisent, pour induire des points de $G'_\mathbf{x}$ pour tout $\mathbf{x} \in U$. On peut aussi supposer que tous les multiples kg_i ($k \in \mathbb{Z}$) distincts de ∞ de ceux de ces générateurs qui sont d'ordre fini se spécialisent en $\mathbf{x}$ et qu'alors $(kg_i)(\mathbf{x}) = kg_i(\mathbf{x})$. Cela entraîne que les générateurs d'ordre fini se spécialisent nécessairement en des éléments de $G_\mathbf{x}$ d'ordre inférieur, et en fait égal (puisque $(kg_i)(\mathbf{x}) \in G'_\mathbf{x} \Rightarrow (kg_i)(\mathbf{x}) \neq 0$). L'application de spécialisation définie sur les générateurs $g_1, \ldots, g_N$ se prolonge alors en un *homomorphisme* de spécialisation $\varphi_\mathbf{x} : G \to G_\mathbf{x}$. De plus, on vérifie que, pour tout $a \in G'$, si $\mathbf{x}$ n'est pas un pôle des coordonnées affines de a et si donc a induit un point $a(\mathbf{x}) \in G'_\mathbf{x}$ par spécialisation, alors $a(\mathbf{x}) = \varphi_\mathbf{x}(a)$.

***Théorème 5.5.2* (Néron).** — *Supposons en plus k de caractéristique 0. Alors il existe une partie hilbertienne H de K^r et un ouvert de Zariski non vide $V \subset U$ tels que pour tout $\mathbf{x} \in H \cap V$, on a $\mathrm{rg}_k(E_\mathbf{x}) \geq \mathrm{rg}_K(E)$. En particulier, si k est un corps hilbertien, il existe des courbes elliptiques $E_\mathbf{x}$ sur k de rang $\geq \mathrm{rg}_K(E)$.*

Démonstration. — Considérons l'ensemble T de tous les points $a \in \mathrm{Tor}(G) \setminus \{\infty\}$. On a $T \subset G \setminus \{\infty\}$. On a supposé plus haut qu'aucun point $\mathbf{x} \in U$ n'est

un pôle d'une coordonnée affine d'un point de T. Le morphisme $\varphi_{\mathbf{x}}$ est alors injectif sur $\mathrm{Tor}(G)$. Le noyau $\ker(\varphi_{\mathbf{x}})$, qui est un groupe abélien de type fini (comme sous-groupe de G qui est abélien de type fini), est donc sans torsion. Le reste de la preuve consiste à montrer que, pour $\mathbf{x}$ dans une certaine partie hilbertienne H, on a $\ker(\varphi_{\mathbf{x}}) = 2\ker(\varphi_{\mathbf{x}})$; cela entraînera $\ker(\varphi_{\mathbf{x}}) = \{0\}$ et donc l'inégalité annoncée sur les rangs.

Nous utiliserons le fait suivant de la théorie des courbes elliptiques [**Sil86**, p.89] :

(*) *Etant donnée une courbe elliptique ϵ sur un corps κ, si $\alpha \in \epsilon(\overline{\kappa})$ et $n \geq 1$ est un entier premier à la caractéristique de κ, alors il existe exactement n^2 points distincts $\alpha_1, \ldots \alpha_{n^2} \in \epsilon(\overline{\kappa})$ tels que $n\alpha_i = \alpha$, $i = 1, \ldots, n^2$.*

et celui-ci qu'on va déduire du lemme 1.7.3

(**) *Etant donné un sous-ensemble fini $F \subset E'(\overline{K})$, notons A_F l'anneau engendré sur $k[\mathbf{X}]$ par l'ensemble $\mathcal{F}$ des coordonnées affines des points de F. Alors, pour tout $\mathbf{x}$ dans un ouvert de Zariski $V_F \subset U$, le morphisme de spécialisation $k[\mathbf{X}] \to \overline{k}$ envoyant $\mathbf{X}$ sur $\mathbf{x}$ se prolonge en un morphisme $\widetilde{\varphi}^F_{\mathbf{x}} : A_F \to \overline{k}$. De plus, si $K(F)$ désigne le corps des fractions de A_F, le morphisme d'anneau $\widetilde{\varphi}^F_{\mathbf{x}}$ induit un morphisme de groupe $\widetilde{\varphi}^F_{\mathbf{x}} : E(K(F)) \to E_{\mathbf{x}}(\overline{k})$, qui est injectif sur F.*

Pour démontrer (**), on note d'abord que, quitte à grossir F, on peut supposer que $\mathcal{F}$ consiste en une réunion finie d'ensembles d'éléments K-conjugués de $\overline{K}$, *i.e.*, d'orbites sous $\mathrm{Gal}(\overline{K}/K)$. Chacune de ces orbites correspond à un polynôme irréductible dans $k(\mathbf{X})[Y]$ et sans racine multiple dans $\overline{k(\mathbf{X})}$ (à savoir le polynôme minimal commun de tous les éléments dans l'orbite). Le lemme 1.7.3 fournit le morphisme $\widetilde{\varphi}^F_{\mathbf{x}} : A_F \to \overline{k}$. On en déduit le morphisme $E(K(F)) \to E_{\mathbf{x}}(\overline{k})$ de la même façon que plus haut on a construit $\varphi_{\mathbf{x}} : G \to G_{\mathbf{x}}$: il s'agit seulement d'étendre la construction à l'extension finie $K(F)$ de K.

Le morphisme $\varphi_{\mathbf{x}} : G \to G_{\mathbf{x}}$ induit un morphisme

$$\overline{\varphi}_{\mathbf{x}} : G/2G \to G_{\mathbf{x}}/2G_{\mathbf{x}}$$

L'ensemble $G/2G$ est fini (en conséquence de Mordell-Weil). Pour tout $\bar{a} \in G/2G$ non nul, choisissons un représentant $a \in G \setminus 2G$ de $\bar{a}$. Notons F_2 l'ensemble fini de tous les points $a_i \in E(\overline{K})$, tels que $2a_i = a$, $i = 1, \ldots, 4$, où $\bar{a}$ décrit $G/2G \setminus \{0\}$. Supposons ensuite que $\mathbf{x}$ soit dans l'ouvert V_{F_2} et considérons un morphisme $\widetilde{\varphi}^{F_2}_{\mathbf{x}} : A_{F_2} \to \overline{k}$ comme dans (**) ci-dessus. Pour tout $\bar{a} \in G/2G$ non nul, comme $a \notin 2G$, pour tout $i = 1, \ldots, 4$, l'une des

deux coordonnées affines de a_i, disons $\xi_i^{\bar{a}}$, n'est pas dans $k(\mathbf{X})$. Notons H_2 la partie hilbertienne de k^r associée à l'ensemble des polynômes minimaux sur $k(\mathbf{X})$ des $\xi_i^{\bar{a}}$, $i = 1, \ldots, 4$, $\bar{a} \in G/2G \setminus \{0\}$. Soit $\mathbf{x} \in H_2 \cap V_{F_2}$. Pour tout $\bar{a} \in G/2G$ non nul, les éléments $\widetilde{\varphi}_{\mathbf{x}}^{F_2}(a_i)$, $i = 1, \ldots, 4$, sont les 4 points de $E_{\mathbf{x}}(\overline{k})$ qui donnent $\varphi_x(a)$ par multiplication par 2, et aucun d'eux n'est dans $E_{\mathbf{x}}(k)$, et donc, $\varphi_x(a) \notin 2G_{\mathbf{x}}$. Conclusion : pour $\mathbf{x} \in H_2 \cap V_{F_2}$, le morphisme $\overline{\varphi}_{\mathbf{x}}$ est injectif.

Notons G_2 [resp. $G_{\mathbf{x},2}$] l'ensemble des points de 2-torsion dans G [resp. $G_{\mathbf{x}}$]. Le morphisme $\varphi_{\mathbf{x}}$ induit un morphisme

$$\varphi_{\mathbf{x}} : G_2 \to G_{\mathbf{x},2}$$

Comme $G_2 \subset \mathrm{Tor}(G)$, ce morphisme est injectif. Nous allons voir que, pour $\mathbf{x}$ convenablement choisi, c'est un isomorphisme. Notons $E_2' = E_2'(\overline{K})$ l'ensemble des 3 points de 2-torsion non triviaux $\infty_i \in E(\overline{K})$, $i = 1, 2, 3$ (notation comme dans (*)). Supposons ensuite que $\mathbf{x}$ soit dans l'ouvert $V_{E_2'}$ et considérons un morphisme $\widetilde{\varphi}_{\mathbf{x}}^{E_2'} : A_{E_2'} \to \overline{k}$ comme dans (**) ci-dessus. Le morphisme induit $\widetilde{\varphi}_{\mathbf{x}}^{E_2'} : E_2' \cup \{\infty\} \to (E_{\mathbf{x}})_2(\overline{k})$ à valeur dans le groupe des 4 points de 2-torsion de $E_{\mathbf{x}}(\overline{k})$ est une bijection : il est injectif d'après (**) et les deux ensembles ont même cardinal. Comme dans le paragraphe ci-dessus, on peut construire une partie hibertienne H_2' telle que pour tout $\mathbf{x} \in H_2' \cap V_{E_2'}$, si $\infty_i \notin E(K)$, alors $\widetilde{\varphi}_{\mathbf{x}}^{E_2}(\infty_i) \notin E_{\mathbf{x}}(k)$ $(i = 1, \ldots, 3)$. Conclusion : pour $\mathbf{x} \in H_2' \cap V_{E_2}$, le morphisme $\varphi_{\mathbf{x}} : G_2 \to G_{\mathbf{x},2}$ est surjectif ; et l'injectivité résulte de celle de $\widetilde{\varphi}_{\mathbf{x}}^{E_2'} : E_2' \cup \{\infty\} \to (E_{\mathbf{x}})_2(\overline{k})$.

Posons alors $V = V_{F_2} \cap V_{E_2'}$ et $H = H_2 \cap H_2'$. Soit $\mathbf{x} \in V \cap H$. Soit u dans le noyau $\ker(\varphi_x)$ du morphisme $\varphi_{\mathbf{x}} : G \to G_{\mathbf{x}}$. On a alors $\varphi_{\mathbf{x}}(u) = 0 \in 2G_{\mathbf{x}}$. D'après ce qui précède, on peut écrire $u = 2v$ avec $v \in G$. Mais alors de $\varphi_{\mathbf{x}}(u) = 0$, on déduit que $\varphi_{\mathbf{x}}(v) \in G_{\mathbf{x},2}$. D'après le paragraphe précédent, il existe $v' \in G_2$ tel que $\varphi_{\mathbf{x}}(v) = \varphi_{\mathbf{x}}(v')$. Mais alors on a $2(v - v') = u \in 2\ker(\varphi_x)$. On a donc bien montré que $\ker(\varphi_x) = 2\ker(\varphi_x)$, ce qui nous restait à établir pour démontrer le théorème 5.5.2. □

5.5.3. Courbes elliptiques de rang ≥ 9. — Le résultat suivant est dû à Néron. Nous renvoyons à [**Ser97**] pour plus de détails sur la preuve que nous esquissons ci-dessous.

Théorème 5.5.3. — *Il existe des courbes elliptiques sur $\mathbb{Q}$ de rang ≥ 9.*

Démonstration. — On part de 9 points $A_i = (X_i, Y_i)$ $(i = 1, \ldots, 9)$ du plan affine $\mathbb{A}^2$, dont les coordonnées sont 18 indéterminées (algébriquement

indépendantes sur $\overline{\mathbb{Q}}$). ll existe une unique cubique projective E passant par ces 18 points : cette condition définit en effet 9 équations en les $10 - 1 = 9$ coefficients d'une cubique donnée *a priori*, à constante multiplicative près ; le système linéaire est cramérien.

Soit K_0 le corps de définition de E, c'est-à-dire, le corps engendré sur $\mathbb{Q}$ par les 9 coefficients définissant l'équation de E. On a *a priori* $K_0 \subset K = \mathbb{Q}(X_1, Y_1, \ldots, X_9, Y_9)$. Par construction, les points $A_1, \ldots, A_9$ sont 9 points K-rationnels sur E.

Notons m [resp. n] le degré de transcendance de K_0 sur $\mathbb{Q}$ [resp. le degré de transcendance de K sur K_0]. On a

• $m \leq 9$: le corps K_0 est engendré sur $\mathbb{Q}$ par 9 coefficients,

• $n \leq 9$: le corps $K_0(X_i, Y_i)$ est de degré de transcendance 1 sur K_0, pour chaque $i = 1, \ldots, 9$,

• $m+n = 18$: $m+n$ est le degré de transcendance sur $\mathbb{Q}$ de $\mathbb{Q}(X_1, Y_1, \ldots, X_9, Y_9)$.

On obtient donc $m = n = 9$.

De $m = 9$ on déduit que E est la cubique "générique", c'est-à-dire celle dont les 9 coefficients donnés à constante multiplicative près sont 9 indéterminées ; en particulier, la cubique E est lisse et définit une courbe elliptique sur le corps K_0. De $n = 9$, on déduit que les 9 points $A_1, \ldots, A_9$ sont $\mathbb{Z}$-linéairement indépendants comme K-points de la K_0-courbe elliptique E. On a donc $\mathrm{rg}_K(E_K) \geq 9$ (où $E_K = E \otimes_{K_0} K$ est la K-courbe elliptique obtenue par extension des scalaires de K_0 à E). La conclusion souhaitée s'obtient alors par spécialisation du corps K dans $\mathbb{Q}$, grâce au théorème 5.5.2. □

5.6. Application à la géométrie

5.6.1. Fibres irréductibles d'un morphisme fini. — Soient B un anneau intègre et A un sous-anneau tels que B soit un A-module de type fini. On suppose de plus que A (et donc B aussi) est une algèbre de type fini sur un corps k parfait. On suppose aussi que B (et donc A aussi) est géométriquement intègre. Géométriquement, cela revient à se donner un morphisme fini $f : V \to U$ entre deux k-schémas affines de type fini géométriquement intègres. La correspondance se fait en posant $V = \mathrm{Spec}(B)$ et $U = \mathrm{Spec}(A)$; f est le morphisme de restriction. Pour tout corps k' contenant k, on pose $V_{k'} = \mathrm{Spec}(B \otimes_k k')$ et $U_{k'} = \mathrm{Spec}(A \otimes_k k')$ et $f_{k'} : V_{k'} \to U_{k'}$ le morphisme de restriction.

Soit a un point fermé de $U_{\overline{k}}$ (un point géométrique). On sait (1.8.2) que ce point est déterminé par (*i.e.*, est le seul au-dessus de) sa restriction à $U_{k(a)}$.

On dira que *la fibre $f^{-1}(a)$ est irréductible sur le corps $k(a)$* s'il n'existe qu'un seul point (fermé) b de $V_{k(a)}$ au-dessus de a vu comme point fermé de $U_{k(a)}$. Cela revient à dire que les points géométriques de V au-dessus de b sont $k(a)$-conjugués (proposition 1.8.10).

Proposition 5.6.1. — *Supposons que k soit un corps hilbertien de caractéristique 0. Alors l'ensemble des points géométriques $a \in U_{\overline{k}}$ tels que la fibre $f^{-1}(a)$ est irréductible sur $k(a)$, est Zariski-dense dans U.*

Remarque 5.6.2. — Pour A de la forme $A = k[T_1, \ldots, T_r]$, la proposition 5.6.1 résulte immédiatement de la définition de "k hilbertien". De plus, on a dans ce cas une conclusion plus forte : "points géométriques $a \in U_{\overline{k}}$" peut être remplacé par "points fermés *k-rationnels* $a \in U$".

Démonstration. — Notons $k(U)$ et $k(V)$ les corps de fonctions de U et V : $k(U) = \mathrm{Frac}(A)$ et $k(V) = \mathrm{Frac}(B)$. Soient $\mathbf{T} = \{T_1, \ldots, T_r\} \subset k(V)$ une base de transcendance de $k(V)$ sur k et y un élément primitif de l'extension finie (séparable[8]) $k(V)/k(\mathbf{T})$; on peut aussi choisir y entier sur $k[\mathbf{T}]$. Notons $p(\mathbf{T}, Y) \in k[\mathbf{T}, Y]$ le polynôme minimal de y sur $\Omega = k(\mathbf{T})$.

Pour démontrer le résultat on peut remplacer U par un ouvert U' et V par son image réciproque V' par f. Notons $\Delta \in k[\mathbf{T}]$ le discriminant de la $k(\mathbf{T})$-base $1, y, \ldots, y^{N-1}$ de $k(V)$ (où $N = [k(V) : k(\mathbf{T})]$). D'après le théorème 1.3.15, le localisé B_{Δ^∞} coincide avec la fermeture intégrale de $k[\mathbf{T}]_{\Delta^\infty}$ dans $k(V)$. Quitte à remplacer V par l'ouvert $V' = \mathrm{Spec}(B_{\Delta^\infty})$, U par $U' = \mathrm{Spec}(A_{\Delta^\infty})$ et $k[\mathbf{T}]$ par $k[\mathbf{T}]_{\Delta^\infty}$, on peut supposer que B est égal à la fermeture intégrale de Ω dans $k(V)$.

D'après le théorème 1.9.1 (ou le théorème 1.9.3), il existe une partie hilbertienne H_P et un ouvert de Zariski non vide O de k^r tels que, pour tout $\mathbf{t} \in H_P \cap O$, il n'existe qu'un seul idéal maximal $\mathcal{Q}$ de B au-dessus de $\mathbf{t}$ lequel vérifie $[B/\mathcal{Q} : k] = [k(V) : k(\mathbf{T})]$. *A fortiori*, $\mathcal{Q} \cap A$ est le seul idéal maximal

[8] L'extension est séparable car on est en caractéristique 0. Plus généralement, cela est vrai sous l'hypothèse "k parfait". Si on veut se dispenser de cette hypothèse (que nous faisons ici pour être en cohérence avec le §1.8.2), on peut supposer seulement que l'extension $k(V)/k$ est séparable au sens des extensions de type fini (*e.g.* [**Lan78**, chapter X §6]), c'est-à-dire, qu'elle admet une base de transcendance $\mathbf{T}$ *séparante*, *i.e.*, telle que, comme ci-dessus, $k(V)/k(\mathbf{T})$ soit séparable. Or, cette hypothèse est en fait contenue dans l'hypothèse "B géométriquement intègre" (proposition 1.8.9). Outre l'existence d'un élément primitif pour l'extension $k(V)/k(\mathbf{T})$, la séparabilité est utilisée pour garantir l'existence d'une clôture galoisienne et donc pouvoir se placer dans la situation des théorèmes 1.9.1 et 1.9.3.

de A au-dessus de $\mathbf{t}$ et on a $[A/(\mathcal{Q}\cap A) : k] = [k(U) : k(\mathbf{T})]$. On en déduit que $[B/\mathcal{Q} : (\mathcal{Q}\cap A)] = [k(V) : k(U)]$.

Notons a un point géométrique sur $U_{\overline{k}}$ au-dessus de $\mathcal{Q}\cap A \in U$. Soit $\mathcal{P}$ un idéal maximal de $V_{k(a)}$ au-dessus de a (vu comme point de $U_{k(a)}$), et donc au-dessus de $\mathcal{Q} \in V$. Le corps résiduel de $\mathcal{P}$ s'obtient à partir de celui de $\mathcal{Q}$ par extension des scalaires à $k(a)$. Comme $k(a) = A/(\mathcal{Q}\cap A)$ est contenu dans $B/\mathcal{Q}$, on obtient que $(B \otimes_k k(a))/\mathcal{P}$ est de degré $[k(V) : k(U)]$ sur $k(a)$. Comme U et V sont géométriquement intègres, ce degré vaut aussi $[k(a)(V) : k(a)(U)]$. Conclusion : il n'existe qu'un seul point (fermé) b de $V_{k(a)}$ au-dessus de a vu comme point fermé de $U_{k(a)}$ (car la somme des degrés résiduels est $\leq [k(a)(V) : k(a)(U)]$ (*cf.* remarque 1.9.2)).

L'ensemble des points géométriques a obtenus de cette façon est Zariski-dense puisque ce sont tous les points fermés de $U_{\overline{k}}$ au-dessus d'un point $\mathbf{t}$ de l'ensemble $H_P \cap O$, lequel est Zariski-dense. □

Remarque 5.6.3. — Dans la preuve on montre le fait suivant qui mérite d'être dégagé :

(*) *Pour tout $a \in U_{\overline{k}}$ sauf dans un fermé propre de Zariski, la fibre $f^{-1}(a)$ est irréductible sur $k(a)$ si et seulement si les points géométriques $\overline{b} \in V_{\overline{k}}$ au-dessus de a sont de degré sur $k(a)$ égal à $[k(V) : k(U)]$ (ils sont alors automatiquement $k(a)$-conjugués).*

5.6.2. Corps de définition des schémas affines. — Soit A un anneau qui est aussi une algèbre sur un corps parfait k, de type fini. De façon équivalente, $U = \mathrm{Spec}(A)$ est un k-schéma affine de type fini.

Proposition 5.6.4. — *Supposons que k soit un corps hilbertien et que U soit géométriquement intègre. Alors si F est une extension finie de k telle que $F \subset k(a)$ pour tout point fermé de U, alors nécessairement $F = k$. En conséquence, l'intersection des corps de définition des points fermés de U est le corps k.*

Ce résultat devient faux si k n'est pas supposé hilbertien : toute courbe affine définie sur $k = \mathbb{R}$ qui n'a pas de points réels fournit un contre-exemple.

Démonstration. — Soient $\mathbf{T} = \{T_1, \ldots, T_r\} \subset k(U)$ une base de transcendance de $k(U)$ sur k et y un élément primitif entier (sur $k[\mathbf{T}]$) de l'extension finie séparable $k(U)/k(\mathbf{T})$. Notons $p(\mathbf{T}, Y) \in k[\mathbf{T}, Y]$ le polynôme minimal de y sur $k(\mathbf{T})$. De l'hypothèse "A géométriquement intègre, il découle que p est absolument irréductible, *i.e.*, irréductible dans $\overline{k}[\mathbf{T}, Y]$ (proposition 1.8.9) ;

en particulier, il est irréductible dans $F[\mathbf{T}, Y]$. Le corps F étant hilbertien (comme extension finie d'un corps hilbertien), l'ensemble des $\mathbf{t} \in k^r$ tels que $p(\mathbf{t}, Y)$ est irréductible dans $F[Y]$ est Zariski-dense. Pour ces points $\mathbf{t}$ vus comme points fermés de $\mathbb{A}^r_F$, notons $a_{\mathbf{t}}$ un point fermé de U_F au-dessus de $\mathbf{t}$. Sauf peut-être pour certains de ces $\mathbf{t}$ dans un fermé propre de Zariski, on a que l'extension résiduelle $F(a_{\mathbf{t}})/F$ est de degré $\deg_Y(p)$. Mais alors, si $(a_{\mathbf{t}})_k$ est le point fermé de U obtenu par restriction de $a_{\mathbf{t}}$ (qui est au-dessus de $\mathbf{t} \in \mathbb{A}^r_k$, on a alors nécessairement $[k((a_{\mathbf{t}})_k) : k] = \deg_Y(p)$. On en déduit que les extensions $k((a_{\mathbf{t}})_k)/k$ et F/k sont linéairement disjointes. D'après l'hypothèse sur F, cela n'est possible que si $F = k$.

La seconde partie de l'énoncé se déduit aisément : noter simplement que, les corps de définition des points fermés de U étant des extensions finies de k (proposition 1.8.11), l'intersection des corps de définition des points fermés de U est *a priori* une extension finie de k. □

CHAPITRE 6

PARTIES HILBERTIENNES DES CORPS DE NOMBRES

6.1. Densité asymptotique des ensembles hilbertiens

Le but de cette section est d'améliorer l'estimation asymptotique du nombre d'entiers $\leq B$ dans une partie hilbertienne que nous avons établie au §2.2.3. Pour cela nous utiliserons le théorème de Siegel sur les points entiers d'une courbe algébrique. Nous commençons par rappeler l'énoncé de ce résultat, que nous utiliserons aussi au §6.2.

6.1.1. Le théorème de Siegel. — On fixe un corps de nombres K et un polynôme $P \in K[T,Y]$ absolument irréductible. On note $C \subset \mathbb{A}^2$ la courbe affine d'équation $P(t,y) = 0$. Pour tout corps $k \supset K$, on note $k(C)$ le corps de fonctions de C sur k et $C(k)$ l'ensemble des points k-rationnels sur C :

$$\begin{cases} k(C) = \mathrm{Frac}\,(k[T,Y]/(P(T,Y))) \\ C(k) = \{(t,y) \in k \times k \mid P(t,y) = 0\} \end{cases}$$

Nous renvoyons à la section 3.3 (notamment au §3.3.3) pour la construction du modèle projectif lisse de C et au §3.1.3 (notamment le §3.1.3.1) pour la correspondance entre places du corps $\overline{k}(C)$ et points de $C(\overline{k})$.

Théorème 6.1.1. — *Soit S un ensemble fini de places de K contenant les places archimédiennes de K et $f \in K(C)$. Supposons qu'il existe une infinité de points $(t,y) \in C(K)$ tels que $|f(t,y)|_\ell \leq 1$ pour tout $\ell \notin S$. Alors*

nécessairement C est de genre $g = 0$, c'est-à-dire, le corps $\overline{K}(C)$ est une extension transcendante pure de $\overline{K}$, et de plus, la fonction f a au plus 2 pôles sur le modèle projectif lisse de C[(1)].

Plus précisément, on est forcément dans l'un des deux cas suivants :

1er cas : il existe $x \in K(C)$ tel que $K(C) = K(x)$ et $f \in K[x]$.

2ème cas : il existe $x \in K(C)$ et une extension quadratique réelle K_1/K tels que $K(C) = K(x)$ et $f(t, y) = \varphi(x)/x^s$ avec $\varphi(x) \in K_1[x]$, $\varphi(0) \neq 0$ et $\deg(\varphi) > s > 0$.

Nous renvoyons à [**Lan83**] pour une démonstration de ce théorème. En prenant $K = \mathbb{Q}$, $f = T$ et S l'ensemble réduit à la place archimédienne ∞ de $\mathbb{Q}$, on obtient le résultat classique suivant.

Corollaire 6.1.2. — *Si la courbe $C : P(t, y) = 0$ avec $P \in \mathbb{Q}[T, Y]$ est de genre $g \neq 0$, alors il n'existe qu'un nombre fini de solutions $(t, y) \in \mathbb{Z}^2$ à l'équation $P(t, y) = 0$.*

Dans son article, Siegel donnait aussi le corollaire suivant.

Corollaire 6.1.3. — *Soit $g(T) \in \mathbb{Z}[T]$ un polynôme non nul ayant au moins deux racines complexes distinctes. Alors le plus grand facteur premier, noté $p(g(m))$, de $g(m)$, où $m \in \mathbb{Z}$, tend vers l'infini quand $m \to \infty$.*

Démonstration. — Supposons le contraire, c'est-à-dire, qu'il existe un nombre réel A et une suite infinie $(m_n)_n$ d'entiers telle que $p(g(m_n)) \leq A$ pour tout n. Notons alors S l'ensemble des places de $\mathbb{Q}$ correspondant aux nombres premiers $\leq A$ ou à ∞. Considérons la courbe $C = \mathbb{A}^1$ (de corps de fonctions $\overline{\mathbb{Q}}(T)$) et la fonction $f = T + \frac{1}{g(T)}$. La fonction T a un pôle (le point $\infty \in \overline{C} = \mathbb{P}^1$) et la fonction $1/g(T)$ en a au moins 2 (correspondant aux 2 zéros distincts de $g(T)$) ; la fonction f a donc au moins 3 pôles sur $\overline{C}$. D'après le théorème de Siegel, seulement un nombre fini des m_n peuvent vérifier $|f(m_n)|_\ell \leq 1$ pour tout $\ell \notin S$; *a fortiori* seul un nombre fini des m_n peuvent vérifier $|g(m_n)|_\ell = 1$ pour tout $\ell \notin S$, c'est-à-dire, avoir tous leurs facteurs premiers $\leq A$; c'est la contradiction désirée. □

(1) Cette condition peut s'exprimer de façon purement arithmétique : si z un élément primitif de l'extension finie $\overline{K}(C)/\overline{K}(f)$ et $M \in \overline{K}(f)[Y]$ le polynôme minimal de z sur $\overline{K}(f)$, alors M a au moins 2 facteurs irréductibles distincts dans l'anneau $\overline{K}((1/f))[Y]$.

6.1.2. Densité asymptotique. —

Théorème 6.1.4. — *Pour toute partie hilbertienne H de $\mathbb{Q}$, le nombre d'entiers dans $H^c \cap [-B, B]$ est un $\mathrm{O}(\sqrt{B})$ (où H^c désigne le complémentaire de H dans $\mathbb{Q}$ et B une variable réelle > 0).*

Le théorème 6.1.4 améliore le théorème 2.2.9 où $\mathrm{O}(\sqrt{B})$ est remplacé par $\mathrm{O}(B^{1-\delta})$ (pour un $\delta > 0$). L'exemple du polynôme $P = Y^2 - T$ montre que l'estimation donnée ici est la meilleure possible.

Démonstration. — D'après la proposition 2.2.5, il existe N polynômes $Q_1, \ldots, Q_N \in \mathbb{Q}[T, Y]$ absolument irréductibles, unitaires en Y, avec $\deg_Y(Q_i) \geq 2$, $i = 1, \ldots, N$, et un ensemble fini tels que

$$V'_{Q_1,\ldots,Q_N} \subset H \cup F$$

ce qui, en posant $V_{Q_i} = \{t \in \mathbb{Q} \mid Q_i(t, Y) \text{ a une racine dans } \mathbb{Q}\}$, s'écrit

$$H^c \subset \bigcup_{i=1}^{N} V_{Q_i} \ \cup \ F$$

Il suffit donc de montrer que le nombre, noté N_{Q_i}, d'entiers dans chacun des ensembles $V_{Q_i} \cap [-B, B]$ est un $\mathrm{O}(\sqrt{B})$, $i = 1, \ldots, N$. Fixons un indice i et notons $Q = Q_i$.

La conclusion souhaitée est évidente si V_Q est fini. Supposons donc V_Q infini. On peut alors appliquer le théorème de Siegel à la courbe $C : Q(t, y) = 0$ et à la fonction T, ce qui conduit à distinguer deux cas :

1er cas : il existe $x \in \mathbb{Q}(C)$ tel que $\mathbb{Q}(C) = \mathbb{Q}(x)$ et $T \in \mathbb{Q}[x]$. La fonction T s'écrit donc $T = \varphi(x)$ avec $\varphi \in \mathbb{Q}[x]$. A un nombre fini d'exceptions, les T-coordonnées des points $(t, y) \in C(\mathbb{Q})$ sont des valeurs du polynôme φ en un point $x \in \mathbb{Q}$; de plus, si t est entier, x est de dénominateur borné (par une constante ne dépendant que de φ). Evaluer N_Q revient donc à évaluer le nombre de rationnels x à dénominateur borné tel que $|\varphi(x)| \leq B$. Ce nombre est un $\mathrm{O}(\sqrt{B^{1/d}})$ où

$$d = \deg(\varphi) = [\overline{\mathbb{Q}}(x) : \overline{\mathbb{Q}}(\varphi(x))] = [\overline{\mathbb{Q}}(C) : \overline{\mathbb{Q}}(T)] = \deg_Y(P) \geq 2$$

2ème cas : il existe $x \in \mathbb{Q}(C)$ et une extension quadratique réelle $K_1/\mathbb{Q}$ tels que $\mathbb{Q}(C) = \mathbb{Q}(x)$ et $T = \varphi(x)/x^s$ avec $\varphi(x) = \varphi_0 x^d + \cdots + \varphi_d \in K_1[x]$, $\varphi(0) \neq 0$ et $\deg(\varphi) > s > 0$.

Le problème est d'évaluer le nombre de solutions $x \in \mathbb{Q}$ de l'équation $\varphi(x)/x^s = t$ où $t \in \mathbb{Z}$ est un entier quelconque tel que $|t| \leq B$. Fixons un

tel entier t. Pour toute place finie ℓ de K_1, on a $|\varphi(x)|_v \leq |x|_\ell^s$. On déduit que

- si $|x|_\ell < 1$, alors $|\varphi_d|_\ell \leq \max(1, |\varphi_0|_\ell, \ldots, |\varphi_{d-1}|_\ell)|x|_\ell$
- si $|x|_\ell > 1$, alors $|\varphi_0|_\ell \leq \max(1, |\varphi_1|_\ell, \ldots, |\varphi_d|_\ell)\frac{1}{|x|_\ell}$

Comme $\varphi_0\varphi_d \neq 0$, on conclut que l'ensemble des places finies ℓ telles que $|x|_\ell \neq 1$ est un ensemble fini ne dépendant que de φ. Plus précisément, il n'y a qu'un nombre fini (dépendant de φ) de possibilités pour l'idéal fractionnaire engendré par x. Il existe donc un ensemble fini $\mathcal{F} \subset K_1$ tel que x s'écrit

$$x = \xi u \text{ avec } \xi \in \mathcal{F} \text{ et } u \text{ unité de } K_1$$

Notons $\omega > 1$ l'unité fondamentale de K_1. Alors x est de la forme $x = \pm\xi\omega^e$ avec $\xi \in F$ et $e \in \mathbb{Z}$. Le nombre de ces x tels que $|\varphi(x)/x^s| \leq B$ est un $\mathrm{O}(\log(B))$. □

Remarque 6.1.5. — (a) On peut également donner une estimation pour le nombre de *rationnels* $t = u/v \in \mathbb{Q}$ tels que $\max(|u|, |v|) \leq B$ et t n'est pas dans une partie hilbertienne H donnée : ce nombre est un $\mathrm{O}(B)$. Le principe de la preuve est similaire, mais il faut remplacer le théorème de Siegel par le théorème de Mordell-Weil pour le genre $g = 1$ et par le théorème de Faltings sur la conjecture de Mordell pour le genre $g \geq 2$[(2)] (voir [**Ser97**, §9.7]).

(b) Il y a des estimations analogues pour le cas plus général des parties hilbertiennes de K^r où K est un corps de nombres et $r \geq 1$ est un entier. Elles sont dues à S. D. Cohen ; pour $K = \mathbb{Q}$, il montre que pour H partie hilbertienne de K^r, le nombre d'entiers dans $H^c \cap [-B, B]$ est un $\mathrm{O}(B^{r-\frac{1}{2}})(\log(B))^\gamma$ pour un nombre réel $\gamma < 1$ (voir [**Ser97**, §13]).

Dans les sections suivantes, on va s'intéresser à des spécialisations de la variable T d'un certain type et étudier si on peut en trouver de ce type dans une partie hilbertienne donnée.

6.2. Progressions géométriques

On s'intéresse ici aux spécialisations de la forme ab^m. Les résultats seront utilisés au §6.3.

[(2)] Une forme faible du théorème de Faltings due à Mumford suffit pour le genre ≥ 2.

6.2.1. Les polynômes $P(T^m, Y)$. — Etant donné un corps k et un polynôme $P(T, Y) \in k(T)[Y] \setminus k(T)$, on définit $e(P)$ [resp. $f(P)$] comme le plus petit entier $e \geq 0$ tel que P ait une racine [resp. soit totalement décomposé] dans le corps $\overline{k}((T^{\frac{1}{e}}))$ des séries de Laurent formelles en $T^{\frac{1}{e}}$, ou ce qui revient au même, tel que le polynôme $P(T^e, Y)$ ait une racine [resp. soit totalement décomposé] dans le corps $\overline{k}((T))$.

Remarque 6.2.1. — (a) En caractéristique 0, le théorème de Puiseux garantit l'existence d'un entier f tel que P est totalement décomposé dans le corps $\overline{k}((T^{\frac{1}{f}}))$; dans ce cas, $e(P)$ et $f(P)$ sont des entiers. En caractéristique $p > 0$, il existe des polynômes sans racine dans $\overline{k}((T^{\frac{1}{e}}))$ pour tout entier $e > 0$, par exemple le *polynôme d'Artin-Schreier* $P(T, Y) = Y^p - Y - 1/T \in \mathbb{F}_p(T)[Y]$; dans ce cas, on a $e(P) = f(P) = -\infty$.

(b) Les entiers $e(P)$ et $f(P)$ ne changent pas si $P(T, Y)$ est remplacé par $P(aT, Y)$, pour $a \in \overline{k}$ quelconque non nul ; leur définition est géométrique.

(c) Si P est irréductible dans $\overline{k}(T)[Y]$, alors P a une racine dans $\overline{k}(T^{\frac{1}{e}})$ si et seulement si P a une racine dans $\overline{k}(T^{\frac{1}{e(P)}})$ si et seulement si P a toutes ses racines dans $\overline{k}(T^{\frac{1}{e(P)}})$ [(3)].

(d) *Interprétation géométrique.* Supposons que P soit irréductible dans $\overline{k}(T)[Y]$ et que k soit de caractéristique 0. Il résulte de la description des extensions finies de $\overline{k}((T))$ (théorème 3.1.1) que l'existence d'une racine de P dans $\overline{k}((T^{\frac{1}{e}}))$ équivaut au fait que l'un des facteurs irréductibles de P dans $\overline{k}((T))[Y]$ est de degré un diviseur de e. Ainsi l'entier $e(P)$ [resp. $f(P)$] est le plus petit [resp. le ppcm] des degrés de ces facteurs ; d'après la correspondance points/places du §3.1.3.1, c'est le plus petit [resp. le ppcm] des ordres des zéros de la fonction T sur le modèle projectif lisse de la courbe $C : P(t, y) = 0$. Si le point $t = 0$ est non ramifié dans l'extension $\overline{k}(C)/\overline{k}(T)$, alors $e(P) = f(P) = 1$; rappelons que c'est le cas notamment quand le polynôme $P(t_0, Y)$ a $d = \deg_Y(P)$ racines distinctes dans $\overline{k}$ (§3.1.3.2).

Le rôle joué par le paramètre $e = e(P)$ est révélé par le lemme suivant.

Lemme 6.2.2. — *Les énoncés suivants sont équivalents :*

(i) *$P(T^e, Y)$ est irréductible dans $k(T)[Y]$.*

[(3)] Quelques observations utiles pour établir cette équivalence : si P a une racine dans $\overline{k}(T^{\frac{1}{e}})$, alors il est totalement décomposé dans $\overline{k}(T^{\frac{1}{e}})$; $T^{\frac{1}{e}} \in \overline{k}((T^{\frac{1}{m}}))$ entraîne que e divise m ; si K est un corps contenant les racines m-ièmes de l'unité et $a \in K$, les sous-extensions d'une extension *kummérienne* $K(\sqrt[m]{a})/K$ sont de la forme $K(\sqrt[d]{a})/K)$ avec $d|m$.

(ii) *$P(T^m, Y)$ est irréductible dans $k(T)[Y]$ pour tout entier $m \geq 1$.*

Démonstration. — Notons P_e le polynôme $P_e(T, Y) = P(T^e, Y)$. Supposons que P_e soit irréductible dans $k(T)[Y]$. Soit $m \geq 1$ un entier. Par définition de e, le polynôme P_e a une racine $\mathcal{Y}(T) \in \overline{k}((T))$. Considérons le diagramme

$$\begin{array}{ccc} k(T^m, \mathcal{Y}(T^m)) & \longrightarrow & k(T, \mathcal{Y}(T^m)) \\ \uparrow & & \uparrow \\ k(T^m) & \longrightarrow & k(T) \end{array}$$

Nous avons

$$[k(T^m, \mathcal{Y}(T^m)) : k(T^m)] = [k(T, \mathcal{Y}(T)) : k(T)] = \deg_Y(P_e)$$

D'autre part, d'après le critère d'irréductibilité d'Eisenstein, le polynôme $X^m - T^m$ est irréductible dans $\overline{k}((T^m))[X]$. En particulier, nous avons

$$[k(T, \mathcal{Y}(T^m)) : k(T^m, \mathcal{Y}(T^m))] = [k(T) : k(T^m)] = m$$

On obtient donc

$$[k(T, \mathcal{Y}(T^m)) : k(T)] = \deg_Y(P_e)$$

ce qui signifie que $P_e(T^m, Y) = P(T^{em}, Y)$ est irréductible dans $k(T)[Y]$. Il en découle immédiatement que $P(T^m, Y)$ est irréductible dans $k(T)[Y]$. □

On peut démontrer le résultat plus précis suivant en utilisant le lemme de Capelli dont nous rappelons préalablement l'énoncé (voir [**Lan78**, VIII, §9, théorème 16] pour une preuve).

Lemme 6.2.3. — *Si K est un corps quelconque, $m \geq 2$ et $a \in K$, $a \neq 0$, le polynôme $X^m - a$ n'est réductible que dans les cas suivants : $a \in K^p$ pour un diviseur premier p de m ou $a \in -4K^4$ et alors $4|m$.*

Pour $P \in k(T)[Y]$ irréductible, nous notons $\mathcal{Y}_P$ une racine dans $\overline{k(T)}$ de P ; $\mathcal{Y}_P$ est un élément primitif du corps de fonctions $k(T)[Y]/(P)$.

Lemme 6.2.4. — *Soit $P = P(T, Y)$ irréductible dans $k(T)[Y]$ et $m \geq 2$ un entier. Les énoncés suivants sont équivalents :*

(i) *Le polynôme $P(T^m, Y)$ est réductible dans $k(T)[Y]$.*

(ii) *$T \in k(T, \mathcal{Y}_P)^p$ pour un diviseur premier p de m, ou bien, 4 divise m et $T \in -4k(T, \mathcal{Y}_P)^4$.*

(iii) *Le polynôme P est un diviseur dans $k(T)[Y]$ d'un polynôme de la forme*

$$\begin{cases} A(T, Y)^p - T, & \text{pour un diviseur premier } p \text{ de } m, \text{ ou bien} \\ 4A(T, Y)^4 + T, & \text{et alors } 4|m \end{cases}$$

où $A(T,Y) \in k(T)[Y]$.

Démonstration. — Considérons le diagramme

$$\begin{array}{ccc} k(T,\mathcal{Y}_P) & \xrightarrow{d_2} & k(T^{1/m},\mathcal{Y}_P) \\ {\scriptstyle \deg_Y(P)}\uparrow & & \uparrow{\scriptstyle d_1} \\ k(T) & \xrightarrow[m]{} & k(T^{1/m}) \end{array}$$

où les entiers à coté des flèches sont les degrés des extensions. La condition (i) est équivalente à $d_1 < \deg_Y(P)$ et donc aussi à $d_2 < m$. Cette dernière condition est équivalente à la réductibilité du polynôme $X^m - T$ dans $k(T,\mathcal{Y}_P)[X]$. L'équivalence entre (i) et (ii) découle alors du lemme de Capelli (lemme 6.2.3. La condition (iii) est une reformulation de la condition (ii). □

Supposons $P(T^m,Y)$ réductible dans $k(T)[Y]$ (pour $m \geq 2$). Soit p l'un des entiers pour lequel le (iii) du lemme 6.2.4 est satisfait (p est un nombre premier ou $p = 4$). Il découle de (ii) que $T \in \overline{k}(T,\mathcal{Y}_P)^p$. Les définitions de $e = e(P)$ et de $\mathcal{Y}_P$ donnent alors que $T \in \overline{k}((T^{1/e}))^p$. Le nombre p est donc un diviseur de e (utiliser la valuation T-adique) ; cela montre en particulier que le lemme 6.2.2 est une conséquence du lemme 6.2.4. L'énoncé suivant résume les résultats de cette section.

Proposition 6.2.5. — *Soit $P(T,Y)$ irréductible dans $k(T)[Y]$ et $m \geq 2$ un entier. Alors :*

— *ou bien $P(T^{e(P)},Y)$ est irréductible dans $k(T)[Y]$ et alors $P(T^m,Y)$ est irréductible dans $k(T)[Y]$, pour tout entier $m > 0$.*

— *ou bien $P(T^{e(P)},Y)$ est réductible dans $k(T)[Y]$ et alors*

(*) *il existe un diviseur p de $e(P)$ tel que p est un nombre premier ou $p = 4$ et $P(T^p,Y)$ est réductible dans $k(T)[Y]$, et*

(**) *$P(T^m,Y)$ est réductible si et seulement si m est un multiple d'un entier p satisfaisant (*). En particulier, si $(m,e(P)) = 1$, alors $P(T^m,Y)$ est irréductible dans $k(T)[Y]$.*

6.2.2. Le résultat central. — Nous démontrerons la plupart des résultats de cette section en nous ramenant à l'énoncé suivant.

Théorème 6.2.6. — *Soient k un corps de nombres et $P(T,Y) \in k(T)[Y]$ un polynôme irréductible admettant une racine dans $\overline{k}((T))$. Soit b un élément de k non nul et non racine de l'unité. Alors $P(b^n,Y)$ est irréductible dans $k[Y]$ pour tout entier n suffisamment grand.*

Remarque 6.2.7. — (a) le résultat est faux si
- P n'a pas de racine dans $\overline{k}((T))$: prendre $P(T,Y) = Y^2 - T$, ou si
- $b = 0$ ou une racine de l'unité : prendre $P(T,Y) = Y(Y-1) - T(T^r - 1)$.

(b) On suppose dans le théorème 6.2.6 que k est un corps de nombres. Si k est plus généralement un corps avec une formule du produit (éventuellement de caractéristique $p > 0$), on peut montrer l'énoncé suivant [**Dèb99b**] :

si $P(T,Y) \in k(T)[Y]$ est irréductible et a <u>toutes</u> ses racines dans $\overline{k}((T))$ et si b est un élément de k de "hauteur" > 0, alors $P(b^n, Y)$ est irréductible dans $k[Y]$ pour <u>une infinité</u> d'entiers $n > 0$.

Cette forme est même établie pour plusieurs polynômes $P_1, \ldots, P_n$. (La forme multipolynomiale du théorème 6.2.6 est également valable mais elle se déduit de façon évidente de la forme énoncée avec un polynôme).

Démonstration du théorème 6.2.6.. — Supposons au contraire que pour un élément $b \in k$ non nul et non racine de l'unité, $P(b^n, Y)$ soit réductible dans $k[Y]$ pour une infinité d'entiers $n > 0$. Posons $f = f(P)$. Il existe un entier u, $0 \leq u \leq f-1$, tel que $P(b^n, Y)$ soit réductible dans $k[Y]$ pour une infinité d'entiers $n > 0$ congrus à u modulo f. Considérons le polynôme $P(b^u T^f, Y)$; il a les propriétés suivantes :
• totalement décomposé dans $\overline{k}((T))$: par définition de f et la remarque 6.2.1.
• irréductible dans $k(T)[Y]$: en effet, $P(T,Y)$ étant irréductible et admettant une racine dans $\overline{k}((T))$, le polynôme $P(b^u T, Y)$ a les mêmes propriétés ; d'après le lemme 6.2.2, on a $P(b^u T^l, Y)$ irréductible pour tout $l > 0$.
• il devient réductible dans $k[Y]$ pour T spécialisé en $T = b^m$ pour une infinité d'entiers $m > 0$.

D'après la proposition 2.2.5, il existe N polynômes $Q_1, \ldots, Q_N \in k[T,Y]$ sans racine dans $k(T)$ et unitaires (en Y) et un ensemble fini $F \subset k$ tels que

$$V'_{Q_1,\ldots,Q_N} \subset H_{P(b^u T^f, Y)} \cup F$$

On en déduit qu'il existe un indice $i \in \{1, \ldots, N\}$ tel que

(*) $Q_i(b^m, Y)$ a une racine dans k pour une infinité d'entiers $m > 0$.

De plus, par construction (voir la preuve de la proposition 2.2.5), chaque polynôme Q_i a une racine (en Y) dans le corps de décomposition (sur $K(T)$) du polynôme P ; en particulier, Q_i a une racine dans $\overline{k}((T))$ $(i = 1, \ldots, N)$.

Nous allons maintenant utiliser le théorème de Siegel (théorème 6.1.1) pour obtenir une contradiction. Notons $C \subset \mathbb{A}^2$ la courbe affine d'équation

$Q_i(t,y) = 0$ et considérons la fonction $f = T + (1/T) \in k(C)$. Soit S l'ensemble fini des places ℓ de k qui vérifient $|b|_\ell \neq 1$ ou bien sont archimédiennes. Si $\ell \notin S$, pour tout entier $m \geq 1$, on a $|b^m|_\ell = 1$ et $|1/b^m|_\ell = 1$ et donc $|b^m + (1/b^m)|_\ell \leq 1$. L'énoncé (*) permet alors de conclure qu'il existe une infinité de points $(t,y) \in C(k)$ tels que $|f(t,y)|_\ell \leq 1$ pour tout $\ell \notin S$.

Comme $\deg_Y Q_i \geq 2$ et que Q_i a au moins une racine dans $k((T))$, la décomposition de Q_i dans $k((T))[Y]$ comporte au moins 2 facteurs. De façon équivalente, la fonction T a au moins 2 zéros sur un modèle projectif $\overline{C}$ de C. D'autre part, la fonction T a au moins un pôle sur $\overline{C}$ (la décomposition de Q_i dans $\overline{\mathbb{Q}}((1/T))[Y]$ comporte au moins 1 facteur). On peut donc conclure que la fonction f a au moins 3 pôles sur $\overline{C}$ ce qui, d'après le théorème de Siegel, est en contradiction avec la conclusion obtenue ci-dessus. □

Remarque 6.2.8. — (a) La preuve montre que la condition "$P(T,Y)$ irréductible dans $k(T)[Y]$ et a une racine dans $\overline{k}((T))$" peut être remplacée par l'hypothèse plus faible

(**) $\quad P(b^u T^{e(P)}, Y)$ *irréductible dans* $k(T)[Y]$, $u = 1, \ldots, e(P) - 1$[(4)].

En effet, d'après le lemme 6.2.2 (qu'on applique au polynôme $P(b^u T, Y)$), la condition (**) entraîne que $P(b^u T^l, Y)$ est irréductible dans $k(T)[Y]$ pour tout entier $l > 0$, en particulier, le polynôme $P(b^u T^f, Y)$ de la démonstration l'est.

Cette remarque permet d'obtenir la conclusion du théorème 6.2.6 dans des cas non couverts par l'énoncé donné : prendre par exemple $P(T,Y) = Y^2 - T(T+1)$. On peut noter que l'hypothèse "$P(T^{e(P)}, Y)$ irréductible dans $\overline{k}(T)[Y]$" garantit la condition (**). Par contre, l'irréductibilité de $P(T^{e(P)}, Y)$ dans $k(T)[Y]$ est insuffisante : prendre $P(T,Y) = Y^2 - 2T$ et $b = 2$.

(b) Pour obtenir les résultats type théorème 6.2.6 sur un corps avec une formule du produit, on ne peut plus utiliser le théorème de Siegel. On utilise à la place le théorème principal de [**Dèb96**] ; il s'agit d'un résultat diophantien dont la conclusion est plus faible que celle du théorème de Siegel mais suffisante pour le problème considéré et qui est valable dans le contexte général des corps avec une formule du produit.

6.2.3. Spécialisations $T = b^m$. —

Théorème 6.2.9. — *Soient k un corps de nombres et $P(T,Y) \in k[T,Y]$ un polynôme absolument irréductible tel que* $\deg_Y(P) \geq 1$. *Soit $b \in k$ tel que*

(4) Cette condition entraîne en fait que $P(b^u T^{e(P)}, Y)$ est irréductible dans $k(T)[Y]$ pour tout $u \geq 1$: écrire $u = \alpha e(P) + u_0$ avec $0 \leq u_0 < e(P)$ et $b^u T^{e(P)} = b^{u_0}(b^\alpha T)^{e(P)}$.

(*) *$b \notin k^\ell$ pour tout nombre premier $\ell | e(P)$ et $-b \notin k^2$ si 4 divise $e(P)$.*

Alors $P(b^m, Y)$ est irréductible dans $k[Y]$ pour une infinité d'entiers m (en fait pour tout m dans une progression arithmétique $(e(P)n + u)_{n \geq 0}$).

Remarque 6.2.10. — (a) Le résultat devient faux si on supprime la condition (*) : prendre $P(T, Y) = Y^\ell - T$ si $b \in k^\ell$ et $P(T, Y) = Y^4 + 4T$ si $-b \in k^2$ (pour les puissances paires de b, la réductibilité de $P(b^m, Y)$ vient de la factorisation $Y^4 + 4T^4 = (Y^2 + 2TY + 2T^2)(Y^2 - 2TY + 2T^2)$). Enfin "pour une infinité d'entiers m" ne peut pas être remplacé par "pour tout entier m suffisamment grand" : prendre $P(T, Y) = Y^\ell - T$.

(b) De même le résultat devient faux si on ne suppose plus P *absolument* irréductible. Prenons par exemple pour P le polynôme minimal de $\sqrt{T} + \sqrt{2}$ sur $\mathbb{Q}(T)$. Les polynômes $P(T^2, Y)$ et $P(2T^2, Y)$ sont réductibles dans $\mathbb{Q}(T)[Y]$: en effet ils ont pour racine $T + \sqrt{2}$ et $\sqrt{2}(1 + T)$ respectivement, qui sont tous deux de degré 2 sur $\mathbb{Q}(T)$, alors que $\deg_Y(P) = 4$. Donc pour $b = 2$, le polynôme $P(b^m, Y)$ est réductible dans $\mathbb{Q}(T)[Y]$, pour tout entier $m \geq 1$.

(c) Si k est plus généralement un corps avec une formule du produit, le résultat subsiste[(5)] moyennant les hypothèses supplémentaires suivantes : il existe un entier f tel que $P(T^f, Y)$ est totalement décomposé soit dans $\overline{k}((T^{1/f}))$ soit dans $\overline{k}(((1/T)^{1/f}))$; b est de hauteur > 0 (voir [**Dèb99b**]).

La preuve du théorème 6.2.9 utilise le lemme suivant.

Lemme 6.2.11. — *Soit $P(T, Y) \in k(T)[Y]$ un polynôme irréductible dans $\overline{k}(T)[Y]$. Soit D_P l'ensemble des diviseurs ℓ de $e = e(P)$ tel que ℓ est un nombre premier ou $\ell = 4$. Soit b un élément de k satisfaisant la condition (*) du théorème 6.2.9. Alors il existe une famille d'entiers $(u_\ell)_{(\ell \in D_P)}$ ayant la propriété suivante : pour tout $\ell \in D_P$, si u est un entier tel que*

$$(**) \qquad \begin{cases} u \not\equiv u_\ell \pmod{\ell} & \text{if } \ell \neq 4 \\ u \not\equiv u_\ell \pmod{\ell} \text{ and } u \not\equiv u_2 \pmod{2} & \text{if } \ell = 4 \end{cases}$$

alors $P(b^u T^\ell, Y)$ est irréductible dans $k(T)[Y]$.

Démonstration. — Pour tout $\ell \in D_P \setminus \{4\}$, on définit l'entier u_ℓ de la façon suivante : si $P(b^u T^\ell, Y)$ est irréductible dans $k(T)[Y]$ pour tout $u > 0$, on pose $u_\ell = 0$; dans le cas opposé, on choisit u tel que $P(b^u T^\ell, Y)$ est réductible dans

(5) Plus précisément, la partie "$P(b^m, Y)$ est irréductible dans $k[Y]$ pour une infinité d'entiers m" subsiste ; la conclusion donnant ces entiers comme termes d'une progression arithmétique n'est pas établie dans [**Dèb99b**].

$k(T)[Y]$ et on pose $u_\ell = u$. Pour $\ell = 4$, on prend pour u_4 un entier arbitraire tel que $b^{-u_4}T \in -4K(T, y_P)^4$; on prend $u_4 = 0$ s'il n'y en a pas.

Soit $\ell \in D_P$ et u un entier satisfaisant (**). Supposons que $P(b^u T^\ell, Y)$ soit réductible dans $k(T)[Y]$. Notons $\mathcal{Y}_P(T)$ une racine dans $\overline{k(T)}$ de $P(T, Y)$.

1er cas : $\ell \neq 4$. D'après le lemme 6.2.4 (appliqué aux polynômes $P(b^u T, Y)$ et $P(b^{u_\ell} T, Y)$), on a $T \in k(T, \mathcal{Y}_P(b^u T))^\ell$ et $T \in k(T, \mathcal{Y}_P(b^{u_\ell} T))^\ell$, ou de façon équivalente, $b^{-u}T$ et $b^{-u_\ell}T$ sont dans $k(T, \mathcal{Y}_P(T))^\ell$. Il en résulte que b^{u-u_ℓ} est la puissance ℓ-ième d'un élément de $k(T, \mathcal{Y}_P)$, lequel est nécessairement dans le corps des constantes $k(T, \mathcal{Y}_P) \cap \overline{k}$ de P. Comme P est supposé absolument irréductible, ce corps des constantes est k. Mais d'après la condition (*), b^{u-u_ℓ} n'appartient à k^ℓ que si $u \equiv u_\ell \pmod{\ell}$. D'où la contradiction recherchée.

2ème cas : $\ell = 4$. D'après le 1er cas, puisque $u \not\equiv u_2 \pmod 2$, $P(b^u T^2, Y)$ est irréductible dans $k(T)[Y]$. Donc $b^{-u}T \notin k(T, \mathcal{Y}_P)^2$ (lemme 6.2.4). Il résulte aussi du lemme 6.2.4 que si $P(b^u T^4, Y)$ est réductible dans $k(T)[Y]$, alors $b^{-u}T$ et $b^{-u_4}T$ sont dans $-4K(T, \mathcal{Y}_P)^4$. On peut conclure comme dans le 1er cas que b^{u-u_4} est la puissance 4-ième d'un élément de k. Il découle alors de "$b \notin k^2$" que $u \equiv u_4 \pmod 2$ et que $b^2 \in k^4$ (puisque $u \not\equiv u_4 \pmod 4$). Donc b ou $-b$ est un carré dans k, contrairement à l'hypothèse. □

Démonstration du théorème 6.2.9.. — Soient $b \in k$ vérifiant la condition (*) de l'énoncé et $(u_\ell)_{(\ell \in D_P)}$ une famille d'entiers vérifiant la conclusion du lemme 6.2.11. En utilisant le lemme chinois (lemme 1.1.6), on trouve un entier u tel que la condition (**) du lemme 6.2.11 soit satisfaite. Pour tout $\ell \in D_P$, le polynôme $P(b^u T^\ell, Y)$ est alors irréductible dans $k(T)[Y]$. La proposition 6.2.5 permet de conclure que $P(b^u T^e, Y)$ est irréductible dans $k(T)[Y]$. Le théorème 6.2.6 fournit alors la conclusion désirée. □

6.2.4. Spécialisations $T = b^m$ (version multipolynomiale). — Le théorème 6.2.9 ne s'étend pas au cas de plusieurs polynômes : en effet, pour $P_1 = Y^2 - T$, $P_2 = Y^2 - 2T$ et $k = \mathbb{Q}$, le nombre $b = 2$ vérifie son hypothèse (*) mais H_{P_1,P_2} ne contient aucune puissance de 2. On peut cependant, en modifiant légèrement la condition (*), établir une version multipolynomiale du théorème 6.2.9. Ce nouvel énoncé (théorème 6.2.12 ci-dessous) reste lui aussi valable plus généralement pour un corps k avec une formule du produit moyennant les hypothèses supplémentaires : $P_1, \ldots, P_n$ totalement décomposés dans $\overline{k}((T^{1/f}))$ pour un entier $f > 0$; b est de hauteur > 0 (voir [**Dèb99b**]).

Théorème 6.2.12. — *Soit $H = H_{P_1,\dots,P_n}$ une partie hilbertienne du corps de nombres k avec $P_1, \dots, P_n \in k(T)[Y]$ irréductibles. Alors il existe une extension finie L de k ayant la propriété suivante. Soit $b \in k$ tel que la condition (*) du théorème 6.2.11 soit satisfaite avec L au lieu de k. Alors H contient une infinité de puissances b^m $(m > 0)$ de b.*

L'extension L/k sera décrite explicitement dans la preuve ; dans l'exemple précédent où $P_1 = Y^2 - T$, $P_2 = Y^2 - 2T$, cette extension est $L = \mathbb{Q}(\sqrt{2})$. La preuve utilisera le lemme suivant qui servira également pour démontrer le théorème 6.2.14 . Dans ce lemme, k est un corps quelconque.

Lemme 6.2.13. — *Soient $P(T, Y) \in k[T, Y]$ un polynôme irréductible tel que $P(T, Y) \neq cT$ $(c \in k)$ et $f \geq 1$ un entier. Soit*

$$P(T^f, Y) = \Pi_1(T, Y) \cdots \Pi_r(T, Y)$$

une décomposition de $P(T^f, Y)$ en irréductibles de $\overline{k}[T, Y]$. On note L une extension finie de k telle que $\Pi_i \in L[T, Y]$, $i = 1, \dots, r$. Soit enfin $\alpha \in k$, $\alpha \neq 0$ tel que $T^f - \alpha$ soit irréductible dans $L[T]$. Alors le polynôme $P(\alpha T^f, Y)$ est irréductible dans $k[T, Y]$.

Démonstration. — Soit $\beta \in \overline{k}$ tel que $\beta^f = \alpha$. Les polynômes $\Pi_1, \dots, \Pi_r$ étant irréductibles dans $\overline{k}[T, Y]$, une décomposition de $P(\alpha T^f, Y) = P((\beta T)^f, Y)$ en irréductibles de $\overline{k}[T, Y]$ est donnée par

$$P(\alpha T^f, Y) = \Pi_1(\beta T, Y) \cdots \Pi_r(\beta T, Y)$$

Supposons que $P(\alpha T^f, Y) = Q(T, Y)R(T, Y)$ avec $Q, R \in k[T, Y]$. On peut écrire

$$Q(T, Y) = aQ_1(\beta T, Y) \quad \text{et} \quad R(T, Y) = \frac{1}{a} R_1(\beta T, Y)$$

avec $Q_1, R_1 \in L[T, Y]$ et $a \in L(\beta)$. Pour $T = 0$ on obtient $Q(0, Y) = aQ_1(0, Y)$. Comme $Q(0, Y) \neq 0$ (sinon $P(0, Y) = 0$, *i.e.*, T divise $P(T, Y)$ et $P(T, Y) = cT$ $(c \in k)$), on a en fait $a \in L$ et on peut supposer $a = 1$. Par hypothèse, le polynôme $T^f - \alpha$ est irréductible dans $L[T]$; en particulier, pour tout entier j, on a $\beta^j \in L$ si et seulement si f divise j. On en déduit que les polynômes Q_1 et R_1 sont de la forme

$$Q_1(T, Y) = Q_2(T^f, Y) \quad \text{et} \quad R_1(T, Y) = R_2(T^f, Y)$$

avec $Q_2, R_2 \in L[T, Y]$. On obtient donc

$$Q(T, Y) = Q_2(\alpha T^f, Y) \quad \text{et} \quad R(T, Y) = R_2(\alpha T^f, Y)$$

On déduit maintenant de $P(\alpha T^f, Y) = Q(T,Y)R(T,Y)$ que $P = Q_2R_2$. Comme, d'après les identités précédentes, on a nécessairement $P_2, Q_2 \in k[T,Y]$, on peut conclure de l'irréductibilité de P dans $k[T,Y]$ que $\deg(Q_2) = 0$ ou $\deg(R_2) = 0$, et donc que $\deg(Q) = 0$ ou $\deg(R) = 0$. □

Démonstration du théorème 6.2.12. — Grâce aux résultats de réduction du chapitre 5, on peut supposer $P_1, \dots, P_n \in k[T,Y] \setminus k[T]$ irréductibles. Soit $f \geq 1$ un entier tel que $P_i(T^f, Y)$ ait une racine dans $\overline{k}((T))$, $i = 1, \dots, n$. Notons L un corps contenant les coefficients des polynômes de la décomposition en irréductibles de $\overline{k}[T,Y]$ de chacun des polynômes $P_1(T^f, Y), \dots, P_n(T^f, Y)$. Soit maintenant $b \in k$ tel que la condition (*) du théorème 6.2.9 soit satisfaite pour ce corps L. D'après le lemme de Capelli (lemme 6.2.3), $T^f - b$ est irréductible dans $L[T]$. D'après le lemme 6.2.13, on a donc $P_i(bT^f, Y)$ irréductible dans $k[T,Y]$, $i = 1, \dots, n$. Le théorème 6.2.6 permet de conclure alors que $P_i(b(b^m)^f, Y)$ est irréductible pour tout entier m assez grand, $i = 1, \dots, n$. □

6.2.5. Spécialisations du type ab^m. — En utilisant des progressions géométriques $(ab^m)_{m\geq 0}$, on peut établir des énoncés où *tous* les termes sont dans une partie hilbertienne donnée (et pas seulement une infinité).

Théorème 6.2.14. — *Soit $H = H_{P_1,\dots,P_n}$ une partie hilbertienne du corps de nombres k avec $P_1, \dots, P_n \in k(T)[Y]$ irréductibles. Soit $b \in k$ non nul et non racine de l'unité. Alors il existe $a \in k$ entier algébrique tel que pour tout entier m sauf un nombre fini, on a $ab^m \in H$, i.e., $P_i(ab^m, Y)$ irréductible dans $k[Y]$, $i = 1, \dots, n$.*

Démonstration. — D'après la proposition 2.2.5, il existe N polynômes $Q_1, \dots, Q_N \in \mathbb{Q}[T,Y]$ absolument irréductibles, unitaires en Y, avec $\deg_Y(Q_i) \geq 2$, $i = 1, \dots, N$, et un ensemble fini tels que

$$V'_{Q_1,\dots,Q_N} \subset H \cup F$$

Soient ε le p.p.c.m. des entiers $e(Q_1), \dots, e(Q_N)$ et $\beta \in \overline{\mathbb{Q}}$ une racine ε-ième de b. Les polynômes $Q_1, \dots, Q_N$ sont irréductibles dans $k(\beta)[T,Y]$. Notons L un corps contenant $k(\beta)$ et les coefficients des polynômes de la décomposition en irréductibles de $\overline{k}[T,Y]$ de chacun des polynômes $Q_1(T^f, Y), \dots, Q_N(T^f, Y)$. Choisissons ensuite $a \in k$ entier, $a \neq 0$ tel que $T^\varepsilon - a$ soit irréductible dans $L[T]$: on peut prendre par exemple pour a tout nombre premier non ramifié dans L, la conclusion souhaitée résultant alors du lemme de Capelli (lemme 6.2.3) ; on peut aussi pour l'existence de a invoquer le

théorème d'irréductibilité de Hilbert (pour le polynôme $T^\varepsilon - X$)[6]. D'après le lemme 6.2.13, chacun des polynômes $Q_1(aT^f, Y), \dots, Q_N(aT^f, Y)$ est irréductible dans $k(\beta)[T, Y]$. Le théorème 6.2.6 permet de conclure alors que $Q_i(a(\beta^m)^f, Y)$ est irréductible dans $k(\beta)[Y]$ pour tout entier m sauf un nombre fini, $i = 1, \dots, N$. En particulier, pour tout entier m sauf un nombre fini, le polynôme $Q_i(ab^m, Y)$ n'a pas de racines dans k, $i = 1, \dots, N$. □

Remarque 6.2.15. — (a) L'extension du théorème 6.2.14 aux parties hilbertiennes d'un corps avec une formule du produit (pour un élément b du corps de hauteur > 0) est un problème ouvert.

(b) Les résultats donnés dans cette section ne sont pas "effectifs" : ils ne donnent pas de borne explicite pour le plus entier m à partir duquel les conclusions sont vraies. Cela est dû à l'ineffectivité du théorème de Siegel. En revanche, les résultats de [**Dèb99b**] sont effectifs, ils sont aussi valables dans un cadre plus général, les corps avec une formule du produit, mais leurs conclusions sont plus faibles (pour le théorème 6.2.6, "pour tout m suffisamment grand" doit être remplacé par "pour une infinité d'entiers").

(c) Il existe d'autres résultats, dûs notamment à Sprindzuk, sur l'irréductibilité des polynômes spécialisés $P(b^m, Y)$, avec de meilleures conclusions mais sous des hypothèses plus fortes sur P et b. Nous renvoyons à [**Dèb86a**], [**Dèb87**] et [**Spr83**] pour ces résultats. On trouvera aussi dans [**Dèb86b**] une forme effective du théorème 6.2.14 dans le cas $k = \mathbb{Q}$. Enfin nous renvoyons à [**Dèb92**] et [**Dèb99b**] pour d'autres compléments.

6.3. Théorème de Hilbert et théorèmes d'approximation

Les résultats du §6.2 permettent de montrer le théorème suivant.

Théorème 6.3.1. — *Soit k un corps de nombres. Soient v_0 une place de k, S un ensemble fini de places de k distinctes de v_0, $(a_v)_{v\in S}$ une famille d'éléments $a_v \in k_v$ (le complété de k pour la métrique induite par v) et $\varepsilon > 0$. Soit $H = H_{P_1,\dots,P_n}$ une partie hilbertienne de k avec $P_1, \dots, P_n \in k(T)[Y]$ irréductibles. Alors il existe $t \in k$ vérifiant les conditions suivantes :*
(i) $|t - a_v|_v < \varepsilon$ *pour tout* $v \in S$,
(ii) $|t|_v \leq 1$, *pour tout* $v \notin S$, $v \neq v_0$,
(iii) $t \in H$.

[6] Noter qu'on ne peut pas ici prendre $a = b$.

Remarque 6.3.2. — (a) L'énoncé avec comme conclusion la seule condition (i) [resp. les conditions (i) et (ii)] est un résultat classique d'approximation, le théorème d'*approximation faible* [resp. d'*approximation forte*] pour les corps de nombres (*e.g.* [**CF67**, chapter II]). La conclusion (iii) seule correspond au théorème d'irréductibilité de Hilbert. Le théorème 6.3.1 affirme que le théorème de Hilbert est "compatible" avec ces résultats d'approximation.

(b) En vertu du théorème d'approximation forte, il suffit de démontrer le théorème 6.3.1 pour a_v égal à un élément $\alpha \in k$ donné (ne dépendant pas de $v \in S$). Autrement dit, il suffit de prouver que

(*) *toute partie hilbertienne H de k est dense dans k pour la "topologie de l'approximation forte".*

Cette conclusion s'étend aux corps munis d'une formule du produit, de caractéristique 0 ou imparfaits de caractéristique $p > 0$ et pour lesquels 0 n'est pas isolé pour la topologie de l'approximation forte [**Dèb99b**]. Par exemple, tout corps global (corps de nombres ou extension finie de $\mathbb{F}_q(T)$) satisfait ces hypothèses.

(c) Il y a un cas particulier du théorème 6.3.1 qu'on déduit aisément du théorème d'irréductibilité de Hilbert, à savoir celui où $k = \mathbb{Q}$ et $v_0 = \infty$.

On peut en effet procéder comme suit. Soit $\alpha \in k$ donné. On choisit $\beta \in \mathbb{Z}$ tel que $|\beta|_v < \varepsilon$ pour tout $v \in S$; le choix de β dans $\mathbb{Z}$ est possible car $v_0 = \infty$. On a alorsLa condition $|\beta|_v \leq 1$ pour tout $v \notin S$, $v \neq v_0$. Le théorème d'irréductibilité de Hilbert, appliqué aux polynômes $P_i(\alpha + \beta T, Y)$, et plus précisément le fait que toute partie hilbertienne de k contient une infinité d'*entiers*, donne la conclusion souhaitée.

(d) Le cas général du théorème 6.3.1 est plus délicat. Nous le déduisons ici des résultats de cette section qui s'appuient sur le théorème de Siegel. Une autre démonstration du théorème 6.3.1, utilisant aussi le théorème de Siegel, a été donnée par Morita [**Mor90**]. Ekhedal [**Eke90**] a donné une autre preuve qui repose sur les bornes de Lang-Weil pour les points rationnels sur les courbes sur les corps finis. La preuve de la généralisation aux corps avec une formule du produit mentionnée ci-dessus utilise les résultats de [**Dèb96**].

Démonstration du théorème 6.3.1. — Pour tout $t \in k$, $H - t$ est encore une partie hilbertienne, à savoir la partie hilbertienne associée aux polynômes $P_1(T + t, Y), \ldots, P_n(T + t, Y)$. En prenant aussi en compte la remarque 6.3.2 (b) ci-dessus, il suffit de montrer que 0 peut être approché (au sens des conditions (i) et (ii) du théorème) par des éléments d'une partie hilbertienne $H = H_{P_1,\ldots,P_n}$ donnée. Choisissons $b \in k$ tel que $|b|_v < 1$ pour tout $v \in S$

et $|b|_v \leq 1$ pour tout $v \notin S$, $v \neq v_0$. D'après le théorème 6.2.14 , il existe $a \in k$ entier algébrique non nul tel que $ab^m \in H$ pour tout m suffisamment grand. A partir d'un certain rang m_0, on a aussi $|ab^m|_v < \varepsilon$ pour tout $v \in S$ et $|ab^m|_v \leq 1$ pour tout $v \notin S$, $v \neq v_0$. □

6.4. Progressions arithmétiques

Le but de cette section est de démontrer le résultat suivant, démontré en 1965 par Davenport, Lewis, Schinzel dans le cas $k = \mathbb{Q}$ (voir [**Sch00**]) et dans le cas général par Fried en 1974 [**Fri74**]. Nous suivrons ici la méthode de Fried, qui fournit une nouvelle preuve du théorème d'irréductibilité de Hilbert (alors que Davenport, Lewis, Schinzel l'utilisent dans leur preuve).

Théorème 6.4.1. — *Soient k un corps de nombres et $H = H_{P_1,\dots,P_n}$ une partie hilbertienne de k avec $P_1, \dots, P_n \in k(T)[Y]$ irréductibles. Alors il existe $a, b \in \mathbb{Z}$, $a > 0$ tels que H contienne la progression arithmétique $(am + b)_{m\in\mathbb{Z}}$.*

6.4.1. Les inégalités de Lang-Weil. — Dans la preuve, on va utiliser les estimations suivantes dues à S. Lang et A. Weil sur le nombre de points rationnels sur les courbes algébriques sur les corps finis ; nous renvoyons à [**FJ04**, chapter 5] pour une preuve.

Théorème 6.4.2. — *Soient $\mathbb{F}_q$ un corps fini de cardinal q, $p(T, Y) \in \mathbb{F}_q[T, Y]$ un polynôme absolument irréductible de degré d et C_p la courbe affine $C_p : p(t, y) = 0$. On a alors*

$$q + 1 - (d - 1)(d - 2)\sqrt{q} - d \leq |C(\mathbb{F}_q)| \leq q + 1 + (d - 1)(d - 2)\sqrt{q}$$

Il existe des généralisation de ces estimations à des variétés de dimension supérieure, démontrées également par Lang et Weil [**LW54**] ; on peut aussi les déduire des *conjectures de Weil* démontrées par Deligne [**Del74**] [**Del80**].

6.4.2. Lemmes préliminaires. — Le premier de ces lemmes est un résultat assez classique de théorie des nombres.

Lemme 6.4.3. — *Soient L un corps de nombres et A'_L l'anneau de ses entiers. Alors il existe une infinité de nombres premiers p totalement décomposés dans l'extension $L/\mathbb{Q}$, c'est-à-dire, tels que pour tout idéal premier $\mathcal{P}$ de A'_L au-dessus de p, le corps résiduel $A'_L/\mathcal{P}$ soit égal au corps premier $\mathbb{F}_p$.*

Démonstration. — Soient $\widehat{L}/\mathbb{Q}$ la clôture galoisienne de $L/\mathbb{Q}$, ξ un élément primitif entier de l'extension $\widehat{L}/\mathbb{Q}$. Soient $f(X) \in \mathbb{Z}[X]$ le polynôme minimal de ξ sur $\mathbb{Q}$ et $d = [\widehat{L} : \mathbb{Q}]$. Il suffit de montrer que pour une infinité de nombres premiers p, le polynôme $f(X)$ a au moins une racine α modulo p. En effet, cela entraîne que, pour tous ces p sauf éventuellement ceux qui divisent le discriminant $\Delta \in \mathbb{Z}$ de la base $1, \xi, \ldots, \xi^{d-1}$, il existe au moins un idéal $\mathcal{P} \subset A'_L$ au-dessus de p, tel que $A'_L/\mathcal{P} \simeq \mathbb{F}_p$ (à savoir le noyau du morphisme $(A'_L)_{\Delta^\infty} \to \mathbb{F}_p$ qui envoie ξ sur $\alpha \in \mathbb{F}_p$). Mais l'extension $\widehat{L}/\mathbb{Q}$ étant galoisienne, *tous* les idéaux $\mathcal{P} \subset A'_L$ au-dessus de tels p, seront alors de corps résiduel $\mathbb{F}_p$ (puisque ces idéaux sont conjugués sous $\mathrm{Gal}(\widehat{L}/\mathbb{Q})$). C'est-à-dire, ces nombres premiers p seront totalement décomposés dans $\widehat{L}/\mathbb{Q}$ et *a fortiori* dans $L/\mathbb{Q}$.

Supposons au contraire qu'il n'existe qu'un nombre fini de nombres premiers $p_1, \ldots, p_r$ pour lesquels $f(x) \equiv 0 \pmod{p_i}$ a une solution. Considérons, pour tout $l \in \mathbb{N}$, l'entier

$$\gamma_l = f\left((\prod_{i=1}^{r} p_i)^l\right)$$

Pour l assez grand, on a

$$v_{p_i}(\gamma_l) \leq v_{p_i}(f(0)),\ i = 1, \ldots, r$$

Il n'y a qu'un nombre fini d'entiers vérifiant cette condition et non divisibles par d'autres nombres premiers que $p_1, \ldots, p_r$. On peut donc conclure qu'il existe $l \in \mathbb{N}$ tel que γ_l soit divisible par un nombre premier $p \neq p_1, \ldots, p_r$. Par construction de γ_l, l'équation $f(x) \equiv 0 \pmod{p}$ a alors au moins une solution $x \in \mathbb{Z}$. □

Lemme 6.4.4. — *Soient k un corps de nombres et $H(T, Y) \in k[T, Y]$ un polynôme absolument irréductible, avec $\deg_Y(P) \geq 1$ et unitaire comme polynôme en Y. Pour tout entier $A \geq 0$, il existe un nombre premier p ne divisant pas A et un entier $b \in \mathbb{Z}$ ayant la propriété suivante : si $t \in \mathbb{Z}$ et $t \equiv b \pmod{p}$ alors $H(t, Y)$ n'a pas de racine dans k.*

Démonstration. — On peut sans restreindre la généralité supposer que H est à coefficients dans l'anneau A'_k des entiers de k. On note
- $\mathcal{Y}_H \in \overline{k(T)}$ une racine de $H(T, \mathcal{Y}_H) = 0$,
- $\Omega/k(T)$ une clôture normale de l'extension $k(T, \mathcal{Y}_H)$,
- θ un élément primitif entier sur $A'_k[T]$ de l'extension $\Omega/k(T)$ et $G(T, Y) \in A'_k[T, Y]$ le polynôme minimal de θ sur $k(T)$,
- $\mathcal{Y}_1, \ldots, \mathcal{Y}_d$ les conjugués de $\mathcal{Y}_H$ sur $k(T)$, *i.e.*, les racines de $H(T, Y)$; on a $d = \deg_Y(H)$ et on supposera $\mathcal{Y}_1 = \mathcal{Y}_H$.

On peut écrire

$$\mathcal{Y}_i = \frac{P_i(T,\theta)}{P_0(T)}$$

avec $P_i \in A'_k[T,Y]$, $i = 1,\dots,d$ et $P_0 \in A'_k[T]$ (indépendant de i). On a donc

$$H(T,Y) = \prod_{i=1}^{d} \left(Y - \frac{P_i(T,\theta)}{P_0(T)} \right)$$

ce qu'on peut écrire

$$H(T,Y) = \prod_{i=1}^{d} \left(Y - \frac{P_i(T,X)}{P_0(T)} \right) \quad [\text{mod } G(T,X)] \qquad (\text{dans } K(T)[X,Y])$$

ou encore, en tirant parti de $G(T,X) \in K[T,Y]$ et est unitaire (en X)
$(*)$

$$P_0(T)^d H(T,Y) = \prod_{i=1}^{d} (P_0(T)Y - P_i(T,X)) \quad [\text{mod } G(T,X)] \quad (\text{dans } K[T,X,Y])$$

Soient $G_1(T,X)$ un facteur irréductible de $G(T,Y)$ dans $\overline{k}[T,X]$ et L le corps engendré sur k par les coefficients de G_1. D'après le théorème de Bertini (théorème 5.1.4), pour tout idéal premier $\mathcal{P}$ de l'anneau A'_L des entiers de L sauf un nombre fini, les réductions $\bar{H}(T,Y)$ et $\bar{G}_1(T,X)$ modulo $\mathcal{P}$ de $H(T,Y)$ et $G_1(T,X)$ sont des polynômes absolument irréductibles. Le corps résiduel $A'_L/\mathcal{P}$ d'un tel premier $\mathcal{P}$ est un corps fini isomorphe à $\mathbb{F}_q$.

Soit $D(T) \in k[T]$ le discriminant du polynôme $H(T,Y)$ relativement à Y et $\bar{D}(T)$ la réduction de $D(T)$ modulo $\mathcal{P}$. On considère l'ensemble

$$\mathcal{T} = \left\{ t \in \mathbb{F}_q \;\middle|\; \begin{array}{c} \exists x \in \mathbb{F}_q |\ \bar{G}_1(t,x) = 0 \\ \bar{D}(t) \neq 0 \\ \bar{P}_0(t) \neq 0 \end{array} \right\}$$

D'après les bornes de Lang-Weil (théorème 6.4.2), le nombre de solutions $(t,x) \in \mathbb{F}_q^2$ de l'équation $\bar{G}_1(t,x) = 0$ est équivalent à q quand $q \to +\infty$. On en déduit que

$$\text{card}(\mathcal{T}) \geq \frac{q}{\deg_Y(G_1)}(1 + \text{o}(1))$$

Pour $t \in \mathcal{T}$, il découle de (*) et de la définition de $\mathcal{T}$ que $\bar{H}(t,Y)$ a d zéros distincts dans $\mathbb{F}_q$. Supposons maintenant que, pour tout $t \in \mathbb{F}_q$, le polynôme $\bar{H}(t,Y)$ a au moins un zéro dans $\mathbb{F}_q$. Alors le nombre $\mathcal{N}$ de solutions $(t,y) \in \mathbb{F}_q^2$ de l'équation $\bar{H}(t,y) = 0$ vérifie

$$\mathcal{N} \geq q + (d-1)\text{card}(\mathcal{T}) > q\left(1 + \frac{d-1}{\deg_Y(G_1)} + \text{o}(1)\right)$$

Cela, d'après les inégalités de Lang-Weil (appliquées ici au polynôme $\bar{H}$), entraîne que q est borné par une constante q_0 ne dépendant que de d.

D'après le lemme 6.4.3, il existe une infinité de premiers $\mathcal{P}$ de L de degré 1, *i.e.*, tels que $A'_L/\mathcal{P}$ soit de degré 1 sur le corps premier, disons $\mathbb{F}_p$, et donc tels que $\mathrm{card}(A'_L/\mathcal{P}) = p$. Choisissons-en un qui soit strictement plus grand que A et q_0. D'après ce qui précède, on peut conclure qu'il existe $t_0 \in \mathbb{F}_p$ tel que $\bar{H}(t_0, Y)$ n'a pas de racine dans $\mathbb{F}_p$.

Prenons $b \in \mathbb{Z}$ tel que $b \equiv t_0 \pmod{p}$. Alors $H(b, Y)$ n'a pas de racine dans k : sinon une racine y serait dans A'_k et on aurait $\bar{H}(t_0, \bar{y}) = 0$, contrairement à ce qu'on a établi ci-dessus. □

6.4.3. Preuve du théorème 4.1. — D'après la proposition 2.2.5, il existe N polynômes $Q_1, \ldots, Q_N \in \mathbb{Q}[T, Y]$ absolument irréductibles, unitaires en Y, avec $\deg_Y(Q_i) \geq 2$, $i = 1, \ldots, N$, et un ensemble fini tels que

$$V'_{Q_1,\ldots,Q_N} \subset H \cup F$$

Il s'agit de trouver $a, b \in \mathbb{Z}$, $a > 0$ tels que $Q_i(am + b, Y)$ n'a pas de racine dans k, $m \in \mathbb{Z}$, $i = 1, \ldots, N$ et tels que $(am + b)_{m\in\mathbb{Z}} \cap F = \emptyset$. Nous allons le démontrer par récurrence sur N.

Supposons $N = 0$. Si $F \cap \mathbb{Z} = \emptyset$, on peut prendre a et b entiers quelconques, avec $a > 0$. Si $F \cap \mathbb{Z} \neq \emptyset$, on pose $\alpha = \min(F \cap \mathbb{Z})$ et $\omega = \max(F \cap \mathbb{Z})$ et alors $b = \alpha - 1$ et $a = \omega - \alpha + 2$ conviennent (noter que $b + a = \omega + 1$).

Supposons maintenant, pour $1 \leq n \leq N$, avoir construit $a_{n-1}, b_{n-1} \in \mathbb{Z}$, $a_{n-1} > 0$ ayant la propriété que pour tout $t \in \mathbb{Z}$, si $t \equiv b_{n-1} \pmod{a_{n-1}}$, alors $Q_i(t, Y)$ n'a pas de racine dans k, $i = 1, \ldots, n-1$ et tels que $(a_{n-1}m + b_{n-1})_{m\in\mathbb{Z}} \cap F = \emptyset$. D'après le lemme 6.4.4, il existe un nombre premier p ne divisant pas a_{n-1} et un entier $b \in \mathbb{Z}$ ayant la propriété suivante : si $t \in \mathbb{Z}$ et $t \equiv b \pmod{p}$ alors $Q_n(t, Y)$ n'a pas de racine dans k. On prend $a_n = a_{n-1}p$ et b_n un entier vérifiant $b_n \equiv b_{n-1} \pmod{a_{n-1}}$ et $b_n \equiv b \pmod{p}$; l'existence d'un tel entier b_n est garantie par le théorème des restes chinois (théorème 1.1.6). Soit $t \in \mathbb{Z}$ tel que $t \equiv b_n \pmod{a_n}$. Alors d'une part $t \equiv b_{n-1} \pmod{a_{n-1}}$ et donc $Q_i(t, Y)$ n'a pas de racine dans k, $i = 1, \ldots, n-1$, et d'autre part $t \equiv b \pmod{p}$ et donc $Q_n(t, Y)$ n'a pas de racine dans k. Enfin la progression arithmétique $(a_n m + b_n)_{m\in\mathbb{Z}}$ ne coupe pas F puisque $(a_n m + b_n)_{m\in\mathbb{Z}} \subset (a_{n-1}m + b_{n-1})_{m\in\mathbb{Z}}$.

Remarque 6.4.5. — Le théorème 6.4.1 peut être amélioré. Le résultat que nous présentons ci-dessous sans démonstration repose sur une méthode différente mais utilise aussi les bornes de Lang-Weil. Il établit d'autre part un

lien avec le théorème de Grunwald. Nous renvoyons à [**DG09**] pour plus de détails.

Soient K un corps de nombres, S un ensemble fini de places finies de K et G un groupe fini. Pour chaque $v \in S$, fixons une extension galoisienne E_v/K_v de groupe $H_v \subset G$. Une question naturelle, appelée *problème de Grunwald* demande s'il existe des extensions galoisiennes E/K de groupe G qui ont pour v-complétions les extension E_v/K_v données ($v \in S$). On sait que la réponse est positive dans les cas suivants : quand G est cyclique d'ordre impair (Grunwald avec une correction de Wang, voir [**NSW08**, (9.2.8)]), et quand G est résoluble d'ordre premier au nombre de racines de l'unité dans $k$is solvable of order prime to the number of roots of 1 in K (Neukirch [**Neu79**], [**NSW08**, (9.5.5)]).

Soit $P(T,Y) \in k[T,Y]$ un polynôme absolument irréductible, unitaire en Y, à coefficients entiers sur $\mathbb{Z}$ et tel que l'extension $k(T)$ par une racine of P, disons N, soit galoisienne de groupe G. On note $\Delta(T)$ le discriminant de P par rapport à Y ; c'est un élément non nul de $k[T]$ à coefficients entiers sur $\mathbb{Z}$.

Théorème 6.4.6. — *On suppose que, pour tout $v \in S^{(7)}$,*

(i) *l'extension E_v/K_v est non ramifiée,*

(ii) *l'ordre q_v du corps résiduel de K_v est $\geq \deg(P)^4$ et sa caractéristique p_v ne divise pas $|G|$,*

(iii) *le polynôme $\Delta(T)$ est non nul modulo l'idéal de valuation de v,*

(iv) *les racines du poynôme $\Delta(T)$ ne "coalescent" pas modulo v, sachant que pour pour deux racines quelconques distinctes t_i, t_j, coalescer signifie que ($|t_i|_{\overline{v}} \leq 1$, $|t_j|_{\overline{v}} \leq 1$ et $|t_i - t_j|_{\overline{v}} < 1$) ou bien ($|t_i|_{\overline{v}} \geq 1$, $|t_j|_{\overline{v}} \geq 1$ et $|t_i^{-1} - t_j^{-1}|_{\overline{v}} < 1$), où $\overline{v}$ est un prolongement quelconque de v à $\overline{K}$.*

Alors il existe des points $t \in K$ tels que $\Delta(t) \neq 0$ et vérifiant :

(a) *le polynôme $P(t,Y)$ est irréductible dans $k[Y]$; en particulier, son corps de décomposition N_t est une extension galoisienne de groupe G.*

(b) *l'extension N_t/K est une solution du problème de Grunwald, c'est-à-dire N_tK_v est K_v-isomorphe à E_v ($v \in S$).*

De plus, l'ensemble de ces points t contient un sous-ensemble du type $K \cap \prod_{v \in T} U_v$ où $U_v \subset K_v$ est un ouvert non vide ($v \in T$) et $T \supset S$ un ensemble fini de places finies de K.

---

(7) Noter qu'étant donnés K et $P(T,Y)$ comme ci-dessus, les conditions (ii), (iii) et (iv) sont réalisées pour toute place v sauf un nombre fini.

Autrement dit, sous les conditions (i)-(iv), il existe des spécialisations $N_t/k(T)$ de l'extension $N/k(T)$ de groupe le groupe G (conclusion hilbertienne) et qui sont solution du problème de Grunwald. Sous les hypothèses faites ici sur $P(T,Y)$ (galoisien sur $k(T)$, absolument irréductible), le théorème 6.3.1 se déduit du cas particulier du théorème 6.4.6 où $S = \emptyset$[8].

6.5. Questions diverses

6.5.1. Parties hilbertiennes universelles. —

6.5.2. Borne pour la plus petite spécialisation. —

6.6. Application à la factorisation de polynômes

On va décrire ici une méthode pour factoriser les polynômes à plusieurs indéterminées à coefficients dans le corps $\mathbb{Q}$.

Pour les polynômes en une variable, il existe des algorithmes efficaces. Pour $f(Y) \in \mathbb{Z}[Y]$ de degré $\leq D$ et de coefficients $\leq H$ en valeur absolue, on peut effectuer la factorisation *en temps polynomial* en D et $\log(H)$, *i.e.* dans un temps $\leq (D + \log(H))^{\mathrm{O}(1)}$ [**LLL82**] (où O(1) est un constante absolue). Il existe des formes plus générales de ce résultat où $\mathbb{Z}$ est remplacé par l'anneau des entiers d'un corps de nombres [**CG82**], [**Len83**].

On ne dispose pas de tels algorithmes pour les polynômes de 2 variables ou plus. Dans la suite, nous nous limitons au cas de 2 variables. Le théorème d'irréductibilité de Hilbert va permettre de se ramener au cas d'une variable. Précisément, donnons-nous un polynôme $P(T,Y) \in \mathbb{Q}[T,Y]$ tel que $\deg_Y(P) \geq 1$. Sans perdre en généralité, on peut supposer que P est à coefficients dans $\mathbb{Z}$ et est unitaire en Y. Soit

$$P(T,Y) = \prod_{i=1}^{r} \Pi_i(T,Y)$$

la décomposition de $P(T,Y)$ dans $\mathbb{Z}[T,Y]$: les polynômes $\Pi_i(T,Y)$ sont irréductibles dans $\mathbb{Z}[T,Y]$ et unitaires en Y.

De façon générale, on appelle *hauteur* d'un polynôme $f \in \mathbb{C}[X_1,\ldots,X_n]$ le plus grand de ses coefficients en module ; on la note $H(P)$ et on note $h(P)$

[8] Le cas général du théorème de Hilbert peut s'en déduire moyennant un argument supplémentaire reposant sur le théorème de Cebotarev.

la *hauteur logarithmique* de P, *i.e.*, $h(P) = \log(H(P))$. Nous allons utiliser le résultat suivant.

Proposition 6.6.1. — *Pour $f_1, f_2 \in \mathbb{C}[X_1, \dots, X_n]$, on a*

$$h(f_1) \leq h(f_1) + h(f_2) \leq h(f_1 f_2) + n \deg(f_1 f_2)$$

Démonstration. — La première inégalité est évidente. Pour la seconde, on introduit les autres "mesures" suivantes d'un polynôme. Pour

$$P(\mathbf{X}) = \sum_{j_1=0}^{d_1} \cdots \sum_{j_n=0}^{d_n} a_{j_1 \dots j_n} X_1^{j_1} \cdots X_n^{j_n}$$

on pose :

$$L_2(P) = \left(\textstyle\sum_{\mathbf{j}} |a_{\mathbf{j}}|^2 \right)^{1/2}$$
$$M(P) = \exp\left(\textstyle\int_0^1 \cdots \int_0^1 \log |P(e^{2i\pi t_1}, \dots, e^{2i\pi t_n})| dt_1 \cdots dt_n \right)$$

De façon immédiate, on a

$$H(P) \leq L_2(P) \leq (d_1 + 1)^{1/2} \cdots (d_n + 1)^{1/2} H(P)$$

De la convexité de la fonction exponentielle on déduit

$$M(P)^2 \leq \int_0^1 \cdots \int_0^1 |P(e^{2i\pi t_1}, \dots, e^{2i\pi t_n})|^2 dt_1 \cdots dt_n = L_2(P)^2$$

soit $M(P) \leq L_2(P)$. L'inégalité suivante, prouvée ci-dessous, est due à Mahler [**Mah62**] :

$$|a_{j_1 \dots j_n}| \leq \binom{d_1}{j_1} \cdots \binom{d_n}{j_n} M(P)$$

On en déduit immédiatement l'inégalité importante

$$H(P) \leq 2^{nd} M(P)$$

où d est le degré total de P.

Démonstration de l'inégalité de Mahler. — Pour $n = 1$, le polynôme P s'écrit

$$P(X) = a_d X^d + \cdots + a_0 = a_d \prod_{j=1}^{d} (X - \alpha_j)$$

On montre préalablement, en utilisant la formule de Jensen

$$\textstyle\int_0^1 \log |f(e^{2i\pi t})| dt = \log |f(0)| + \sum_{|\zeta| \leq 1, f(\zeta) = 0} \log |\zeta|$$
(pour toute fonction holomorphe f sur un ouvert $\supset \overline{D(O,1)}$)

que

$$(*) \qquad M(P) = |a_d| \prod_{j=1}^{d} \max(1, |\alpha_j|)$$

On obtient alors la majoration voulue en écrivant les coefficients en fonction des racines du polynôme.

Pour $n \geq 1$, écrivons $P(\mathbf{X})$ sous la forme

$$P(\mathbf{X}) = \sum_{j_1=0}^{d_1} P_{j_1}(X_2, \ldots, X_n)\, X_1^{j_1}$$

D'après le cas $n = 1$, on a pour tous nombres complexes $z_2, \ldots, z_n$ et pour tout $j_1 = 0, \ldots, d_1$:

$$\log |P_{j_1}(z_2, \ldots, z_n)| \leq \log \binom{d_1}{j_1} + \int_0^1 \log |P(e^{2i\pi t_1}, z_2, \ldots, z_n)| dt_1$$

ce qui, en intégrant par rapport à $z_2, \ldots, z_n$ le long du cercle unité, puis en prenant les exponentielles, conduit à

$$M(P_{j_1}) \leq \binom{d_1}{j_1} M(P) \qquad (j_1 = 0, \ldots, d_1)$$

En itérant cet argument, on obtient l'inégalité annoncée (*). □

L'intérêt de la mesure $M(P)$ est qu'elle est multiplicative : pour tout $f_1, f_2 \in \mathbb{C}[X_1, \ldots, X_n]$, on a la formule

$$M(f_1 f_2) = M(f_1) M(f_2)$$

On obtient, en posant $\deg(f_1 f_2) = \delta$

$$H(f_1) H(f_2) \leq 2^{n\delta} M(P_1) M(P_2) = 2^{n\delta} M(P_1 P_2) \leq 2^{n\delta} (\delta + 1)^{n/2} H(P_1 P_2)$$

L'inégalité annoncée résulte alors de $2^\delta (\delta + 1)^{1/2} \leq e^\delta$ si $\delta \geq 2$. □

On a donc les renseignements suivants sur les polynômes $\Pi_1, \ldots, \Pi_r$:

$$\begin{cases} \deg_T(\Pi_i) \leq \deg_T(P) \\ \deg_Y(\Pi_i) \leq \deg_Y(P) \\ \deg(\Pi_i) \leq \deg(P) \\ h(\Pi_i) \leq h(P) + 2\deg(P) \end{cases}$$

Supposons maintenant que l'on connaisse un nombre t dans la partie hilbertienne $H_{\Pi_1, \ldots, \Pi_r} \subset \mathbb{Q}$. La factorisation

$$P(t, Y) = \prod_{i=1}^{r} \Pi_i(t, Y)$$

est alors la décomposition de $P(t,Y)$ en irréductibles de $\mathbb{Q}[Y]$. Supposons que celle-ci puisse être déterminée *a priori*, par exemple en utilisant l'algorithme de Lenstra-Lenstra-Lovász [**LLL82**] et soit donnée par

$$P(t,Y) = \prod_{i=1}^{r} \pi_i(Y)$$

On obtient alors le nombre r et les degrés $\deg_Y(\Pi_1), \ldots, \deg_Y(\Pi_r)$; notons les $d_i = \deg(\pi_i) = \deg_Y(\Pi_i)$, $i = 1, \ldots, r$. On peut ensuite chercher les polynômes $\Pi_1, \ldots, \Pi_r$ sous la forme

$$\Pi_i(T,Y) = \sum_{j=0}^{d_i} \Pi_{ij}(T) Y^j, \quad i = 1, \ldots, r$$

où les polynômes $\Pi_{ij}(T)$ sont à coefficients dans $\mathbb{Z}$ et de degré $\leq \deg_T(P)$. Si les polynômes π_i sont donnés par

$$\pi_i(Y) = \sum_{j=0}^{d_i} \pi_{ij} Y^j, \quad i = 1, \ldots, r$$

avec $\pi_{ij} \in \mathbb{Z}$, on a

$$\Pi_{ij}(t) = \pi_{ij} \quad i = 1, \ldots, r \text{ et } j = 1, \ldots, d_i$$

Si au lieu d'*un* nombre t, on connait N nombres $t_1, \ldots, t_N$ dans la partie hilbertienne $H_{\Pi_1,\ldots,\Pi_r}$, avec $N \geq \deg_T(P)+1$, le problème est ramené à résoudre $\sum_{i=1}^{r} d_i$ systèmes linéaires de N équations à $\deg_T(P)+1$ inconnues. De plus, si $N \geq \deg_T(P)+1$, ces systèmes ont tous une solution unique.

Exemple 6.6.2. — (G. Durlet) Soit

$$P(T,Y) = Y^4 - TY^3 + (T+1)Y^2 + (T^2-T)Y - 2T^2 + 2T$$

Pour $T = 3$, on trouve $P(3,Y) = (Y^2-2)(Y^2-3Y+6)$. Cela indique que la décomposition de $P(T,Y)$ ne comporte pas de facteur de degré 1 (en Y). Pour $T = 4$, on trouve $P(4,Y) = (Y^2-3)(Y^2-4Y+8)$. Si la décomposition de $P(T,Y)$ comporte exactement 2 facteurs Π_1 et Π_2 de degré 2, une troisième valeur $T = t$ pour laquelle $P(t,Y)$ se décompose en 2 facteurs de degré 2 permettra de déterminer Π_1 et Π_2. La spécialisation $T = 5$ ne convient pas car $P(5,Y) = (Y-2)(Y+2)(Y^2-5Y+10)$. Pour $T = 6$, on trouve $P(6,Y) = (Y^2-5)(Y^2-6Y+12)$. Parmi les diverses identifications de $\Pi_1(t,Y)$ et $\Pi_2(t,Y)$ aux facteurs de $P(t,Y)$ pour $t \in \{3,4,6\}$, il en figure une qui conduit à la

décomposition cherchée, si l'hypothèse "$P(T,Y)$ produit de 2 facteurs de degré 2" est exacte. Dans le cas contraire, $P(T,Y)$ serait irréductible. L'identification

$$\begin{cases} \Pi_1(3,Y) = Y^2 - 2 \\ \Pi_1(4,Y) = Y^2 - 3 \\ \Pi_1(6,Y) = Y^2 - 5 \end{cases} \quad \text{et} \quad \begin{cases} \Pi_2(3,Y) = Y^2 - 3Y + 6 \\ \Pi_2(4,Y) = Y^2 - 4Y + 8 \\ \Pi_2(6,Y) = Y^2 - 6Y + 12 \end{cases}$$

conduit à

$$P(T,Y) = (Y^2 - T + 1)(Y^2 - TY + 2T)$$

De façon générale, le problème est de pouvoir déterminer effectivement suffisamment de points dans la partie hilbertienne $H_{\Pi_1,\dots,\Pi_r}$. On ne connaît pas explicitement les polynômes $\Pi_1, \dots, \Pi_r$. On sait cependant qu'ils sont de degré relatifs en T et Y bornés respectivement par $\deg_T(P)$ et $\deg_Y(P)$ et de hauteur logarithmique $\leq h(P) + 2\deg(P)$. Il n'y a qu'un nombre fini de tels polynômes. Théoriquement donc, les éléments de la partie hilbertienne associée a l'ensemble de tous ces polynômes conviendront. En pratique, il s'agit d'en trouver effectivement. Ainsi pour pouvoir déduire de la méthode un algorithme de factorisation en temps polynomial, il faudrait pouvoir disposer d'une *bonne borne pour la plus petite bonne spécialisation* pour le théorème de Hilbert. De façon précise, la question est de

Problème 6.6.3. — Trouver une constante $C = C(n, D, h)$ dépendant de n, d et h la plus petite possible et telle que, si $P_1, \dots, P_n$ sont n polynômes irréductibles dans $\mathbb{Z}[T,Y]$, unitaires en Y, de degré $\leq D$ et de hauteur logarithmique $\leq h$, alors la partie hilbertienne contient un nombre $u/v \in \mathbb{Q}$ tel que $\max(\log(|u|), \log(|v|)) \leq C$.

La première borne de ce type a été donnée dans [**Dèb96**] ; l'énoncé ci-dessus est démontré avec la borne

$$C = 10^{10} D^{100nD^2 \operatorname{Log}(D)} \, (h^2 + 1)$$

Cette borne a été améliorée dans [**SZ95**] où la dépendance en D a été ramenée de $D^{D^{0(1)}}$ à $D^{0(1)}$, puis dans [**Wal05**] où la borne obtenue

$$C = (2^{109} 2^{76 \deg_Y(P)} \deg_T(P)^{64} h^{19})^4$$

dépend polynomialement de h et de $\deg_T(P)$ mais encore exponentiellement de $\deg_Y(P)$. Il faudrait rendre polynomiale cette dernière dépendance pour obtenir un *algorithme déterministe de factorisation en temps polynomial des polynômes en* 2 *variables*, comme celui de [**LLL82**] l'est en 1 variable. Cela est possible dans le cas galoisien, c'est-à-dire, quand l'extension engendrée sur $\mathbb{Q}(T)$ par une racine de $P(T,Y)$ est une extension galoisienne [**Wal05**]. On

montre dans [**DW08**] que ce l'est aussi sous certaines hypothèses sur le groupe de Galois, par exemple quand il est résoluble et que son action sur les racines est primitive, mais le cas général n'est pas couvert.

CHAPITRE 7

GROUPE FONDAMENTAL ET REVÊTEMENTS TOPOLOGIQUES

7.1. Groupe fondamental

7.1.1. Homotopie des chemins. — Soit X un espace topologique. Un *chemin* dans X est une application continue d'un intervalle fermé $[a, b]$ dans X où $a < b$. Les valeurs en a et en b sont respectivement l'*origine* et l'*extrémité du chemin*. On a la notion de
- *chemin constant* basé en $x \in X$: $c_x(t) = x$ pour tout $t \in [a, b]$.
- *chemin inverse* d'un chemin c : c'est le chemin $\overline{c}$ défini par $\overline{c}(t) = c(a+b-t)$.
- *chemin composé* : si $c : [a, b] \to X$ et $c' : [a', b'] \to X$ sont deux chemins tels que l'extrémité de c coincide avec l'origine de c', le chemin composé est l'application :

$$\begin{cases} [a, b+b'-a'] & \to & X \\ t & \to & (cc')(t) = \begin{cases} c(t) \text{ si } a \leq t \leq b \\ c'(t+a'-b) \text{ si } b \leq t \leq b+b'-a' \end{cases} \end{cases}$$

Remarque 7.1.1. — (a) Le chemin cc' s'obtient en parcourant c puis c'. On trouve aussi la convention inverse dans la littérature, c'est-à-dire, c' d'abord puis c. Les deux ont des avantages et des inconvénients. Ce choix aura une incidence au moment de définir l'action de la monodromie.

(b) Souvent, l'intervalle de définition des chemins est fixé égal à $[0, 1]$. Ce point est mineur et n'a aucune incidence sur la suite. Notre définition présente seulement quelques avantages techniques.

Deux chemins c et c' définis sur $[a,b]$ sont dits *homotopes* entre x et y s'il existe une application continue $H : [0,1] \times [a,b] \to X$ telle que

$$\begin{cases} H(0,t) = c(t) \text{ pour tout } t \in [a,b] \\ H(1,t) = c'(t) \text{ pour tout } t \in [a,b] \\ H(s,a) = x \text{ et } H(s,b) = y \text{ pour tout } s \in [0,1] \end{cases}$$

Deux chemins c et c' d'origine x et d'extrémité y sont dits *homotopes* entre x et y s'il existe un reparamétrisation de ces chemins sur un même intervalle $[a,b]$ — de façon précise, deux homéomorphismes croissants φ et φ' entre $[a,b]$ et les intervalles de paramétrisation initiaux de c et de c' — tels que les chemins $c\varphi$ et $c'\varphi'$, tous deux paramétrés par $[a,b]$ soient homotopes au sens précédent.

Proposition 7.1.2. — *Cette définition ne dépend pas de la reparamétrisation choisie pour les deux chemins.*

Démonstration. — Si ψ et ψ' sont deux homéorphismes croissants entre $[u,v]$ et $[a,b]$ et $H : [0,1] \times [a,b] \to X$ une homotopie entre $c\varphi$ et $c'\varphi'$, alors on obtient une homotopie $[0,1] \times [u,v] \to X$ entre $c\varphi\psi$ et $c\varphi'\psi'$ en composant H à droite par la correspondance

$$\begin{cases} [0,1] \times [u,v] & \to & X \\ (s,t) & \to & (s,(1-s)\psi(t) + s(\psi'(t)) \end{cases}$$

qui, à s fixé correspond à un homéomorphisme croissant entre $[u,v]$ et $[0,1]$. □

En particulier, on peut utiliser pour φ et φ' la paramétrisation linéaire naturelle d'un segment de $\mathbb{R}$ par $[0,1]$.

La relation d'homotopie est une relation d'équivalence.

> [Réflexivité : $(s,t) \to c(t)$ est une homotopie de c à c.
> Symétrie : utiliser la correspondance $H(s,t) \leftrightarrow H(1-s,t)$.
> Transitivité : prendre le même intervalle $[0,1]$ de paramétrisation pour les trois chemins ; alors, avec des notations évidentes $H(2s,t)$ pour $s \in [0,1/2]$ et $H'(2s-1,t)$ pour $s \in [1/2,1]$ définit une homotopie entre le premier et le troisième.]

Théorème 7.1.3. — *Soient c, c' et c'' trois chemins sur X paramétrés respectivement par $[a,b]$, $[a',b']$ et $[a'',b'']$.*

(a) *Si c et c' sont homotopes entre x et y, et si y est l'origine de c'', alors les chemins composés cc'' et $c'c''$ sont homotopes. De la même façon, si x est l'extrémité de c'', alors les chemins composés $c''c$ et $c''c'$ sont homotopes.*

(b) *Si c joint x à y, c' joint y à z et c'' joint z à w, alors les chemins $(cc')c''$ et $c(c'c'')$ sont égaux.*

(c) *Si c joint x à y et c_x est le chemin constant égal à x, alors le chemin $c_x c$ est homotope à c. Si c_y est le chemin constant égal à y, alors le chemin $c_x c$ est homotope à c.*

(d) *Si c joint x à y, alors les chemins $c\bar{c}$ et $\bar{c}c$ sont homotopes à c_x et c_y.*

Démonstration. — (a) Soient c et c' deux chemins homotopes entre x et y et c'' un chemin d'origine y. On veut montrer que les chemins composés cc'' et $c'c''$ sont homotopes.

1er cas. Supposons d'abord que c et c' sont tous deux paramétrés par $[a,b]$. Avec des notations évidentes, $K(s,t) = H(s,t)$ pour $t \in [a,b]$ et $K(s,t) = c''(t+a'-b)$ pour $t \in [b, b+b''-a']$ définit une homotopie entre cc'' et $c'c''$.

2ème cas. Cas général. Soit $\varphi : [a,b] \to [a',b']$ un homéomorphisme croissant. D'après le 1er cas, les deux chemins $c.c''$ et $(c'\varphi).c''$ définis sur $[a, b+b''-a'']$ sont homotopes. Si $\tilde{\varphi}$ est l'homéomorphisme defini sur $[a, b+b''-a'']$ par $\tilde{\varphi} = \varphi$ sur $[a,b]$ et $\tilde{\varphi}(t) = t + b' - b$ sur $[b, b+b''-a'']$, alors on a

$$((c'\varphi).c'') \circ \tilde{\varphi}^{-1} = c'.c''$$

La relation d'homotopie étant transitive, on obtient bien l'homotopie de cc'' et $c'c''$. La preuve est similaire pour le seconde moitié de l'énoncé (a).

(b) Simple vérification.

(c) Supposons c et c_y paramétrés par $[0,1]$. L'application définie par

$$H(s,t) = \begin{cases} c\left(\frac{2t}{1+s}\right) & \text{pour} \quad 0 \leq t \leq \frac{1+s}{2} \\ y & \text{pour} \quad \frac{1+s}{2} \leq t \leq 1 \end{cases}$$

définit une homotopie de cc_y vers c. On procède pareillement pour construire une homotopie de $c_x c$ vers c.

(d) Supposons c paramétré par $[0,1]$. L'application $H : [0,1] \times [0,1] \to X$ définie par

$$H(s,t) = \begin{cases} x & \text{pour} \quad 0 \leq t \leq \frac{s}{2} \\ c(2t-s) & \text{pour} \quad \frac{s}{2} \leq t \leq \frac{1}{2} \\ c(2-2t-s) & \text{pour} \quad \frac{1}{2} \leq t \leq \frac{2-s}{2} \\ x & \text{pour} \quad \frac{2-s}{2} \leq t \leq 1 \end{cases}$$

définit une homotopie de $\bar{c}c$ vers c_x. On procède pareillement pour construire une homotopie de $c\bar{c}$ vers c_y. □

7.1.2. Groupe fondamental. —

7.1.2.1. Groupoïde fondamental. — Si c est un chemin joignant x à y, on note $[c]$ sa classe d'homotopie et $\Pi_{x,y}(X)$ l'ensemble des classes d'homotopie de chemins joignant x à y. Le composition des chemins induit une "loi de composition" sur l'ensemble

$$\Pi(X) = \bigsqcup_{x,y} \Pi_{x,y}(X)$$

Précisément, pour $[c] \in \Pi_{x,y}$ et $[c'] \in \Pi_{y,z}$, on pose $[c][c'] = [cc']$. Cette définition a un sens d'après le théorème 7.1.3. Il y a un petit abus de langage car cette loi n'est pas définie partout. D'après le théorème 7.1.3, cette loi satisfait aux axiomes suivants :
(i) axiomes d'associativité (quand ils ont une sens).
(ii) existence d'un neutre à droite et et d'un neutre à gauche pour chaque sous-ensemble $\Pi_{x,y}(X)$.
(iii) existence d'un inverse pour tout élément.

Cela confère à $\Pi(X)$ un structure de *groupoïde*. On l'appelle le *groupoïde fondamental (ou de Poincaré)* de X.

7.1.2.2. Groupe fondamental. —

Théorème 7.1.4. — *Soit $x \in X$. La composition des chemins induit une structure de groupe sur l'ensemble $\Pi_{x,x}(X)$ des classes d'homotopie de chemins basés en x (c'est-à-dire joignant x à x).*

Le groupe $\Pi_{x,x}(X)$ est appelé groupe fondamental de X basé en x et est noté $\pi_1(X, x)$.

Proposition 7.1.5. — *Soit c un chemin joignant x à y. La correspondance $[\gamma] \to [c\gamma\overline{c}]$ induit un isomorphisme α_c du groupe $\pi_1(X, y)$ sur le groupe $\pi_1(X, x)$. Cet isomorphisme ne dépend que de la classe d'homotopie $[c]$ du chemin c. De façon plus précise, si c' est un chemin joignant x à y, on a $\alpha_{c'} = [c'\overline{c}]\, \alpha_c\, [c'\overline{c}]^{-1}$.*

Démonstration. — Les résultats du §7.1.1 montrent que α_c est bien défini et justifient d'autre part le calcul suivant

$$\begin{aligned} \alpha_c(\gamma\gamma') &= [c\gamma\gamma'\overline{c}] \\ &= [c]\ [\gamma]\ [\gamma']\ [c]^{-1} \\ &= [c]\ [\gamma]\ [c]^{-1}\ [c]\ [\gamma']\ [c]^{-1} \\ &= \alpha_c(\gamma)\ \alpha_c(\gamma') \end{aligned}$$

ce qui prouve que α_c est un homomorphisme. Son inverse est $\alpha_{\overline{c}}$. La formule $\alpha_{c'} = [c'\overline{c}]\,\alpha_c\,[c'\overline{c}]^{-1}$ s'établit de la même façon. □

Corollaire 7.1.6. — *Si x et y sont dans une même composante connexe par arcs, alors les groupes $\pi_1(X,x)$ et $\pi_1(X,y)$ sont isomorphes.*

Quand X est connexe par arcs, tous les groupes fondamentaux sont isomorphes. On parle *du* groupe fondamental de X, que l'on désigne par $\pi_1(X)$.

7.1.2.3. Propriétés fonctorielles. — Si $f : X \to Y$ est une application continue, la correspondance $c \to f \circ c$ qui transforme un chemin sur X en un chemin sur Y, est compatible avec

∗ la relation d'homotopie (c'est-à-dire : $[c] = [c'] \Rightarrow [f \circ c] = [f \circ c']$)

[Clair : composée avec f, une homotopie sur X entre c et c' devient une homotopie sur Y entre $f \circ c$ et $f \circ c'$.]

∗ la composition des chemins (c'est-à-dire : $f \circ (cc') = (f \circ c)(f \circ c')$).

On notera $f_* : \Pi(X) \to \Pi(Y)$ l'application induite par cette correspondance sur les classes d'homotopie.

Proposition 7.1.7. — *L'application f_* induit un homomorphisme du groupe fondamental $\pi_1(X,x)$ vers le groupe fondamental $\pi_1(Y,f(x))$. De plus la correspondance $f \to f_*$ est fonctorielle, c'est-à-dire, $(Id_X)_* = Id_{\pi_1(X)}$ et $(f \circ g)_* = f_* \circ g_*$.*

Corollaire 7.1.8. — *Le groupe fondamental d'un espace topologique connexe par arcs est un invariant topologique, c'est-à-dire : deux espaces connexes par arcs ont des groupes fondamentaux isomorphes s'ils sont homéomorphes.*

7.2. Calculs de groupes fondamentaux

Nous commençons par des rappels sur quelques espaces classiques dont nous calculerons ensuite le groupe fondamental.

7.2.1. Quelques espaces classiques. —

7.2.1.1. Espaces projectifs et sphères. —

Définition 7.2.1. — Soient K un corps et V un K-espace vectoriel de dimension finie.

(a) L'espace projectif $\mathbb{P}(V)$ est l'ensemble des droites vectorielles de V. Pour tout entier $n > 0$, on pose $\mathbb{P}^n(K) = \mathbb{P}(K^{n+1})$.

(b) $\mathbb{P}(V)$ s'identifie au quotient $V \setminus \{O\}/K^\times$. Pour tout $(n+1)$-uplet $(x_0, \ldots, x_n) \in K^{n+1} \setminus (0, \ldots, 0)$, on note $(x_0 : \cdots : x_n) \in \mathbb{P}^n(K)$ sa classe modulo $K^\times$. Si $K = \mathbb{R}$ ou $\mathbb{C}$, on munit $\mathbb{P}(V)$ de la topologie quotient.

On vérifie que l'espace $\mathbb{P}^n(K)$ correspond à l'ensemble des points K-rationnels de la variété projective $\mathbb{P}^n_{\mathbb{Z}}$ définie en géométrie algébrique (*Cf.* §3.3.2).

L'espace projectif $\mathbb{P}^1(K)$ s'identifie aussi à l'ensemble $K \cup \{\infty\}$, constitué de K et d'un point supplémentaire appelé point à l'infini.

Exercice 7.2.2. — Montrer que l'action naturelle de $\mathrm{GL}(V)$ sur V induit une action fidèle de $\mathrm{PGL}(V) = \mathrm{GL}(V)/K^\times$ sur $\mathbb{P}(V)$.

Pour tout entier $m \geq 0$, on désigne par S^m la sphère unité de $\mathbb{R}^{m+1}$. L'espace $\mathbb{P}^n(\mathbb{R})$ s'identifie à l'espace $S^n/\{-1, 1\}$ des vecteurs unitaires de $\mathbb{R}^{n+1}$ au signe près, $\mathbb{P}^n(\mathbb{C})$ à l'espace S^{2n+1}/S^1 des vecteurs unitaires de $\mathbb{C}^n$ modulo les complexes de module 1.

Exercice 7.2.3. — Montrer que l'action de $\mathrm{PGL}(2) = \mathrm{PGL}(K^2)]$ sur $\mathbb{P}^1(K)$ correspond, *via* l'identification $\mathbb{P}^1(K) = K \cup \{\infty\}$, à l'action des homographies $(az + b)/(cz + d)$ sur $K \cup \{\infty\}$.

Pour $K = \mathbb{R}$, l'isomorphisme $\mathbb{P}^1(\mathbb{R}) \simeq \mathbb{R} \cup \{\infty\}$ est un homéomorphisme si $\mathbb{R} \cup \{\infty\}$ est muni de la topologie du compactifié de $\mathbb{R}$ pour laquelle les ouverts sont les boules ouvertes de $\mathbb{R}$ et les complémentaires des boules fermées centrées en l'origine. L'homéomorphisme provient de la correspondance qui envoie (u, v) sur u/v si $v \neq 0$ et sur ∞ sinon : cette correspondance est continue (utiliser le critère séquentiel pour les points $(a, 0)$ avec $a \neq 0$), passe au quotient et donne une application $\mathbb{P}^1(\mathbb{R}) \to \mathbb{R} \cup \{\infty\}$ continue et bijective et donc un homéomorphisme car les espaces sont compacts.

On a aussi un homéomorphisme entre $\mathbb{P}^1(\mathbb{R})$ et S^1, que fournit la projection à partir de $(0, 1)$:

$$\begin{array}{ccc} S^1 & \to & \mathbb{P}^1(\mathbb{R}) \\ (x, y) & \to & \begin{cases} (y-1 : x) & \text{si } y \neq 1 \\ (-x : y+1) & \text{si } y \neq -1 \end{cases} \end{array}$$

dont la réciproque est :

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{R}) & \to & S^1 \\ (u, v) & \to & \left(\dfrac{-2uv}{u^2+v^2}, \dfrac{v^2-u^2}{u^2+v^2}\right) \end{array}$$

[On montre successivement que f est définie, que g est définie et continue, que $f \circ g(u : v) = (u : v)$ (le calcul donne $(u^2 : uv)$ si $(u \neq 0)$ et $(uv : v^2)$ si $(v \neq 0)$) et que $g \circ f(x, y) = (x, y)$[(1)].]

Les applications ci-dessus sont plus généralement définies avec $\mathbb{R}$ remplacé par n'importe quel corps K. Il faut comprendre alors S^1 comme la courbe d'équation $x^2 + y^2 = 1$ et les applications fournissent un isomorphisme au sens algébrique entre cette courbe et $\mathbb{P}^1$.

On montre similairement que la *sphère de Riemann* $\mathbb{P}^1(\mathbb{C})$ est homéomorphe au compactifié $\mathbb{C} \cup \{\infty\}$ et à S^2.

[Pour le premier homéomorphisme, on procède comme pour $\mathbb{P}^1(\mathbb{R})$. Pour le second, on utilise la projection stéréographique $p : S^2 \setminus \{N(0, 0, 1)\} \to \mathbb{C}$ qui à un point $M \neq N$ de S^1 associe le point intersection de (NM) avec le plan réel identifié à $\mathbb{C}$. Cette application est un homéomorphisme, se prolonge continûment par $p(N) = \infty$, *etc.*]

Exercice 7.2.4. — Montrer que $\mathbb{P}^2(\mathbb{C})$ est homéomorphe à $\mathbb{C}^2 \cup \mathbb{P}^1$.

Proposition 7.2.5. — *Pour tout entier $n > 0$, les espaces topologiques $\mathbb{P}^n(\mathbb{C})$ et $\mathbb{P}^n(\mathbb{R})$ sont connexes et compacts.*

Démonstration. — Ces propriétés se déduisent des isomorphismes $\mathbb{P}^n(\mathbb{C}) \simeq \mathbb{C}^{n+1}/\mathbb{C}^\times \simeq S^{2n+1}/S^1$ et $\mathbb{P}^n(\mathbb{R}) \simeq \mathbb{R}^{n+1}/\mathbb{R}^\times \simeq S^n/\{\pm 1\}$. □

7.2.1.2. Tores. — Pour tout $m > 0$, on appelle *tore* l'espace $T^m = (S^1)^m$. Il est homéomorphe à $\mathbb{R}^m/\mathbb{Z}^m$ (voir que $t \to exp(2i\pi t)$ induit une bijection continue entre $\mathbb{R}/\mathbb{Z}$ et S^1, donc un homéomorphisme puisque $\mathbb{R}/\mathbb{Z}$ et S^1 sont compacts ($\mathbb{R}/\mathbb{Z}$ est compact car égal à $[0, 1]/\mathbb{Z}$). On en déduit que le tore T^m est connexe et compact.

On appelle *tore complexe* l'espace topologique $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \simeq T^2$ où ω_1 et ω sont deux nombres complexes tels que $\omega_1/\omega_2 \notin \mathbb{R}$. Le tore complexe s'identifie à un polygone à 4 cotés, chacun de ces côtés étant identifié avec le côté opposé. On obtient ainsi la représentation habituelle en forme de bouée ou de beignet du tore complexe à 1 trou.

(1) On peut aussi utiliser la projection stéréographique $p : S^1 \setminus \{N(0, 1)\} \to \mathbb{R}$ qui à un point $M \neq A$ de S^1 associe le point intersection de (NM) avec Ox. Cette application est un homéomorphisme, se prolonge continûment par $p(N) = \infty$, *etc.*

7.2.2. Espaces simplement connexes. —

Définition 7.2.6. — Soit X un espace topologique non vide connexe par arcs. Les propriétés suivantes sont équivalentes.

(i) Les groupes fondamentaux $\pi_1(X, x)$ $(x \in X)$ sont triviaux.

(ii) Il existe $x \in X$ tel que le groupe fondamental $\pi_1(X, x)$ est trivial.

(iii) Deux chemins ayant même origine et même extrémité sont homotopes.

Un espace topologique X vérifiant ces propriétés est dit simplement connexe.

Démonstration. — (i)⇒ (iii) : si γ et γ' joignent x à y, on a, d'après (i), $[\gamma'\overline{\gamma}] = [c_x]$, ce dont on déduit $[\gamma] = [\gamma']$.

(iii)⇒ (i) : banal

(ii)⇔ (i) : d'après le corollaire 7.1.6. □

Exemple 7.2.7. — (a) Un sous-ensemble $X \subset \mathbb{R}^n$ qui est étoilé par rapport à un de ses points x (*e.g.* convexe) est simplement connexe.

> [Si c joint x à x, l'application donnée par $F(s,t) = sx + (1-s)c(t)$ définit une homotopie de c au chemin constant x.]

(b) $\mathbb{C} \setminus \{0\}$ n'est pas simplement connexe.

> [En effet d'après la théorie de Cauchy, l'intégrale le long d'un chemin γ d'une fonction continue sur un ouvert U contenant γ ne dépend pas du représentant de la classe d'homotopie de $[\gamma]$ dans U. En particulier, elle est nulle le long d'un chemin fermé si U est simplement connexe. On sait bien que le long du cercle unité, l'intégrale de $1/z$ est non nulle.]

(c) Si X et Y sont simplement connexes, alors le produit $X \times Y$ l'est aussi. Cela résulte du résultat plus général suivant.

Proposition 7.2.8. — *Soient X et Y deux espaces topologiques, $p_X : X \times Y \to X$ et $p_Y : X \times Y \to Y$ les deux projections et (x, y) un point de $X \times Y$. L'application $(p_X)_* \times (p_Y)_*$ est un isomorphisme de $\pi_1(X \times Y, (x, y))$ sur $\pi_1(X, x) \times \pi_1(Y, y)$.*

7.2.3. Le cercle S^1 et les tores T^m. — On note p l'application $\mathbb{R} \to S^1$ définie par $p(t) = \exp(2i\pi t)$. Pour tout entier $n \in \mathbb{Z}$, on note γ_n le chemin défini sur $[0, 1]$ par $\gamma_n(t) = p(nt)$. Le résultat principal est le suivant.

Théorème 7.2.9. — *La correspondance $\Theta : n \to [\gamma_n]$ est un isomorphisme de groupes de $\mathbb{Z}$ sur $\pi_1(S^1, 1)$.*

La démonstration utilise le résultat classique suivant sur le relèvement des applications à valeurs dans le cercle.

Théorème 7.2.10. — *Soit K un produit d'intervalles fermés bornés et $f : K \to S^1$ une application continue.*

(a) *Il existe une application continue $\varphi : K \to \mathbb{R}$ telle que $p \circ \varphi = f$. On dit que φ est un relèvement de f.*

(b) *Deux relèvements de f diffèrent d'une application constante égale à un entier.*

Démonstration. — (b) provient de la connexité de K. Pour (a), l'outil essentiel est le fait que l'application p induit un homéomorphisme entre tout intervalle ouvert $]a, a + 2\pi[$ de longueur 2π et $S^1 \setminus \{e^{ia}\}$. Ainsi l'existence du relèvement φ est claire si f n'est pas surjective. Dans le cas général, grâce à la compacité de K qui entraîne que f est uniformément continue, on peut découper K en un nombre fini de petits " polyintervalles" compacts K_i sur lesquels f n'est pas surjective et où il existe donc un relèvement f_i de f ($i \in I$). On peut ordonner ces polyintervalles de telle sorte que l'intersection de chacun d'eux avec la réunion des précédents soit connexe. On peut alors, en procédant par récurrence, recoller tous les relèvements f_i ($i \in I$), après les avoir éventuellement modifié par une constante. □

Démonstration du théorème 7.2.9. — Si c est un chemin dans S^1 basé en 1 paramétré par $[a, b]$, notons $\tilde{c} : [a, b] \to \mathbb{R}$ l'unique relèvement de relèvement de c tel que $\tilde{c}(a) = 0$. L'extrémité $\tilde{c}(b)$ de $\tilde{c}$ est un entier. Appelons le le degré de c et notons le $\deg(c)$. Pour tout entier n, $\widetilde{\gamma_n} = [0, n]$ (paramétré par $[0, 1]$ par $t \to nt$) et donc $\deg(\gamma_n) = n$.

Pour voir que Θ est surjective, montrons que

$$(*) \qquad [c] = \Theta(\deg(c))$$

Posons $n = \deg(c)$. Les chemins $\tilde{c}$ et $[0, n]$ sont deux chemins dans $\mathbb{R}$ de mêmes extrémités 0 et n. Comme $\mathbb{R}$ est simplement connexe, ils sont homotopes. Les chemins $p \circ \tilde{c} = c$ et $p \circ [0, n] = \gamma_n$ le sont *a fortiori*. D'où $\gamma_n = \Theta(n) = [c]$.

Montrons que Θ est injective. Supposons $[\gamma_n] = [\gamma_m]$, c'est-à-dire : il existe une homotopie $H : [0, 1] \times [0, 1] \to S_1$ joignant γ_n à γ_m. Soit $\tilde{H}$ l'unique relèvement de H tel que $\tilde{H}(0, 0) = 0$. L'application partielle $\tilde{H}(s, 1)$ est continue et à valeurs dans $\mathbb{Z}$; elle est donc constante. En particulier, $\widetilde{\gamma_n} = (t \to \widetilde{H}(0, t))$ et $\widetilde{\gamma_m} = (t \to \widetilde{H}(1, t))$ ont même extrémité, c'est-à-dire $n = m$. [On a

$\widetilde{\gamma_n} = (t \to \widetilde{H}(0,t))$ car les deux termes sont des relèvements de γ_n valant 0 en 0].

Enfin Θ est un homomorphisme de groupes. En effet, le chemin $[0, n+m]$ est un relèvement de $\gamma_n\gamma_m$ commençant en 0. Donc $\deg(\gamma_n\gamma_m) = n+m$. De la formule ci-dessus, on déduit alors que $[\gamma_n][\gamma_m] = \Theta(n+m)$. □

Corollaire 7.2.11. — *Le groupe fondamental du tore T^m est $\mathbb{Z}^m$.*

Démonstration. — Conséquence de la définition $T^m = (S^1)^m$ et de la proposition 7.2.8. □

7.2.4. Rétracte par déformation. —

Définition 7.2.12. — (a) Un sous-espace Y de X est un rétracte de X s'il existe une application continue $r : X \to Y$ telle que $r(y) = y$ pour tout $y \in Y$. L'application r est appelée rétraction de X sur Y.

(b) Un sous-espace Y de X est un rétracte par déformation de X s'il existe une rétraction $r : X \to Y$ et une application continue $H : [0,1] \times X \to X$ telles que
(i) $H(0,x) = x$ pour tout $x \in X$.
(ii) $H(1,x) = r(x)$ pour tout $x \in X$.
(iii) $H(s,y) = y$ pour tout $y \in Y$ et tout $s \in [0,1]$.

Exemple 7.2.13. — (a) Un point x d'un espace X est un rétracte de X : l'application $X \to X$ constante égale à x est un rétraction de X sur x.

(b) La sphère unité S^m de $\mathbb{R}^{m+1}$ est un rétracte de la boule unité ouverte privée de l'origine. Par exemple, une rétraction est donnée par l'application $x \to x/ \parallel x \parallel$.

(c) Plus précisément, la sphère unité S^m de $\mathbb{R}^{m+1}$ est un rétracte par déformation de la boule unité privée de l'origine. Par exemple, une rétraction par déformation est donnée par l'application

$$(s,x) \to s\frac{x}{\parallel x \parallel} + (1-s)x$$

(d) S^1 n'est pas un rétracte de $\mathbb{C}$. Plus généralement le (a) du théorème 7.2.14 ci-dessous montre que tout rétracte d'un espace simplement connexe est simplement connexe.

Théorème 7.2.14. — *Soit Y un sous-espace de X, $i : Y \to X$ l'injection canonique et $y \in X$.*

(a) *Si Y est un rétracte de X, alors l'homomorphisme $i_* : \pi_1(Y, y) \to \pi_1(X, y)$ est injectif.*

(b) *Si Y est un rétracte de X par déformation, alors l'homomorphisme $i_* : \pi_1(Y, y) \to \pi_1(X, y)$ est un isomorphisme.*

Démonstration. — (a) Si $r : X \to Y$ est une rétraction de X sur Y, $r \circ i = \mathrm{Id}_Y$. On en déduit que $(r \circ i)_* = r_* \circ i_*$ est un isomorphisme, d'où l'injectivité de i_*. De façon plus parlante, si H est une homotopie dans X d'un chemin basé en y contenu dans Y au chemin constant c_y, alors $r \circ H$ est une homotopie dans Y de $r \circ c = c$ au chemin constant $r \circ c_y = c_y$.

(b) D'après le lemme 7.2.15 ci-dessous, $(i \circ r)_* = i_* \circ r_*$ est un isomorphisme. La surjectivité de i_* en résulte. □

Lemme 7.2.15. — *Soit $x \in X$. Sous les hypothèses de* (b)*, il existe une rétraction de X sur Y telle que l'homomorphisme $(i \circ r)_*$ de $\pi_1(X, x)$ vers $\pi_1(X, r(x))$ soit induit par la conjugaison par la classe $[\gamma]$ d'un chemin γ dans X joignant x à $r(x)$.*

Démonstration. — Soit $r : X \to Y$ une rétraction par déformation de X sur Y et $H : [0, 1] \times X \to X$ une application continue vérifiant les conditions (i), (ii), (iii) de la définition 7.2.12. Soit γ le chemin de X défini par $\gamma(s) = H(s, x)$ ($s \in [0, 1]$). Le chemin γ joint x à $r(x)$. La conjugaison par $[\gamma]^{-1}$, c'est-à-dire, la correspondance $[c] \to [\gamma]^{-1}[c][\gamma]$, est, comme $(i \circ r)_*$, un homomorphisme de $\pi_1(X, x)$ vers $\pi_1(X, r(x))$. Montrons que ces deux homomorphismes sont égaux.

Soit c un chemin dans X basé en x paramétré par $[0, 1]$. On souhaite montrer que les chemins $r \circ c$ et $\bar{\gamma} \circ c \circ \gamma$ sont homotopes dans X. Soit $G : [0, 1] \times [0, 1] \to X$ l'application définie par

$$G(s,t) = \begin{cases} \bar{\gamma}(2t) = \gamma(1-2t) & \text{pour} \quad 0 \le t \le \frac{1-s}{2} \\ H\left[s, c\left(\frac{4t+2s-2}{3s+1}\right)\right] & \text{pour} \quad \frac{1-s}{2} \le t \le \frac{s+3}{4} \\ \gamma(4t-3) & \text{pour} \quad \frac{s+3}{4} \le t \le 1 \end{cases}$$

On a

$$\begin{cases} G(0,t) = (\bar{\gamma} \circ c \circ \gamma)(t) \\ G(1,t) = H(c(t), 1) = r \circ c(t) \\ G(s,0) = G(s,1) = \gamma(1) = r(x) \end{cases}$$

Conclusion : G est une homotopie de $\bar{\gamma} \circ c \circ \gamma$ à $r \circ c$. On a donc

$$[\gamma]^{-1}[c][\gamma] = [r \circ c] = r_*([c])$$

□

Corollaire 7.2.16. — *Les groupe fondamentaux de $\mathbb{R}^2$ privé d'un point et du disque unité ouvert privé de l'origine sont tous deux isomorphes à $\mathbb{Z}$.*

Démonstration. — L'espace $\mathbb{R}^2 \setminus \{(0,0)\}$ est homéomorphe au disque unité ouvert privé de l'origine. Ce dernier se rétracte par déformation sur S^1. Ces trois espaces ont donc le même groupe fondamental, à savoir $\mathbb{Z}$ (théorème 7.2.9). □

7.2.5. Théorème de Van Kampen. — Soit X un espace topologique connexe par arcs et X_1, X_2 deux ouverts non vides connexes par arcs tels que $X_1 \cup X_2 = X$. On suppose aussi que $X_1 \cap X_2$ est non vide et connexe par arcs. Soit $x \in X_1 \cap X_2$. On a le diagramme commutatif suivant.

$$\begin{array}{ccc} \pi_1(X_1, x) & \xrightarrow{k_1} & \pi_1(X, x) \\ {\scriptstyle j_1}\uparrow & & \uparrow{\scriptstyle k_2} \\ \pi_1(X_1 \cap X_2, x) & \xrightarrow{j_2} & \pi_1(X_2, x) \end{array}$$

***Théorème 7.2.17* (Van Kampen)**. — *Le groupe fondamental $\pi_1(X, x)$ possède les propriétés suivantes :*

(a) *Il est engendré par les images de k_1 et k_2.*

(b) *Il vérifie la propriété suivante : si $h_i : \pi_1(X_i, x) \to G$, $i = 1, 2$, sont deux homomorphisme de groupes et si $h_1 \circ j_1 = h_2 \circ j_2$, alors il existe un unique homomorphisme $h : \pi_1(X, x) \to G$ tel que $h \circ k_i = h_i$, $i = 1, 2$.*

Corollaire 7.2.18. — *Si X_1 et X_2 sont simplement connexes, alors $X_1 \cup X_2$ l'est aussi.*

Exemple 7.2.19. — (a) L'espace S^2 (en fait S^m pour tout entier $m \geq 2$) est simplement connexe. (Pour $m = 1$, le groupe fondamental est $\mathbb{Z}$).

> [En effet, soient x_1, x_2 deux points distincts de S^m et $U_i = S^m \setminus \{x_i\}$, $i = 1, 2$. Alors S^m s'écrit comme réunion des deux ouverts X_1 et X_2 qui sont simplement connexes car homéomorphes à $\mathbb{R}^m$. Leur intersection, qui est homéomorphe à $\mathbb{R}^m$ privé d'un point, est connexe par arcs si $m \geq 2$.]

(b) Si $m \geq 3$, l'espace $\mathbb{R}^m$ privé d'un point est simplement connexe. (Pour $m = 1$, l'espace n'est pas connexe, pour $m = 2$, le groupe fondamental est $\mathbb{Z}$).

[L'espace $\mathbb{R}^m$ privé d'un point est homéomorphe à la boule unité ouverte de $\mathbb{R}^m$ privée de l'origine, qui se rétracte par déformation sur S_{m-1}.]

Pour une preuve du théorème de Van Kampen, voir par exemple [**God71**]. Il y a deux parties. Le (a) s'obtient directement à partir de la définition du groupe fondamental comme ensemble de classes d'homotopie de chemins [**God71**, chapitre VI, proposition 4.1]. L'énoncé (b) peut être vu comme une application de la théorie des revêtements (qu'il faudrait placer dans les applications de la section §7.7 ; voir §7.7.4). L'homomorphisme $h_i : \pi_1(X_i, x) \to G$ correspond à un revêtement galoisien $f_i : Y_i \to X_i$, $i = 1, 2$. Par la condition $h_1 \circ j_1 = h_2 \circ j_2$, les restrictions $f_i^{-1}(X_1 \cap X_2) \to X_1 \cap X_2$, $i = 1, 2$, sont des revêtements équivalents. On peut alors recoller Y_1 à Y_2 *via* l'homéomorphisme $f_1^{-1}(X_1 \cap X_2) \simeq f_2^{-1}(X_1 \cap X_2)$. Cela fournit un revêtement galoisien $Y \to X$. L'homomorphisme associé $\pi_1(X_i, x) \to G$ est essentiellement l'homomorphisme h cherché (voir [**God71**, chapitre X, §1.1]).

7.2.6. Droite complexe privée de r points. —

7.2.6.1. Groupes libres. — Soit S un ensemble. Pour $s \in S$ et $n \in \mathbb{Z}$ on désigne la paire (s, n) par s^n. Soit $F(S)$ l'ensemble des suites finies (ou mots) $\mathbf{s^n} = (s_1^{n_1}, \ldots, s_k^{n_k})$ (notés aussi $s_1^{n_1} \cdots s_k^{n_k}$) vérifiant

$$k \in \mathbb{N}; s_1, \ldots, s_k \in S; n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}; s_i \neq s_{i+1}, i = 1, \ldots, k-1$$

Si $\mathbf{s^n} = (s_1^{n_1}, \ldots, s_k^{n_k})$ et $\mathbf{t^m} = (t_1^{m_1}, \ldots, t_\ell^{m_\ell})$ sont deux éléments de $F(S)$, on définit le produit $\mathbf{s^n t^m}$ par concaténation de la façon suivante : $\mathbf{s^n t^m}$ est le mot obtenu en accolant $\mathbf{t^m}$ à la droite de $\mathbf{s^n}$, puis en éliminant les termes qui s'annulent, c'est-à-dire, ceux de la forme s^n, s^{-n}.

[De façon précise, il y a élimination si $s_k = t_1 = s$. Dans ce cas, on remplace $s^{n_k}.s^{m_1}$ par $s^{n_k+m_1}$ si $n_k + m_1 \neq 0$. Si $n_k + m_1 = 0$, on supprime s^{n_k} et s^{m_1} et on réapplique la procédure aux deux mots $(s_1^{n_1}, \ldots, s_{k-1}^{n_{k-1}})$ et $\mathbf{t^m} = (t_2^{m_2}, \ldots, t_\ell^{m_\ell})$.]

Cette loi donne à $F(S)$ une structure de groupe ; l'élément neutre est le mot vide $\emptyset$; l'inverse de $\mathbf{s^n}$ est $(s_k^{-n_k}, \ldots, s_1^{-n_1})$. Le groupe $F(S)$ est appelé groupe libre d'alphabet S.

Proposition 7.2.20. — *Le groupe libre $F(S)$ vérifie la propriété universelle suivante :*

(*) *Toute application $f : S \to G$ de l'ensemble S vers un groupe G se prolonge de façon unique en un homomorphisme de groupes $F(S) \to G$,*

qui le caractérise à unique isomorphisme près. C'est-à-dire : si $\mathfrak{F}$ est un groupe et $S \hookrightarrow \mathfrak{F}$ est une injection tels que la propriété universelle ci-dessus est satisfaite, alors il existe un unique isomorphisme entre $F(S)$ et $\mathfrak{F}$ qui prolonge l'injection $S \hookrightarrow \mathfrak{F}$.

Démonstration. — Laissée en exercice. □

Corollaire 7.2.21. — *S'il existe une bijection entre deux ensembles S et S', alors les groupes $F(S)$ et $F(S')$ sont isomorphes.*

A isomorphisme près, les groupes libres $F(S)$ ne dépendent que du cardinal de S. Etant donné un cardinal r, on notera $F(r)$ le groupe libre à r éléments (à isomorphisme près).

Théorème 7.2.22. — *Tout groupe G de type fini est quotient d'un groupe libre en un nombre fini de générateurs.*

Démonstration. — Soient $g_1, \ldots, g_r$ des générateurs en nombre fini r de G. Dès qu'un ensemble S a au moins r éléments, il existe une surjection de S sur l'ensemble $\{g_1, \ldots, g_r\}$. Cette surjection se prolonge en un homomorphisme $\varphi : F(S) \to G$ qui est aussi surjectif. Le groupe G est donc isomorphe au quotient $F(S)/\ker(\varphi)$. □

Quand G possède des générateurs $g_1, \ldots, g_r$ pour lesquels il existe une surjection $s : S \to \{g_1, \ldots, g_r\}$ avec S fini et telle que le noyau $\ker(\varphi)$ de l'homomorphisme $\varphi : F(S) \to G$ est de type fini, on dit que le groupe G est *de présentation finie*, ou qu'il peut être *défini par générateurs et relations*. Tout ensemble fini R des générateurs de $\ker(\varphi)$ s'appelle un ensemble de relations satisfaites par G. Si R est un sous-ensemble fini de $F(r)$, le groupe $F(r)/ < R >$ est de présentation finie. On le note plus simplement $F(r)/R$.

Exemple 7.2.23. — (a) Par définition, le groupe abélien libre à r éléments est le groupe $F(r)/[F(r), F(r)]$. Il est de présentation finie ; l'ensemble de ses relations est constitué des $xyx^{-1}y^{-1}$ où x et y décrivent l'ensemble des générateurs de $F(r)$. D'autre part, il est isomorphe à $\mathbb{Z}^r$.

> [On montre que l'homomorphisme canonique $F(x_1, \ldots, x_r) \to \mathbb{Z}^r$ (qui envoie x_i sur le $i$ième vecteur de la base canonique) satisfait la propriété universelle de $F(r)/[F(r), F(r)]$. C'est-à-dire, d'être

le plus grand quotient abélien de $F(r)$. Autrement dit, tout homomorphisme surjectif $F(r) \to G$ avec G abélien se factorise par le morphisme $F(r) \to F(r)/[F(r), F(r)]$.]

(b) Soit $F(r)$ le groupe libre à r générateurs $x_1, \ldots, x_r$. Le groupe $F(r)/x_1 \cdots x_r$ est isomorphe à $F(r-1)$.

[On montre que $F(r)/x_1 \cdots x_r$ et l'injection $\{x_1, \ldots, x_{r-1}\} \hookrightarrow F(r)/x_1 \cdots x_r$ satisfont la propriété universelle de $F(r-1)$.]

7.2.6.2. Droite complexe privée de r points. — On calcule le groupe fondamental de la droite complexe privée de r points, c'est-à-dire du plan réel $\mathbb{R}^2$ privé de r points. On en déduira celui de $\mathbb{P}^1(\mathbb{C})$ privé de r points.

Théorème 7.2.24. — *Soient $t_1, \ldots, t_r$ r points distincts de $\mathbb{R}^2$. Le groupe fondamental de $X = \mathbb{R}^2 \setminus \{t_1, \ldots, t_r\}$ est isomorphe au groupe libre $F(r)$ à r générateurs.*

Démonstration. — On le démontre par récurrence sur r. Le résultat est vrai pour $r = 0$ (car $\mathbb{R}^2$ est simplement connexe). Soient $t_1, \ldots, t_{r+1}$ $r+1$ points distincts de $\mathbb{R}^2$ et $X = \mathbb{R}^2 \setminus \{t_1, \ldots, t_{r+1}\}$. Soit D une droite séparant un point des r autres. De façon plus précise, soit ℓ une forme linéaire affine telle que, pour un certain $\alpha > 0$:

$$\begin{cases} \ell(t_i) < -\alpha, i = 1, \ldots, r \\ \ell(t_{r+1}) > \alpha \end{cases}$$

Notons X_1 et X_2 l'intersection de X avec respectivement les demi-plans $\{\ell(x) > -\alpha\}$ et $\{\ell(x) < \alpha\}$. Les hypothèses du théorème de Van-Kampen sont satisfaites. L'intersection $X_1 \cap X_2$ est convexe donc simplement connexe (c'est une bande parallèle à D). L'espace X_1 est homéomorphe à $\mathbb{R}^2$ privé de r points. D'après l'hypothèse de récurrence, son groupe fondamental est le groupe libre $F(r)$. L'espace X_2 est homéomorphe à $\mathbb{R}^2$ privé de 1 point. D'après le corollaire 7.2.16, son groupe fondamental est le groupe $\mathbb{Z} = F(1)$. Le théorème 7.2.17 s'applique : le groupe fondamental de X en satisfait les conclusions (a) et (b). C'est un exercice facile de vérifier que ces conclusions sont satisfaites par le groupe libre $F(r+1)$ et le caractérisent. □

Remarque 7.2.25. — On peut préciser comment obtenir r générateurs indépendants de $\pi_1(\mathbb{R}^2 \setminus \{t_1, \ldots, t_r\})$. Soit t_0 un point de $X_1 \cap X_2$ distinct des points $t_1, \ldots, t_r$. Pour chaque point t_i, soit x_i un lacet "tournant une fois" dans le sens positif autour du point t_i ($i = 1, \ldots, r$). Si les lacets $x_1, \ldots, x_r$

ne se croisent pas mutuellement, ils forment un ensemble de générateurs indépendants de $\pi_1(\mathbb{R}^2 \setminus \{t_1, \ldots, t_r\}$.

7.2.6.3. Droite projective complexe privée de r points. —

Théorème 7.2.26. — *Soient $t_1, \ldots, t_r$ r points distincts de $\mathbb{P}^1(\mathbb{C})$. Le groupe fondamental de $X = \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$ est isomorphe au quotient du groupe $\pi_1(\mathbb{C} \setminus \{t_1, \ldots, t_r\})$, identifié au groupe libre $F(r)$ à r générateurs $x_1, \ldots, x_r$, par la relation $x_1 \cdots x_r = 1$, et donc aussi au groupe libre $F(r-1)$ à r générateurs.*

Démonstration. — Si on souhaite juste la conclusion $\pi_1(X) \simeq F(r-1)$, il suffit de dire que, pour $r \geq 1$, $\mathbb{P}^1(\mathbb{C})$ privé de r points est homéomorphe à $\mathbb{R}^2$ privé de $r-1$ points, et que $\mathbb{P}^1(\mathbb{C})$ (privé de 0 point) est simplement connexe car homéomorphe à S^2. Pour démontrer le résultat plus précis, on procède comme suit.

On voit $\mathbb{P}^1(\mathbb{C})$ comme $\mathbb{C} \cup \{\infty\}$ avec ∞ distinct des points $t_1, \ldots, t_r$. Soient B une boule fermée de $\mathbb{C}$, centrée en l'origine et de rayon $r > 0$, contenant les points $t_1, \ldots, t_r$. Soient X_1 une boule ouverte de $\mathbb{C}$ contenant B et $X_2 = \mathbb{P}^1(\mathbb{C}) \setminus B$.

L'espace X_1 est homéomorphe au plan réel privé de r points. Il est donc connexe par arcs et son groupe fondamental est, d'après le paragraphe précédent, le groupe libre $F(r)$. L'espace X_2 est homéomorphe à la boule ouverte centrée en O et de rayon $1/r$ [par exemple par la correspondance $z \to 1/z$ qui transforme un nombre complexe de module a en un nombre complexe de module $1/a$]. L'espace X_2 est donc connexe par arcs et simplement connexe. L'espace $X_1 \cap X_2$ est connexe par arcs et se rétracte par déformation sur S^1. Son groupe fondamental est donc isomorphe à $\mathbb{Z}$. Plus précisément, si pour chaque point t_i, x_i un lacet "tournant une fois" dans le sens positif autour du point t_i, $i = 1, \ldots, r$, un générateur est le produit $x_1 \cdots x_r$.

D'après le théorème de Van-Kampen, le groupe $\pi_1(X)$ est un groupe engendré par $x_1, \ldots, x_r$ qui a la propriété que tout homomorphisme de $F(r) =< x_1, \ldots, x_r >$ qui est nul sur le produit $x_1 \cdots x_r$ se factorise par lui. Ce groupe est donc bien le quotient $F(r)/x_1 \cdots x_r$. □

Remarque 7.2.27. — (a) On a calculé le groupe fondamental de $\mathbb{P}^1(\mathbb{C})$ privé de r points. L'espace $\mathbb{P}^1(\mathbb{R})$ privé de r points lui présente moins d'intérêt : pour $r = 0$, c'est S^1, son groupe est donc $\mathbb{Z}$, pour $r = 1$, c'est $\mathbb{R}$ qui est simplement connexe ; pour $r \geq 2$, l'espace obtenu n'est pas connexe.

(b) L'espace $\mathbb{P}^1(\mathbb{C})$ est simplement connexe. En fait cela se généralise aux dimensions supérieures : $\mathbb{P}^m(\mathbb{C})$ est simplement connexe pour tout $m \geq 2$. Le résultat est un peu plus compliqué pour les espaces projectifs réels : le groupe fondamental de $\mathbb{P}^1(\mathbb{R})$ est $\mathbb{Z}$ et celui de $\mathbb{P}^m(\mathbb{R})$ est $\mathbb{Z}/2$ pour tout $m \geq 2$. Ces résultats peuvent être vus comme cas particulier d'un résultat général sur le groupe fondamental d'un complexe cellulaire [**God71**, p. 96].

7.2.7. Tore complexe à g trous. —

Théorème 7.2.28. — *Soient X un tore à g trous et $a_1, \dots b_g$ les cycles correspondants aux bords du polygone. Le groupe fondamental de X est isomorphe au quotient du groupe libre $F(2g)$ à $2g$ générateurs $a_1, \dots b_g$ par la relation $\prod_{i=1}^{g}[a_i, b_i] = 1$.*

Démonstration. — Soient Q un point intérieur au polygone, $X_1 = X \setminus \{Q\}$ et X_2 l'intérieur du polygone. L'espace X_2 est simplement connexe. L'espace X_1 se rétracte par déformation sur le bord du polygone qu'il faut voir comme un bouquet B de $2g$ cercles C_i, $i = 1, \dots, 2g$ ayant un unique point x en commun.

Montrons par récurrence que le groupe fondamental de B est le groupe libre en les $2g$ générateurs $a_1, \dots, b_g$. On choisit x_i sur C_i distinct de x. L'espace $U_1 = B \setminus \{x_1, \dots, x_{2g-1}\}$ se rétracte par déformation sur C_{2g}. L'espace $U_2 = B \setminus \{x_{2g}\}$ se rétracte par déformation sur $C_1 \cup \dots \cup C_{2g-1}$. Enfin $U_1 \cap U_2$ se rétracte par déformation sur x et est donc simplement connexe. Le théorème de Van Kampen et l'hypothèse de récurrence conduisent bien à la conclusion annoncée.

L'espace $X_1 \cap X_2$ est homéomorphe au disque épointé. Son groupe fondamental est donc $\mathbb{Z}$. Plus précisément, un générateur est le chemin constitué par le bord du polygone, c'est-à-dire, le chemin $a_1 b_1 a_1 b_1^{-1} \cdots a_g b_g a_g b_g^{-1}$. Le théorème de Van Kampen, appliqué au recouvrement de X par X_1 et X_1, fournit la conclusion du théorème 7.2.28. □

On termine ce chapitre par un résultat sans démonstration qui généralise simultanément les théorèmes 7.2.26 et 7.2.28.

Théorème 7.2.29. — *Soient T un tore à g trous et $a_1, \dots b_g$ les cycles correspondants aux bords du polygone. Soient $t_1, \dots, t_r$ r points distincts de T. Le groupe fondamental de $X = T \setminus \{t_1, \dots, t_r\}$ est isomorphe au quotient du groupe libre $F(2g+r)$ à $2g+r$ générateurs $a_1, \dots b_g$, $x_1, \dots, x_r$ par la relation $\prod_{i=1}^{g}[a_i, b_i]\ x_1 \cdots x_r = 1$.*

7.3. Revêtements topologiques

Les espaces topologiques sont toujours supposés séparés.

7.3.1. Généralités. —

Proposition 7.3.1. — *Soit B un espace topologique et $f : X \to B$ une application continue. Les assertions suivantes sont équivalentes :*

(a) *Pour tout $b \in B$, il existe un voisinage U de B, un espace discret non vide D et un homéomorphisme $\Phi : f^{-1}(U) \to U \times D$ tel que $p_1 \circ \Phi$ coincide avec f, où $p_1 : U \times D \to U$ est la première projection.*

(b) *Pour tout $b \in B$, il existe un voisinage U de B et une famille $(V_d)_{d\in D}$ paramétrée par un ensemble D non vide vérifiant*
(i) *Les ensembles V_d sont des ouverts de X deux à deux disjoints.*
(ii) $f^{-1}(U) = \bigcup_{d\in D} V_d$.
(iii) *Pour tout $d \in D$, f induit un homéomorphisme $f_d : V_d \to U$.*

Une application continue $f : X \to B$ ayant ces propriétés est appelée revêtement de B. Un ouvert U vérifiant (a) et (b) est dit trivialisant.

Démonstration. — (a) $\Rightarrow$ (b). Pour tout $d \in D$, on pose

$$V_d = \{x \in f^{-1}(U) | \Phi(x) = (f(x), d)\}$$

Comme D est discret et Φ continue, V_d est un ouvert de X. Les conditions (i) et (ii) sont immédiates. La condition (iii) provient de ce que Φ induit sur V_d un homéomorphisme entre V_d et $U \times \{d\}$.

(b) $\Rightarrow$ (a) On définit l'application $\Phi : f^{-1}(U) \to U \times D$ de la manière suivante. Pour tout $x \in f^{-1}(U)$, il existe un unique $d \in D$ tel que $x \in V_d$. On pose alors $\Phi(x) = (f(x), d)$. Cette application est bijective : sa réciproque associe à tout $(b, d) \in U \times D$ l'image de b par la réciproque de f_d. On munit D de la topologie discrète. L'application Φ est continue [utiliser que les V_d sont ouverts] ainsi que sa réciproque. □

Remarque 7.3.2. — Un revêtement est une application surjective et ouverte.

> [La surjectivité est claire. Soient O un ouvert de X et $x \in O$. Soit $b = f(x)$ et U un ouvert de X comme dans (b). Il existe $d \in D$ tel que $x \in V_d$. Alors $f(O \cap V_d) = f_d(O \cap V_d)$ est un ouvert de B contenant b et inclus dans $f(O)$.]

Exemple 7.3.3. — (a) Pour tout ensemble F, l'application $f : B \times F \to B$ donnée par $f(b, d) = b$ est un revêtement de l'espace topologique B. Pour tout $b \in B$, on peut prendre $U = B$ dans la proposition 7.3.1. Le revêtement est dit trivial.

(b) Les applications $\exp : \mathbb{C} \to \mathbb{C}^\times$ et $\exp : i\mathbb{R} \to S^1$ sont des revêtements.

> [Pour tout $a \in \mathbb{R}$, $\mathbb{C}$ auquel on a retiré la demi-droite $[Oe^{ia})$ (resp. $S^1 \setminus \{e^{ia}\}$) est un ouvert trivialisant.]

(c) Pour tout entier d, les applications $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$ et $m_d : S^1 \to S^1$ définis par $m_d(z) = z^d$ sont des revêtements.

(d) *Revêtement de la droite par une courbe algébrique.* Soient $P(T, Y) \in \mathbb{C}[T, Y] \setminus \mathbb{C}[T]$ un polynôme. Considérons la courbe affine plane C_P d'équation $P(t, y) = 0$. Notons $(\mathbb{A}^1)^*(\mathbb{C})$ l'ensemble des nombres $t \in \mathbb{C}$ qui ne sont pas racines du discriminant $\Delta(T)$ de $P(T, Y)$ relativement à Y et $C_P^*(\mathbb{C})$ le sous-ensemble de $C_P(\mathbb{C})$ des points complexes (t, y) de la courbe tels que $t \in (\mathbb{A}^1)^*(\mathbb{C})$. La première projection $p_T : (t, y) \to t$ induit un revêtement $\mathbb{C}_P^*(\mathbb{C}) \to (\mathbb{A}^1)^*(\mathbb{C})$ de degré $d = \deg_Y(P)$.

> [Pour tout $t \in (\mathbb{A}^1)^*(\mathbb{C})$, le polynôme $P(t, Y)$ admet d racines simples $y_1, \ldots, y_d$. Le théorème des fonctions implicites, qu'on applique à chacun des points (t, y_i), $i = 1, \ldots, d$, fournit un voisinage ouvert trivialisant de t.]

7.3.2. Vocabulaire. — L'espace B est appelé *base du revêtement*. On utilise fréquemment le terme "revêtement" et pour l'application f et pour l'espace du haut X. Le revêtement est *trivial* si B est un ouvert trivialisant, c'est-à-dire si X est homéomorphe à un produit $B \times F$ (avec F discret) et f correspond à la première projection.

Un revêtement $f : X \to B$ est en particulier un *homéomorphisme local*, c'est-à-dire : tout élément $x \in X$ a un voisinage ouvert V tel que $f(V)$ soit ouvert et que f induise un homéomorphisme entre V et $f(V)$. L'espace X hérite donc des propriétés locales de B ; X hérite aussi de la séparation de B.

Les applications $f_d^{-1} : U \to X$ sont des *sections* de f au-dessus de U. De façon générale, une section s de f au-dessus de U est une application continue $s : U \to X$ telle que $f \circ s = \mathrm{Id}_U$. Une section de f est forcément injective. Plus précisément s est un homéomorphisme de U sur l'ouvert $s(U)$.

> [Sa réciproque est $f|_{s(U)}$. L'ensemble $s(U)$ est ouvert : soient $b \in U$ et $U' \subset U$ un voisinage ouvert de b trivialisant f et $(V'_d)_{d \in D}$ les ouverts disjoints de $f^{-1}(U')$. Il existe $d \in D$ tel que $s(b) \in V'_d$.

Comme s est continue, il existe U'' voisinage ouvert de b tel que $s(U'') \subset V'_d$. On a alors $s(U'') = f^{-1}(U'') \cap V'_d$: pour l'inclusion "$\supset$", si $x \in f^{-1}(U'') \cap V'_d$, alors $s(f(x)) = x$ car les deux termes ont même image par f et sont tous les deux dans V'_d où f est injective. Conclusion : $s(U'')$ est un voisinage ouvert de $s(b)$ inclus dans $s(U)$.]

Si deux sections s, s' d'un revêtement f au-dessus de U coincident en un point b alors elles coincident sur un voisinage de b.

[Comme s et s' sont continues, b a un voisinage U tel que $s(U)$ et $s'(U)$ sont contenus dans un ouvert où f est injective ; s et s' sont nécessairement égales sur U.]

Si U est de plus connexe, alors s et s' coincident sur U.

[Le sous-ensemble de U où $s = s'$ est ouvert et fermé.]

On a une notion de *morphisme de revêtements*. Si $f : X \to B$ et $f' : X' \to B$ sont deux revêtements, alors un morphisme entre ces deux revêtements est une application continue $\chi : X \to X'$ telle que $f' \circ \chi = f$. Les notions de d'*isomorphisme*, d'*endomorphisme*, d'*automorphisme* sont définies de façon habituelle.

Exemple 7.3.4. — (a) L'application $g : \mathbb{C} \to \mathbb{C}^\times$ donnée par $g(z) = \exp(z/d)$ est un morphisme du revêtement $\exp : \mathbb{C} \to \mathbb{C}^\times$ vers le revêtement $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$.

(b) Pour tout entier $d > 0$ et pour chaque racine $d$ième ζ de 1, l'application $\mathbb{C}^\times \to \mathbb{C}^\times$ donnée par $z \to \zeta z$ est un automorphisme du revêtement $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$.

7.3.3. Fibres. — Pour tout $b \in B$, on appelle *fibre au-dessus de* b du revêtement f l'ensemble $f^{-1}(b)$. Si U est un ouvert trivialisant contenant b alors la fibre $f^{-1}(b)$ est en bijection avec l'ensemble discret F de la proposition 7.3.1. Un revêtement est dit *localement fini* ("finite-to-one map" en anglais) si les fibres sont des ensembles finis. La proposition ci-dessous montre alors que si la base B est connexe, les fibres ont le même cardinal d, qu'on appelle le *degré* du revêtement. On dira dans ce cas que le revêtement est un revêtement fini, ou plus précisément, un revêtement à d feuillets.

Proposition 7.3.5. — *Soit $f : X \to \mathbb{P}^1$ un revêtement. Supposons la base B connexe. Alors les fibres sont toutes en bijection. En particulier, elles ont le même cardinal si le revêtement est localement fini.*

Démonstration. — Pour F espace topologique discret, notons B_F le sous-ensemble de B des points b tel que la fibre $f^{-1}(b)$ est en bijection avec F. L'ensemble B_F est ouvert : si $b \in B_F$, tout ouvert trivialisant contenant b est inclus dans B_F. L'ensemble B_F est fermé. En effet soit b un point adhérent à B_F. Si U est un ouvert trivialisant contenant b, U coupe B_F. Les fibres au-dessus des points de U, en particulier $f^{-1}(b)$, sont en bijection avec F. Conclusion : si B est connexe, alors B_F est vide ou égal à B. □

Exemple 7.3.6. — Les fibres du revêtement $\exp : \mathbb{C} \to \mathbb{C}^\times$ sont isomorphes à $\mathbb{Z}$. Les revêtements $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$ donnés par $z \to z^d$ sont des revêtement à d feuillets. Les revêtements de la droite par une courbe algébrique définis dans l'exemple 7.3.3 sont des revêtements de degré $\deg_Y P$.

7.3.4. Opérations. — On a la notion de revêtement induit, de revêtement produit, de revêtement quotient.

7.3.4.1. Restriction de l'espace du haut. — La restriction $f : X' \to f(X')$ d'un revêtement $f : X \to B$ à un sous-ensemble $X' \subset X$ de X n'est pas un revêtement en général : prendre pour f le revêtement trival $X = \mathbb{R}\times\{0,1\} \to \mathbb{R}$ et $X' = \mathbb{R} \times \{0\} \cup \mathbb{R}^\times \times \{1\}$. On a cependant le résultat suivant.

Proposition 7.3.7. — *Soit $f : X \to B$ un revêtement de base B connexe et localement connexe. Si C est une partie non vide ouverte et fermée de X, l'application $f : C \to B$ est un revêtement. En particulier, pour tout $t \in B$, $f^{-1}(t) \cap C \neq \emptyset$.*

Le résultat s'applique notamment dans le cas où C est une composante connexe de X (ou une réunion de composantes connexes de X). En effet les composantes connexes de X sont ouvertes car E localement connexe (puisque B l'est) et fermées (elles le sont toujours).

Démonstration. — Soit $b \in B$ et U un ouvert trivialisant connexe contenant b. On a donc $f^{-1}(U) = \bigcup_{d\in D} V_d$ où les V_d sont des ouverts disjoints homéomorphes à U. Comme C est une partie ouverte et fermée de B et que chaque V_d est connexe, pour tout $d \in D$, on a $V_d \cap C = \emptyset$ ou $V_d \subset C$. L'ensemble $f^{-1}(U) \cap C$ est donc réunion disjointe des ouverts V_d pour lesquels $V_d \cap C \neq \emptyset$. Il reste juste à voir qu'il en existe au moins un tel ouvert V_d, c'est-à-dire que $f^{-1}(U) \cap C \neq \emptyset$. On montre de la même façon que pour la proposition 7.3.5 que les ensembles $f^{-1}(b) \cap C$, $b \in B$, ont même cardinal. □

Exemple 7.3.8. — (a) $f : C_P^*(\mathbb{C}) \to (\mathbb{A}^1)^*(\mathbb{C})$ est le revêtement de la droite complexe donné par une courbe algébrique $P(t, y) = 0$ (exemple 7.3.3) et C est le sous-ensemble de $C_P^*(\mathbb{C})$ des zéros d'un facteur irréductible de $P(T, Y)$.

(b) Le résultat est faux si B n'est pas connexe : prendre pour X les points réels de tangente non verticale de $y^2 = t(t+1)(t+2)$; on a $B =]-2, -1[\cup]0, +\infty[$; la projection sur t n'est pas surjective quand on la restreint à une composante connexe de X.

7.3.4.2. Restriction de la base. — Si $f : X \to B$ est un revêtement et $B' \subset B$ une partie de B, on vérifie aisément que $f : f^{-1}(B') \to B'$ est un revêtement (à autant de feuillets).

Exemple 7.3.9. — Le revêtement $\exp : i\mathbb{R} \to S^1$ est obtenu par restriction de la base à partir de $\exp : \mathbb{C} \to \mathbb{C}^\times$.

7.3.4.3. Produit fibré. — Si $f : X \to B$ et $f' : X' \to B$ sont deux revêtements, on définit le produit fibré $X \times_B X'$ comme le sous-ensemble de $X \times X'$ des couples (x, x') tels que $f(x) = f'(x')$. La correspondance $(x, x') \to f(x) = f'(x')$ définit un revêtement $f \times_B f' : X \times_B X' \to B$.

> [Pour tout $b \in B$, la fibre au-dessus de b dans le produit fibré est le produit cartésien $f^{-1}(b) \times f'^{-1}(b)$. Si $x \to (f(x), d(x))$ est un homéomorphisme entre $f^{-1}(U)$ et $U \times F$ et $x \to (f'(x), d'(x))$ est un homéomorphisme entre $f'^{-1}(U)$ et $U \times F'$, alors $(x, x') \to (f(x), d(x), d'(x'))$ est un homéomorphisme entre $(f \times_B f')^{-1}(U)$ et $U \times F \times F'$.]

De plus les deux projections $X \times_B X' \to X$ et $X \times_B X' \to X$ sont aussi des revêtements. Le diagramme suivant résume la situation.

$$\begin{array}{ccc} X \times_B X' & \xrightarrow{p_X} & X \\ {\scriptstyle p_{X'}}\downarrow & & \downarrow{\scriptstyle f} \\ X' & \xrightarrow{f'} & B \end{array}$$

Le produit fibré satisfait la propriété universelle suivante. Si $\varphi : Y \to X$ et $\varphi' : Y \to X'$ sont deux revêtements tels que $f' \circ \varphi' = f \circ \varphi$, alors il existe un unique revêtement $F : Y \to X \times_B X'$ tel que $p_X \circ F = \varphi$ et $p_{X'} \circ F = \varphi'$.

Remarque 7.3.10. — Il y a aussi une notion (moins intéressante) de produit direct $f \times f' : X \times X' \to B \times B'$ de deux revêtements $f : X \to B$ et $f : X' \to B'$ de base éventuellement distinctes.

7.3.4.4. Revêtement quotient. — Soient $\widetilde{f} : \widetilde{X} \to B$ et $f : X \to B$ deux revêtements de B. On dit que f est un quotient de $\widetilde{f}$ ou que $\widetilde{f}$ se factorise par f s'il existe un revêtement $g = \widetilde{X} \to X$ tel que $f \circ g = \widetilde{f}$.

Exemple 7.3.11. — Le revêtement $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$ donné par $z \to z^d$ est un quotient de $\exp : \mathbb{C} \to \mathbb{C}^\times$. En effet, on a $\exp = m_d \circ g$ où $g : \mathbb{C} \to \mathbb{C}^\times$ est donné par $g(z) = \exp(z/d)$.

7.4. Monodromie

7.4.1. Actions de groupes. — Si S est un ensemble, on note $\mathrm{Per}(S)$ l'ensemble des permutations de S, c'est-à-dire des bijections $S \to S$. Si $S = \{1, \ldots, d\}$, on note $\mathrm{Per}(S) = S_d$. Muni de la composition des applications, l'ensemble $\mathrm{Per}(S)$ est un groupe. On notera "$\cdot$" la loi définie par : $a \cdot b = b \circ a$, $a, b \in \mathrm{Per}(S)$.

Remarque 7.4.1. — Le produit $a \cdot b$ correspond au produit des permutations de S vues comme actions notées à droite. Plus précisément, pour $s \in S$ et $f \in \mathrm{Per}(S)$, on peut noter le résultat de la permutation a sur l'élément s de deux façons :
- notation comme action à gauche (ou notation fonctionnelle) : $f(s)$ ou $f.s$
- notation comme action à droite : s^f ou $(s)f$ ou encore $s.f$.

Pour un produit de deux éléments $a, b \in \mathrm{Per}(S)$, les deux notations se correspondent par les formules

$$(a \circ b)(s) := a(b(s)) = (s^b)^a := s^{(b \cdot a)}$$

Cela a une incidence sur le calcul dans S_d. Par exemple, on a :

$$\begin{cases} (123) \circ (23) = (12) \\ (123) \cdot (23) = (13) \end{cases}$$

Une *action à gauche* d'un groupe G sur un ensemble S est :
- un homomorphisme T de G dans le groupe $(\mathrm{Per}(S), \circ)$, (c'est-à-dire $T(ab) = T(a) \circ T(b)$), ou, de façon équivalente,
- un anti-homomorphisme de G dans le groupe $(\mathrm{Per}(S), .)$, (c'est-à-dire $T(ab) = T(b) \cdot T(a)$).

On note $T(a)(s)$ ou $a(s)$ ou $a \cdot s$ le résultat de l'action de $a \in G$ sur $s \in S$.

Une *action à droite* d'un groupe G sur un ensemble S est :
- un homomorphisme T de G dans le groupe $(\mathrm{Per}(S), .)$, (c'est-à-dire $T(ab) = T(a) \cdot T(b)$), ou, de façon équivalente,

- un anti-homomorphisme de G dans le groupe $(\mathrm{Per}(S), \circ)$, (c'est-à-dire $T(ab) = T(b) \circ T(a)$).
On note $s^{T(a)}$ ou s^a ou $s.a$ le résultat de l'action de $a \in G$ sur $s \in S$.

Une action à droite d'un groupe $(G, \times)$ est une action à gauche du groupe G pour la loi duale $*$ définie par $a * b = b \times a$. On peut donc se contenter dans la théorie de l'une des deux notions. Nous préférerons souvent les actions à gauche pour pour lesquelles la notation correspond à la notation fonctionnelle.

Deux actions (à gauche) $T : G \to \mathrm{Per}(S)$ et $T' : G \to \mathrm{Per}(S')$ sont dites *équivalentes* s'il existe une bijection $\gamma : S \to S'$ telle que $\gamma \circ T(g) = T'(g) \circ \gamma$ $(g \in G)$, (ou, de façon équivalente, si $T(g)(x) = y$, alors $T'(g)(\gamma(x)) = \gamma(y)$).

Etant donnés une action (à gauche) $T : G \to \mathrm{Per}(S)$ et un élément $s \in S$, on appelle *orbite de* s l'ensemble $O(s) = T(G)(s) = \{T(g)(s) | g \in G\}$ et *fixateur de* s le sous groupe $G(s) = \{g \in G | T(g)(s) = s\}$ de G. L'orbite $O(s)$ est en bijection avec l'ensemble quotient $G/G(s)$. Une action $T : G \to \mathrm{Per}(S)$ est dite *transitive* si $S \neq \emptyset$ et si S ne consiste qu'en une seule orbite. Plus généralement, si $k \geq 1$, l'action T est dite *k-transitive* si T induit une action transitive sur l'ensemble des k-uplets à coordonnées distinctes de S.

Si G est un groupe et H un sous-groupe d'indice d, l'ensemble des d classes à gauche de G modulo H est noté $G/\cdot H$. L'action de G par translation à gauche sur $G/.H$ est définie par $g \cdot (xH) = gxH$ $(x, g \in G)$. C'est une action à gauche transitive de G sur $G/\cdot H$.

Proposition 7.4.2. — *Inversement soit $T : G \to \mathrm{Per}(S)$ une action à gauche transitive. Soit $s \in S$. Alors l'action T est équivalente à l'action par translation à gauche sur l'ensemble $G/\cdot G(s)$ des classes à gauche de G modulo le fixateur $G(s)$ de s. (On a un résultat semblable à droite).*

Les classes d'équivalence d'actions transitives d'un groupe G correspondent donc aux classes d'équivalence de sous-groupes de G pour la relation de conjugaison dans G.

> [On laisse le lecteur vérifier que si deux actions transitives $G \to S_d$ sont équivalentes (par $\sigma \in S_d$), alors les fixateurs d'un même élément s sont conjugués dans G [par un élément de G envoyant s sur $\sigma(s)$]. Et que si deux sous-groupes sont conjugués, alors les actions par translations à gauche sur les classes à gauche sont équivalentes.]

Démonstration. — Pour tout $x \in G$, $T(x)(s)$ ne dépend que de la classe à gauche $xG(s)$. La correspondance $xG(s) \to T(x)(s)$ induit une bijection γ :

$G/\cdot G(s) \to S$. On vérifie facilement que, pour tout $g \in G$ et tout $xG(s) \in G/\cdot G(s)$, on a : $\gamma\,[g \cdot (xG(s))] = T(g)(\gamma(xG(s))$. □

7.4.2. Relèvement des chemins. — Le résultat suivant, qu'on appelle propriété de relèvement des chemins et qui généralise le théorème 7.2.10, est à la base de la classification des revêtements.

Théorème 7.4.3. — *Soit $f : X \to B$ un revêtement. Soient $c : [a,b] \to B$ un chemin et $x \in f^{-1}(c(a))$ un point dans la fibre du point initial de c. Alors il existe un unique chemin $\widetilde{c} : [a,b] \to X$ tel que $f \circ \widetilde{c} = c$ et de point initial x.*

Démonstration. — On généralise la preuve du théorème 7.2.10.

Existence. Tout point $c(t)$ ($t \in [a,b]$) a un voisinage ouvert trivialisant V_t [Dans le cas de S^1, on avait pris comme ouvert trivialisant S^1 privé d'un point]. Comme c est continue, il existe un intervalle $[u_t, v_t]$ tel que $c([u_t, v_t]) \subset V_t$. Comme $[a,b]$ est compact, on peut recouvrir $[a,b]$ par un nombre fini de ces intervalles $[u_i, v_i]$, $i = 1, \ldots, m$. Quitte à les réordonner, on peut supposer les v_i croissant. On a alors $u_{i+1} \leq v_i$. Les intervalles $[v_i, v_{i+1}]$, $i = 0, \ldots, m-1$ (où on a posé $v_0 = a$) ont la propriété de recouvrir $[a,b]$ et d'avoir une image par c contenue dans un ouvert trivialisant U_i. On définit $\widetilde{c}$ par récurrence : sur $[v_i, v_{i+1}]$, $\widetilde{c}$ est le composé de c avec l'unique section $U_i \to X$ envoyant $c(v_i)$ sur l'extrémité $\widetilde{c}(v_i)$ du chemin $\widetilde{c}|_{[v_{i-1}, v_i]}$ (et sur x pour $i = 0$).

Unicité. L'ensemble des points $t \in [a,b]$ où deux relèvements de c coincident est un ensemble ouvert [même argument que pour les sections] et fermé. □

Comme le théorème 7.2.10, le théorème 7.4.3 se généralise au problème du relèvement des applications d'un produit d'intervalles fermés bornés dans B. Cela permet de montrer l'énoncé suivant.

Théorème 7.4.4. — *Soit x un point fixé de X et $f(x) = t_0$.*

(a) *La correspondance qui, à un chemin $c : [a,b] \to B$ joignant t à t' associe le chemin $\widetilde{c}$, induit une application $\widetilde{\cdot} : \Pi_{t_0,t'}(B) \to \bigsqcup_{y|f(y)=t'} \Pi_{x,y}(X)$.*

(b) *La correspondance qui, à un chemin $c : [a,b] \to B$ basé en t_0 associe l'extrémité $\widetilde{c}(b)$ du chemin $\widetilde{c}$, induit une injection*

$$\Omega_x : \pi_1(B, t_0)/f_*(\pi_1(X,x))\cdot \to f^{-1}(t_0)$$

de l'ensemble des classes à droite modulo $f_*(\pi_1(X,x))$ dans la fibre $f^{-1}(t_0)$.

> [Dans le cas de S^1, l'injection Ω_x est l'application "degré". Dans ce cas, on avait cependant en plus que cette injection est un homomorphisme de groupes.]

(c) *L'image de cette injection est l'ensemble des points de* $f^{-1}(t_0)$ *qui sont dans la même composante connexe par arcs que* x.

(d) *L'application* $f_* : \pi_1(X,x) \to \pi_1(B,t_0)$ *est injective. Son image est le sous-groupe* $H_x \subset \pi_1(B,t_0)$ *des éléments* $[c] \in \pi_1(B,t_0)$ *tels que* $\Omega_x([c]) = x$.

Démonstration. — (a) Il s'agit de montrer que si c_1 et c_2 sont deux chemins homotopes sur B joignant t_0 à t', alors les chemins $\widetilde{c_1}$ et $\widetilde{c_2}$ sont homotopes sur X. Une homotopie H sur B entre les chemins $c_i : [a,b] \to B$, $i = 1,2$, a un unique relèvement $\widetilde{H}$ valant x au point $(0,a)$. La correspondance $s \to \widetilde{H}(s,b)$ est nécessairement constante. L'application $\widetilde{H}$ est donc une homotopie entre les chemins de mêmes extrémités $t \to \widetilde{H}(0,t)$ et $\widetilde{H}(1,t)$. Ces derniers relèvent respectivement c_1 et c_2 et commencent en x : ce sont donc $\widetilde{c_1}$ et $\widetilde{c_2}$.

(b) Il faut voir tout d'abord que $\widetilde{c}(b)$ ne dépend que de la classe d'homotopie $[c]$ de c. Cela résulte de (a). Soient ensuite deux chemins c_1 et c_2, basés en t_0 tels que $c_1 = (f \circ \gamma) \cdot c_2$ avec γ chemin sur X basé en x. On a $\widetilde{f \circ \gamma} = \gamma$ et aussi $\widetilde{(f \circ \gamma)} \cdot c_2 = \gamma \cdot \widetilde{c_2}$. On en déduit $\widetilde{c_1} = \gamma \cdot \widetilde{c_2}$. En particulier $\widetilde{c_1}$ et $\widetilde{c_2}$ ont même extrémité. Cela montre que Ω_x est bien définie. Voyons que Ω_x est injective. Soient deux chemins $c_i : [a,b] \to B$, $i = 1,2$, basés en t_0 tels que $\widetilde{c_1}(b) = \widetilde{c_2}(b)$. Alors $\widetilde{c_1}$ et $\widetilde{c_2}$ ont mêmes extrémités. Le chemin $\widetilde{\Delta} = \widetilde{c_1} \cdot (\widetilde{c_2})^{-1}$ est basé en x et vérifie $f_*([\widetilde{\Delta}]) = [c_1][c_2]^{-1}$.

(c) Soit $x' \in f^{-1}(t_0)$ dans la même composante connexe par arcs que x. Il existe donc un chemin γ sur X joignant x à x'. Le chemin $c = f \circ \gamma$ est un chemin fermé sur B basé en t_0 et évidemment $\widetilde{c}(b) = x'$. Conclusion : x' est dans l'image de Ω_x. L'inclusion inverse, c'est-à-dire que les points dans l'image de Ω_x soient dans la même composante connexe par arcs que x, est banale.

(d) Si γ est un chemin sur X commençant en x, alors $\widetilde{f \circ \gamma} = \gamma$ et, en utilisant (a), $\widetilde{f_*([\gamma])} = [\gamma]$. Ceci montre d'une part que f_* est injective, et d'autre part que l'image de f_* est dans le groupe H_x. Inversement si $[c]$ est dans H_x, alors, par définition de H_x, $\widetilde{c}$ est un chemin fermé de X basé en x et évidemment $f_*([\widetilde{c}]) = [c]$. □

7.4.3. Action de la monodromie. — Soit $f : X \to B$ un revêtement. Le paragraphe précédent permet de construire, pour tout point $t_0 \in B$ une action

$$T = T_{t_0} : \pi_1(B,t_0) \to \mathrm{Per}(f^{-1}(t_0))$$

A toute classe $[c] \in \pi_1(B,t_0)$, on associe la permutation $T([c])$ de la fibre $f^{-1}(t_0)$ qui envoie chaque élément $x \in f^{-1}(t_0)$ sur l'extrémité du relèvement de c de point initial x.

[Que, pour tout $[c] \in \pi_1(B, t_0)$, $T([c])$ soit une bijection, résulte des deux formules

$$\begin{cases} T([c_1][c_2]) = T([c_2]) \circ T([c_1]) \text{ pour tout } [c_1], [c_2] \in \pi_1(B, t_0) \\ T(1) = T([c_{t_0}]) = \mathrm{Id} \end{cases}$$

La première est immédiate. Pour la seconde, on remarque que, pour tout $x \in f^{-1}(t_0)$, le chemin constant c_x relève c_{t_0}.]

Cette action est appelée *action de la monodromie* sur la fibre $f^{-1}(t_0)$. Il s'agit d'une loi à droite si $\mathrm{Per}(f^{-1}(t_0))$ est muni de la composition "$\circ$". Cependant l'opérateur T est habituellement (et comme ci-dessus) notée à gauche. Si on préfère voir la monodromie comme une action à gauche, il faut alors munir $\mathrm{Per}(f^{-1}(t_0)$ de la loi duale ".", ou alors adopter la convention inverse de la nôtre pour le produit des chemins (*Cf.* remarques 7.4.1 et 7.1.1).

Remarque 7.4.5. — Plus généralement, on peut définir la monodromie comme la donnée, pour tout $(t, t') \in B \times B$ de l'(anti-)homomorphisme

$$T = T_{t,t'} : \Pi_{t,t'} \to Bij(f^{-1}(t), f^{-1}(t'))$$

qui, à la classe $[c] \in \Pi_{t,t'}$ d'un chemin sur B joignant t à t', associe la bijection $T([c])$ entre les deux fibres $f^{-1}(t)$ et $f^{-1}(t')$, qui envoie chaque élément $x \in f^{-1}(t)$ sur l'extrémité du relèvement de c de point initial x.

Soient t_0 et t'_0 deux points de B et γ un chemin joignant t_0 à t'_0. Les deux actions T_{t_0} et $T_{t'_0}$ sont reliées de la façon suivante : pour tout $[c] \in \pi_1(B, t'_0)$,

$$T_{t_0}([\gamma c \gamma^{-1}]) = T_{t_0,t'_0}([\gamma])\ T_{t'_0}([c])\ (T_{t_0,t'_0}([\gamma]))^{-1}$$

Supposons la base B connexe par arcs et le revêtement fini. Les fibres ont donc le même cardinal d (proposition 7.3.5) et peuvent donc être identifiées à $\{1, \ldots, d\}$. D'autre part, les groupes $\pi_1(B, t_0)$ peuvent être identifiés *au* groupe fondamental $\pi_1(B)$ (proposition 7.1.5). La formule ci-dessus montre que l'action de la monodromie est compatible avec ces identifications et permet de voir l'action de la monodromie sur une fibre du revêtement comme une action, définie à équivalence près,

$$T : \pi_1(B) \to S_d$$

En combinant cela avec le théorème 7.4.3, on obtient l'énoncé suivant.

Théorème 7.4.6. — *Soit $f : X \to B$ un revêtement de base B connexe par arcs et localement connexe par arcs.*

(a) *Les orbites de l'action $T : \pi_1(B) \to S_d$ de la monodromie correspondent aux composantes connexes de X. En particulier, l'action de la monodromie est transitive si et seulement si l'espace X est connexe par arcs.*

(b) *Supposons X connexe. Si $G = T(\pi_1(B))$ est le groupe image de T, le groupe fondamental $\pi_1(X)$ s'identifie au groupe $T^{-1}(G(1))$ où $G(1)$ est le fixateur de 1 pour l'action $G \hookrightarrow S_d$. Le groupe $\pi_1(X)$ donc, à isomorphisme près, un sous-groupe d'indice d de $\pi_1(B)$.*

Démonstration. — (a) Soit t_0 un point de B. La correspondance est donnée de la façon suivante. Soit C une composante connexe de X. L'espace X étant localement connexe par arcs (car B l'est), C est une composante connexe par arcs de X. L'ensemble $C \cap f^{-1}(t_0)$ est non vide (proposition 7.3.7) et correspond à une même orbite de T_{t_0} (théorème théorème 7.4.3). On associe cette orbite à C. Inversement, étant donnée une orbite de l'action de T sur $f^{-1}(t_0)$, on lui associe la composante connexe des points dans cette orbite. Ces correspondances sont clairement inverses l'une de l'autre.

> [Si on change de point t_0, l'action de la monodromie ne change pas à équivalence près ; en particulier, les orbites des deux actions se correspondent : plus précisément, il existe une bijection entre les deux ensembles d'orbites qui envoie chaque orbite sur une orbite de même longueur.]

La première partie de (b) est une reformulation de théorème 7.4.3 (d) dans le cas où X est connexe par arcs. La seconde provient de $[G : G(1)] = d$. □

Le groupe image $G = T(\pi_1(B))$ est appelé le *groupe de monodromie* du revêtement. On le notera $G(f)$ ou $G(X/B)$. Le groupe $G(f)$ est défini à conjugaison près dans S_d. Précisément, le groupe de monodromie $G(f)$, est, à conjugaison près, le groupe $T_{t_0}(\pi_1(B, t_0))$ où t_0 est un point quelconque de B et où la fibre $f^{-1}(t_0)$ est identifiée à $\{1, \ldots, d\}$. On peut le voir comme le groupe

$$\pi_1(B, t_0)/\ker(T_{t_0}) \simeq \pi_1(B, t_0)/\bigcap_{i=1}^{d} f_*(\pi_1(X, x_i))$$

où $x_1, \ldots, x_d$ sont les points de la fibre $f^{-1}(t_0)$.

7.5. Classification des revêtements et applications

On suppose désormais l'espace base B connexe par arcs et localement connexe par arcs.

7.5.1. Revêtements et représentations du groupe fondamental. — D'après la section précédente, à tout revêtement connexe $f : X \to B$ de B de degré d, on peut associer, pour tout point $t_0 \in B$, une action à droite $T : \pi_1(B, t_0) \to S_d$ transitive, ou, ce qui revient au même, d'après la proposition 7.4.2, un sous-groupe d'indice d de $\pi_1(B, t_0)$.

Proposition 7.5.1. — *Si $f : X \to B$ et $g : X \to B$ sont deux revêtements équivalents, alors les actions correspondantes $\pi_1(B, t_0) \to S_d$ sont équivalentes.*

Démonstration. — Soit $\chi : X \to X'$ un isomorphisme entre les deux revêtements. Cet isomorphisme induit une bijection, notée encore χ de la fibre $f^{-1}(t_0)$ vers la fibre $g^{-1}(t_0)$. Si c est un chemin sur B basé en t_0 et $\widetilde{c}$ le relèvement de c sur X commençant en un point x, alors $\chi \circ c$ est le relèvement de c sur X' commençant en $\chi(x)$. Cela donne la conclusion désirée : si l'action de la monodromie de f (resp. de g) sur la fibre $f^{-1}(t_0)$ (resp. sur la fibre $g^{-1}(t_0)$) est notée T_f (resp. T_g), on a, pour tout $[c] \in \pi_1(B, t_0)$,

$$\chi \circ T_f([c]) = T_g([c]) \circ \chi$$

□

On va construire une correspondance inverse de la correspondance

"revêtement de $B \to$ action de $\pi_1(B)$".

Cela montrera en particulier que la réciproque de la proposition 7.5.1 est vraie (corollaire 7.5.3).

On suppose désormais que B est aussi localement simplement connexe. Supposons donnés un point $t_0 \in B$ et une action à droite transitive $T : \pi_1(B, t_0) \to S_d$. On va construire un revêtement $f_T : X_T \to B$ tel que l'action de la monodromie sur la fibre $f_T^{-1}(t_0)$ soit équivalente à l'action T. Posons $G = T(\pi_1(B, t_0))$ et notons H le sous-groupe $H = T^{-1}(G(1))$.

7.5.1.1. Définition de $f_T : X_T \to B$. — On note $\Pi_{t_0,.}(B)$ l'ensemble $\bigsqcup_{t \in B} \Pi_{t_0,t}(B)$ des classes d'homotopie de chemins sur B commençant en t_0. Pour tout $[c] \in \Pi_{t_0,.}(B)$, on note $f_\infty([c])$ l'extrémité de $[c]$. Deux éléments $[c_1], [c_2] \in \Pi_{t_0,.}(B)$ sont dits équivalents si $f_\infty([c_1]) = f_\infty([c_2])$ et si $[c_1][c_2]^{-1} \in H$. L'ensemble X_T est défini comme l'ensemble quotient de $\Pi_{t_0,.}(B)$ par cette relation d'équivalence et f_T comme l'application induite par f_∞ sur X_T. Pour tout $[c] \in \Pi_{t_0,.}(B)$, on notera $H[c] \in X_T$ sa classe d'équivalence.

7.5.1.2. Topologie sur X_T. — Pour tout $H[c] \in X_T$, on définit une base de voisinages de $H[c]$ de la manière suivante. Si U est un voisinage simplement connexe de $t = f_T(H[c])$, on note $\mathcal{V}_U([c])$ l'ensemble des éléments $H[c\delta]$ où δ décrit l'ensemble des chemins joignant t à un point de U. On vérifie facilement que l'ensemble des $\mathcal{V}_U([c])$ où U décrit une base de voisinages simplement connexes de t, constitue une base de voisinages de $H[c]$ sur l'espace X_T.

7.5.1.3. L'application f_T est un revêtement. — Soient $t_0 \in B$ et U un voisinage simplement connexe de t_0. L'ensemble $f_T^{-1}(U)$ est égal à la réunion disjointe des $\mathcal{V}_U([cc_0])$ où c_0 est un chemin joignant t_0 à un point de U et $[c]$ décrit un ensemble $[c_1], \ldots, [c_d]$ de représentants des classes à droite de $\pi_1(B, t_0)$ modulo H.

> [Par définition, $f_T^{-1}(U)$ est l'ensemble des classes de chemins $[\gamma]$ joignant t_0 à un point de U, modulo H. Fixons un point t de U et un chemin c_0 joignant t_0 à t. Pour tout $H[\gamma] \in f_T^{-1}(U)$, si δ est un chemin dans U joignant l'extrémité de γ à t, alors le chemin $\gamma\delta\overline{c_0}$ est un chemin fermé basé en t_0 et dont la classe d'homotopie ne dépend pas de δ. Modulo H, cette classe de chemins ne peut prendre que d valeurs, à savoir, les d éléments $H[c_1], \ldots, H[c_d]$. La classe initiale $[\gamma]$ est donc de la forme $H[c_i c_0 \delta^{-1}]$, $i = 1, \ldots, d$ et où δ^{-1} est un chemin quelconque dans U joignant t à un point de U.]

Cela montre que f_T est un revêtement [la description de $f_T^{-1}(U)$ montre en particulier que f_T est continue]. Enfin l'application f_T induit sur chaque $\mathcal{V}_U([c_i c_0])$ un homéomorphisme sur U. Sa réciproque est l'application qui à un point $t' \in U$ associe la classe $H[c_i c_0 \delta]$ où δ est un chemin quelconque dans U joignant t à t'. Cette dernière application est clairement continue [l'image réciproque d'un ouvert de type $\mathcal{V}_V([c])$ avec $V \subset U$ est égal à V].

7.5.1.4. L'action de la monodromie de f_T est équivalente à T. — Soit $c : [0,1] \to B$ un chemin fermé basé en un point de B, par exemple t_0. Soit $x \in X_T$ un point tel que $f_T(x) = t_0$. Le point x est de la forme $H[c_i]$ pour un indice $i = 1, \ldots, d$. Considérons le chemin suivant C paramétré par $[0,1]$: pour $s \in [0,1]$, $C(s) = H[c_i c(st)]$ est la classe à droite modulo H du chemin produit du chemin c_i et du chemin $t \to c(st)$ joignant t_0 à $c(s)$. L'application $s \to C(s)$ est continue,

> [Si $s_0 \in [0,1]$ et U est un voisinage simplement connexe de $c(s_0)$, il existe un voisinage I de s_0 tel que $c(I) \subset U$. On a alors $C(I) \subset \mathcal{V}_U([C(s_0)])$.]

relève le chemin c et commence en $C(0) = H[c_i] = x$. Son extrémité est $C(1) = H[c_i c]$. L'action de monodromie de $[c]$ sur la fibre $f_T^{-1}(t_0)$ correspond donc à la multiplication à droite sur les classes à droite de $\pi_1(B, t_0)$ modulo H. D'après la proposition 7.4.2 et la définition de H, cette action est équivalente à l'action T.

7.5.1.5. Si T et T' sont deux actions $\pi_1(B, t_0) \to S_d$ équivalentes, alors les revêtements correspondants sont équivalents. — Supposons qu'il existe $\sigma \in S_d$ tel que $T'(x) = \sigma T(x)\sigma^{-1}$ pour tout $x \in \pi_1(B, t_0)$. Le groupe H' associé à T' est alors $H' = T^{-1}(G(\sigma(1)))$. Soit $\delta \in \pi_1(B, t_0)$ tel que $T(\delta)(1) = \sigma(1)$ [δ existe car T transitive] ; on a alors $H' = \delta H \delta^{-1}$. La correspondance $[c] \to [\delta c]$ induit une application de X_T vers $X_{T'}$ [car si $[c_1 c_2^{-1}] \in H$ alors $[(\delta c_1)(\delta c_2)^{-1}] \in \delta H \delta^{-1} = H'$]. On vérifie facilement que cette application $X_T \to X'_T$ est une équivalence entre les deux revêtements $f_T : X_T \to B$ et $f_{T'} : X_{T'} \to B$.

7.5.1.6. A équivalence près, le revêtement $f_T : X_T \to B$ ne dépend pas du point t_0. — Soit γ un chemin sur B joignant t_0 à un second point base t'_0, la conjugaison $\alpha_{[\gamma]}$ par $[\gamma]$ (c'est-à-dire : $\alpha_{[\gamma]}([c]) = [\gamma][c][\gamma]^{-1}$), identifie les groupes $\pi_1(B, t'_0)$ et $\pi_1(B, t_0)$. Soit $T' = T \circ \alpha_{[\gamma]}$ l'action $\pi_1(B, t'_0) \to S_d$ déduite de cette identification. Alors la correspondance $[c] \to [\gamma c]$ induit une équivalence $X_T \to X_{T'}$.

7.5.1.7. Si $T : \pi_1(B, t_0) \to S_d$ est l'action de monodromie d'un revêtement $f : X \to B$, alors le revêtement $f_T : X_T \to B$ est équivalent à $f : X \to B$. — Soit $x \in X$ le point dans la fibre $f^{-1}(t_0)$ correspondant à 1 dans l'identification de $f^{-1}(t_0)$ avec $\{1, \ldots, d\}$. Pour $y \in X$, on choisit un chemin sur X joignant x à y et on définit $\chi(y)$ comme la classe $H[f \circ c]$ modulo H du chemin $f \circ c$. Cette définition ne dépend pas du chemin c : si c' est un second chemin sur X joignant y_1 à y, la différence $[f \circ (c' c^{-1})]$ est dans $f_*(\pi_1(X, t_0))$ qui, d'après le théorème 7.4.3, s'identifie au sous-groupe $H = T^{-1}(G(1))$ de $\pi_1(B, t_0)$. La correspondance $y \to \chi(y)$ définit une équivalence entre les revêtements $f : X \to B$ et $f_T : X_T \to B$. La réciproque de χ associe à toute classe $H[c]$ modulo H l'extrémité du chemin sur X relevant c et commençant en x.

7.5.1.8. Résultats. — L'énoncé suivant regroupe les conclusions principales de la construction précédente. Essentiellement, les revêtements d'un espace B connexe, localement connexe par arcs et localement simplement connexe correspondent, à équivalence près, aux représentations transitives, ou, ce qui revient au même, au sous-groupes, du groupe fondamental de B. Par exemple, les revêtements de $\mathbb{C}^\times$ correspondent aux sous-groupes de $\mathbb{Z}$. Ces

sous-groupes sont de la forme $d\mathbb{Z}$, $d > 0$. Les revêtements correspondants sont les revêtements $z \to z^d$.

Théorème 7.5.2. — *Soit B un espace topologique connexe par arcs, localement connexe par arcs et localement simplement connexe.*

(a) *Les classes d'équivalence de revêtements $f : X \to B$ connexes de degré d de B correspondent de façon biunivoque aux classes d'équivalence d'actions transitives $T : \pi_1(B) \to S_d$, ou encore aux classes d'équivalence de sous-groupes d'indice d de $\pi_1(B)$ pour la relation de conjugaison dans $\pi_1(B, t_0)$.*

(b) *Plus précisément, étant donné un point $t_0 \in B$, la correspondance*

$$\begin{array}{ccc} \text{classe d'équivalence} & & \text{classe d'équivalence} \\ \text{de revêtements} & \longrightarrow & \text{de l'action de monodromie} \\ f : X \to B & & T : \pi_1(B, t_0) \to S_d \\ \text{connexes de degré } d & & \text{sur la fibre } f^{-1}(t_0) \end{array}$$

a pour réciproque la correspondance

$$\begin{array}{ccc} \text{classe d'équivalence} & & \text{classe d'équivalence} \\ \text{d'actions transitives} & \longrightarrow & \text{du revêtement} \\ T : \pi_1(B, t_0) \to S_d & & f_T : X_T \to B \end{array}$$

(c) *Ces deux correspondances ne dépendent pas du choix du point $t_0 \in B$ modulo l'identification habituelle $\pi_1(B, t_0) \simeq \pi_1(B, t_0')$.*

Corollaire 7.5.3. — *Sous les hypothèses précédentes, si les actions de monodromie de deux revêtements de B sont équivalentes, alors les revêtements sont équivalents.*

Démonstration. — Combiner §7.5.1.5 et §7.5.1.7. □

Remarque 7.5.4. — On a supposé les revêtements finis afin de simplifier les notations. Mais cette hypothèse n'a joué aucun rôle dans la construction. le théorème 7.5.2 est donc valable plus généralement pour des revêtements connexe de fibre en bijection avec un ensemble donné D. Il faut juste remplacer "de degré d" par "de fibre en bijection avec D" et S_d par $\mathrm{Per}(D)$.

7.5.2. Quotients d'un revêtement. — Les quotients d'un revêtement $f : X \to B$ correspondent essentiellement aux sous groupes de $\pi_1(B)$ qui contiennent $\pi_1(X)$.

De faqn précise, soient $f : X \to B$ et $f' : X' \to B'$ deux revêtements connexes de B. Soient $x \in X$ tel que $f(x) = t_0$ et $x' \in X'$ tel que $f'(x') = t_0$. Les deux revêtements f et f' correspondent à deux sous-groupes $H = f_*(\pi_1(X, x))$ et $H' = f'_*(\pi_1(X', x'))$ de $\pi_1(B, t_0)$, ou, de façon équivalente, à deux actions $T : \pi_1(B, t_0) \to S_d$ et $T' : \pi_1(B, t_0) \to S_{d'}$.

Proposition 7.5.5. — *Le revêtement $f' : X' \to B'$ est un quotient du revêtement $f : X \to B$ si et seulement si H est inclus dans l'un des sous-groupes conjugués de H' dans $\pi_1(B, t_0)$.*

Démonstration. — ($\Rightarrow$) : Si $f = f' \circ g$ où $g : X \to X'$ est un revêtement, on a alors $g_*(\pi_1(X, x) \subset \pi_1(X', g(x))$. On en déduit $f_*(\pi_1(X, x)) \subset f'_*(\pi_1(X', f(x)))$. Le groupe de gauche est H. Le groupe $\pi_1(X', g(x))$ étant conjugué à $\pi_1(X', x')$ (puisque $f'(x') = f'(g(x)) = t_0$), celui de droite est conjugué à H' dans $\pi_1(B, t_0)$.

($\Leftarrow$) : Notons comme au §7.5.1 $f_T : X_T \to B$ et $f_{T'} : X_{T'} \to B$ les revêtements associés aux actions T et T'. On peut supposer $H \subset H'$. Il est clair alors que le revêtement $f_{T'}$ est un quotient du revêtement f_T [revenir à la définition de X_T et $X_{T'}$]. Cela achève la démonstration puisque les revêtements f_T et $f_{T'}$ sont respectivement équivalents à f et f'. □

Exemple 7.5.6. — Soient m_d et $m_{d'}$ les deux revêtements $\mathbb{C}^\times \to \mathbb{C}^\times$ donnés par $z \to z^d$ et $z \to z^{d'}$. Le revêtement m_d est quotient de $m_{d'}$ si et seulement si $d'\mathbb{Z} \subset d\mathbb{Z}$, c'est-à-dire, si et seulement si $d|d'$.

7.5.3. Revêtement universel. — La remarque 7.5.4 permet d'appliquer les résultats du §7.5.1 au cas où l'action $T : \pi_1(B, t_0) \to \mathrm{Per}(\pi_1(B, t_0))$ donnée est la multiplication à droite sur $\pi_1(B, t_0)$. Avec les notations précédentes, on a $D = \pi_1(B, t_0)$ et $H = \{1\}$. Le revêtement $X_T \to B$ correspondant est noté $\widetilde{f} : \widetilde{B} \to B$ et est appelé le *revêtement universel* de B.

Les éléments de $\widetilde{B}$ sont les classes d'homotopie de chemins sur B commençant en t_0 modulo la relation d'équivalence qui identifie deux classes de même extrémité. L'application $\widetilde{f}$ associe à tout élément $[c]$ de $\widetilde{B}$ l'extrémité du chemin correspondant c. L'action T ci-dessus est libre. Le groupe fondamental de $\widetilde{B}$ est donc trivial, c'est-à-dire : le revêtement universel $\widetilde{B}$ est simplement connexe.

De la proposition 7.5.5, on déduit la propriété universelle suivante qui caractérise le revêtement universel (à équivalence près).

Théorème 7.5.7. — *Tout revêtement connexe $f : X \to B$ de B est un quotient du revêtement universel $\widetilde{f} : \widetilde{B} \to B$ de B.*

Remarque 7.5.8. — La proposition 7.5.5 montre en fait que si $E \to B$ est un revêtement simplement connexe de B, alors E vérifie la propriété universelle ci-dessus et donc est le revêtement universel de B. Cela montre par exemple que le revêtement universel de $\mathbb{C}^\times$ est $\mathbb{C}$, celui de S^1 est $\mathbb{R}$, que le revêtement universel d'un espace simplement connexe est lui-même, etc.

7.5.4. Existence de revêtements finis. —

Corollaire 7.5.9. — *Si un espace B connexe par arcs, localement connexe par arcs et localement simplement connexe est simplement connexe, alors tout revêtement fini de B est trivial.*

Démonstration. — Soit $f : X \to B$ un revêtement de B. Il s'agit de montrer que la restriction $f_C : C \to B$ de f à toute composante connexe C de X est un homéomorphisme. L'action de monodromie est une action du groupe $\pi_1(B)$ qui est trivial. Comme cette action est transitive sur toute fibre de f_C, les fibres de f_C ne comportent qu'un élément.

> [Ce résultat aurait pu être établi plus tôt. C'est en fait une conséquence de théorème de relèvement des chemins. Soient y_1, y_2 deux points dans la fibre $f^{-1}(t_0)$ d'un revêtement connexe $f : X \to B$. Soit γ un chemin sur X joignant y_1 à y_2, son image $f \circ \gamma$ est un chemin fermé sur B et est donc homotope au chemin constant c_{t_0} (B est simplement connexe). Le chemin constant c_{y_1} est l'unique relèvement de c_{t_0} commençant en y_1. D'après le théorème 7.4.3, c_{y_1} et γ ont même extrémité, d'où $y_1 = y_2$.]

□

Remarque 7.5.10. — (a) La réciproque du corollaire 7.5.9 est vraie si l'espace B est un tore complexe à g trous. C'est-à-dire, si son groupe fondamental est non trivial, c'est-à-dire, si $g > 0$, alors un tore complexe à g trous possède des revêtements finis non triviaux. En effet, pour $d > 0$ entier quelconque, considérons l'homomorphisme du groupe libre $F(2g) = F(a_1, \ldots, a_g, b_1, \ldots, b_g)$ à $2g$ générateurs envoyant chacun des générateurs sur le même d-cycle de S_d. Cet homomorphisme se factorise par le quotient de $F(2g)$ par l'unique relation $\prod_{1 \leq i \leq g} [a_i, b_i] = 1$ (puisque chacun

des commutateurs $[a_i, b_i]$, $i = 1, \ldots, g$ est trivial) et induit donc une action $\pi_1(B) \to S_d$ qui est transitive par construction. Cette action correspond à un revêtement de degré d du tore complexe B. Cet argument se généralise facilement au cas d'un tore complexe à g trous privé de r points (qui n'est simplement connexe que pour $g = r = 0$).

(b) Pour des espaces B généraux, la réciproque du corollaire 7.5.9 peut être fausse. C'est-à-dire : un espace peut avoir un groupe fondamental non trivial et n'avoir aucun revêtement fini. En effet, on peut montrer que tout groupe est groupe fondamental d'un espace topologique B. Or il existe des groupes non triviaux n'admettant aucun sous-groupe propre d'indice fini, par exemple les groupes simples infinis.

7.5.5. Forme topologique du Problème Inverse de la Théorie de Galois. — La construction du §7.5.1 permet de montrer le résultat suivant qui est le point de départ de l'approche moderne du Problème Inverse de la Théorie de Galois.

Théorème 7.5.11. — *Tout groupe fini est le groupe de monodromie d'un revêtement $X \to \mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}$ de la droite projective complexe $\mathbb{P}^1(\mathbb{C})$ privée d'un certain nombre r (dépendant de G) de points $t_1, \ldots, t_r$.*

Démonstration. — Il suffit de combiner les théorèmes 7.2.22 et 7.2.26 aux résultats du §7.5.1. L'entier r doit être choisi plus grand que le nombre minimal de générateurs de G. □

7.6. Groupe des automorphismes d'un revêtement

On suppose désormais l'espace base B connexe par arcs, localement connexe par arcs et localement simplement connexe.

7.6.1. Première description. — Soit $f : X \to B$ un revêtement de degré d. Les automorphismes du revêtement, c'est-à-dire, les homéomorphismes $\chi : X \to X$ tels que $f \circ \chi = f$ forment un groupe noté $\mathrm{Aut}(f)$ (ou $\mathrm{Aut}(X/B)$ quand le contexte est clair).

Soient t_0 un point de B et $f^{-1}(t_0) = \{x_1, \ldots, x_d\}$ la fibre au-dessus de t_0. Chaque automorphisme du revêtement permute les points de $f^{-1}(t_0)$ et induit donc une action à gauche

$$\Lambda_{t_0} : (\mathrm{Aut}(f), \circ) \to (\mathrm{Per}(f^{-1}(t_0)), \circ)$$

Rappelons d'autre part qu'on a une action à droite

$$T_{t_0} : (\pi_1(B, t_0), .) \to (\mathrm{Per}(f^{-1}(t_0)), \circ)$$

et que le groupe image $T(\pi_1(B, t_0))$ est le groupe de monodromie $G(f)$ du revêtement.

Théorème 7.6.1. — *On suppose X connexe. Alors le groupe* $\mathrm{Aut}(f)$ *est fini de cardinal $\leq d$. L'homomorphisme Λ_{t_0} est injectif et a pour image le sous-groupe de* $\mathrm{Per}(f^{-1}(t_0))$ *des permutations de $f^{-1}(t_0)$ qui commutent aux éléments du groupe de monodromie $G(f)$.*

Si une numérotation de la fibre $f^{-1}(t_0)$ par $\{1, \ldots, d\}$ est donnée, on peut identifier $\mathrm{Aut}(f)$ à son image dans S_d, qui coincide avec le groupe $\mathrm{Cen}_{S_d} G(f)$. Le théorème 7.6.1 va résulter des deux lemmes suivants.

Lemme 7.6.2. — *Si X est connexe, le groupe* $\mathrm{Aut}(f)$ *opère librement sur l'ensemble des points de X. C'est-à-dire, si un automorphisme $\chi \in \mathrm{Aut}(f)$ a un point fixe, il est trivial.*

Démonstration. — Soit $\chi \in \mathrm{Aut}(f)$ tel que χ fixe un point $x \in X$. Soit y un point quelconque de X et γ un chemin sur X joignant x à y. Le chemin $\chi \circ \gamma$ joint x à $\chi(y)$ et relève le chemin $f \circ \gamma$ (car $\chi \circ f = f$). Le chemin initial γ a les mêmes propriétés. Par unicité du relèvement des chemins, on obtient $\chi \circ \gamma = \gamma$. En particulier $\chi(y) = y$, pour tout $y \in X$. □

En prévision de la suite, nous démontrons un résultat un peu plus général que ce dont nous avons besoin pour le théorème 7.6.1. Soient $f : X \to B$ et $f' : X' \to B$ deux revêtements connexes. Notons $\mathrm{Mor}(f, f')$ l'ensemble des morphismes $\chi : X \to X'$ entre les revêtements f et f'. Soit t_0 un point de B. Tout morphisme $\chi \in \mathrm{Mor}(f, f')$ induit une application entre les fibres $f^{-1}(t_0)$ et $f'^{-1}(t_0)$. Cela fournit une application

$$\Lambda_{t_0} : \mathrm{Mor}(f, f') \to \mathrm{App}(f^{-1}(t_0), f'^{-1}(t_0))$$

à valeurs dans l'ensemble des applications de $f^{-1}(t_0)$ dans $f'^{-1}(t_0)$. On note T_{t_0} et T'_{t_0} les actions de monodromie de f et f' relatives au point base t_0.

Lemme 7.6.3. — *L'image de l'application Λ_{t_0} est l'ensemble des bijections $\omega \in \mathrm{App}(f^{-1}(t_0), f'^{-1}(t_0))$ telles que, pour tout $[c] \in \pi_1(B, t_0)$,*

$$(*) \qquad \omega^{-1} \circ T'_{t_0}([c]) \circ \omega = T_{t_0}([c])$$

Démonstration. — Soient $\chi \in \mathrm{Mor}(f, f')$ et $[c] \in \pi_1(B, t_0)$. Si γ est un chemin sur X relevant c et joignant x à y, alors $\chi \circ \gamma$ est l'unique relèvement de c sur X' commençant en $\chi(x)$. On obtient alors que si $T_{t_0}([c])(x) = y$ alors $T'_{t_0}([c])(\chi(x)) = \chi(y)$. Ce qui s'écrit encore

$$\Lambda_{t_0}(\chi)^{-1} \circ T'_{t_0}([c]) \circ \Lambda_{t_0}(\chi) = T_{t_0}([c])$$

Il reste à montrer qu'un élément $\omega \in \mathrm{App}(f^{-1}(t_0), f'^{-1}(t_0))$ qui vérifie $(*)$ est de la forme $\Lambda_{t_0}(\chi)$ pour un certain $\chi \in \mathrm{Mor}(f, f')$. Fixons un point $x_1 \in f^{-1}(t_0)$. Pour ω comme ci-dessus et γ un chemin sur X joignant x_1 à x, on définit $\chi_{\omega,\gamma}(x)$ comme l'extrémité du relèvement sur X' de $f \circ \gamma$ qui commence en $\omega(x_1)$.

Le point $\chi_{\omega,\gamma}(x)$ ne dépend pas du chemin γ choisi. En effet, soit γ' un second chemin joignant x_1 à x. Fixons aussi δ un chemin joignant x à x_1. Si $\chi_{\omega,\gamma}(x) \neq \chi_{\omega,\gamma'}(x)$ alors on a aussi $\chi_{\omega,\gamma\delta}(x_1) \neq \chi_{\omega,\gamma'\delta}(x_1)$. Il s'agit donc de voir que si γ est un chemin fermé basé en x_1, alors l'unique relèvement sur X' de $f \circ \gamma$ commençant en $\omega(x_1)$ se termine toujours au même point, qui ne peut être que $\omega(x_1)$ [valeur pour $[\delta] = 1$]. Cela revient à montrer que

$$T'_{t_0}([f \circ \gamma])(\omega(x_1)) = \omega(x_1)$$

Or $x_1 = T_{t_0}([f \circ \gamma])(x_1)$ (puisque γ est basé en x_1). L'égalité ci-dessus résulte donc de la formule $(*)$.

La correspondance $x \to \chi_{\omega,\gamma}(x)$ définit donc une application $\chi_\omega : X \to X'$. Il est clair que $\chi_\omega \circ f' = f$ et que χ_ω est continue. Montrons que χ_ω coincide avec ω sur la fibre $f^{-1}(t_0)$. Soit $x \in f^{-1}(t_0)$. Il existe un chemin c sur B basé en t_0 tel que $T_{t_0}([c])(x_1) = x$. Le chemin c se relève donc en un chemin γ sur X joignant x_1 à x. Le chemin c se relève aussi en un chemin sur X' commençant en $\omega(x_1)$. L'extrémité de ce dernier chemin est

$$\chi_\omega(x) = T'_{t_0}([c])(\omega(x_1)) = \omega \circ T_{t_0}([c])(x_1) = \omega(x)$$

□

Démonstration du théorème 7.6.1. — Le lemme 7.6.2 entraîne que Λ_{t_0} est injective et que $|\mathrm{Aut}(f)| \leq d$. Le reste du théorème 7.6.1 correspond au cas particulier du lemme 7.6.3 où $X = X'$ et $\chi \in \mathrm{Aut}(f)$, à ceci près qu'il reste à voir que χ_ω est bijective. Cela va résulter de $\chi_1 = \mathrm{Id}$ et $\chi_{\omega'\omega} = \chi_{\omega'} \circ \chi_\omega$. La première formule est évidente. Montrons la seconde. Si γ est un chemin sur X joignant x_1 à x et γ_ω l'unique relèvement de $f \circ \gamma$ commençant en $w(x_1)$, alors $\chi_{\omega'}(\gamma_\omega)$ est un chemin relevant $f \circ \gamma$ et commençant en $\chi_{\omega'}(w(x_1)) = (\omega' \circ \omega)(x_1)$. D'où $\chi_{\omega' \circ \omega}(x) = \chi_{\omega'}(\chi_\omega(x))$. □

7.6.2. Seconde description. — Le groupe des automorphismes d'un revêtement peut aussi être vu de la façon suivante.

Théorème 7.6.4. — *Si* $G \subset \mathrm{Per}(f^{-1}(t_0))$ *désigne le groupe de monodromie du revêtement* $f : X \to B$ *et si* $x_1 \in f^{-1}(t_0)$ *est un point de la fibre au-dessus de* t_0*, alors on a les (anti-)isomorphismes suivants*

$$\mathrm{Aut}(f) \simeq \mathrm{Nor}_G G(x_1)/G(x_1) \simeq \mathrm{Nor}_{\pi_1(B,t_0)}(f_*(\pi_1(X,x_1))/f_*(\pi_1(X,x_1))$$

Cette seconde description provient d'un résultat général de théorie des groupes. Soit $T : G \to S_d$ une action à gauche transitive. Notons $G(1)$ le fixateur de 1. L'ensemble $G/\cdot G(1)$ des classes à gauche de G modulo $G(1)$ peut être identifié à $\{1, \ldots, d\}$ par la correspondance $aG(1) \to T(a)(1)$.

Pout tout $g \in \mathrm{Nor}_G G(1)$, la multiplication *à droite* par g respecte les classes à gauche, c'est-à-dire, passe au quotient $G/\cdot G(1)$:

> [En effet, si $aG(1) = bG(1)$, c'est-à-dire, si $b^{-1}a \in G(1)$, alors $(bg)^{-1}ag = g^{-1}(b^{-1}a)g \in G(1)$.]

Cela permet de définir une action

$$\perp : \mathrm{Nor}_G G(1) \to \mathrm{Per}(G/.G(1)) = S_d$$

définie par $\perp(g)(aG(1)) = agG(1)$, c'est-à-dire, après identification de $\mathrm{Per}(G/.G(1))$ avec S_d, $\perp(g)(i) = a_i g(1)$ où a_i est n'importe quel élément de G tel que $a_i(1) = i$. Il s'agit d'une action à droite : $\perp(gg') = \perp(g') \circ \perp(g)$.

Lemme 7.6.5. — *L'anti-homomorphisme* $\perp$ *induit un anti-isomorphisme entre les deux groupes* $\mathrm{Nor}_G G(1)/G(1)$ *et* $\mathrm{Cen}_{S_d}(G)$*. On a en particulier* $|\mathrm{Cen}_{S_d}(G)| \leq d$*.*

Démonstration. — Il est clair que $\ker(\perp) = G(1)$. L'inclusion $\perp(\mathrm{Nor}_G G(1)) \subset \mathrm{Cen}_{S_d}(G)$ est également facile. En effet, pour tout $h \in \mathrm{Nor}_G G(1)$ et $g \in G$, on a $T(g) \circ \perp(h) = \perp(h) \circ T(g)$: en fait, $\perp(h)$ correspond à la multiplication à droite sur $G/\cdot G(1)$ et $T(g)$ à la multiplication à gauche.

Pour obtenir l'inclusion inverse, nous allons montrer que

$$|\mathrm{Nor}_G G(1)/G(1)| = |\mathrm{Cen}_{S_d}(G)| = |S|$$

où

$$S = \{i \in \{1, \ldots, d\} \mid h(i) = i \text{ pour tout } h \in G(1)\}$$

Pour tout $g \in \mathrm{Nor}_G G(1)$, $gG(1) = G(1)g$. En particulier, $g(1) \in S$. Considérons la correspondance $g \to g(1)$ de $\mathrm{Nor}_G G(1)$ dans S. Clairement elle induit une injection $\mathrm{Nor}_G G(1)/G(1) \hookrightarrow S$. De plus elle est surjective. En effet si $i \in S$, alors pour tout $g_i \in G$ tel que $g_i(1) = i$,

$g_i \in \mathrm{Nor}_G G(1)$ $[g_i^{-1} h g_i(1) = g_i^{-1} h(i) = g_i^{-1}(i) = 1]$. Cela démontre que $|\mathrm{Nor}_G G(1)/G(1)| = |S|$.

Pour tout $h \in \mathrm{Cen}_{S_d}(G)$, $h(1) \in S$. La correspondance $h \to h(1)$ de $\mathrm{Cen}_{S_d}(G)$ dans S est injective : si $h(1) = 1$, alors h fixe aussi toute l'orbite de 1 sous G. La surjectivité provient de

$$|\mathrm{Cen}_{S_d}(G)| \leq |S| = [\mathrm{Nor}_G G(1) : G(1)] \leq |\mathrm{Cen}_{S_d}(G)|$$

Cela démontre que $|\mathrm{Cen}_{S_d}(G)| = |S|$ et achève la preuve du lemme 7.6.5. □

7.7. Revêtements galoisiens

7.7.1. Définitions. —

Proposition 7.7.1. — *Un revêtement connexe $f : X \to B$ de degré d est dit galoisien s'il vérifie les conditions équivalentes suivantes :*
(i) $|\mathrm{Aut}(f)| = d$.
(ii) *Pour tout $t_0 \in B$, le groupe $\mathrm{Aut}(f)$ agit transitivement (et librement) sur la fibre $f^{-1}(t_0)$.*
(iii) *Pour tout $t_0 \in B$ et tout $x \in f^{-1}(t_0)$, le groupe $f_*(\pi_1(X, x))$ est un sous-groupe normal de $\pi_1(B, t_0)$.* [(2)]

Dans ce cas, le groupe $\mathrm{Aut}(f)$ des automorphismes de f est anti-isomorphe au groupe de monodromie $G(f)$ du revêtement f et donc aussi au groupe $\pi_1(B, t_0)/f_*(\pi_1(X, x))$.

Démonstration. — On sait que le groupe $\mathrm{Aut}(f)$ opère librement sur la fibre $f^{-1}(t_0)$. Donc cette action est transitive si et seulement si $|\mathrm{Aut}(f)| = d$. D'où l'équivalence entre (i) et (ii). La suite d'(anti-)isomorphismes

$$\begin{aligned} \mathrm{Aut}(f) &\simeq \mathrm{Cen}_{S_d}(G(f)) \\ &\simeq \mathrm{Nor}_G G(1)/G(1) \\ &\simeq \mathrm{Nor}_{\pi_1(B,t_0)} f_*(\pi_1(X, x))/f_*(\pi_1(X, x)) \end{aligned}$$

indique que (i) équivaut à "$G(1)$ distingué dans G" ce qui équivaut à "$T_{t_0}^{-1}(G(1)) = f_*(\pi_1(X, x))$ distingué dans $T_{t_0}^{-1}(G) = \pi_1(B, t_0)$". Si c'est le

[(2)] Dans (ii) et (iii), "Pour tout $t_0 \in B$" peut être remplacé par "Il existe $t_0 \in B$".

cas, on a aussi

$$\begin{aligned}\mathrm{Aut}(f) &\simeq \pi_1(B,t_0)/f_*(\pi_1(X,x))\\ &= \pi_1(B,t_0)\Big/\textstyle\bigcap_{[c]\in\pi_1(X,t_0)} f_*(\pi_1(X,x))^{[c]}\\ &= \pi_1(B,t_0)/\textstyle\bigcap_{i=1}^{d} f_*(\pi_1(X,x_i)) \text{ (où } f^{-1}(t_0)=\{x_1,\dots,x_d\})\\ &= G(f)\end{aligned}$$

[Pour l'avant-dernière égalité , identifier $\pi_1(X,x)$ au fixateur de 1 dans l'action T_{t_0} de monodromie, ce qui donne $\pi_1(X,x)^{[c]} = \pi_1(X,x_i)$ où $T_{t_0}([c])(1) = i$.]

□

Exemple 7.7.2. — (a) Le revêtement $m_d : \mathbb{C}^\times \to \mathbb{C}^\times$ donné par $m_d(z) = z^d$ est galoisien. Son groupe d'automorphismes est isomorphe au groupe μ_d des racines d-ièmes de 1.

(b) Soit $P(T,Y) \in \mathbb{C}[T,Y]$ un polynôme irréductible. On verra que le revêtement (connexe) $C_P^*(\mathbb{C}) \to (\mathbb{A}^1)^*(\mathbb{C})$ (défini dans l'exemple 7.3.3) est galoisien si et seulement si le corps

$$\mathbb{C}(T)[Y]/(P(T,Y)$$

est une extension galoisienne de $\mathbb{C}(T)$. Et dans ce cas, le groupe d'automorphismes de ce revêtement est le groupe de Galois de l'extension ci-dessus.

7.7.2. Clôture galoisienne. — Soit $f : X \to B$ un revêtement connexe de degré d. On construit ci-dessous la *clôture galoisienne* de f, c'est-à-dire le "plus petit revêtement galoisien de f".

Notons $f^d : X_B^d \to B$ le produit fibré de d copies de f. C'est-à-dire, $X_B^d = X \times_B \times \cdots \times_B X$ est l'ensemble des d-uplets $(x_1,\dots,x_d) \in X^d$ tels que $f(x_i) = f(x_j)$, $i,j = 1,\dots,d$. Notons U_B^d le sous-ensemble de X_B^d constitué des points $(x_1,\dots,x_d) \in X_B^d$ de coordonnées distinctes. D'après la proposition 7.3.7 et le lemme 7.7.5 ci-dessous, la restriction de f^d à U_B^d est un revêtement.

Lemme 7.7.3. — *U_B^d est un sous-ensemble ouvert et fermé de X_B^d.*

Démonstration. — L'ensemble U_B^d est clairement ouvert. Montrons qu'il est fermé. Soit $(\mathbf{x}_n)_{n>0}$ une suite de points $\mathbf{x}_n = (x_{n,1},\dots,x_{n,d})$ de U_B^d convergeant vers un point $\mathbf{x} = (x_1,\dots,x_d) \in X_B^d$. Soit U un ouvert trivialisant f contenant $t = f(x_1) = \dots = f(x_d)$ et $(V_i)_{1\le i\le d}$ la famille d'ouverts disjoints de X composant $f^{-1}(U)$. Pour $i = 1,\dots,d$, notons W_i celui des ouverts $V_1,\dots,V_d$ qui contient x_i. Pour n suffisamment grand, on a alors $x_{n,i} \in W_i$, $i = 1,\dots,d$. Comme les points $x_{n,i}$, $i = 1,\dots,d$ sont distincts et que f est injective sur

chaque V_i, les ouverts $W_1, \ldots, W_d$ sont nécessairement distincts et disjoints. En particulier, les points $x_1, \ldots, x_d$ sont distincts, c'est-à-dire, $\mathbf{x} \in U_B^d$. □

Le revêtement $f_d : U_B^d \to B$ est de degré $d!$. De plus son groupe d'automorphismes contient le groupe symétrique S_d : chaque élément $\omega \in S_d$ définit un automorphisme χ_ω par $\chi_\omega(x_1, \ldots, x_d) = (x_{\omega(1)}, \ldots, x_{\omega(d)})$.

L'espace U_B^d n'est pas forcément connexe. Notons $\widehat{X}_1, \ldots, \widehat{X}_t$ ses composantes connexes. Notons $\widehat{f}_i : \widehat{X}_i :\to B$ la restriction de f^d à $\widehat{X}_i$, $i = 1, \ldots, t$.

Théorème 7.7.4. — *Les revêtements $\widehat{f}_i : \widehat{X}_i \to B$, $i = 1, \ldots, t$ sont des revêtements galoisiens équivalents. Leur groupe d'automorphismes est anti-isomorphe au groupe de monodromie $G(f)$ du revêtement initial $f : X \to B$. Les propriétés suivantes caractérisent les revêtements $\widehat{f} : \widehat{X} \to B$ de cette classe d'équivalence.*

(a) *$\widehat{f} : \widehat{X} \to B$ est un revêtement galoisien.*

(b) *Il existe un revêtement galoisien $f_X : \widehat{X} \to X$ tel que $f \circ f_X = \widehat{f}$. En d'autres termes, $f : X \to B$ est un quotient de $\widehat{f} : \widehat{X} \to B$.*

(c) *Tout revêtement galoisien $g : \widehat{Y} \to B$ qui se factorise par $f : X \to B$ se factorise par $\widehat{f} : \widehat{X} \to B$.*

Démonstration. — Soit $t_0 \in B$ et $x_1, \ldots, x_d$ les points de la fibre $f^{-1}(t_0)$. Un revêtement $\widehat{f} : \widehat{X} \to B$ vérifiant (a), (b), (c) correspond, à équivalence près, au plus grand sous-groupe normal $\widehat{H}$ de $\pi_1(B, t_0)$ contenu dans $f_*(\pi_1(X, x_1))$, qui vaut

$$\widehat{H} = \bigcap_{[c] \in \pi_1(B, t_0)} [f_*(\pi_1(X, x_1))]^{[c]} = \bigcap_{i=1}^{d} f_*(\pi_1(X, x_i))$$

Conclusion : la clôture galoisienne $\widehat{f} : \widehat{X} \to B$ de $f : X \to B$ existe et est unique, à équivalence près. Son groupe d'automorphismes $\mathrm{Aut}(f)$ est anti-isomorphe au groupe $\pi_1(B, t_0)/\widehat{H} = G(f)$.

Montrons maintenant que les revêtements $\widehat{f}_i : \widehat{X}_i \to B$ sont équivalents à $\widehat{f} : \widehat{X} \to B$, $i = 1, \ldots, t$. Montrons tout d'abord que $\widehat{f}_i : \widehat{X}_i \to B$ est un revêtement de degré $|G(f)|$, $i = 1, \ldots, d$. Les composantes connexes $\widehat{X}_1, \ldots, \widehat{X}_t$ correspondent aux orbites de la monodromie sur la fibre $(f^d)^{-1}(t_0)$ et le degré des revêtements associés correspond à la longueur de ces orbites. La fibre $(f^d)^{-1}(t_0)$ correspond aux d-uplets

$$(H[c_1], \ldots, H[c_d])$$

de classes à droite modulo le sous-groupe $H \subset \pi_1(B, t_0)$ des chemins sur B basés en t_0. L'action par monodromie d'un chemin c basé en t_0 correspond alors à la permutation induite par la multiplication à droite par $[c]$:

$$(H[c_1], \ldots, H[c_d]) \to (H[c_1][c], \ldots, H[c_d][c])$$

Le fixateur d'un point dans cet action est l'intersection des fixateurs de chacun des points de la fibre $f^{-1}(t_0)$ par la monodromie sur X, c'est-à-dire le groupe $\bigcap_{i=1}^{d} f_*(\pi_1(X, x_i))$. La longueur de l'orbite de ce même point est l'indice de ce groupe dans le groupe $\pi_1(B, t_0)$, c'est-à-dire $|G(f)|$.

Le fait que $\widehat{f_i} : \widehat{X}_i \to B$ est galoisien, $i = 1, \ldots, d$ résulte du lemme 7.7.5 ci-dessous (appliqué au revêtement $f_B^d : U_B^d \to B$, au groupe $G = S_d$ et à $C = \widehat{X}_i$).

D'après la propriété (c) du revêtement $\widehat{f} : \widehat{X} \to B$, il existe un revêtement $g : \widehat{X}_i \to \widehat{X}$ tel que $\widehat{f} \circ g = \widehat{f_i}$, $i = 1, \ldots, t$. Comme les revêtements $\widehat{f} : \widehat{X} \to B$ et $\widehat{f_i} : \widehat{X}_i \to B$ ont même degré, à savoir $|G(f)|$, le revêtement $g : \widehat{X}_i \to \widehat{X}$ est de degré 1, et donc est une équivalence entre les deux revêtements $\widehat{f}$ et $\widehat{f_i}$, $i = 1, \ldots, t$. □

Lemme 7.7.5. — *Soit $f : X \to B$ un revêtement de degré d. Supposons que le groupe* $\mathrm{Aut}(f)$ *possède un sous-groupe G qui opère transitivement sur une fibre $f^{-1}(t_0)$, ($t_0 \in B$). Alors la restriction de f à toute composante connexe C de X est un revêtement galoisien.*

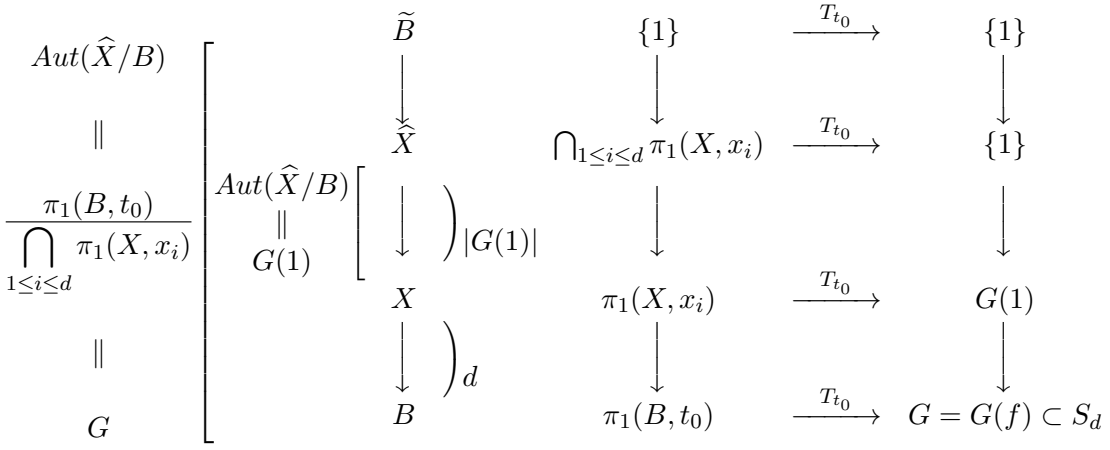
Démonstration. — Soit C une composante connexe de X. On sait déjà que la restriction $f|_C : X \to B$ est un revêtement. Montrons que ce revêtement est galoisien.

Soient $x, y \in (f|_C)^{-1}(t_0) = f^{-1}(t_0) \cap C$. D'après les hypothèses, il existe un élément $g \in G \subset \mathrm{Aut}(f)$ tel que $g(x) = y$. L'automorphisme g induit une permutation de l'ensemble des composantes connexes de X. Mais comme $x, y \in C$, on a nécessairement $g(C) = C$. L'automorphisme g induit donc un automorphisme de la restriction $f|_C : C \to B$ qui envoie x sur y. Conclusion : le groupe $\mathrm{Aut}(f|_C)$ agit transitivement sur la fibre $(f|_C)^{-1}(t_0)$, c'est-à-dire, $f|_C : C \to B$ est galoisien. □

7.7.3. Correspondance de Galois. — Les conclusions et le diagramme suivants résument la situation.

Théorème 7.7.6. — *Les revêtements $X \to B$ d'un espace B correspondent aux sous-groupes H de $\pi_1(B)$. Dans cette correspondance, le groupe H s'identifie au groupe $\pi_1(X)$. Les revêtements galoisiens correspondent aux*

sous-groupes H qui sont distingués dans $\pi_1(B)$, le groupe d'automorphismes $\mathrm{Aut}(X/B)$ *s'identifiant alors au groupe quotient $\pi_1(B)/\pi_1(X)$. Le "plus grand" revêtement de B correspond au sous-groupe trivial de $\pi_1(B)$; il est simplement connexe et galoisien de groupe d'automorphismes $\pi_1(B)$; c'est le revêtement universel $\widetilde{B}$ de B.*



Remarque 7.7.7. — Le théorème 7.7.6 est à comparer à l'énoncé analogue qu'on connaît pour les extensions algébriques d'un corps K de caractéristique 0. (Pour un corps de caractéristique quelconque, il faut remplacer ci-dessous "algébrique" par "algébrique séparable").

Les extensions algébriques E/K d'un corps K correspondent aux sous-groupes H du groupe de Galois absolu $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$. Dans cette correspondance, le groupe H s'identifie au groupe G_E. Les extensions galoisiennes correspondent aux sous-groupes H qui sont distingués dans G_K, le groupe de Galois $\mathrm{Gal}(E/K)$ s'identifiant alors au quotient $\mathrm{G}_K/\mathrm{G}_E$. La "plus grande" extension algébrique de K correspond au sous-groupe trivial de G_K ; elle est algébriquement close et galoisienne de groupe de Galois G_K ; c'est la clôture algébrique $\overline{K}$ de K.

7.7.4. Applications. —

7.7.4.1. Forme topologique du problème inverse de Galois. — On peut réénoncer le théorème 7.5.11 sous la forme suivante.

Théorème 7.7.8. — *Tout groupe fini G est le groupe d'automorphismes d'un revêtement galoisien $X \to \mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}$ de la droite projective complexe $\mathbb{P}^1(C)$ privée d'un certain nombre r (dépendant de G) de points $t_1, \ldots, t_r$.*

7.7.4.2. Théorème de Van Kampen. —

CHAPITRE 8

THÉORÈME D'EXISTENCE DE RIEMANN

Dans ce chapitre, l'espace base B est la droite projective $\mathbb{P}^1(\mathbb{C})$ privée éventuellement d'un ensemble fini $D = \{t_1, \ldots, t_r\}$ de points. Si $f : X \to B$ est un revêtement, l'espace X hérite de la structure de surface de Riemann de B. Ce chapitre comporte deux parties. La première consiste à montrer qu'on peut compléter f en un "revêtement ramifié" $\overline{f} : \overline{X} \to \mathbb{P}^1$ entre surfaces de Riemann *compactes*. C'est le théorème d'existence de Riemann. La seconde montre qu'à ce revêtement ramifié $\overline{f} : \overline{X} \to \mathbb{P}^1$, on peut associer une extension finie de corps $M(\overline{X})/\mathbb{C}(T)$ de degré égal au degré du revêtement initial f. De plus, si le revêtement f est galoisien, l'extension $M(\overline{X})/\mathbb{C}(T)$ est galoisienne de groupe de Galois (anti-)isomorphe au groupe $\mathrm{Aut}(f)$ des automorphismes du revêtement f. Cela permet de résoudre le Problème Inverse de la Théorie de Galois sur $\mathbb{C}(T)$.

8.1. Variétés et surfaces de Riemann

8.1.1. Définitions. — On appelle *variété topologique de dimension réelle* n un espace topologique X séparé (non nécessairement connexe), localement homéomorphe à $\mathbb{R}^n$, c'est-à-dire, ayant la propriété que tout point possède un voisinage homéomorphe à $\mathbb{R}^n$ (ou de façon équivalente, à une boule ouverte de $\mathbb{R}^n$). Si $n = 2m$, on peut remplacer $\mathbb{R}^n$ par $\mathbb{C}^m$; l'entier m s'appelle alors la dimension complexe de X.

Un *atlas réel* de X est la donnée de $(U_\alpha, f_\alpha)_\alpha$ où $(U_\alpha)_\alpha$ est un recouvrement ouvert de X et $f_\alpha : U_\alpha \to D_\alpha$ est un homéomorphisme entre U_α et un ouvert D_α de $\mathbb{R}^n$. Chaque (U_α, f_α) s'appelle une *carte*. Les applications $f_\beta \circ f_\alpha^{-1}$ sont des applications entre ouverts de $\mathbb{R}^n$ induisant un homéomorphisme entre

$f_\alpha(U_\alpha \cap U_\beta) \subset D_\alpha$ et $f_\beta(U_\alpha \cap U_\beta) \subset D_\beta$. On les appelle les *fonctions de transition* ou *changements de cartes*.

Si $n = 2m$, on a aussi la notion d'*atlas complexe* de X. On obtient la définition en remplaçant $\mathbb{R}^n$ par $\mathbb{C}^m$ dans la définition d'atlas réel.

La variété X a une structure réelle ... (resp. complexe ...) s'il existe un atlas réel (resp. complexe) pour lequel les fonctions de transition sont des morphismes pour la structure ... La structure ... peut être par exemple une structure :
- topologique : on demande aux fonctions de transition d'être des morphismes topologiques, c'est-à-dire continus. Dans ce cas on n'ajoute rien à la définition de variété topologique.
- $\mathbb{R}$-différentiable : on parle de *variété différentiable réelle*.
- C^∞-réelle : on parle de *variété C^∞ réelle*.
- $\mathbb{C}$-différentiables : on parle de *variété différentiable complexe*.
- $\mathbb{R}$-analytiques : on parle de *variété analytique réelle*.
- $\mathbb{C}$-analytiques : on parle de *variété analytique complexe*.

Deux atlas $((U_\alpha, f_\alpha)_\alpha)$ et $((V_\beta, g_\beta)_\beta)$ donnant une structure ... à une variété X sont dits équivalents si la réunion est un atlas ..., c'est-à-dire, si les $f_\alpha \circ g_\beta^{-1}$ ont la propriété ... (là où ils sont définis). On appelle structure ... une classe d'équivalence d'atlas donnant une structure ... à la variété.

Remarque 8.1.1. — (a) On a les implications suivantes entre les diverses structures : $\mathbb{C}$-analytique $\Leftrightarrow$ $\mathbb{C}$-différentiable et $\mathbb{R}$-analytique $\Rightarrow$ C^∞ réel $\Rightarrow$ $\mathbb{R}$-différentiable.

(b) Une variété complexe de dimension m a une structure de variété réelle de dimension $2m$, qu'on appelle structure réelle induite.

Définition 8.1.2. — On appelle *surface de Riemann* toute variété analytique complexe X de dimension 1. C'est-à-dire, l'espace X possède un atlas $\{(U_\alpha, f_\alpha)_\alpha\}$ pour lequel les applications f_α sont des homéomorphismes entre U_α et un ouvert de $\mathbb{C}$ et tel que les changement de cartes sont des fonctions holomorphes.

Si X et X' sont deux surfaces de Riemann pourvues d'atlas respectifs $\{(U_\alpha, f_\alpha)_\alpha\}$ et$\{(U'_\alpha, f'_\alpha)_\alpha\}$, une fonction $f : X \to X'$ est un *morphisme* de surfaces de Riemann si les applications $f'_\beta \circ f \circ f_\alpha^{-1}$ sont des fonctions holomorphes (là où elles sont définies). Une *fonction holomorphe* (resp. *méromorphe*) sur X est un morphisme $X \to \mathbb{C}$ (resp. $X \to \mathbb{P}^1(\mathbb{C})$). Une fonction $f : X \to \mathbb{P}^1(\mathbb{C})$

est une fonction méromorphe si et seulement si les applications $f_\alpha^{-1} \circ f$ sont des fonctions méromorphes (au sens usuel des fonctions complexes) sur U_α.

Les morphismes de surfaces de Riemann héritent des propriétés locales des fonctions holomorphes : principe des zéros isolés, théorème de l'image ouverte, etc. Une autre conséquence est que l'ensemble des fonctions méromorphes sur une surface de Riemann connexe X est un corps. On le note $M(X)$.

8.1.2. Exemples. —

8.1.2.1. Espaces obtenus par déformation d'ouverts de $\mathbb{R}^n$. — $\mathbb{R}^n$, ses ouverts, les espaces homéomorphes à des ouverts de $\mathbb{R}^n$ sont des variétés analytiques réelles, et analytiques complexes si n est pair.

8.1.2.2. Espaces projectifs. — $\mathbb{P}^1(\mathbb{C})$: Les deux cartes $(\mathbb{C}, z \to z)$ et $(\mathbb{C}^\times \cup \{\infty\}, z \to 1/z)$ donnent à $\mathbb{P}^1(\mathbb{C})$ une structure de surface de Riemann.

$\mathbb{P}^1(\mathbb{R})$ est une variété analytique réelle ; un atlas est obtenu par restriction à partir de celui donné pour $\mathbb{P}^1(\mathbb{C})$. On déduit que $S^1(\mathbb{R})$ est une variété analytique réelle de dimension 1.

$\mathbb{P}^n(\mathbb{C})$ est une variété analytique complexe de dimension n. Les ouverts $U_\alpha = \{x_\alpha \neq 0\}$, donnés avec l'isomorphisme naturel avec $\mathbb{C}^n$ en forment un recouvrement. Les changements de carte sont donnés par les correspondances

$$(t_1/t_\alpha, \ldots, t_n/t_\alpha)\ (i \neq \alpha) \to (t_1/t_\beta, \ldots, t_n/t_\beta)\ (i \neq \beta)$$

c'est-à-dire, en coordonnées intrinsèques

$$(x_1, \ldots, x_n)\ (i \neq \alpha) \to (x_1/x_\beta, \ldots, 1/x_\beta, \ldots, x_n/x_\beta)\ (i \neq \beta)$$

$\mathbb{P}^n(\mathbb{R})$ est une variété analytique ; un atlas est obtenu par restriction à partir de celui donné pour $\mathbb{P}^n(\mathbb{C})$.

8.1.3. Courbes complexes. — Etant donné un polynôme $P(T, Y) \in \mathbb{C}[T, Y]$, considérons la courbe affine plane C_P d'équation $P(t, y) = 0$. On munit les ensembles $C_P(\mathbb{C})$ (resp. $C_P(\mathbb{R})$) des points complexes (resp. réels) de la topologie induite de celle de $\mathbb{C}^2$.

Exercice 8.1.3. — Montrer que $C_P(\mathbb{C})$ est non compact si $\deg(P) > 0$, que $C_P(\mathbb{R})$ peut être compact, que $C_P(\mathbb{R})$ peut être non connexe même si P est irréductible (contrairement à $C_P(\mathbb{R})$, voir la proposition 8.1.4 ci-dessous), que $C_P(\mathbb{C})$ peut-être connexe sans que P soit irréductible, que $C_P(\mathbb{C})$ et $C_P(\mathbb{R})$ sont d'intérieur vide, que $C_P(\mathbb{C})$ n'a pas de points isolés (voir lemme 8.3.13), que $C_P(\mathbb{R})$ en a au plus un nombre fini.

Une courbe affine n'est pas n'est pas forcément une variété. Ainsi, sur la courbe réelle plane $C : y^2 = x^3 - x^2$; le point $(0, 0)$ n'admet aucun voisinage homéomorphe à $\mathbb{R}$ (si on enlève le point double, on obtient localement 4 (et non 2) composantes connexes).

De façon générale, on définit C_P^{reg} comme l'ouvert de C_P des points dits *réguliers* où le gradient n'est pas nul. Les points en dehors de C_P^{reg} sont dits *singuliers*.

Proposition 8.1.4. — *$C_P^{\mathrm{reg}}(\mathbb{C})$ est une surface de Riemann (non fermée), qu'on notera S_P. Elle est connexe si le polynôme $P(T, Y)$ définissant C_P est irréductible.*

Démonstration. — D'après le théorème des fonctions implicites, au voisinage de tout point $(x, y) \in C_P^{\mathrm{reg}}$, au moins une des deux projections $(x, y) \to x$ est un homéomorphisme sur son image. Plus précisément, si $P'_Y(x_0, y_0) \neq 0$, il existe un voisinage ouvert U de (x_0, y_0) et un disque ouvert D centré en x_0[(1)] tel que la projection $(x, y) \to x$ soit un homéomorphisme f entre U et D. On peut choisir D de telle sorte que la réciproque f^{-1} soit donnée par $f^{-1}(x) = (x, y(x))$ où $y(x)$ est une série entière en $x - x_0$ convergeant dans D. L'ensemble de tous ces homéomorphismes locaux constitue un atlas analytique complexe sur C_P^{reg}. L'énoncé sur la connexité sera démontré au chapitre 8 (théorème 8.3.12). □

Corollaire 8.1.5. — *Si X est une courbe projective lisse irréductible définie sur $\mathbb{C}$ (par exemple le modèle projectif lisse de la courbe plane C_P), alors $X(\mathbb{C})$ est une surface de Riemann connexe compacte.*

Démonstration. — La compacité provient du fait que X peut être plongé comme fermé de Zariski dans un espace projectif $\mathbb{P}^n$ et qu'en conséquence $X(\mathbb{C})$ est un fermé pour la topologie complexe de l'espace topologique compact $\mathbb{P}^n(\mathbb{C})$. Au voisinage de tout point $x \in X(\mathbb{C})$, la courbe X est isomorphe à une courbe affine non singulière en x. L'application du théorème des fonctions implicites (comme ci-dessus si la courbe est plane ou sous sa forme plus générale sinon) fournissent des homéomorphismes locaux au voisinage de tout point x, lesquels constituent un atlas analytique complexe sur $X(\mathbb{C})$. L'énoncé sur la connexité résultera également du théorème 8.3.12. □

(1) On peut choisir D de rayon supérieur ou égal à la distance entre x_0 et la racine la plus proche du discriminant de P par rapport à Y.

Structure conjuguée sur S_P. On note c la conjugaison complexe sur $\mathbb{C}$; on utilise aussi parfois la notation usuelle $c(z) = \overline{z}$. Si X est une variété complexe de dimension m et $(U_\alpha, f_\alpha)_\alpha$ un atlas complexe, on appelle structure conjuguée sur X la structure induite par l'atlas $(U_\alpha, cf_\alpha)_\alpha$. Les fonctions de transition sont les fonctions

$$\begin{aligned} z \ \to \ cf_\beta \ (cf_\alpha)^{-1}(z) \ &= (cf_\beta {f_\alpha}^{-1} c)(z) \\ &= \overline{(f_\beta f_\alpha^{-1})(\overline{z})} \end{aligned}$$

Autrement dit, à une fonction de transition $z \to \varphi(z) = \sum a_n (z - z_0)^n$ sur S_P correspond la fonction de transition $z \to \overline{\varphi}(z) = \sum \overline{a_n}(z - \overline{z_0})^n$ pour la structure conjuguée. On notera V^* la variété V munie de sa structure conjuguée.

Pour les surfaces de Riemann de type S_P, on a aussi une action de la conjugaison complexe sur les points de $S_P \subset \mathbb{C}^2$. On note $\overline{S_P}$ l'ensemble des conjugués de points de S_P. L'ensemble $\overline{S_P}$ est homéomorphe à la surface de Riemann S_P. On a plus précisément :

Proposition 8.1.6. — *Soit $P(X,Y) \in \mathbb{C}[X,Y]$ un polynôme. On note $\overline{P}(X,Y)$ le polynôme déduit de P par conjugaison sur les coefficients. Alors la surface de Riemann $S_{\overline{P}}$ coincide avec la surface de Riemann ${\overline{S_P}}^*$.*

Démonstration. — Les ensembles sous-jacents sont clairement les mêmes. Il faut voir que les atlas sont équivalents. Soit $(U_\alpha, f_\alpha)_\alpha$ un atlas de la surface de Riemann S_P. Par définition de $\overline{S_P}$ et de la structure conjuguée, l'ensemble des données locales $(\overline{U_\alpha}, cf_\alpha c)_\alpha$ constitue un atlas de la surface de Riemann ${\overline{S_P}}^*$. Si comme pour l'atlas construit dans la preuve de la proposition 8.1.4 (U_α, f_α) est la restriction à $U_\alpha \subset S_P$ de la première ou de la seconde projection, alors $(\overline{U_\alpha}, cf_\alpha c)$ est la restriction à $\overline{U_\alpha} \subset S_{\overline{P}}$ de la première ou de la seconde projection respectivement. L'ensemble des données locales $(\overline{U_\alpha}, cf_\alpha c)_\alpha$ constitue alors un atlas de la surface de Riemann $S_{\overline{P}}$. □

Proposition 8.1.7. — *Supposons de plus que $P(X,Y)$ soit irréductible. Les assertions suivantes sont équivalentes.*

(i) *$S_P = \overline{S_P}$ (comme ensembles).*

(ii) *Il existe $Q \in \mathbb{R}[X,Y]$ tel que $S_P = S_Q$ (comme surfaces de Riemann).*

Quand elles sont vérifiées, on dit que la courbe plane S_P peut être définie sur $\mathbb{R}$. L'ensemble $C_P^{\mathrm{reg}}(\mathbb{R})$ des points réels réguliers de $S_P = S_Q$ a alors une structure naturelle de variété analytique réelle de dimension 1.

L'implication (ii) ⇒ (i) est évidente. La réciproque repose sur le lemme suivant.

Lemme 8.1.8. — *Soient* $A(X,Y), B(X,Y) \in \mathbb{C}[X,Y]$ *deux polynômes irréductibles. S'ils ont une infinité de zéros communs, alors il existe* $\lambda \in \mathbb{C}$ *tel que* $A(X,Y) = \lambda\, B(X,Y)$.

Démonstration. — On peut supposer que $\deg_Y(A) > 0$; sinon on échange X et Y. Cela entraîne cette propriété :

(*) Pour tout $a \in \mathbb{C}$, le polynôme $A(a,Y)$ n'a qu'un nombre fini de racines, c'est-à-dire n'est pas nul.

En effet, si $A(a,Y) = 0$, alors $A(X,Y)$ est divisible par $X - a$ et donc $A(X,Y) = \delta(X-a)$ ($\delta \in \mathbb{C}$) puisque A est irréductible ; cela contredit $\deg_Y(A) > 0$.

On a alors aussi $\deg_Y(B) > 0$ car dans le cas contraire, $B(X,Y) = \gamma\,(X-a)$ ($\gamma \in \mathbb{C}$) et l'hypothèse entraîne que $A(a,y) = 0$ pour une infinité de y ce qui contredit (*).

Les polynômes A et B sont irréductibles dans l'anneau principal $\mathbb{C}(X)[Y]$ (lemme de Gauss). Les idéaux qu'ils engendrent sont soit égaux, soit premiers entre eux. S'il sont premiers entre eux, il existe d'après Bezout, $U(X,Y)$, $V(X,Y)$ dans $\mathbb{C}[X,Y]$ et $R(X) \in \mathbb{C}[X]$ non nul, tels que

$$U(X,Y)A(X,Y) + V(X,Y)B(X,Y) = R(X)$$

Mais cela interdit à A et B d'avoir une infinité de zéros communs (utiliser (*) une nouvelle fois). Les idéaux engendrés par A et B sont donc égaux, ce qui signifie que A et B diffèrent d'un élément $U(X) \in \mathbb{C}(X)$. Comme A et B sont primitifs, $U(X) \in \mathbb{C}[X]^\times = \mathbb{C}$. □

Démonstration de la proposition 8.1.7. — Supposons (i). D'après le lemme, on a $P(X,Y) = \lambda\overline{P}(X,Y)$ avec $\lambda \in \mathbb{C}$. Nécessairement, λ est de module 1 et s'écrit donc $\lambda = \bar{d}/d$ pour un $d \in \mathbb{C}$[(2)]. Le polynôme $Q = d\,P$ satisfait (ii). La structure de variété analytique réelle sur $C_{\mathrm{reg}}(\mathbb{R})$ provient du fait que les fonctions de transition sont analytiques réelles au voisinage des points (réguliers) réels. □

Remarque 8.1.9. — La proposition 8.1.7 est aussi une conséquence du Nullstellensatz (théorème 1.7.6) : puisque P s'annule là où s'annule $\overline{P}$, il existe une puissance de P dans l'idéal engendré par $\overline{P}$, et vice-versa. Mais pour appliquer le Nullstellensatz, il faut montrer au préalable, que si $S_P = S_{\overline{P}}$, alors P et $\overline{P}$ ont exactement les mêmes zéros : le nombre fini de points singuliers échappe *a priori* à l'hypothèse $S_P = S_{\overline{P}}$. Il faut donc quand même démontrer

(2) on peut prendre $d = (\overline{\lambda} + 1)$.

la version plus faible du lemme 8.1.8 où on suppose que A et B ont, à un nombre fini près, les mêmes zéros, c'est-à-dire, que, pour la topologie de Zariski, l'adhérence d'un fermé F auquel on a enlevé un nombre fini de points, est égale au fermé F.

8.1.4. Tores. — L'espace topologique S^1 peut être vu comme les points réels de la courbe algébrique $x^2+y^2=1$. Tous ses points sont réguliers. D'après le paragraphe précédent, S^1 a une structure naturelle de variété analytique réelle de dimension 1. Le tore T^m est donc naturellement une variété analytique réelle (compacte et connexe) de dimension m.

Le tore complexe $\mathbb{C}/(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2) \simeq \mathbb{C}/\mathbb{Z}^2 \simeq T^2$ a aussi une structure de surface de Riemann.

(Si p désigne la surjection $\mathbb{C} \to \mathbb{C}/\mathbb{Z}^2$, les 4 ouverts suivants recouvrent $\mathbb{C}/\mathbb{Z}^2 = p([0,1[\times[0,1[) : U_1 = p(]0,1[\times]0,1[)$, $U_2 = p(]-1/2,1/2[\times]0,1[)$, $U_3 = p(]0,1[\times]-1/2,1/2[)$, et $U_4 = p(]0,1[\times]-1/2,1/2[)$. On obtient un système de cartes en faisant correspondre à tout point $M \in U_\alpha$ l'unique représentant dans le domaine associé c'est-à-dire le produit d'intervalles définissant U_α. Sur

$$U_1 \cap U_2 = p(]0,1/2[\times]0,1[\cup]1/2,1[\times]0,1[)$$

par exemple, le changement de carte est $z \to z$ sur la partie gauche et $z \to z+1$ (ou $z-1$) sur la partie droite.)

8.1.5. Topologie des surfaces réelles. —

Définition 8.1.10. — On appelle *surface réelle* toute variété analytique réelle de dimension 2. La surface est dite *orientable* s'il existe un atlas $(U_\alpha, f_\alpha)_\alpha$ tel que $f_\alpha(U_\alpha) = \mathbb{R}^2$ pour tout α et les fonctions de transition conservent l'orientation de $\mathbb{R}^2$ [(3)].

On vérifie que cette définition ne dépend pas du représentant de l'atlas dans sa classe d'équivalence.

Les fonctions analytiques complexes conservant l'orientation, les surfaces de Riemann sont orientables.

Il existe un théorème de classification des surfaces réelles. Nous ne l'utiliserons pas et renvoyons à [**Rey89**, chapitre II] pour une démonstration.

[(3)] c'est-à-dire, préservent le générateur du groupe fondamental de $\mathbb{R}^2 \setminus \{(0,0)\}$, ou encore, préservent le signe de l'indice par rapport à un point d'un chemin tournant autour.

Théorème 8.1.11. — (a) *Une surface compacte est une surface de Riemann si et seulement si elle est orientable.* [(4)]

(b) *Toute surface de Riemann compacte connexe est homéomorphe soit à la sphère de Riemann S^2 soit à un polygone à $4g$ côtés consécutifs $a_g, b_g, a_g^{-1}, b_g^{-1}, \ldots, a_1, b_1, a_1^{-1}, b_1^{-1}$ où a_i et b_i doivent être identifiés respectivement aux inverses de a_i^{-1} et b_i^{-1}, $i = 1, \ldots, g$. En particulier, une telle surface est homéomorphe à un "tore complexe à g trous".*

(d) *L'entier g est un invariant topologique appelé genre topologique de la surface de Riemann.*

Remarque 8.1.12. — (a) Le ruban de Möbius n'est pas une surface de Riemann, car non orientable (voir [**God71**, p.43]).

(b) Il faut distinguer le "tore complexe à g trous" du tore T^m défini en §7.2.1.2. Le tore T^m est une variété de dimension réelle m alors que le tore complexe à g trous est de dimension réelle 2. Seul le tore T^2 coincide avec un tore complexe, à savoir, le tore complexe à 1 trou $\mathbb{C}/\mathbb{Z}^2$.

8.2. Complétion

8.2.1. Enoncé. — On note $\overline{B}$ la droite projective complexe $\mathbb{P}^1(\mathbb{C})$ ou plus généralement une surface de Riemann connexe compacte, c'est-à-dire un tore complexe à g trous. Soient $D = \{t_1, \ldots, t_r\}$ un ensemble de r points distincts de $\overline{B}$ et $B = \overline{B} \setminus D$. En particulier, B satisfait les hypothèses des chapitres précédents : B est connexe, localement connexe par arcs et localement simplement connexe.

Soit $f : X \to B$ un revêtement fini. L'espace X a une structure de surface de Riemann :

> [Soit $\{(U_\alpha, f_\alpha)_\alpha\}$ un atlas sur B. On peut supposer que les ouverts U_α trivialisent f. Si on note $V_{\alpha,1}, \ldots, V_{\alpha,d}$ les ouverts disjoints constituant $f^{-1}(U_\alpha)$, alors la famille $\{(V_{\alpha,i}, f_\alpha \circ f)_{\alpha,i}\}$ constitue un atlas sur X.]

Le revêtement $f : X \to B$ est un morphisme de surfaces de Riemann pour cette structure [regardée sur les cartes, l'application f est l'identité $z \to z$ et est donc holomorphe].

(4) Plus précisément "compacte" $\Rightarrow$ "triangulable" qui avec "orientable" donne "surface de Riemann ".

Théorème 8.2.1. — *Il existe un unique morphisme de surfaces de Riemann compactes $\overline{f} : \overline{X} \to \overline{B}$ tel que la restriction $\overline{f} : \overline{f}^{-1}(B) \to B$ soit un revêtement équivalent à $f : X \to B$. De plus, $\overline{X} \setminus \overline{f}^{-1}(B)$ est fini ; en particulier $\overline{X}$ est connexe si X l'est.*

Il s'agit de prolonger le revêtement au-dessus des points $t_1, \ldots, t_r$. On explique dans le paragraphe suivant comment on le fait localement.

8.2.2. Revêtements d'un disque épointé. — On note D le disque unité ouvert de $\mathbb{C}$ et $D^\times$ le disque unité privé de son centre.

Lemme 8.2.2. — *Soit $\varphi : M \to D^\times$ un revêtement fini. Alors il existe une surface de Riemann $\overline{M}$, une injection $i : M \hookrightarrow \overline{M}$ et un morphisme de surfaces de Riemann $\overline{\varphi} : \overline{M} \to D$ tel que la restriction $\overline{\varphi} : \overline{\varphi}^{-1}(D^\times) \to D^\times$ soit un revêtement équivalent (via i) à $\varphi : M \to D^\times$.*

Démonstration. — On peut supposer M connexe : sinon on travaille sur chaque composante connexe (proposition 7.3.7). Le revêtement $\varphi : C \to D^\times$ est alors un revêtement connexe, de degré fini d. Ce revêtement correspond à un sous groupe d'indice d du groupe fondamental $\pi_1(D^\times)$ (théorème 7.5.2). Ce groupe est isomorphe à $\mathbb{Z}$ (corollaire 7.2.16) et n'a donc qu'un seul sous-groupe d'indice d. La classe d'équivalence de revêtements correspondant à ce sous-groupe est celle du revêtement $m_d : D^\times \to D^\times$ donnée par $z \to z^d$. Ce revêtement se prolonge en un revêtement $D \to D$ par $m_d(0) = 0$. On pose $\overline{M} = D$; l'injection $M \hookrightarrow \overline{M}$ s'obtient en composant l'injection $D^\times \hookrightarrow D$ avec l'équivalence $\chi : M \to D^\times$ entre les revêtements φ et m_d. □

Remarque 8.2.3. — Le lemme 8.2.2 se généralise de façon évidente au cas d'un revêtement $\varphi : M \to B$ d'un espace B de la forme $B = \overline{B} \setminus \{t\}$ où $\overline{B}$ est homéomorphe à D *via* un homéomorphisme θ envoyant B sur $D^\times$. L'espace $\overline{B}$ étant muni de la structure de surface de Riemann de D, le résultat peut s'énoncer de la façon suivante.

Addendum 8.2.4. — *Pour chaque composante connexe C de M, il existe une surface de Riemann $\overline{C}$ contenant C et un morphisme de surfaces de Riemann $\overline{\varphi} : \overline{C} \to \overline{B}$ vérifiant*
(i) *$\overline{C} \setminus C$ consiste en un unique point m_C.*
(ii) *$\overline{\varphi}(m_C) = t$,*
(iii) *$\overline{C}$ est analytiquement isomorphe au disque D,*
(iv) *La restriction $\overline{\varphi} : \overline{\varphi}^{-1}(B) \to B$ coincide avec le revêtement $\varphi : C \to B$.*

[Le revêtement $\theta\circ\varphi : C \to D^\times$ est équivalent à un revêtement $m_d : D^\times \to D^\times$. Notons $\chi : C \to D^\times$ l'homéomorphisme correspondant (voir diagramme ci-dessous). On ajoute un point m_C à C et on note $\overline{C} = C \cup \{m_C\}$. On prolonge χ par $\chi(m_C) = 0$. On munit $\overline{C}$ de la structure de surface de Riemann obtenue par transport de celle de D par la bijection χ. L'application $\overline{\varphi} : \overline{C} \to \overline{B}$ est celle qui prolonge φ et envoie m_C sur t.]

$$\begin{array}{ccc} C & \xrightarrow{\chi} & D^\times \\ {\scriptstyle d}\big(\big\downarrow & & \big\downarrow{\scriptstyle m_d} \\ B & \xrightarrow{\theta} & D^\times \end{array}$$

8.2.3. Preuve du théorème 8.2.1. —

8.2.3.1. Existence. — Soit $f : X \to B$ un revêtement fini. Pour tout $i = 1, \ldots, r$, on choisit D_i un voisinage ouvert de t_i dans $\overline{B}$ homéomorphe au disque unité ouvert de $\mathbb{C}$ et tel que les ouverts $D_1, \ldots, D_r$ soient deux à deux disjoints. On pose $D_i^\times = D_i \setminus \{t_i\}$. Notons $\varphi_i : f^{-1}(D_i^\times) \to D_i^\times$ la restriction de f à $f^{-1}(D_i^\times)$, $i = 1, \ldots, r$. D'après le lemme 8.2.2, on peut ajouter un point m à chaque composante connexe C de $f^{-1}(D_i^\times)$ puis prolonger φ_i en ce point (par $\varphi_i(m) = t_i$) et obtenir de cette façon un morphisme de surface de Riemann $\overline{\varphi_C} : C \cup \{m\} \to D_i$, $i = 1, \ldots, r$.

Soit S l'ensemble total des points ajoutés à X de cette façon. C'est un ensemble fini : S a autant d'éléments qu'il y a de composantes connexes dans tous les espaces $f^{-1}(D_i^\times)$, $i = 1, \ldots, r$. Posons $\overline{X} = X \cup S$; $\overline{X}$ est une surface de Riemann qui contient X. Soit ensuite $\overline{f}$ l'application $\overline{X} \to B$ égale à f sur X et prolongeant chacune des applications $\overline{\varphi_C}$ ci-dessus, C décrivant l'ensemble des composantes connexes de $f^{-1}(D_i^\times)$, $i = 1, \ldots, r$. L'application $\overline{f}$ est définie [car $f = \overline{\varphi_C}$ là où elles sont toutes deux définies], prolonge f et est un morphisme de surfaces de Riemann [c'est une notion locale].

Il reste à voir que $\overline{X}$ est compact, en particulier séparé. Pour la séparation le seul problème est de voir qu'on peut séparer les points de M au-dessus d'un même point t_i, $i = 1, \ldots, r$. Mais deux points distincts dans la fibre $\overline{f}^{-1}(t_i)$ correspondent à deux points m et m' ajoutés à deux composantes connexes C et C' distinctes de $f^{-1}(D_i^\times)$. Par construction, les ouverts $C \cup \{m\}$ et $C' \cup \{m'\}$ sont des ouverts disjoints de $\overline{X}$.

Quant à la compacité, elle résulte de la propreté du morphisme $\overline{f}$. C'est-à-dire : l'image réciproque par $\overline{f}$ de tout compact de $\overline{B}$ est un compact de

$\overline{X}$. En particulier, $f^{-1}(\overline{B}) = \overline{X}$ est compact. Pour voir que $\overline{f}$ est propre, on remarque que c'est une propriété locale sur la base, c'est-à-dire : il suffit de montrer qu'il existe un recouvrement ouvert de $\overline{X}$ par des ouverts U tels que chacune des restrictions $\overline{f} : f^{-1}(U) \to U$ soit propre. Or cela résulte d'une part du fait qu'un revêtement (ici $X \to B$) est propre, d'autre part que les morphismes $m_d : D \to D$ $(z \to z^d)$ du lemme 8.2.2 sont également propres.

8.2.3.2. Unicité. — Soit $\overline{f'} : \overline{X'} :\to \overline{B}$ un deuxième morphisme de surfaces de Riemann tel que $\overline{f'} : \overline{f'}^{-1}(B) \to B$ soit un revêtement équivalent à $f : X \to B$. Les deux revêtements $\overline{f} : \overline{f}^{-1}(B) \to B$ et $\overline{f'} : \overline{f'}^{-1}(B) \to B$ sont donc équivalents, *via* un homéomorphisme χ qui est automatiquement un isomorphisme analytique. Le lemme 8.2.5 ci-dessous montre que χ se prolonge en un isomorphisme analytique $\overline{\chi} : \overline{X} \to \overline{X'}$.

Lemme 8.2.5. — *Soient $f : X \to B$ et $f' : X' \to B$ deux revêtements et $\overline{f} : \overline{X} \to \overline{B}$ et $\overline{f'} : \overline{X'} \to \overline{B}$ deux morphismes de surfaces de Riemann compactes prolongeant respectivement f et f'. Soit $\chi : X \to X'$ un morphisme entre les revêtements $f : X \to B$ et $f' : X' \to B$. Alors χ se prolonge de façon unique en un morphisme $\overline{\chi} : \overline{X} \to \overline{X'}$ de surfaces de Riemann tel que $\overline{f'} \circ \overline{\chi} = \overline{f}$.*

Démonstration. — L'unicité est claire (puisque χ est donnée sur une partie dense). Voyons l'existence. Pour chaque $i = 1, \ldots, r$, on choisit D_i un voisinage de t_i dans B homéomorphe au disque unité ouvert D et tel que les ouverts $D_1, \ldots, D_r$ soient deux à deux disjoints.

Pour chaque composante connexe C de $\overline{f}^{-1}(D_i \setminus \{t_i\})$, $i = 1, \ldots, r$, notons $\widetilde{C}$ l'ensemble C complété des points de la fibre $\overline{f}^{-1}(t_i)$ qui sont adhérents à C dans $\overline{X}$. La restriction $\overline{f} : \widetilde{C} \to D_i$ est un morphisme analytique ; d'autre part, c'est une application propre.

> [L'application $\overline{f} : \overline{X} \to \overline{B}$ est propre : l'image réciproque d'un compact est un fermé ($\overline{f}$ est continue) du compact $\overline{X}$. Déduisons en que la restriction $\overline{f} : \widetilde{C} \to D_i$ de $\overline{f}$ à $\widetilde{C}$ est également propre. Si K est un compact de D_i, son image réciproque par cette restriction est $\overline{f}^{-1}(K) \cap \widetilde{C}$. Montrons que c'est un fermé du compact $\overline{f}^{-1}(K)$. Soit $(x_n)_n$ une suite d'éléments de $\overline{f}^{-1}(K) \cap \widetilde{C}$ convergeant vers $x \in \overline{f}^{-1}(K)$. L'image $\overline{f}(x)$ de x est un élément de K ; en particulier $\overline{f}(x) \in D_i$. Si $x \in f^{-1}(D_i \setminus \{t_i\})$, alors $x \in C \subset \widetilde{C}$ (car C est fermé dans $f^{-1}(D_i \setminus \{t_i\})$). Le second cas est celui où $f(x) = t_i$. Alors, comme x est adhérent à C dans $\overline{X}$ (car les points de $\widetilde{C}$, en

particulier les x_n le sont), x fait partie des points ajoutés à C pour constituer $\widetilde{C}$.]

L'argument ci-dessous montre que, à isomorphisme analytique près, la restriction $\overline{f} : \widetilde{C} \to D_i$ est l'application $z \to z^d$ du disque unité D vers lui-même.

[Soit $\overline{m} : \overline{M} \to D$ un morphisme analytique de surfaces de Riemann connexes prolongeant l'application $D^\times \to D^\times$ donnée par $m_d(z) = z^d$. On suppose de plus que $\overline{m}$ est propre. Nécessairement $0 \in \overline{M}$: sinon l'image réciproque d'un disque fermé centré en 0 ne serait pas compacte. La restriction de $\overline{m}$ à $D = D^\times \cup \{0\}$ est donc l'application $z \to z^d$. De plus le point 0 est un zéro d'ordre d de $\overline{m}$. Supposons qu'il y ait un autre point m que 0 dans la fibre $\overline{m}^{-1}(0)$. Ce point serait forcément non isolé dans $\overline{M}$ (car $\overline{M}$ est connexe). D'après le théorème de l'image ouverte [**Rud78**, théorème 10.32], les points proches et distincts de 0 auraient strictement plus de d antécédents par $\overline{m}$.]

Cela entraîne en particulier que, pour toute composante connexe C de $\overline{f}^{-1}(D_i \setminus \{t_i\})$, le point t_i a un unique antécédent $m_C \in \overline{X}$ par $\overline{f}$ qui est adhérent à C, $i = 1, \ldots, r$. De même, pour toute composante connexe C' de $\overline{f'}^{-1}(D_i \setminus \{t_i\})$, le point t_i a un unique antécédent $m_{C'} \in \overline{X'}$ par $\overline{f'}$ qui est adhérent à C', $i = 1, \ldots, r$.

Si C est une composante connexe de $\overline{f}^{-1}(D_i \setminus \{t_i\})$, on note C^χ la composante connexe de $\overline{f'}^{-1}(D_i \setminus \{t_i\})$ contenant $\chi(C)$, $i = 1, \ldots, r$. On prolonge le morphisme χ en une application $\overline{\chi} : \overline{X} \to \overline{X'}$ en posant $\overline{\chi}(m_C) = m_{C^\chi}$ pour toute composante connexe C de $f^{-1}(D_i^\times)$, $i = 1, \ldots, r$. L'application $\overline{\chi}$ est clairement continue et satisfait $\overline{f'} \circ \overline{\chi} = \overline{f}$. Le théorème des singularités illusoires [c'est-à-dire : une fonction qui est bornée sur un disque et holomorphe sur le disque privé de son centre est holomorphe sur le disque tout entier [**Rud78**, théorème 10.20]] permet de conclure que $\overline{\chi}$ est un morphisme analytique. □

8.3. Algébrisation

8.3.1. Réciproque du théorème 8.2.1. — Le but de ce paragraphe est le théorème 8.3.3 qui constitue une réciproque du théorème 8.2.1. Si $f : \overline{X} \to \overline{B}$ est un morphisme non constant entre surfaces de Riemann connexes compactes, alors il existe un ensemble B tel que $\overline{B} \setminus B$ est fini et tel que la restriction $f : f^{-1}(B) \to B$ est un revêtement.

L'ensemble B au-dessus duquel le morphisme $f : \overline{X} \to \overline{B}$ induit un revêtement sera l'ensemble des points de $\overline{B}$ au-dessus desquels f n'est pas *ramifiée*. Ce résultat est vrai sans l'hypothèse de compacité, à condition que f soit supposée *propre* (voir théorème 8.3.1). L'hypothèse de compacité assure la propreté et entraîne que $\overline{B} \setminus B$ est fini.

Pour tout point $x_0 \in X$, on définit l'*indice de ramification* $e_{x_0}(f)$ de f en x de la façon suivante. On choisit une carte (U_α, f_α) en x_0 et une carte (V_β, g_β) en $f(x_0)$. Il existe une série entière $\varphi(z) = \sum_{n\geq 0} a_n(z - f_\alpha(x_0))^n$ convergeant dans $f_\alpha(U_\alpha)$ et telle que $\varphi(f_\alpha(x)) = g_\beta(f(x))$ pour tout $x \in U_\alpha$. L'entier $e_{x_0}(f)$ est défini comme l'ordre en $f_\alpha(x_0)$ de $\varphi(z) - a_0$, c'est-à-dire comme le premier indice $n > 0$ tel que $a_n \neq 0$. On vérifie facilement que cette définition ne dépend pas des cartes choisies. Un point x_0 est dit *ramifié* pour f si $e_{x_0}(f) > 1$ et non ramifié sinon. Un point t_0 est appelé *point de ramification* de f si la fibre $f^{-1}(t_0)$ contient au moins un point ramifié.

Théorème 8.3.1. — *Soient X et B deux surfaces de Riemann connexes et $f : X \to B$ un morphisme non ramifié, c'est-à-dire, $e_x(f) = 1$ pour tout $x \in X$. On suppose que de plus que f est propre, c'est-à-dire : l'image réciproque par f de tout compact est compact. Alors $f : X \to B$ est un revêtement fini.*

Le lemme 8.3.2 ci-dessous intervient dans la démonstration du théorème 8.3.1 et en d'autres endroits du chapitre.

Lemme 8.3.2. — *Soit $g : M \to N$ une application fermée. Soit $n \in N$ et $\{m_i|_i \in I\}$ la fibre de g au-dessus de n. Soient U un voisinage ouvert de n et $(V_i)_{i\in I}$ une famille d'ouverts de M tels que $m_i \in V_i$ et $g(V_i) \subset U$, pour tout $i \in I$. Alors il existe un voisinage ouvert U' de n tel que $g^{-1}(U') \subset \bigcup_{1\leq i\leq r} V_i$.*

Démonstration. — L'application g étant fermée, l'ensemble $g(M \setminus \bigcup_i V_i)$ est un fermé F' ne contenant pas n. L'ensemble $U' = U \setminus F'$ est donc un voisinage ouvert de n et par construction $g^{-1}(U') \subset \bigcup_i V_i$. □

Démonstration du théorème 8.3.1. — Le morphisme f étant non ramifié est un homéomorphisme local. Montrons que f est un revêtement. Soit $b \in B$. La fibre $f^{-1}(b)$ est un ensemble fini $\{x_1, \ldots, x_d\}$ car discret [ensemble des zéros de l'application holomorphe $f(x) - b$] et compact [car f est propre]. Comme f est un homéomorphisme local, il existe un voisinage ouvert U de b et pour chaque $i = 1, \ldots, d$, un voisinage ouvert V_i de x_i tel que f induise un homéomorphisme entre V_i et U et tel que les ouverts $V_1, \ldots, V_d$ soient disjoints. L'application f est aussi fermée (voir ci-dessous). D'après le lemme 8.3.2, il existe un voisinage ouvert $U' \subset U$ de b tel que $f^{-1}(U') \subset \bigcup_i V_i$. On conclut alors que $f^{-1}(U')$ est

la réunion disjointe des ouverts $V_i \cap f^{-1}(U')$ qui sont chacun homéomorphe à U' *via* f.

> [f est fermée : Soit $(x_n)_n$ une suite d'un fermé F de X ayant la propriété que $(f(x_n))_n$ tend vers $y \in B$. L'ensemble K constitué des termes de la suite $(f(x_n))_n$ et de sa limite y est un compact. Son image réciproque $f^{-1}(K)$ est un compact de X contenant les termes de la suite $(x_n)_n$. On peut donc extraire une sous-suite de $(x_n)_n$ convergeant vers un point $x \in F$ vérifiant $f(x) = y$.]

□

Théorème 8.3.3. — *Soient $\overline{X}$ et $\overline{B}$ deux surfaces de Riemann connexes compactes et $f : \overline{X} \to \overline{B}$ un morphisme non constant. Alors*

(a) *L'ensemble des points de ramification de f est un ensemble fini $D = \{t_1, \ldots, t_r\}$.*

(b) *Si $B = \overline{B} \setminus D$ et $X = f^{-1}(B)$, la restriction $\widetilde{f} : X \to B$ de f à $f^{-1}(B)$ est un revêtement fini (donc propre).*

(c) *Pour tout $t \in \overline{B}$, on a $\sum_{x|f(x)=t} e_x(f) = \deg(f)$.*

Remarque 8.3.4. — (a) On dit que f est un *revêtement ramifié* de degré $d = \deg(f)$. Toutes les fibres $f^{-1}(b)$ ont même nombre d'éléments, comptés avec multiplicité. Il résulte du (c) du théorème 8.3.3 qu'un point $b \in \overline{B}$ est un point de ramification de f si et seulement si la fibre $f^{-1}(b)$ a strictement moins de $d = \deg(f)$ éléments.

(b) En combinant les théorèmes 8.2.1, 8.3.1 et 8.3.3, on obtient que si $B = \overline{B} \setminus D$ est une surface de Riemann compacte connexe privée d'un ensemble fini D, alors tout morphisme non ramifié $f : X \to B$ de surfaces de Riemann connexes se prolonge en un morphisme $\overline{f} : \overline{X} \to \overline{B}$ de surfaces de Riemann connexes compactes si et seulement si f est propre.

(c) *Diviseur d'une fonction méromorphe.* Le théorème 8.3.3 s'applique notamment quand $\overline{B} = \mathbb{P}^1(\mathbb{C})$. Les morphismes $\overline{X} \to \mathbb{P}^1(\mathbb{C})$ correspondent à des fonctions méromorphes sur $\overline{X}$. On obtient que toute fonction méromorphe f sur une surface de Riemann connexe compacte $\overline{X}$ induit un revêtement fini de $\mathbb{P}^1(\mathbb{C})$ privé d'un nombre fini de points.

Il résulte du (c) du théorème 8.3.3 que f a autant de zéros que de pôles, comptés avec multiplicité. Si $x \in \overline{X}$, on note $\mathrm{ord}_x(f)$ l'ordre de f en x, qui est

défini par :

$$\mathrm{ord}_x(f) = \begin{cases} 0 \text{ si } f(x) \neq 0, \infty \\ e_x(f) \text{ si } f(x) = 0 \\ -e_x(f) \text{ si } f(x) = \infty \end{cases}$$

Que f ait autant de zéros que de pôles s'écrit alors

$$\sum_{x \in \overline{X}} \mathrm{ord}_x(f) = 0$$

On note aussi $\mathrm{div}(f)$ l'expression formelle

$$\sum_{x \in \overline{X}} \mathrm{ord}_x(f)\ (x)$$

qu'on appelle le *diviseur* de f. Plus généralement, on appelle diviseur de $\overline{X}$ tout élément du groupe abélien libre engendré par les éléments de $\overline{X}$, c'est-à-dire toute somme formelle $\sum_{x \in \overline{X}} n_x\ (x)$, où n_x est un entier, nul pour presque tout $x \in \overline{X}$. Il y a une notion de *degré* d'un diviseur : c'est la somme finie $\sum_{x \in \overline{X}} n_x$. D'après la formule plus haut, le diviseur d'une fonction méromorphe sur une surface de Riemann connexe compacte est un diviseur de degré nul.

Démonstration du théorème 8.3.3. — (a) Sur un ouvert U_α d'un atlas sur $\overline{X}$, un point de ramification correspond *via* des cartes à un zéro de la dérivée d'une fonction holomorphe. L'ensemble D est donc discret et par conséquent fini puisque $\overline{X}$ est compact.

(b) Comme $\overline{X}$ est compact, f est propre (car continue) [L'image réciproque d'un compact est un fermé dans un compact]. De manière immédiate, la restriction $\widetilde{f} : X \to B$ de f à $X = f^{-1}(B)$ est propre également. Par définition de B, $f : X \to B$ est un morphisme non ramifié. D'après le théorème 8.3.1, $f : X \to B$ est un revêtement fini.

(c) Pour tout $t \in \overline{B}$, notons $d(t)$ le terme de gauche dans la formule à établir. Si $t \in B$, on a évidemment $d(t) = \mathrm{card}(f^{-1}(t)) = \deg(\widetilde{f})$. Soit maintenant $t \in \overline{B}$ quelconque. Notons $x_1, \ldots, x_r$ les points de la fibre $f^{-1}(t)$. On peut trouver des ouverts disjoints $V_1, \ldots, V_r$ tels que $x_i \in V_i$, $i = 1, \ldots, r$. La fonction f est fermée (car f continue et $\overline{X}$ compact). D'après le lemme 8.3.2, il existe un voisinage ouvert U' de t tel que

$$f^{-1}(U') \subset \bigcup_i V_i$$

On peut aussi supposer les ouverts $V_1, \ldots, V_r$ suffisamment petits pour que, *via* des cartes, f corresponde, pour chaque indice $i = 1, \ldots, r$, à une fonction

holomorphe

$$\varphi_i(z) = a_{i,o} + \sum_{n \geq e_{x_i}(f)} a_{i,n} z^n \qquad (\text{avec } a_{i,e_{x_i}(f)} \neq 0)$$

sur un disque centré en 0. Tout élément $t' \in U'$ proche et distinct de t a exactement $e_{x_i}(f)$ antécédents dans V_i, $i = 1, \ldots, r$. Combiné à l'inclusion précédente, cela fournit

$$\deg(\widetilde{f}) = \mathrm{card}(f^{-1}(t)) = \sum_{i=1}^{r} e_{x_i}(f) = d(t)$$

□

8.3.2. Corps des fonctions méromorphes. — Soit $f : \overline{X} \to \overline{B}$ un morphisme non constant entre surfaces de Riemann connexes compactes, par exemple, le morphisme que le théorème 8.2.1 permet d'associer à tout revêtement $f : f^{-1}(B) \to B$ de $B = \overline{B} \setminus D$, où $D \subset \overline{B}$ est fini. Considérons le corps $M(\overline{X})$ (resp. $M(\overline{B})$) des fonctions méromorphes sur $\overline{X}$ (resp. sur $\overline{B}$). Notons $\widetilde{f} : X \to B$ le revêtement induit par f en dehors des points de ramification et d le degré de f, vu comme revêtement ramifié.

Soit $f^* : M(\overline{B}) \to M(\overline{X})$ l'application donnée par $f^*(\varphi) = \varphi \circ f$. L'application f^* est un homomorphisme de corps, forcément injectif.

Lemme 8.3.5. — *Le corps $M(\overline{X})$ est une extension finie du corps $f^*(M(\overline{B}))$ de degré $[M(\overline{X}) : f^*(M(\overline{B}))] \leq d$.*

Démonstration. — Il s'agit de montrer que pour toute fonction méromorphe $g \in M(\overline{X})$, l'extension $M(\overline{B})(g)/f^*(M(\overline{B}))$ est finie de degré $\leq d$.

> [Supposons cela démontré. Posons $\mathcal{M} = f^*(M(\overline{B}))$. Si on prend ensuite $g \in M(\overline{X})$ de degré maximal d_m sur $\mathcal{M}$, on aura $M(\overline{X}) = \mathcal{M}(g)$. En effet si $h \in M(\overline{X})$, d'après le théorème de l'élément primitif (théorème 1.3.10), on a $\mathcal{M}(g,h) = \mathcal{M}(g + \lambda h)$ sauf pour un nombre fini de $\lambda \in \mathbb{C}$. On a alors $[\mathcal{M}(g,h) : \mathcal{M}] = d_m$ et donc $\mathcal{M}(g,h) = \mathcal{M}(g)$, c'est-à-dire $h \in \mathcal{M}(g)$.]

Soit $g \in M(\overline{X})$. Quitte à remplacer g par $(ag + b)/cg + d)$ avec a, b, c, d convenablement choisis, on peut supposer que si $x \in \overline{X}$ est un point ramifié de f, alors $g(x) \neq \infty$.

> [L'ensemble des points ramifiés de f est fini. On choisit $z_0 \in \mathbb{C}$ distinct des valeurs de g en ces points, puis $a, b, c, d \in \mathbb{C}$ tel que $(az_0 + b)/(cz_0 + d) = \infty$.]

Soit U l'ouvert de B constitué des points $b \in \overline{B}$ tels que $g(x) \neq \infty$ pour tout $x \in f^{-1}(b)$. L'ouvert U contient tous les points de ramification de f. Considérons les d "fonctions symétriques élémentaires" définies sur U par

$$\sigma_1(b) = \sum_{x|f(x)=b} e_x(f)g(x), \qquad \dots \qquad , \sigma_d(b) = \prod_{x|f(x)=b} e_x(f)g(x)$$

Soit $U' \subset U$ l'ouvert de $\overline{B}$ constitué des points $b \in U$ tels que $e_x(f) = 1$ pour tout $x \in f^{-1}(b)$. La restriction de f à $f^{-1}(U')$ est un revêtement $f^{-1}(U') \to U'$. Au voisinage de b il existe d sections $s_1, \dots, s_d$ de f qui permettent de réécrire les fonctions $\sigma_1, \dots, \sigma_d$:

$$\sigma_1(b) = \sum_{i=1}^{d} (g \circ s_i)(b), \qquad \dots \qquad , \sigma_d(b) = \prod_{i=1}^{d} (g \circ s_i)$$

Les sections $s_1, \dots, s_d$ et la fonction g étant holomorphes, on obtient que les fonctions $\sigma_1, \dots, \sigma_d$ sont des fonctions de b holomorphes sur U'.

Montrons qu'elles sont méromorphes sur $\overline{B}$. Soit $b \in \overline{B} \setminus U'$. Il y a deux cas.

1er cas : $b \notin U$, c'est-à-dire : il existe des éléments $x \in f^{-1}(b)$ tels que $g(x) = \infty$. Dans ce cas, à cause de la réduction préalable, tous les points de la fibre $f^{-1}(b)$ sont non ramifiés pour f. Soit (V_β, g_β) une carte au voisinage de b telle que $g_\beta(b) = 0$. Alors $g_\beta \circ f$ s'annule en tous les points de $f^{-1}(b)$. La fonction g étant méromorphe, il existe un entier n tel que $(g_\beta \circ f)^m g$ soit holomorphe en chaque point de $f^{-1}(b)$. On en déduit que les fonctions

$$\sum_{i=1}^{d} (g_\beta \circ f \circ s_i)^m (g \circ s_i) = g_\beta^m \sigma_1, \qquad \dots \qquad , \prod_{i=1}^{d} (g_\beta \circ f \circ s_i)^{m^d} (g \circ s_i) = g_\beta^{m^d} \sigma_d$$

sont holomorphes en b (où $s_1, \dots, s_d$ sont d sections de f au voisinage de b).

2ème cas : $b \in U \setminus U'$, c'est-à-dire : il existe des points ramifiés dans la fibre $f^{-1}(b)$. Mais aucun point de $f^{-1}(b)$ n'est un pôle de g. On va montrer dans ce cas que les fonctions σ_i sont continues en b. Le théorème des singularités illusoires permettra de conclure qu'elles sont holomorphes en b.

Soit $(b_n)_{n>0}$ une suite de $\overline{B}$ convergeant vers b. Notons $\{x_1, \dots, x_r\}$ la fibre de f au-dessus de b. En utilisant le lemme 8.3.2, on peut trouver un voisinage ouvert U de b et une famille d'ouverts bornés $\overline{V_1}, \dots, \overline{V_r}$ de $\overline{X}$ tels que $\overline{V_i} \cap \overline{V_j} = \emptyset$ si $i \neq j$, tels que $x_i \in \overline{V_i}$, $i = 1, \dots, r$ et tels que $f^{-1}(U) \subset \bigcup_{1 \leq i \leq r} \overline{V_i}$. A partir d'un certain rang n_0, tous les termes b_n sont dans U. Pour tout indice $i = 1, \dots, r$, notons e_i l'indice de ramification de f en x_i. Ce nombre e_i est aussi le nombre d'éléments dans V_i de chaque fibre $f^{-1}(u)$ $(u \in U)$. Pour tout

$u \in U$, posons

$$\sigma_{i,1}(u) = \sum_{x \in V_i | f(x)=u} e_x(f) g(x), \qquad \ldots \qquad , \sigma_{i,e_i}(u) = \prod_{x \in V_i | f(x)=u} e_x(f) g(x)$$

Pour tout $i = 1, \ldots, r$ et tout $j = 1, \ldots, e_i$, la suite $(\sigma_{i,j}(b_n))_{n \geq n_0}$ converge vers $\sigma_{i,j}(b)$.

> [Cela résulte du fait suivant. Si pour chaque $n > 0$, on choisit $x_n \in V_i$ tel que $f(x_n) = b_n$, alors la suite $(x_n)_{n>0}$ converge vers x_i. Pour obtenir cela, on montre que x_i est la seule valeur d'adhérence possible ; comme $\overline{V_i}$ est compact, cela suffit.]

Cela entraîne que la suite $(\sigma_i(b_n))_n$ converge vers $\sigma_i(b)$, $i = 1, \ldots, d$.

Conclusion : on a montré que les fonctions $\sigma_1, \ldots, \sigma_d$ sont des fonctions méromorphes sur $\overline{B}$. D'autre part, on a :

$$g^d - f^*(\sigma_1) g^{d-1} + \ldots + (-1)^d f^*(\sigma_d) = 0$$

[C'est vrai sur U par construction.] Cela montre que g est algébrique sur $f^*(M(\overline{B}))$ de degré $\leq d$. □

Le lemme 8.3.5 est particulièrement intéressant dans le cas où $\overline{B} = \mathbb{P}^1(\mathbb{C})$. En effet, le corps $M(\mathbb{P}^1(\mathbb{C}))$ est le corps $\mathbb{C}(T)$ des fonctions rationnelles à coefficients dans $\mathbb{C}$.

Théorème 8.3.6. — (a) *Le corps $M(\mathbb{P}^1(\mathbb{C}))$ est isomorphe au corps $\mathbb{C}(T)$ des fonctions rationnelles à coefficients dans $\mathbb{C}$.*

(b) *Si $f : \overline{X} \to \mathbb{P}^1(\mathbb{C})$ est une fonction méromorphe non constante sur une surface de Riemann connexe compacte, l'homomorphisme de corps $f^* : M(\mathbb{P}^1) \hookrightarrow M(\overline{X})$ a pour image le sous-corps $\mathbb{C}(f)$ de $M(\overline{X})$.*

Démonstration. — Notons T la fonction $\mathbb{P}^1(\mathbb{C}) \to \mathbb{C}$ définie par $T(x : y) = x/y$ si $y \neq 0$. C'est une fonction méromorphe sur $\mathbb{P}^1(\mathbb{C})$: elle correspond au morphisme identité $\mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Montrons que $M(\mathbb{P}^1(\mathbb{C})) = \mathbb{C}(T)$.

Toute fonction rationnelle $\varphi(T) \in \mathbb{C}(T)$ est une fonction méromorphe sur $\mathbb{P}^1(\mathbb{C})$. De plus, si

$$\varphi(T) = \prod_{i=1}^{r} (T - a_i)^{m_i} \qquad (a_i \neq a_j \text{ si } i \neq j)$$

alors le diviseur de f est

$$\sum_{i=1}^{r} m_i \, (a_i) \; - \; \left(\sum_{i=1}^{r} m_i \right) (\infty)$$

Si $g \in M(\mathbb{P}^1(\mathbb{C}))$ est non constante, il est facile de construire une fonction rationnelle $\varphi(T) \in \mathbb{C}(T)$ de T telle que $g/\varphi(T)$ n'ait ni zéros ni pôles sur $\mathbb{P}^1(\mathbb{C})$, et donc soit une fonction holomorphe sur $\mathbb{P}^1(\mathbb{C})$. Le lemme 8.3.7 suivant permet de conclure que $g = \lambda\varphi(T)$ où $\lambda \in \mathbb{C}$. Ce qui achève la démonstration de (a). Le (b) provient du fait que l'homomorphisme f^* est défini par $f^*(\varphi) = \varphi \circ f$ pour tout $\varphi \in M(\mathbb{P}^1(\mathbb{C})$. L'image de f^* est le corps engendré sur $\mathbb{C}$ par $f^*(T) = T \circ f = \mathrm{Id} \circ f = f$. □

Lemme 8.3.7. — *Toute fonction holomorphe $f : \overline{X} \to \mathbb{C}$ sur une surface de Riemann connexe compacte est constante.*

Démonstration. — Si f était non constante, $f(\overline{X})$ serait un compact ouvert non vide. □

8.3.3. Correspondance entre revêtements et extensions de corps. — Soit f un fonction méromorphe sur une surface de Riemann connexe compacte $\overline{X}$. D'après le lemme 8.3.5 , l'extension $M(\overline{X})/\mathbb{C}(f)$ est finie de degré inférieur au degré de f, vu comme revêtement ramifié de $\mathbb{P}^1$. Nous allons montrer qu'il y a en fait égalité de ces degrés. L'inégalité restant à démontrer repose sur un résultat profond de la théorie des surfaces de Riemann, à savoir l'existence de suffisamment de fonctions méromorphes sur une surface de Riemann. De façon précise, on a le résultat suivant que nous admettrons. Pour une démonstration, nous renvoyons à [**Rey89**] ou [**Völ96**].

Théorème 8.3.8. — *Soit $\overline{X}$ une surface de Riemann connexe et $x_1, \ldots, x_n$ des points distincts de $\overline{X}$. Alors il existe une fonction méromorphe $g \in M(\overline{X})$ telle que $g(x_i) \neq g(x_j)$ si $x_i \neq x_j$. Autrement dit, les fonctions méromorphes séparent les points.*

Corollaire 8.3.9. — *Le corps $M(\overline{X})$ des fonctions méromorphes sur une surface de Riemann compacte connexe est un corps de fonctions d'une variable sur $\mathbb{C}$, c'est-à-dire un corps de type fini et de degré de transcendance* 1 *sur $\mathbb{C}$.*

Démonstration. — D'après le théorème 8.3.8, il existe une fonction méromorphe f sur $\overline{X}$. D'après le lemme 8.3.5 et le théorème 8.3.6, le corps $M(\overline{X})$ est une extension finie de $\mathbb{C}(f)$ (qui est une extension transcendante pure de $\mathbb{C}$ de degré de transcendance 1). □

Remarque 8.3.10. — On n'a pas besoin du théorème 8.3.8 si la surface de Riemann $\overline{X}$ est donnée par un revêtement ramifié $f : \overline{X} \to \mathbb{P}^1$. En effet, dans

ce cas, on sait que $\overline{X}$ a au moins une fonction méromorphe non constante, à savoir f.

Théorème 8.3.11. — *Soit f une fonction méromorphe sur une surface de Riemann connexe compacte $\overline{X}$ et soit $\widetilde{f} : X \to B$ le revêtement induit par f en dehors des points de ramification.*

(a) *Le corps $M(\overline{X})$ des fonctions méromorphes sur $\overline{X}$ est une extension finie du corps $\mathbb{C}(f)$ de degré $[M(\overline{X}) : \mathbb{C}(f)] = \deg(\widetilde{f})$.*

(b) *Si le revêtement $\widetilde{f}$ est galoisien, l'extension $M(\overline{X})/\mathbb{C}(f)$ est galoisienne de groupe de Galois anti-isomorphe au groupe $\mathrm{Aut}(\widetilde{f})$ des automorphismes de $\widetilde{f}$.*

Démonstration. — (a) On sait déjà que $M(\overline{X})$ est une extension finie de $\mathbb{C}(f)$ de degré $\leq \deg(\widetilde{f})$ (lemme 8.3.5). Soit $t \in B$; la fibre $f^{-1}(t)$ comporte $d = \deg(\widetilde{f})$ éléments $x_1, \ldots, x_d$. D'après le théorème 8.3.8, il existe une fonction $g \in M(\overline{X})$ prenant des valeurs distinctes aux points $x_1, \ldots, x_d$. Si $P(T, Y) \in \mathbb{C}[T, Y]$ est un polynôme tel que $P(f, g) = 0$, ces valeurs $g(x_1), \ldots, g(x_d)$ sont des racines de $P(t, Y)$, d'où

$$d \leq \deg_Y(P) \leq [\mathbb{C}(f, g) : \mathbb{C}(f)] \leq [M(\overline{X}) : \mathbb{C}(f)]$$

(b) D'après le lemme 8.2.5, tout automorphisme $\chi \in \mathrm{Aut}(\widetilde{f})$ se prolonge de façon unique en un automorphisme analytique $\overline{X} \to \overline{X}$, noté encore χ pour simplifier, tel que $f \circ \chi = f$. Comme d'habitude, on note χ^* l'automorphisme de $M(\overline{X})$ défini par $\chi^*(g) = g \circ \chi$ pour tout $g \in M(\overline{X})$. Cet isomorphisme est un $\mathbb{C}(f)$-automorphisme, c'est-à-dire fixe les éléments de $\mathbb{C}(f)$. Le théorème 8.3.8 permet de voir que la correspondance $\chi \to \chi^*$ est injective.

> [Soit χ un automorphisme du revêtement, prolongé à $\overline{X}$. Si $\chi \neq \mathrm{Id}$, il existe $x \in \overline{X}$ tel que $\chi(x) \neq x$. Soit $f \in M(\overline{X})$ tel que $f(x) \neq f(\chi(x))$. Cela montre que $\chi^*(f) \neq f$.]

On en déduit que l'extension $M(\overline{X})/\mathbb{C}(f)$ a au moins $d = |\mathrm{Aut}(\widetilde{f})| = \deg(\widetilde{f})$ $\mathbb{C}(f)$-automorphismes. Mais comme $\deg(\widetilde{f}) = [M(\overline{X}) : \mathbb{C}(f)]$, cela entraîne que l'extension $M(\overline{X})/\mathbb{C}(f)$ est galoisienne de degré d. La correspondance $\chi \to \chi^*$ fournit un anti-isomorphisme entre $\mathrm{Aut}(\widetilde{f})$ et $\mathrm{Gal}(M(\overline{X})/\mathbb{C}(f)$. □

8.3.4. Problème inverse de la Théorie de Galois sur $\mathbb{C}(T)$. — On peut maintenant démontrer le résultat suivant énoncé au chapitre 2.

Théorème 2.4.1 — *Tout groupe fini G est le groupe de Galois d'une extension galoisienne de $\mathbb{C}(T)$.*

Démonstration. — Il suffit de combiner le théorème 7.7.8, le théorème 8.2.1 et le théorème 8.3.11. □

Plus généralement, grâce aux résultats du chapitre 7 et de ce chapitre, on obtient le théorème 2.4.2 que nous avions appelé "forme pratique du théorème d'existence de Riemann" au chapitre 2, que nous recopions ci-dessous.

Théorème 2.4.2 — *Supposons donnés un groupe fini G et un entier $r > 0$ et r points distincts $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$. Alors il existe une correspondance bijective entre*
- l'ensemble des extensions de corps $E/\mathbb{C}(T)$ galoisiennes de groupe G non ramifiées en dehors de $t_1, \ldots, t_r$, modulo les $\mathbb{C}(T)$-isomorphismes, et
- l'ensemble des r-uplets $(g_1, \ldots, g_r) \in G^r$ tels que $\langle g_1, \ldots, g_r \rangle = G$ et $g_1 \cdots g_r = 1$, modulo la conjugaison (composante par composante) par des éléments de G.

8.3.5. Courbes algébriques. — Soit $P(T, Y) \in \mathbb{C}[T, Y]$ un polynôme. On note $C_P : P(t, y) = 0$ la courbe algébrique associée. Rappelons aussi les notations suivantes introduites dans le chapitre 7 (exemple 7.3.3) : $(\mathbb{A}^1)^*(\mathbb{C})$ désigne l'ensemble des nombres $t \in \mathbb{C}$ qui ne sont pas racines du discriminant $\Delta(T)$ de $P(T, Y)$ relativement à Y et $C_P^*(\mathbb{C})$ le sous-ensemble de $C_P(\mathbb{C})$ des points complexes (t, y) de la courbe $C_P : P(t, y) = 0$ tels que $t \in (\mathbb{A}^1)^*(\mathbb{C})$. Réintroduisons aussi le corps $\mathbb{C}(C_P)$ des fonctions de la courbe C_P :

$$\mathbb{C}(C_P) = \mathrm{Frac}\left(\frac{\mathbb{C}[T, Y]}{(P(T, Y))}\right)$$

C'est une extension de degré $\deg_Y(P)$ du corps $\mathbb{C}(T)$.

Le résultat suivant contient en particulier quelques résultats relatifs aux courbes algébriques évoqués au cours des chapitres précédents comme la connexité de la courbe $C_P(\mathbb{C})$ (voir proposition 8.1.4). La démonstration que nous donnons n'utilise pas le théorème 8.3.8.

Par contre, elle utilise les paragraphes §3.3.3 et §3.3.4 sur le modèle projectif lisse d'une courbe. On sait d'après ces paragraphes qu'il existe une courbe projective lisse irréductible $\overline{C_P}$ sur $\mathbb{C}$ munie d'un morphisme $T : \overline{C_P} \to \mathbb{P}^1$ vérifiant les propriétés suivantes. La courbe affine $C_P^*(\mathbb{C})$ se plonge dans $\overline{C_P}(\mathbb{C})$ et la différence $\overline{C_P}(\mathbb{C}) \setminus C_P^*(\mathbb{C})$ est un ensemble fini ; en particulier, C_P^*, C_P et $\overline{C_P}$ sont birationnels, leur corps de fonctions est $\mathbb{C}(C_P)$.

La courbe complexe $\overline{C_P}(\mathbb{C})$ est une surface de Riemann compacte (corollaire 8.1.5). Les éléments de $\mathbb{C}(C_P)$ induisent des fonctions méromorphes sur $\overline{C_P}(\mathbb{C})$.

Théorème 8.3.12. — *Soit $P(T,Y)$ un polynôme irréductible dans $\mathbb{C}[T,Y]$ tel que $\deg_Y(P) > 0$.*

(a) *Si F est un sous-ensemble fini quelconque de $C_P(\mathbb{C})$ et $X = C_P(\mathbb{C}) \setminus F$, alors X est un espace topologique connexe. C'est une surface de Riemann connexe si X est contenu dans l'ensemble $C_P^{\mathrm{reg}}(\mathbb{C})$ des points réguliers de C.*

(b) *La surface de Riemann $\overline{C_P}(\mathbb{C})$ est connexe. De plus, le corps $M(\overline{C_P}(\mathbb{C}))$ est $\mathbb{C}(T)$-isomorphe au corps $\mathbb{C}(C_P)$.*

(c) *Le revêtement $p_T : C_P^*(\mathbb{C}) \to (\mathbb{A}^1)^*(\mathbb{C})$ est galoisien si et seulement si l'extension $\mathbb{C}(C_P)/\mathbb{C}(T)$ est galoisienne. Dans ce cas, le groupe d'automorphismes du revêtement est (anti-)isomorphe au groupe de Galois de l'extension $\mathbb{C}(C_P)/\mathbb{C}(T)$. De façon plus générale, les groupes $\mathrm{Aut}(p_T)$ et $\mathrm{Aut}(\mathbb{C}(C_P)/\mathbb{C}(T))$ sont (anti-)isomorphes.*

Démonstration. — Notons B' l'ensemble $p_T(X) \cap (\mathbb{A}^1)^*(\mathbb{C})$ obtenu en retirant à l'ensemble $p_T(X(\mathbb{C}))$ les nombres complexes $t \in \mathbb{C}$ qui sont racine du discriminant $\Delta(T)$ de $P(T,Y)$ relativement à Y. Posons $X' = p_T^{-1}(B'(\mathbb{C}))$. Nous allons montrer que $X'(\mathbb{C})$ est connexe. Cela entraînera que $X(\mathbb{C})$ et $\overline{C_P}(\mathbb{C})$ sont connexes : en effet, $X'(\mathbb{C})$ est dense dans chacun des deux espaces $X(\mathbb{C})$ et $\overline{C_P}(\mathbb{C})$ puisqu'on passe du premier aux seconds en ajoutant un nombre fini de points, qui ne sont pas isolés. En effet, ces points ne sont pas isolés sur $\overline{C_P}(\mathbb{C})$ car $\overline{C_P}(\mathbb{C})$ est une surface de Riemann et ils ne sont pas isolés sur $X(\mathbb{C})$ en vertu du lemme 8.3.13 qui suit cette démonstration.

La première projection p_T induit un revêtement $p_T : X'(\mathbb{C}) \to B'(\mathbb{C})$. Soit $\mathcal{C}$ une composante connexe de $X'(\mathbb{C})$ et soit $\overline{\mathcal{C}}$ l'adhérence de $\mathcal{C}$ dans $\overline{C_P}(\mathbb{C})$; $\overline{\mathcal{C}}$ est une surface de Riemann compacte connexe. La restriction $T|_{\overline{\mathcal{C}}}$ de la fonction T (vue comme fonction méromorphe sur $\overline{C_P}(\mathbb{C})$) à $\overline{\mathcal{C}}$ est une fonction méromorphe et non constante (car induite par p_T qui est non constante sur $\mathcal{C}$; $p_T : \mathcal{C} \to B'(\mathbb{C})$ est même surjective (proposition 7.3.7)). D'après le lemme 8.3.5 et le théorème 8.3.6, on a

$$[M(\overline{\mathcal{C}}) : \mathbb{C}(T|_{\overline{\mathcal{C}}})] \leq \deg(p_T|_{\mathcal{C}}) \leq \deg(p_T) = \deg_Y(P)$$

D'un autre côté, les éléments de $\mathbb{C}(C_P)$ induisent des fonctions méromorphes sur $\overline{C_P}(\mathbb{C})$ et aussi sur $\overline{\mathcal{C}}$. D'où l'inclusion $\mathbb{C}(C_P) \subset M(\overline{\mathcal{C}})$ qui entraîne

$$[M(\overline{\mathcal{C}}) : \mathbb{C}(T|_{\overline{\mathcal{C}}})] \geq [\mathbb{C}(C_P)|_{\overline{\mathcal{C}}} : \mathbb{C}(T|_{\overline{\mathcal{C}}})] = [\mathbb{C}(C_P) : \mathbb{C}(T)] = \deg_Y(P)$$

[L'égalité $[\mathbb{C}(C_P)|_{\overline{\mathcal{C}}} : \mathbb{C}(T|_{\overline{\mathcal{C}}})] = [\mathbb{C}(C_P) : \mathbb{C}(T)]$] ci-dessus provient du fait que la restriction $\mathbb{C}(C_P) \to \mathbb{C}(C_P)|_{\overline{\mathcal{C}}}$ (où $\mathbb{C}(C_P)|_{\overline{\mathcal{C}}}$ doit être vu à l'intérieur de $M(\overline{\mathcal{C}})$) est un isomorphisme de corps :

cette application est surjective par construction et injective comme morphisme de corps.

On obtient

$$[M(\overline{\mathcal{C}}) : \mathbb{C}(T)] = \deg_Y(P) = \deg(p_T) = \deg(p_T|_{\mathcal{C}})$$

Conclusions :

• $\deg(p_T) = \deg(p_T|_{\mathcal{C}})$ donne que $\mathcal{C} = X'(\mathbb{C})$ est connexe (proposition 7.3.7). Dans $\overline{C_P}(\mathbb{C})$ on a donc $\overline{\mathcal{C}} = \overline{X'(\mathbb{C})} = \overline{C_P}(\mathbb{C})$,

• $[M(\overline{C_P}(\mathbb{C})) : \mathbb{C}(T)] = \deg_Y(P)$, joint à $M(\overline{C_P}(\mathbb{C})) \supset \mathbb{C}(C_P)$, fournit ensuite $M(\overline{C_P}(\mathbb{C})) = \mathbb{C}(C_P)$.

Cela termine la démonstration de (a) et (b).

(c) Dans le sens "⇒", on peut invoquer le théorème 8.3.11 combiné avec l'égalité $M(\overline{C_P}(\mathbb{C})) = \mathbb{C}(C_P)$. Mais cela utilise le théorème 8.3.8. L'argument suivant donne l'ensemble de l'énoncé (c) sans recourir au théorème 8.3.8.

Tout élément $\chi \in \mathrm{Aut}(\mathbb{C}(C_P)/\mathbb{C}(T))$ induit un automorphisme du revêtement algébrique $T : \overline{C_P} \to \mathbb{P}^1$ (c'est-à-dire un isomorphisme algébrique $\chi : \overline{C_P} \to \overline{C_P}$ tel que $T \circ \chi = T$). La restriction de cet automorphisme à $C_P^*(\mathbb{C})$ est un automorphisme $\widetilde{\chi}$ du revêtement $p_T : C_P^*(\mathbb{C}) \to (\mathbb{A}^1)^*(\mathbb{C})$. La correspondance

$$\begin{cases} \mathrm{Aut}(\mathbb{C}(C_P)/\mathbb{C}(T)) & \to & \mathrm{Aut}(p_T) \\ \chi & \to & \widetilde{\chi} \end{cases}$$

est injective.

Inversement, tout élément $\chi \in \mathrm{Aut}(p_T)$ induit un automorphisme analytique $\overline{\chi}$ de $\overline{C_P}(\mathbb{C})$ (lemme 8.2.5). Considérons l'homomorphisme

$$\begin{cases} \mathrm{Aut}(p_T)) & \to & M(\overline{C_P}(\mathbb{C}))/\mathbb{C}(T) (\simeq \mathrm{Aut}(\mathbb{C}(C_P)/\mathbb{C}(T))) \\ \chi & \to & \chi^* : g \to g \circ \overline{\chi} \end{cases}$$

L'argument ci-dessous montre que cet homomorphisme est injectif.

> [Soit $\chi \neq 1 \in \mathrm{Aut}(p_T)$. Il existe $x \in \overline{C_P}(\mathbb{C})$ tel que $\overline{\chi}(x) \neq x$. En fait, $\chi(x) \neq x$ pour tout $x \in C_P^*(\mathbb{C})$ (l'action de $\mathrm{Aut}(p_T)$ est libre). On choisit x de telle façon qu'on connaisse une fonction $\overline{g} \in M(\overline{C_P}(\mathbb{C}))$ qui sépare les points de $f^{-1}(f(x))$. Cela est plus facile que dans le théorème 8.3.11 où on avait dû invoquer le théorème 8.3.8 : on peut prendre pour $\overline{g}$ la projection p_Y sur la variable Y et alors tous les éléments $x \in C_P^*(\mathbb{C})$ conviennent sauf un nombre fini. Pour les x bien choisis, on a $\overline{g}(x) \neq \overline{g}(\chi(x))$, d'où $\chi^*(\overline{g}) \neq \overline{g}$.]

Les précédents arguments montrent que $\mathrm{Aut}(p_T)$ et $\mathrm{Aut}(\mathbb{C}(C_P)/\mathbb{C}(T))$ sont deux groupes (anti-)isomorphes. Le reste de l'énoncé (c) en découle. □

Lemme 8.3.13. — *Si $P(T,Y) \in \mathbb{C}[T,Y]$ est un polynôme, l'ensemble $C(\mathbb{C})$ des points complexes de la courbe $C : P(t,y) = 0$ n'a pas de points isolés.*

Démonstration. — Soit $(t_0, y_0) \in \mathbb{C}^2$ un point tel que $P(t_0, y_0) = 0$. S'il s'agit d'un point non singulier, on peut appliquer le théorème implicites : *via* une des deux projections, la courbe est au voisinage de (t_0, y_0) homéomorphe à un disque ouvert. Le cas d'un point (t_0, y_0) singulier est plus difficile. Le raisonnement ci-dessous explique comment se ramener au cas non singulier.

On peut supposer que $(t_0, y_0) = (0, 0)$ et que le polynôme $P(T, Y)$ est irréductible dans $\mathbb{C}[T, Y]$. On peut supposer que $P(0, Y) \neq 0$: sinon $P(T, Y) = aT$ et $(0, 0)$ est non singulier. Supposons donc $P(0, Y) \neq 0$. Soit e l'ordre de multiplicité de $P(0, Y)$ en 0.

Notons $D = \mathbb{C} \setminus (\mathbb{R}^- \setminus \{0\}$ et $u^{1/e}$ la détermination principale de la racine e-ième sur D. Posons ensuite $Q(t, u) = P(t, u^{1/e})$. On a

$$\begin{aligned} \frac{\partial Q}{\partial u}(0,u) &= \frac{d}{du}(P(0,u^{1/e})) \\ &= \frac{\partial P}{\partial Y}(0,u^{1/e}).\frac{u^{\frac{1-e}{e}}}{e} \end{aligned}$$

Par définition de e, $(\partial P/\partial Y)(0, Y)$ a un zéro d'ordre $e - 1$ en 0. On obtient

$$\frac{\partial Q}{\partial u}(0,u) = q(u^{1/e})$$

où q est un polynôme non nul en 0. On peut appliquer le théorème des fonctions implicites à l'équation $Q(t, u) = 0$. L'ensemble de ses solutions est, au voisinage de $(0, 0)$, homéomorphe, *via* la projection sur t, à un disque. En particulier, le point $(0, 0)$ n'est pas isolé sur la courbe $Q(t, u) = 0$. Cela entraîne que le point $(0, 0)$ n'est pas isolé sur la courbe $P(t, y) = 0$ [si (t, u) est un zéro de $Q(t, u) = 0$ proche de $(0, 0)$, alors $(t, u^{1/e})$ est un zéro de $P(t, y) = 0$ proche de $(0, 0)$]. □

8.4. La descente de $\mathbb{C}$ à $\overline{\mathbb{Q}}$

8.5. Espaces de modules de Hurwitz

8.6. Applications arithmétiques

BIBLIOGRAPHIE

[AM69] M. F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, Mass., 1969.

[Ami75] Yvette Amice. *Les nombres p-adiques*. Collection SUP. P.U.F., 1975.

[CF67] J W. S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, London and New York, 1967.

[CG82] A. L. Chistov and D. Yu. Grigoryev. Polynomial-time factoring of the multivariable polynomials over a global field. *LOMI preprint E-5-82*, 1982.

[CH85] Kevin Coombes and David Harbater. Hurwitz families and arithmetic galois groups. *Duke Math. J.*, 52 :821–839, 1985.

[CZ98] Pietro Corvaja and Umberto Zannier. Values of rational functions on non-hilbertian fields and a question of weissauer. *Isr. J. Math.*, 105 :323–335, 1998.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers : field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30 :303–338, 1997.

[DD04] Pierre Dèbes and Bruno Deschamps. Corps ψ-libres et théorie inverse de Galois infinie. *J. Reine Angew. Math.*, 574 :197–218, 2004.

[Dèb01] Pierre Dèbes. Théorème d'irréductibilité de Hilbert. *cours DEA université Lille*, 2000/01. math.univ-lille1.fr/ pde/.

[Dèb86a] Pierre Dèbes. G-fonctions et théorème d'irréductibilité de Hilbert. *Acta Arith.*, 47(4) :371–402, 1986.

[Dèb86b] Pierre Dèbes. Parties hilbertiennes et progressions géométriques. *C. R. Acad. Sci. Paris Sér. I Math.*, 302(3) :87–90, 1986.

[Dèb87] Pierre Dèbes. Résultats récents liés au théorème d'irréductibilité de Hilbert. In *Sém. Th. Nombres, Paris, 1985-86*, pages 19–37. Birkhauser, 1987.

[Dèb92] Pierre Dèbes. On the irreducibility of the polynomials $p(t^m, y)$. *J. Number Theory*, 42(2) :141–157, 1992.

[Dèb96] Pierre Dèbes. Hilbert subsets and s-integral points. *Manuscripta Mathematica*, 89 :107–137, 1996.

[Dèb99a] Pierre Dèbes. Arithmétique et espaces de modules de revêtements. In *Number Theory in Progress*, Proceedings of the Number Theory conference in Zakopane (K. Gyory, H. Iwaniec and J. Urbanowicz ed.), pages 75–102. Walter de Gruyter, 1999.

[Dèb99b] Pierre Dèbes. Density results for Hilbert subsets. *Indian J. Pure and Applied Math.*, 30(1) :109–127, 1999.

[Dèb99c] Pierre Dèbes. Regular realization of abelian groups with controlled ramification. In *Applications of Curves over Finite Fields*, volume 245 of *Contemporary Math.*, pages 109–115. AMS, 1999.

[Dèb01] Pierre Dèbes. Théorie inverse de Galois et géométrie - une introduction. In *Arithmétique des revêtements algébriques*, volume 5 of *Séminaires et Congrès*, pages 1–26. SMF, 2001.

[Del74] Pierre Deligne. La conjecture de Weil I. *Publ. Math. IHES*, 43 :273–308, 1974.

[Del80] Pierre Deligne. La conjecture de Weil II. *Publ. Math. IHES*, 52 :137–252, 1980.

[Des01] Bruno Deschamps. Corps pythagoriciens, fermatiens et p-réduisants. *J. Number Theory*, 88(1) :114–128, 2001.

[DF99] Pierre Dèbes and Michael D. Fried. 'integral specialization of families of rational functions. *Pacific J. Math.*, 190(1) :45–85, 1999.

[DG09] Pierre Dèbes and Nour Ghazi. Galois covers over number fields and the Hilbert-Grunwald problem. *preprint*, 2009.

[DH99] Pierre Dèbes and Dan Haran. Almost hilbertian fields. *Acta Arith.*, 88/3(4) :269–287, 1999.

[DW08] Pierre Dèbes and Yann Walkowiak. Bounds for Hilbert's irreducibility theorem. *Pure & Applied Math. Quarterly*, 4(4) :1059–1083, 2008.

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988)1989*, volume 91 of *Progress in Mathematics*, pages 241–248. Birkhäuser, 1990.

[FD90] Michael D. Fried and Pierre Dèbes. Rigidity and real residue class fields. *Acta Arith.*, 56(4) :291–323, 1990.

[FJ88] Michael D. Fried and Moshe Jarden. On σ-hilbertian fields. *Pacific J. Math.*, 185(2) :307–313, 1988.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. first edition 1986.

[Fri74] Michael D. Fried. On Hilbert's irreducibility theorem. *J. Number Theory*, 6 :211–231, 1974.

[Fri99] Michael D. Fried. Variables separated polynomials and moduli spaces. In *Number Theory in Progress*, Proceedings of the Number Theory conference in Zakopane (K. Gyory, H. Iwaniec and J. Urbanowicz ed.), page 169228. Walter de Gruyter, 1999.

[FV92] Michael D. Fried and Helmut Völklein. The embedding problem over a Hilbertian PAC-field. *Ann. of Math. (2)*, 135(3) :469–481, 1992.

[God71] Claude Godbillon. *Eléments de Topologie Algébrique*. Collection Méthodes. Hermann, Paris, 1971.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New-York, 1977.

[Hur91] A. Hurwitz. Über Riemann'sche Flächen mit gegebenen Verzweigunspunkten. *Math. Ann.*, 39 :1–61, 1891.

[KN71] W. Krull and J. Neukirch. Die Struktur der absoluten galoisgruppe über dem Körper $\mathbf{r}(\mathrm{t})$. *Math. Ann.*, 193 :197–209, 1971.

[Lan78] Serge Lang. *Algebra*. World Student Series. Addison-Wesley, 1978.

[Lan83] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, New-York, 1983.

[Len83] A. K. Lenstra. Factoring polynomials over algebraic number fields. In *Proc. Conf. Math. Foundations of Computer Science*, volume 176 of *Lecture Notes in Computer Science*, pages 389–396. 1983.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261 :515–534, 1982.

[LW54] Serge Lang and André Weil. Number of points on varieties in finite fields. *Amer. J. Math.*, 76 :819–827, 1954.

[MÖ2] Peter Müller. Finiteness results for hilbert's irreducibility theorem. *Ann. Inst. Fourier*, 52(4) :983–1015, 2002.

[Mah62] Kurt Mahler. On some inequalities for polynomials in several variables. *J. London Math. Soc.*, 37 :341–344, 1962.

[Mal70] Bernard Malgrange. Sur les points singuliers des équations différentielles linéaires. *Enseign. Math.*, 20 :147–176, 1970.

[Mal79] Marie-Paule Malliavin. *Algèbre commutative*. poly cours. Paris 6, 1979.

[Mor90] Yasuo Morita. A note on hilbert's irreducibility theorem. *Proc. Japan. Acad. Ser. A*, 66, 1990.

[Neu79] Jürgen Neukirch. On solvable number fileds. *Invent. Math.*, 53 :135–164, 1979.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren de mathematischen Wissenschaften*. Springer, 2008.

[Rey89] Eric Reyssat. *Quelques aspects des surfaces de Riemann*. Birkhauser, 1989.

[Rud78] Walter Rudin. *Analyse réelle et complexe*. Masson, 1978.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres*. Collection Méthodes. Hermann, Paris, 1967.

[Sch76] Wolfgang M. Schmidt. *Equations over finite fields*. Springer-Verlag, 1976.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University, 2000.

[Ser62] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1962.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. research Notes in Mathematics. Jones and Bartlett, Boston, London, 1992.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997.

[Sil86] Joe Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[Spr83] Vladimir G. Sprindzuk. Arithmetic specializations in polynomials. *J. Reine Angew. Math.*, 340 :26–52, 1983.

[SZ95] Andrzej Schinzel and Umberto Zannier. The least admissible value of the parameter in Hilbert's irreducibility theorem. *Acta Arith.*, 69(3) :293–302, 1995.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.

[Wal05] Yann Walkowiak. Théorème d'irréductibilité de Hilbert effectif,. *Acta Arith.*, 116(3) :343–362, 2005.