

CORPS LOCAUX ET APPLICATIONS

Cours accéléré de DEA

Alain Kraus

Université de Paris VI

Septembre 2000

Table des matières

Introduction	1
Chapitre I. Anneaux de valuation discrète	3
I. Généralités	3
II. Exemples	6
III. Caractérisations des anneaux de valuation discrète	8
IV. L'anneau local d'une courbe algébrique en un point lisse	13
V. L'anneau \mathbb{Z}_p	15
Chapitre II. Anneaux de Dedekind	19
I. Définition et exemples	19
II. Le groupe des classes d'idéaux d'un anneau de Dedekind	21
III. La valuation discrète associée à un idéal maximal	25
IV. Théorème d'approximation	28
Chapitre III. Extensions et ramification	31
I. La forme Trace et l'homomorphisme Norme	31
II. Anneaux de Dedekind et extensions	35
III. Ramification	37
IV. Cas des extensions galoisiennes	41
V. Substitution de Frobenius	45
Chapitre IV. Discriminant et ramification	47
I. Discriminant	47
II. Quelques propriétés de $\delta_{B/A}$	48
III. Lien avec la ramification	50
IV. Exemples	52
Chapitre V. Corps valués et complétion	57
I. Valeur absolue	57
II. Le théorème d'Ostrowski	60
III. Valuation	62
IV. Topologie associée à une valeur absolue	65
V. Le complété d'un corps valué	67
VI. Développement de Hensel	75
VII. Caractérisation des corps valués localement compacts	76
Chapitre VI. Lemme de Hensel et applications	79
I. Première version du lemme de Hensel	79
II. Deuxième version du lemme de Hensel	81
III. Structure du groupe des unités	83

IV. Polynômes d'Eisenstein	85
V. Quelques applications au corps \mathbb{Q}_p	86
Chapitre VII. Extensions d'un corps valué complet	89
I. Théorème du prolongement	89
II. Cas où v est une valuation discrète	91
III. Extension et complétion	96
Chapitre VIII. Applications Diophantiennes	101
I. Énoncé des bornes de Weil sur les corps finis	101
II. Les quartiques de Fermat $x^4 + y^4 = cz^4$	102
III. L'équation de Fermat locale	105
IV. L'équation $x^2 + y^2 + z^2 = 0$	107
V. Loi de réciprocité quadratique	108
Appendice I. Espaces vectoriels topologiques et corps valués	111
Appendice II. Espaces de Baire	115
Appendice III. Corps des séries de Puiseux	119
Bibliographie	123

Introduction

Un corps complet pour une valuation discrète est parfois appelé, un corps *local*. Les extensions finies du corps \mathbb{Q}_p des nombres p -adiques, et du corps $K((T))$ des séries formelles à coefficients dans un corps K , sont des exemples de tels corps. L'objectif de ce cours est de présenter une introduction à la théorie des corps locaux. Sa lecture suppose connus le programme d'algèbre commutative enseigné en Maîtrise et, à certains endroits, la théorie de Galois classique des extensions finies de corps.

On abordera l'étude des anneaux de valuation discrète, des anneaux de Dedekind, de la ramification, des corps valués, de leurs complétions, et de leur comportement par passage aux extensions finies. Un chapitre est par ailleurs consacré au lemme de Hensel qui est, entre autres, un outil essentiel pour l'étude locale des équations Diophantiennes. Il se trouve à ce sujet quelques applications dans le dernier chapitre.

Bien entendu, il existe une quantité massive d'exposés dans la littérature traitant de ces questions et de leurs développements comme, par exemple, la théorie des corps de nombres ou la théorie du corps de classes, dont ce cours peut constituer un préliminaire. J'ai indiqué, dans les références bibliographiques, certains ouvrages présentant ces notions et dont la plupart m'ont été utiles à l'élaboration de ce polycopié. Pendant sa rédaction, j'ai bénéficié de conversations avec D. Bernardi, E. Halberstadt, M. Lazarus et P. Mazet. Je les en remercie vivement.

Chapitre I — Anneaux de valuation discrète

Dans toute la suite, un anneau, sans autre précision, sera toujours supposé commutatif et unitaire.

I. Généralités

Nous aurons à considérer dans ce chapitre l'ensemble $\mathbb{Z} \cup \{+\infty\}$ obtenu en adjoignant à \mathbb{Z} un élément noté $+\infty$. On le munit de la structure d'ensemble totalement ordonnée qui induit l'ordre usuel sur \mathbb{Z} et telle que $+\infty \geq n$ pour tout entier n . On prolonge par ailleurs la loi additive de \mathbb{Z} à cet ensemble, en posant $(+\infty) + n = n + (+\infty) = +\infty$ et $(+\infty) + (+\infty) = +\infty$. L'ensemble $\mathbb{Z} \cup \{+\infty\}$ est ainsi muni d'une structure de monoïde commutatif, dont la loi interne est compatible avec la relation d'ordre.

Considérons désormais un corps K .

Définition 1.1. Une valuation discrète définie sur K est une application surjective

$$v : K \rightarrow \mathbb{Z} \cup \{+\infty\},$$

de K sur $\mathbb{Z} \cup \{+\infty\}$, telle que pour tout élément x et y de K , l'on ait :

- a) $v(x) = +\infty$ si et seulement si $x = 0$;
- b) $v(xy) = v(x) + v(y)$;
- c) $v(x + y) \geq \inf(v(x), v(y))$.

La restriction de v à $K^* = K \setminus \{0\}$ est un homomorphisme de groupes surjectif de K^* sur \mathbb{Z} . D'après b), on a $v(1) = v(-1) = 0$, puis $v(x) = v(-x)$ pour tout $x \in K$, et si x est non nul, l'on a $v(x^{-1}) = -v(x)$.

Lemme 1.1. Soit $(x_i)_{1 \leq i \leq n}$ une famille d'éléments de K . On a

$$(1) \quad v\left(\sum_{i=1}^n x_i\right) \geq \inf_i(v(x_i)).$$

S'il existe un unique indice k tel que $v(x_k) = \inf_i(v(x_i))$, les deux membres de l'inégalité (1) sont égaux. En particulier, si x et y sont deux éléments de K tels que $v(x) \neq v(y)$, l'on a $v(x + y) = \inf(v(x), v(y))$.

Démonstration : L'inégalité (1) se déduit de c) par récurrence sur n . Soit k un indice comme indiqué dans l'énoncé. Posons $y = \sum_{i \neq k} x_i$ et $z = \sum x_i$. D'après (1), on a les inégalités $v(y) > v(x_k)$ et $v(z) \geq v(x_k)$. Supposons alors $v(z) > v(x_k)$; on a $x_k = z - y$. Il vient $v(x_k) \geq \inf(v(z), v(y)) > v(x_k)$, ce qui conduit à une contradiction. D'où le lemme.

Terminologie. Si x est dans K , on dit que $v(x)$ est la valuation de x . L'ensemble des éléments x de K tels que $v(x) \geq 0$ est un sous-anneau de K , qui est appelé l'anneau de valuation de v .

Définition 1.2. Soit A un anneau intègre de corps des fractions K . On dit que A est un anneau de valuation discrète, s'il existe une valuation discrète définie sur K , dont A soit l'anneau de valuation.

Énonçons les premières propriétés des anneaux de valuation discrète.

Lemme 1.2. Soit A un anneau de valuation discrète muni d'une valuation v . Un élément x de A est une unité de A (i.e. est inversible dans A) si et seulement si $v(x) = 0$.

Démonstration : Soit x un élément de A . Si x est une unité, il existe $y \in A$ tel que $xy = 1$. D'où $v(x) + v(y) = 0$, ce qui implique $v(x) = 0$ (car $v(x)$ et $v(y)$ sont positifs). Inversement, si $v(x) = 0$, x est non nul, et la valuation de l'inverse de x dans K , qui est $-v(x)$, est nulle. Donc x est inversible dans A . D'où le lemme.

Corollaire 1.1. Un corps n'est pas un anneau de valuation discrète.

Démonstration : Supposons qu'il existe un corps L qui soit un anneau de valuation discrète pour une valuation v . Puisque tout élément non nul de L est inversible, on a $v(x) = 0$ pour tout $x \neq 0$ (lemme 1.2), ce qui conduit à une contradiction, car v est surjective.

Proposition 1.1. Soit A un anneau de valuation discrète muni d'une valuation v .

- a) L'anneau A est local[†]. Son idéal maximal \mathfrak{M}_A est non nul. L'idéal \mathfrak{M}_A est le sous-ensemble de A formé des éléments x satisfaisant à l'inégalité $v(x) > 0$. On l'appelle l'idéal de valuation de v .
- b) Soit K le corps des fractions de A . Pour tout x dans K^* , l'un des éléments x ou x^{-1} appartient à A .
- c) L'anneau A est principal.
- d) Les idéaux non nuls de A sont les idéaux \mathfrak{M}_A^n , où n est un entier naturel.
- e) On a l'égalité

$$(2) \quad \bigcap_{n \geq 1} \mathfrak{M}_A^n = \{0\}.$$

Démonstration : a) : Cette assertion résulte directement du lemme 1.2 et de son corollaire, compte-tenu du fait que l'ensemble des éléments x de A tels que $v(x) > 0$ est un idéal de A .

b) : Pour tout $x \in K^*$, on a $v(x^{-1}) = -v(x)$, ce qui entraîne l'assertion.

c) : Soit I un idéal non nul de A . L'ensemble $v(I \setminus \{0\})$, qui est contenu dans \mathbb{N} , possède un plus petit élément k . Soit x un élément non nul de I tel que $v(x) = k$. Montrons que

[†] Rappelons qu'un anneau est dit local s'il possède un unique idéal maximal. Par exemple, un corps est un anneau local qui n'est pas un anneau de valuation discrète (cor. 1.1). En fait, un anneau est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal (cf. le fait qu'un élément non inversible d'un anneau appartient à un idéal maximal).

I est l'idéal principal engendré par x . Soit y un élément de I . On a $v(y) \geq v(x)$, donc y/x est de valuation positive, et il existe ainsi $t \in A$ tel que $y = tx$; d'où l'assertion.

d) : Soit I un idéal non nul de A . Soient a un générateur de I et π un générateur de \mathfrak{M}_A . Aux unités près, π est l'unique élément irréductible dans A (car dans un anneau principal un élément irréductible engendre un idéal maximal). Il existe donc un entier naturel n et une unité u de A tels que l'on ait $a = \pi^n u$. Cela prouve que I est contenu dans l'idéal de A engendré par π^n , qui n'est autre que \mathfrak{M}_A^n . Inversement, $\pi^n = au^{-1}$ appartient à I . D'où $I = \mathfrak{M}_A^n$.

e) : Soient I l'intersection des idéaux \mathfrak{M}_A^n ($n \geq 1$) et x un élément de I . Pour tout entier n , on a $v(x) \geq n$. Il en résulte que $v(x) = +\infty$, et donc $x = 0$. D'où l'égalité (2).

Terminologie. Soient A un anneau de valuation discrète et \mathfrak{M}_A son idéal de valuation. Un générateur de \mathfrak{M}_A s'appelle une uniformisante de A . Le corps A/\mathfrak{M}_A est le corps résiduel de A .

Lemme 1.3. Soit A un anneau de valuation discrète de corps des fractions K . Il existe une unique valuation discrète v sur K dont A soit l'anneau de valuation. Si \mathfrak{M}_A est l'unique idéal maximal de A , v est donnée sur A par l'égalité

$$(3) \quad v(x) = \text{Max} \left\{ n \geq 0 ; x \in \mathfrak{M}_A^n \right\} \quad (x \in A).$$

(On notera que la donnée de v sur A suffit à déterminer v sur K .)

Démonstration : Soient v et v' deux valuations discrètes sur K dont A est l'anneau de valuation. D'après la prop. 1.1, A est principal et possède un unique élément irréductible π , qui engendre \mathfrak{M}_A . Si x est un élément de K^* , il existe donc un entier relatif n et une unité u de A tels que l'on ait $x = \pi^n u$. Puisque v et v' sont des homomorphismes surjectifs de K^* sur \mathbb{Z} , on a nécessairement $v(\pi) = v'(\pi) = 1$, ce qui entraîne $v = v'$ (cf. lemme 1.2). Par ailleurs, l'égalité (3), prolongée convenablement à K , définit une valuation discrète sur K , dont l'anneau de valuation est A . En effet, si x est un élément non nul de A , il existe un plus grand entier n tel que x soit dans \mathfrak{M}_A^n (cf. l'égalité (2)), qui n'est autre que l'exposant de π dans la décomposition de x en produit d'éléments irréductibles (qui est ici une puissance de π). Les conditions de la définition 1.1 sont alors faciles à vérifier.

Lemme 1.4. Soit A un anneau. Pour que A soit un anneau de valuation discrète, il faut et il suffit qu'il soit principal et qu'il possède un unique idéal premier non nul.

Démonstration : Supposons que A soit principal et que A ait un unique idéal premier non nul \mathfrak{p} . Soit π un générateur de \mathfrak{p} . Puisqu'un élément irréductible de A engendre un idéal premier non nul, π est (aux unités près) l'unique élément irréductible de A . Soit K le corps des fractions de A . Pour tout $x \in K^*$, il existe un entier n et une unité u tels que l'on ait $x = \pi^n u$. L'entier n ne dépend pas du choix du générateur π . En posant

$v(x) = n$ et $v(0) = +\infty$, on définit ainsi une application $v : K \rightarrow \mathbb{Z} \cup \{+\infty\}$ qui est une valuation discrète sur K , dont A est l'anneau de valuation. L'implication inverse résulte de la prop. 1.1 (car les idéaux premiers non nuls d'un anneau principal sont maximaux). D'où le lemme.

II. Exemples

Nous allons donner dans ce paragraphe des exemples classiques d'anneaux de valuation discrète.

1) Localisé d'un anneau principal par rapport à un idéal premier non nul

Commençons par quelques rappels sur la localisation des anneaux intègres.

Localisation des anneaux intègres

Soient A un anneau intègre et S une partie multiplicative de A : S contient 1 et est stable pour la multiplication. Supposons que 0 ne soit pas dans S . On définit une relation d'équivalence sur l'ensemble $A \times S$ en convenant que deux couples (a, s) et (b, t) sont en relation si $at - bs = 0$ (A est intègre). On note a/s la classe d'équivalence de (a, s) , et $S^{-1}A$ l'ensemble de ces classes. Les égalités

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} \quad \text{et} \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'},$$

définissent une structure d'anneau sur $S^{-1}A$, et l'application $i_S : A \rightarrow S^{-1}A$, qui à a associe $a/1$, est un homomorphisme d'anneaux injectif. Cela permet d'identifier canoniquement A et son image dans $S^{-1}A$, ce que l'on fera dans la suite sans autre précision. Le couple $(S^{-1}A, i_S)$ possède la propriété universelle suivante : pour tout homomorphisme u de A dans un anneau B , tel que les éléments de $u(S)$ soient inversibles dans B , il existe un unique homomorphisme v de $S^{-1}A$ dans B tel que l'on ait $v \circ i_S = u$. En prenant pour S la partie multiplicative $A \setminus \{0\}$, on obtient le corps des fractions K de A . Pour toute partie multiplicative S , l'anneau $S^{-1}A$ est alors un sous-anneau de K dont le corps des fractions est K . L'application $\mathfrak{P} \mapsto \mathfrak{P} \cap A$ réalise une bijection de l'ensemble des idéaux premiers de $S^{-1}A$ sur l'ensemble des idéaux premiers de A disjoints de S . On notera qu'il n'en va pas de même en ce qui concerne les idéaux maximaux (l'idéal nul est un idéal maximal de \mathbb{Q} et pas de \mathbb{Z}).

Si \mathfrak{P} est un idéal premier de A , $S = A \setminus \mathfrak{P}$ est une partie multiplicative de A . L'anneau $S^{-1}A$ se note $A_{\mathfrak{P}}$: c'est le localisé de A en \mathfrak{P} . L'ensemble $\mathfrak{P}A_{\mathfrak{P}}$ des éléments de $A_{\mathfrak{P}}$ de la forme a/s où a est dans \mathfrak{P} est un idéal premier de $A_{\mathfrak{P}}$. Si b/t n'est pas dans $\mathfrak{P}A_{\mathfrak{P}}$, b n'est pas dans \mathfrak{P} , de sorte que b/t est inversible dans $A_{\mathfrak{P}}$. On déduit de là que $A_{\mathfrak{P}}$ est un anneau local d'idéal maximal $\mathfrak{P}A_{\mathfrak{P}}$. L'anneau quotient $A_{\mathfrak{P}}/\mathfrak{P}A_{\mathfrak{P}}$ est un corps isomorphe au corps des fractions de A/\mathfrak{P} , via l'application canonique (passée au quotient)

$$\frac{a}{s} \mapsto \frac{a + \mathfrak{P}}{s + \mathfrak{P}}.$$

Considérons alors un anneau principal A . Soient K son corps des fractions, et \mathfrak{P} un idéal premier non nul de A . Soient π un générateur de \mathfrak{P} et $v : K^* \rightarrow \mathbb{Z}$ l'application qui à un élément x de K^* , associe l'exposant de π (éventuellement négatif) dans la décomposition de x en produit d'éléments irréductibles de A . Cette application v définit une valuation discrète sur l'anneau K , dont l'anneau de valuation est $A_{\mathfrak{P}}$ et dont l'idéal de valuation est $\mathfrak{P}A_{\mathfrak{P}}$. Le corps résiduel est canoniquement isomorphe à A/\mathfrak{P} . Ainsi, $A_{\mathfrak{P}}$ est (par définition) un anneau de valuation discrète.

Tel est par exemple le cas du localisé de \mathbb{Z} en un nombre premier p , le corps résiduel étant alors isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

2) L'anneau des séries formelles en une variable sur un corps

Soit K un corps. Rappelons qu'une série entière formelle à coefficients dans K est la donnée d'une suite $(a_n)_{n \geq 0}$ d'éléments de K (un polynôme étant une suite dont tous les éléments sont nuls sauf un nombre fini d'entre eux). L'ensemble de ces suites est muni d'une structure d'anneau définie par les égalités :

$$(a_n) + (b_n) = (a_n + b_n) \quad \text{et} \quad (a_n) \cdot (b_n) = (c_n), \quad \text{où} \quad c_n = \sum_{i+j=n} a_i b_j.$$

On note souvent

$$X = (0, 1, 0, \dots, 0, \dots) \quad \text{et} \quad (a_n) = \sum_{n \geq 0} a_n X^n.$$

On obtient ainsi l'anneau $K[[X]]$ des séries entières formelles en l'indéterminée X à coefficients dans K . C'est un anneau intègre. Les éléments inversibles (a_n) sont ceux tels que a_0 soit non nul. Le complémentaire de ces éléments est l'idéal principal engendré par X . En particulier, $K[[X]]$ est un anneau local. Le corps des fractions de $K[[X]]$ est le corps $K((X))$ des séries formelles en la variable X sur K : un élément f de $K((X))$ s'écrit sous la forme

$$f = \sum_{n \in \mathbb{Z}} a_n X^n,$$

où il n'existe qu'un nombre fini d'entiers négatifs tels que a_n soit non nul. On définit l'ordre de f (ou la valuation de f) comme étant le plus petit entier relatif n_0 tel que a_{n_0} ne soit pas nul. On obtient ainsi une valuation discrète sur $K((X))$, dont l'anneau de valuation est $K[[X]]$, qui est ainsi un anneau de valuation discrète. L'idéal de valuation est l'idéal engendré par X et le corps résiduel est isomorphe à K .

3) L'anneau des germes de fonctions holomorphes en un point

Étant donné un point a du plan complexe, on définit ce que l'on appelle l'ensemble O_a des germes de fonctions holomorphes en a : soit A l'ensemble des fonctions holomorphes définies sur un voisinage de a . On munit cet ensemble de la relation d'équivalence consistant

à identifier deux éléments $f : U \rightarrow \mathbb{C}$ et $g : V \rightarrow \mathbb{C}$ de A , s'il existe un voisinage W de a contenu dans $U \cap V$ tel que f et g coïncident sur W . L'ensemble quotient ainsi obtenu est l'ensemble O_a . Il est naturellement muni d'une structure d'anneau, et est isomorphe au sous-anneau de $\mathbb{C}[[X]]$ formé des séries convergentes. L'ensemble O_a^* de ses éléments inversibles est constitué des éléments représentés par une fonction non nulle en a . Le complémentaire de O_a^* est donc l'idéal principal \mathfrak{M}_a engendré par la classe de la fonction $z \mapsto z - a$. Ainsi O_a est un anneau local d'idéal maximal \mathfrak{M}_a . C'est un anneau intègre dont le corps des fractions $\text{Frac}(O_a)$ est formé des classes de fonctions méromorphes définies au voisinage de a (il s'agit des classes d'équivalence de fonctions au sens précédent). On définit alors la valuation d'un élément f de $\text{Frac}(O_a)$ comme étant l'ordre du zéro de f en a . On obtient ainsi une valuation discrète sur $\text{Frac}(O_a)$ dont O_a est l'anneau de valuation. L'idéal de valuation est \mathfrak{M}_a et le corps résiduel est isomorphe à \mathbb{C} .

Cet exemple vaut, en remplaçant le plan complexe par n'importe quelle surface de Riemann S , compte-tenu du fait que n'importe quel point de S possède un voisinage homéomorphe à un ouvert de \mathbb{C} .

4) L'anneau local d'une courbe algébrique en un point lisse

Soit V un ensemble algébrique affine irréductible contenu dans \mathbb{C}^n . Soient I l'idéal de V et

$$A = \mathbb{C}[X_1, \dots, X_n]/I,$$

l'anneau de coordonnées de V . On l'appelle aussi l'anneau des fonctions régulières sur V . C'est un anneau canoniquement isomorphe à l'anneau des applications de V dans \mathbb{C} qui sont les restrictions à V d'une fonction polynôme sur \mathbb{C}^n . Puisque V est irréductible, I est un idéal premier, et A est un anneau intègre. Le corps des fractions K de A est le corps des fonctions de V .

Supposons que le degré de transcendance de K sur \mathbb{C} soit 1, autrement dit, que V soit une courbe algébrique affine. Soit P un point de V . Notons \mathfrak{M}_P l'idéal de A formé des fonctions régulières qui s'annulent en P . C'est un idéal maximal de A (A/\mathfrak{M}_P est isomorphe à \mathbb{C} via le morphisme d'évaluation en P). On définit l'anneau local O_P de V en P comme étant le localisé de A en l'idéal \mathfrak{M}_P (c'est l'anneau des fonctions régulières en P). C'est un anneau local noethérien intègre (le localisé d'un anneau noethérien est noethérien). Si P est un point lisse, on montre que $\mathfrak{M}_P O_P$ est un idéal principal, et dans ce cas O_P est un anneau de valuation discrète (cf. la prop. 1.2 ci-dessous). On reviendra sur ce point dans le paragraphe IV.

III. Caractérisations des anneaux de valuation discrète

Proposition 1.2. *Soit A un anneau. Alors, A est un anneau de valuation discrète si et seulement si A est un anneau local noethérien dont l'idéal maximal est engendré par un élément non nilpotent.*

Démonstration : Le fait qu'un anneau de valuation discrète vérifie les conditions de l'énoncé a déjà été démontré (cf. prop. 1.1). Inversement, soit \mathfrak{M} l'idéal maximal de A . Puisque A est local noethérien, on a l'égalité [†]

$$(4) \quad \bigcap_{n \geq 0} \mathfrak{M}^n = \{0\}.$$

Soit π un générateur de \mathfrak{M} . Si x un élément non nul de A , il existe d'après (4), un entier n tel que x soit dans \mathfrak{M}^n et pas dans \mathfrak{M}^{n+1} . Il existe donc une unité u de A tels que l'on ait $x = \pi^n u$. Puisque π n'est pas nilpotent, on déduit de là que A est intègre. En posant $n = v(x)$, on définit ainsi une application v de l'ensemble $A \setminus \{0\}$ à valeurs dans \mathbb{N} , qui se prolonge de façon naturelle au corps des fractions K de A à valeurs dans $\mathbb{Z} \cup \{+\infty\}$. On vérifie alors que v est une valuation discrète sur K . Par construction, A est l'anneau de valuation de v . D'où le résultat.

Théorème 1.1. *Soit A un anneau intègre noethérien. Alors, A est un anneau de valuation discrète si et seulement si les deux conditions suivantes sont réalisées :*

- a) *A est intégralement clos ^{††} ;*
- b) *A possède un unique idéal premier non nul.*

Démonstration : Si A est un anneau de valuation discrète, il est principal (prop. 1.1) et est donc intégralement clos. D'après *loc. cit.* il vérifie aussi la condition b).

Inversement, supposons que A vérifie les conditions a) et b), et montrons que c'est un anneau de valuation discrète. Soit K le corps des fractions de A . D'abord la condition b) entraîne que A est un anneau local dont l'idéal maximal \mathfrak{M} est non nul. D'après la prop. 1.2, il suffit alors de montrer que \mathfrak{M} est un idéal principal. Soit \mathfrak{M}' le sous- A -module de K défini par l'égalité

$$\mathfrak{M}' = \{x \in K ; x\mathfrak{M} \subseteq A\}.$$

Lemme 1.5. *Le A -module \mathfrak{M}' est noethérien ^{†††}.*

[†] Dans un anneau local noethérien, l'intersection des puissances de l'idéal maximal est réduite à $\{0\}$. C'est une conséquence du lemme d'Artin-Rees (cf. par exemple [Ma], p. 141-142).

^{††} Rappelons qu'un élément d'un anneau B contenant A est entier sur A s'il est racine d'un polynôme unitaire à coefficients dans A . On dit que A est intégralement fermé dans B si tout élément de B qui est entier sur A appartient à A . On dit que A est intégralement clos s'il est intègre et s'il est intégralement fermé dans son corps des fractions. Par exemple, si A est factoriel il est intégralement clos : soit $x \in K$ où K est le corps des fractions de A . On a une équation de dépendance intégrale $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$, où les a_i sont dans A . En écrivant x sous la forme a/b , avec a et b premiers entre eux, on constate que b divise a^n , ce qui entraîne que b est inversible dans A , et donc que x est dans A .

Exercice : montrer que si d est un entier relatif sans facteur carré, le sous-anneau de \mathbb{C} engendré par \mathbb{Z} et \sqrt{d} est intégralement clos si et seulement si l'on a $d \equiv 2$ ou $3 \pmod{4}$.

Démonstration : Soit y un élément non nul de \mathfrak{M} . Par définition, \mathfrak{M}' est un sous- A -module de $y^{-1}.A$. Or A étant noethérien, $y^{-1}.A$ est un A -module noethérien et donc \mathfrak{M}' aussi. D'où le lemme.

Soit $\mathfrak{M}.\mathfrak{M}'$ le produit des idéaux \mathfrak{M} et \mathfrak{M}' (c'est l'ensemble des éléments de K qui s'écrivent comme une somme finie $\sum x_i y_i$, où $x_i \in \mathfrak{M}$ et $y_i \in \mathfrak{M}'$). On a en fait

$$(5) \quad \mathfrak{M}.\mathfrak{M}' = \mathfrak{M} \quad \text{ou bien} \quad \mathfrak{M}.\mathfrak{M}' = A.$$

En effet, par définition $\mathfrak{M}.\mathfrak{M}'$ est contenu dans A et c'est un idéal de A . Par ailleurs, A étant contenu dans \mathfrak{M}' , l'idéal maximal \mathfrak{M} est contenu dans $\mathfrak{M}.\mathfrak{M}'$, ce qui entraîne (5). On va alors démontrer les trois assertions suivantes :

- I. Si $\mathfrak{M}.\mathfrak{M}' = A$, l'idéal \mathfrak{M} est principal.
- II. Si $\mathfrak{M}.\mathfrak{M}' = \mathfrak{M}$, on a $\mathfrak{M}' = A$ (c'est une conséquence de a)).
- III. On a $\mathfrak{M}' \neq A$ (c'est une conséquence de b)).

Elles impliquent le résultat : on déduit des assertions II et III et de l'égalité (5), que $\mathfrak{M}.\mathfrak{M}' = A$, et d'après I, \mathfrak{M} est donc principal.

Preuve de l'assertion I : il existe des éléments $x_i \in \mathfrak{M}$ et $y_i \in \mathfrak{M}'$ tels que l'on ait $\sum x_i y_i = 1$. Puisque pour tout j , $x_j y_j$ est dans A , il existe un indice i tel que $x_i y_i$ ne soit pas dans \mathfrak{M} . On montre alors que l'on a

$$(6) \quad \mathfrak{M} = x_i.A,$$

i.e. que \mathfrak{M} est engendré par x_i . En effet, l'anneau A étant local, $x_i y_i$ est un élément inversible u de A . On a ainsi l'égalité $(u^{-1} x_i) y_i = 1$. Si z est un élément de \mathfrak{M} , $y_i z$ est dans A , et l'on a $z = x_i u^{-1} (y_i z)$. D'où l'égalité (6) et l'assertion I.

Preuve de l'assertion II : on considère un élément x appartenant à \mathfrak{M}' . On va montrer que x est entier sur A , ce qui, puisque A est intégralement clos, entraînera que x est dans A . Par hypothèse, on a l'inclusion $x\mathfrak{M} \subseteq \mathfrak{M}$. Pour tout entier $n \geq 1$, $x^n \mathfrak{M}$ est donc contenu dans \mathfrak{M} , et en particulier x^n est dans \mathfrak{M}' . Soit I_n le sous- A -module de K engendré par $\{1, x, \dots, x^n\}$. Les I_n forment une suite croissante de sous-modules de \mathfrak{M}' . Elle est donc stationnaire (lemme 1.5) et il existe un entier n assez grand tel que x^n appartienne à I_{n-1} . On obtient ainsi une relation de dépendance intégrale $x^n = \sum b_i x^i$ à coefficients dans A , ce qui prouve que x est entier sur A . D'où l'assertion II.

††† Rappelons qu'un module M est dit noethérien si tous ses sous-modules sont de type fini, ou ce qui revient au même, si toute suite croissante de sous-modules de M est stationnaire. Un module de type fini sur un anneau noethérien est un module noethérien. Un sous-module d'un module noethérien est noethérien.

Preuve de l'assertion III : soit x un élément non nul de \mathfrak{M} . Soit S la partie multiplicative de A formée des puissances de x . Montrons d'abord que l'on a

$$(7) \quad S^{-1}A = K.$$

Supposons que $S^{-1}A$ soit strictement contenu dans K . Alors $S^{-1}A$ n'est pas un corps, et il existe donc un idéal maximal \mathfrak{p} non nul dans $S^{-1}A$. Puisque x est inversible dans $S^{-1}A$, x n'appartient pas à \mathfrak{p} , et en particulier on a

$$(8) \quad \mathfrak{p} \cap A \neq \mathfrak{M}.$$

Considérons par ailleurs, un élément $\alpha = y/x^n$ non nul de \mathfrak{p} . L'élément $y = x^n\alpha$ est non nul et est dans \mathfrak{p} , par conséquent $\mathfrak{p} \cap A$ est un idéal premier non nul de A . D'après la condition b), on a donc $\mathfrak{p} \cap A = \mathfrak{M}$, ce qui contredit (8) et prouve l'égalité (7).

Il s'agit maintenant de montrer l'existence d'un élément de \mathfrak{M}' qui ne soit pas dans A . Considérons pour cela un élément z non nul de \mathfrak{M} . D'après (7), il existe t dans A et un entier $m \geq 1$ tels que l'on ait $1/z = t/x^m$; on a $x^m = tz$. Ainsi, tout élément de \mathfrak{M} a une puissance qui appartient à l'idéal de A engendré par z . Soit $\{x_1, \dots, x_k\}$ une partie génératrice de \mathfrak{M} (\mathfrak{M} est de type fini car A est noethérien). Choisissons un entier $n \geq 1$ assez grand pour que x_i^n appartienne à zA pour tout i , et un entier N tel que $N > k(n-1)$. L'idéal \mathfrak{M}^N est contenu dans zA (\mathfrak{M}^N est engendré par les monômes en les x_i de degré total N et dans chacun de ces monômes intervient au moins un x_i^n). Il existe donc un plus petit entier $N_0 \geq 1$ tel que \mathfrak{M}^{N_0} soit contenu dans zA . Soit alors y un élément de \mathfrak{M}^{N_0-1} qui ne soit pas dans zA (par convention on pose $\mathfrak{M}^0 = A$). La partie $\mathfrak{M}y$ est donc contenue dans zA , et ainsi l'élément y/z appartient à \mathfrak{M}' . Or y/z n'est pas dans A (y n'est pas dans zA). D'où le fait que $\mathfrak{M}' \neq A$ et l'assertion I.

Cela termine la démonstration du théorème.

Énonçons maintenant des conditions nécessaires et suffisantes pour qu'un anneau local, noethérien, intègre, dont tous les idéaux premiers non nuls sont maximaux, soit un anneau de valuation discrète.

Proposition 1.3. *Soit A un anneau local noethérien intègre de dimension 1 [†]. Soient \mathfrak{M} l'idéal maximal de A et $k = A/\mathfrak{M}$ le corps résiduel. Les conditions suivantes sont équivalentes :*

- a) A est un anneau de valuation discrète ;
- b) A est intégralement clos ;
- c) l'idéal \mathfrak{M} est principal ;
- d) l'anneau quotient $\mathfrak{M}/\mathfrak{M}^2$ est un k -espace vectoriel de dimension 1 ;
- e) chaque idéal non nul de A est une puissance de \mathfrak{M} ;

f) il existe un élément π de A tel que tout idéal non nul de A soit de la forme $\pi^k A$, où k est un entier naturel.

Démonstration : L'équivalence a) \iff b) : si A est un anneau de valuation discrète, il est principal (prop. 1.1) et donc intégralement clos. Inversement, le fait que A soit local intègre et de dimension 1 entraîne que A possède un unique idéal premier non nul. D'après le th. 1.1, A est donc un anneau de valuation discrète.

L'équivalence a) \iff c) : elle résulte de la prop. 1.2.

L'équivalence c) \iff d) : supposons \mathfrak{M} principal. On a $\mathfrak{M} = xA$, où $x \in A$, et donc $x + \mathfrak{M}^2$ engendre le k -espace vectoriel $\mathfrak{M}/\mathfrak{M}^2$. L'assertion d) résulte alors du fait que \mathfrak{M} est distinct de \mathfrak{M}^2 (lemme 1.6 ci-dessous). Inversement, si la condition d) est vérifiée, le fait que \mathfrak{M} soit principal résulte du lemme de Nakayama $\dagger\dagger$.

L'implication a) \implies e) a été prouvée dans la prop. 1.1.

Prouvons e) \implies f). On a $\mathfrak{M} \neq \mathfrak{M}^2$ (lemme 1.6) : soit π un élément de $\mathfrak{M} \setminus \mathfrak{M}^2$. Il existe un entier $r \geq 1$ tel que $\pi A = \mathfrak{M}^r$ ($r \neq 0$ car $\pi \in \mathfrak{M}$). Nécessairement on a $r = 1$ et donc $\mathfrak{M} = \pi A$. Pour tout entier $k \geq 0$, on a donc $\mathfrak{M}^k = \pi^k A$. D'où f).

Par ailleurs, l'implication f) \implies c) est évidente. Pour obtenir la proposition 1.3, il reste donc à démontrer le lemme suivant :

Lemme 1.6. Soit A un anneau local noethérien de dimension 1. Soit I l'idéal maximal de A . Pour tout entier naturel n , on a $I^n \neq I^{n+1}$.

Démonstration : L'énoncé est vrai si $n = 0$. Supposons qu'il existe un entier $n \geq 1$ tel que $I^n = I^{n+1}$. Le lemme de Nakayama entraîne alors $I^n = 0$ (I^n est un A -module de type fini car A est noethérien). On déduit de là que I est le seul idéal premier de A (pour tout idéal premier \mathfrak{p} de A , on a l'inclusion I^n est contenu dans \mathfrak{p} , et donc $\mathfrak{p} = I$). Cela contredit le fait que A est de dimension 1. D'où le lemme.

On utilisera dans le prochain paragraphe le résultat suivant :

\dagger Un anneau A est dit de dimension 1 si la longueur maximale des chaînes strictement croissantes d'idéaux premiers de A est 1. Dans le cas où A est intègre, cela revient à demander que A ne soit pas un corps et que tous les idéaux premiers non nuls de A soient maximaux (un corps est de dimension 0). Par exemple, un anneau principal qui n'est pas un corps est de dimension 1.

Exercice : Soient I l'idéal de $\mathbb{C}[X, Y]$ engendré par $Y^2 - X^3 - 1$ et A l'anneau $\mathbb{C}[X, Y]/I$. Montrer que A est noethérien intègre de dimension 1 et n'est pas principal. Montrer que les localisés de A par rapport à ses idéaux maximaux sont des anneaux de valuation discrète.

$\dagger\dagger$ La version de ce lemme que l'on utilise ici est la suivante : soient A un anneau local d'idéal maximal I et M un A -module de type fini. Soit $(x_i + IM)_{1 \leq i \leq n}$ une A/I -base de M/IM . Alors, le système $(x_i)_{1 \leq i \leq n}$ engendre M (en particulier, si $M = IM$ alors $M = 0$).

Proposition 1.4. *Soit A un anneau local noethérien intègre. Soient \mathfrak{M} l'idéal maximal de A et $k = A/\mathfrak{M}$ le corps résiduel. Si le k -espace vectoriel $\mathfrak{M}/\mathfrak{M}^2$ est de dimension 1, A est un anneau de valuation discrète. Les uniformisantes de A sont les éléments de \mathfrak{M} qui ne sont pas dans \mathfrak{M}^2 .*

Démonstration : D'après le lemme de Nakayama, \mathfrak{M} est un idéal principal, et A est donc un anneau de valuation discrète (prop. 1.2). Il résulte aussi de ce lemme qu'un élément de \mathfrak{M} qui n'est pas dans \mathfrak{M}^2 est une uniformisante de A . Par ailleurs, une uniformisante de A n'appartient pas à \mathfrak{M}^2 , car d'après l'hypothèse faite, \mathfrak{M} et \mathfrak{M}^2 sont distincts. D'où le résultat.

IV. L'anneau local d'une courbe algébrique en un point lisse

On reprend les notations de l'alinéa 4) du paragraphe II. On part d'une courbe algébrique affine V irréductible plongée dans \mathbb{C}^n (i.e. un fermé algébrique irréductible contenu dans \mathbb{C}^n , de dimension 1). Soient I l'idéal de V dans $\mathbb{C}[X_1, \dots, X_n]$ et $(f_i)_{1 \leq i \leq t}$ un système générateur de I . On va utiliser les résultats prouvés dans le paragraphe précédent pour démontrer l'énoncé suivant :

Théorème 1.2. *Soit P un point lisse de V . L'anneau local de V en P est un anneau de valuation discrète.*

Rappelons d'abord la définition d'un point lisse de V :

Définition 1.3. *Soit P un point de V . On dit que P est un point lisse de V (ou que V est lisse en P), si le rang de la matrice dont l'élément de la i -ème ligne et de la j -ième colonne est (pour $1 \leq i \leq t$ et $1 \leq j \leq n$)*

$$\frac{\partial f_i}{\partial x_j}(P),$$

est égal à $n - 1$. Cette matrice est appelée la matrice Jacobienne de V en P . On dit que V est lisse si tous ses points le sont.

Considérons désormais un point lisse P de V . Soient A l'anneau de coordonnées de V , \mathfrak{M}_P l'idéal de A formé des fonctions nulles en P . Le A -module $\mathfrak{M}_P/\mathfrak{M}_P^2$ est naturellement muni d'une structure d'espace vectoriel de dimension finie sur $A/\mathfrak{M}_P = \mathbb{C}$ (A étant noethérien, \mathfrak{M}_P est de type fini, et les images d'un système générateur de \mathfrak{M}_P dans $\mathfrak{M}_P/\mathfrak{M}_P^2$ engendrent $\mathfrak{M}_P/\mathfrak{M}_P^2$ comme \mathbb{C} -espace vectoriel). Nous allons montrer l'énoncé suivant :

Proposition 1.5. *Le \mathbb{C} -espace vectoriel $\mathfrak{M}_P/\mathfrak{M}_P^2$ est de dimension 1.*

Démonstration : Posons $P = (a_1, \dots, a_n) \in \mathbb{C}^n$. Soit I_P l'idéal maximal de $\mathbb{C}[X_1, \dots, X_n]$ engendré par les $X_i - a_i$, pour i entre 1 et n . On considère l'application

$$\theta : \mathbb{C}[X_1, \dots, X_n] \rightarrow \mathbb{C}^n,$$

définie, pour tout F dans $\mathbb{C}[X_1, \dots, X_n]$, par l'égalité

$$\theta(F) = \left(\frac{\partial F}{\partial X_1}(P), \dots, \frac{\partial F}{\partial X_n}(P) \right).$$

L'application θ est \mathbb{C} -linéaire et le système $(\theta(X_i - a_i))_{1 \leq i \leq n}$ est la base canonique de \mathbb{C}^n . La restriction θ' de θ à I_P est donc une surjection de I_P sur \mathbb{C}^n , dont le noyau est l'idéal I_P^2 (cf. la formule de Taylor [†]). Par conséquent, θ' réalise un isomorphisme \mathbb{C} -linéaire de I_P/I_P^2 sur \mathbb{C}^n . Puisque I est contenu dans I_P , on déduit de là que les \mathbb{C} -espaces vectoriels $\theta(I)$ et $(I + I_P^2)/I_P^2$ sont isomorphes.

Par ailleurs, I étant engendré par les polynômes f_i , $\theta(I)$ est engendré comme \mathbb{C} -espace vectoriel par les $\theta(f_i)$, pour i compris entre 1 et n . En effet, si $(g_i)_{1 \leq i \leq t}$ est une famille de polynômes de $\mathbb{C}[X_1, \dots, X_n]$, l'on a

$$\theta\left(\sum_{i=1}^t g_i f_i\right) = \sum_{i=1}^t g_i(P) \theta(f_i).$$

On déduit de là que la dimension sur \mathbb{C} de $\theta(I)$ est le rang de la matrice Jacobienne en P , i.e. est $n - 1$ puisque P est lisse.

Cela étant, on a $\mathfrak{M}_P = I_P/I$, $\mathfrak{M}_P^2 = (I_P^2 + I)/I$, et donc les \mathbb{C} -espaces vectoriels $\mathfrak{M}_P/\mathfrak{M}_P^2$ et $I_P/(I_P^2 + I)$ sont isomorphes. Or $I_P/(I_P^2 + I)$ est (canoniquement) \mathbb{C} -isomorphe à $I_P/I_P^2/(I_P^2 + I)/I_P^2$. La dimension sur \mathbb{C} de $\mathfrak{M}_P/\mathfrak{M}_P^2$ est donc $n - (n - 1) = 1$. D'où le résultat.

Terminons la démonstration du théorème : soit O_P l'anneau local de V en P . Il est noethérien intègre (le localisé d'un anneau noethérien est noethérien). L'idéal maximal de O_P est $\mathfrak{M}_P O_P$. Par ailleurs, les \mathbb{C} -espaces vectoriels $\mathfrak{M}_P O_P/(\mathfrak{M}_P O_P)^2$ et $\mathfrak{M}_P/\mathfrak{M}_P^2$ sont canoniquement isomorphes ^{††}. Les propositions 1.4 et 1.5 entraînent alors le théorème.

Exemple. Soit V le fermé algébrique affine de \mathbb{C}^2 dont l'idéal dans $\mathbb{C}[X, Y]$ est engendré par $Y^2 - X^3 - X$. Il s'agit d'une courbe plane irréductible et lisse (s'en convaincre).

[†] Rappelons que si $F \in \mathbb{C}[X_1, \dots, X_n]$ et $P = (a_1, \dots, a_n) \in \mathbb{C}^n$, l'on a

$$F = \sum_{k \in \mathbb{N}} \sum_{i_1 + \dots + i_n = k} \frac{1}{i_1! \dots i_n!} (X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n} \frac{\partial^k}{\partial X_1^{i_1} \dots \partial X_n^{i_n}} F(P).$$

^{††} On utilise le fait que si \mathfrak{M} un idéal maximal d'un anneau A , les A/\mathfrak{M} -espaces vectoriels $\mathfrak{M}/\mathfrak{M}^2$ et $\mathfrak{M}A_{\mathfrak{M}}/\mathfrak{M}^2 A_{\mathfrak{M}}$ sont isomorphes, via l'application qui à $x + \mathfrak{M}^2$ associe $x/1 + \mathfrak{M}^2 A_{\mathfrak{M}}$.

Posons $P = (0, 0)$. L'anneau local O_P est un anneau de valuation discrète. Une uniformisante est donnée par un générateur de $\mathfrak{M}_P O_P$, autrement dit par un élément qui est dans $\mathfrak{M}_P O_P$ mais pas dans $(\mathfrak{M}_P O_P)^2$. Explicitons un tel générateur. Notons pour cela x et y les deux fonctions coordonnées de V , ainsi que leurs images dans O_P . On a alors $\mathfrak{M}_P O_P = (x, y)$. De l'égalité $y^2 = x^3 + x$ il résulte que x appartient à $(\mathfrak{M}_P O_P)^2$. Cela entraîne que $y + (\mathfrak{M}_P O_P)^2$ est une base de $\mathfrak{M}_P O_P / (\mathfrak{M}_P O_P)^2$ et donc que y est un générateur de $\mathfrak{M}_P O_P$ (cf. par exemple le lemme de Nakayama).

Cet exemple se généralise comme suit :

Proposition 1.6. *Soit V une courbe algébrique plane irréductible et lisse. Soient P un point de V et L une droite de \mathbb{C}^2 passant par P , qui n'est pas tangente à V en P [†]. Alors, l'image de L dans O_P est une uniformisante de O_P .*

Démonstration : Quitte à effectuer un changement de coordonnées affines, on peut supposer que P est le point de coordonnées $(0, 0)$, que la tangente à V en P est la droite d'équation $Y = 0$ et que L est la droite d'équation $X = 0$. Notons x et y les fonctions coordonnées sur V ainsi que leurs images dans O_P . Tout revient à montrer que l'idéal maximal de O_P , que l'on notera ici \mathfrak{M}_P , est engendré par x . On a $\mathfrak{M}_P = (x, y)$. Par ailleurs, compte-tenu des hypothèses faites, si $F \in \mathbb{C}[X, Y]$ est un générateur de l'idéal de V , on peut écrire F sous la forme $F = YG + X^2H$ tels que $G - 1$ appartienne à l'idéal (X, Y) et que H soit dans $\mathbb{C}[X]$. Si g et h désignent les images de G et H dans O_P , on a ainsi $yg = -x^2h$ et $g(P) \neq 0$. Puisque g est inversible dans O_P , cela montre que y appartient à l'idéal de O_P engendré par x , et donc que $\mathfrak{M}_P = (x)$. D'où le résultat.

Terminons ce chapitre en donnant un exemple typique d'anneau de valuation discrète, l'anneau des entiers p -adiques.

V. L'anneau \mathbb{Z}_p

Soit p un nombre premier. Nous allons construire l'anneau \mathbb{Z}_p des entiers p -adiques. Pour tout entier $n \geq 1$, posons

$$A_n = \mathbb{Z}/p^n\mathbb{Z}.$$

Pour $n \geq 2$, notons $\varphi_n : A_n \rightarrow A_{n-1}$ l'application qui à $x + p^n\mathbb{Z}$ associe $x + p^{n-1}\mathbb{Z}$. C'est un homomorphisme d'anneaux surjectif. Le noyau de φ_n est $p^{n-1}A_n$.

[†] Rappelons qu'une droite de \mathbb{C}^2 est une courbe de degré 1, autrement dit, une courbe dont l'idéal est engendré par un polynôme de la forme $aX + bY + c$. Par ailleurs, si V est une courbe plane dont l'idéal est engendré par $F \in \mathbb{C}[X, Y]$, et si $P = (u, v)$ est un point lisse de V , la tangente à V en P est la droite d'équation

$$(\partial F / \partial X)(P)(X - u) + (\partial F / \partial Y)(P)(Y - v) = 0.$$

Par définition, un entier p -adique est un élément $(\dots, x_n, x_{n-1}, \dots, x_1)$ de l'anneau produit

$$A = \prod_{n \geq 1} A_n,$$

tel que, pour tout entier $n \geq 2$, l'on ait

$$(9) \quad x_n \in A_n \quad \text{et} \quad \varphi_n(x_n) = x_{n-1}.$$

On note \mathbb{Z}_p l'ensemble des entiers p -adiques. On définit l'addition et la multiplication dans \mathbb{Z}_p par les égalités

$$(10) \quad (x_n) + (y_n) = (x_n + y_n) \quad \text{et} \quad (x_n)(y_n) = (x_n y_n).$$

L'ensemble \mathbb{Z}_p est ainsi muni d'une structure d'anneau commutatif unitaire de caractéristique 0, qui est en fait un sous-anneau de A . L'anneau \mathbb{Z} se plonge diagonalement dans \mathbb{Z}_p et c'est le seul homomorphisme d'anneaux unitaires de \mathbb{Z} dans \mathbb{Z}_p . Cela permet d'identifier \mathbb{Z} à un sous-anneau de \mathbb{Z}_p . On dispose d'un homomorphisme d'anneaux

$$\pi_n : \mathbb{Z}_p \rightarrow A_n,$$

qui à $(x_n)_{n \geq 1} \in \mathbb{Z}_p$ associe sa n -ième composante x_n . On a $\pi_{n-1} = \varphi_n \circ \pi_n$. Par ailleurs, π_n est surjectif : cela résulte du fait que les applications φ_k sont surjectives, et que la donnée de $x_n \in A_n$ détermine les x_k pour k compris entre 1 et $n-1$.

Démontrons maintenant que \mathbb{Z}_p est un anneau de valuation discrète.

Lemme 1.7. *Le noyau de π_n est $p^n \mathbb{Z}_p$. En particulier, l'application π_n , passée au quotient, réalise un isomorphisme d'anneaux de $\mathbb{Z}_p / p^n \mathbb{Z}_p$ sur A_n .*

Démonstration : D'abord, il est immédiat que le noyau de π_n contient $p^n \mathbb{Z}_p$. Inversement, considérons un élément $x = (x_n)_{n \geq 1}$ dans \mathbb{Z}_p tel que $\pi_n(x) = 0$ (on a alors $x = (\dots, x_{n+1}, 0, \dots, 0)$). Choisissons, pour tout entier $k \geq 1$, un représentant a_k dans \mathbb{Z} de x_{n+k} . Montrons que pour tout $k \geq 1$, l'on a

$$(11) \quad a_k \equiv 0 \pmod{p^n}.$$

Cette congruence est vraie si $k = 1$: on a les égalités $\varphi_{n+1}(x_{n+1}) = a_1 + p^n \mathbb{Z} = x_n = 0$, i.e. p^n divise a_1 . Soit alors k un entier ≥ 2 . On a $\varphi_{n+k}(x_{n+k}) = x_{n+k-1}$, autrement dit, on a $a_k + p^{n+k-1} \mathbb{Z} = a_{k-1} + p^{n+k-1} \mathbb{Z}$. Donc si a_{k-1} est divisible par p^n , il en est de même de a_k . D'où la congruence (11). Posons alors $a_k = p^n b_k$. Pour tout $k \geq 1$, on a $b_{k+1} \equiv b_k \pmod{p^k \mathbb{Z}}$, par conséquent la suite $y = (b_k + p^k \mathbb{Z})$ est un élément de \mathbb{Z}_p . On a l'égalité $x = p^n y$. En effet, on a $p^n y = (\dots, p^n(b_1 + p^{n+1} \mathbb{Z}), 0, \dots, 0) = (\dots, a_1 + p^{n+1} \mathbb{Z}, 0, \dots, 0) = x$. D'où le lemme.

Lemme 1.8. Soit $x = (\dots, x_{n+1}, x_n, \dots, x_1)$ un élément de \mathbb{Z}_p . Les conditions suivantes sont équivalentes :

- a) x est inversible dans \mathbb{Z}_p ;
- b) on a $x_1 \neq 0$;
- c) x n'est pas divisible par p .

Démonstration : a) \implies b) : si x est inversible dans \mathbb{Z}_p , pour tout $n \geq 1$, x_n est inversible dans A_n , donc x_1 n'est pas nul.

b) \implies c) : cette implication est immédiate.

c) \implies a) : Si x n'est pas divisible par p , il existe un entier n tel que p ne divise pas x_n . Pour tout entier $k \geq n$, cela entraîne que p ne divise pas x_k (car $\varphi_{k+1}(x_{k+1}) = x_k$), autrement dit, que x_k est inversible dans A_k . Par ailleurs, les images de x_n dans les A_k pour $k < n$ sont aussi inversibles. On déduit de là que x est inversible et le résultat.

On dit qu'un élément inversible de \mathbb{Z}_p est une unité p -adique. On notera U le groupe des unités p -adiques.

Lemme 1.9. Tout élément non nul de \mathbb{Z}_p s'écrit de manière unique sous la forme $p^n u$, où n est un entier naturel et où u appartient à U .

Démonstration : Soit x un élément non nul de \mathbb{Z}_p . Par définition, il existe un plus grand entier $n \geq 1$ tel que $\pi_n(x)$ soit nul. D'après le lemme 1.7, x appartient donc à $p^n \mathbb{Z}_p$ et pas à $p^{n+1} \mathbb{Z}_p$. D'après le lemme 1.8, il existe donc une unité p -adique u telle que l'on ait $x = p^n u$. On vérifie ensuite qu'une telle écriture est unique.

On notera que cette démonstration prouve que l'on a

$$(12) \quad \bigcap_{n \geq 0} p^n \mathbb{Z}_p = \{0\}.$$

Il résulte immédiatement du lemme 1.9 que :

Corollaire 1.2. L'anneau \mathbb{Z}_p est intègre.

On note \mathbb{Q}_p le corps des fractions de \mathbb{Z}_p . C'est le corps des nombres p -adiques. On déduit du lemme 1.9 une application

$$v : \mathbb{Z}_p \rightarrow \mathbb{N} \cup \{+\infty\},$$

en posant $v(0) = +\infty$, et qui à tout élément x non nul de \mathbb{Z}_p associe l'entier naturel n intervenant dans l'écriture de x sous la forme $p^n u$ où $u \in U$. On prolonge alors v à \mathbb{Q}_p de façon évidente. On obtient ainsi une valuation discrète sur \mathbb{Q}_p dont l'anneau de valuation est \mathbb{Z}_p , l'idéal de valuation est $p\mathbb{Z}_p$ (p est une uniformisante) et dont le corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p$ est canoniquement isomorphe à $\mathbb{Z}/p\mathbb{Z}$. En particulier :

Corollaire 1.3. L'anneau \mathbb{Z}_p est un anneau de valuation discrète.

Exercices

- 1) Soit a un entier relatif. On suppose que pour tout entier $n \geq 1$, la congruence $x^2 \equiv a \pmod{p^n}$ possède une solution dans \mathbb{Z} . Montrer que a est un carré dans \mathbb{Z}_p .
- 2) Montrer que le polynôme $1 + X + \dots + X^{p-1} \in \mathbb{Z}_p[X]$ est irréductible sur \mathbb{Q}_p .
- 3) Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p . Montrer qu'il n'existe pas de valuation discrète définie sur $\overline{\mathbb{Q}_p}$. En particulier, la fermeture intégrale de \mathbb{Z}_p dans $\overline{\mathbb{Q}_p}$ n'est pas un anneau de valuation discrète ; en fait, cet anneau ne possède pas d'élément irréductible.

Chapitre II — Anneaux de Dedekind

I. Définition et exemples

Définition 2.1. Soit A un anneau. On dit que A est un anneau de Dedekind s'il est noethérien, intégralement clos, et si tout idéal premier non nul de A est maximal.

Exemples d'anneaux de Dedekind

1) Les anneaux principaux ;

2) l'anneau d'entiers d'un corps de nombres, i.e. d'une extension finie de \mathbb{Q} (ce résultat sera prouvé au chapitre suivant).

Comme l'a remarqué Kummer (1810-1893), en rapport avec l'étude de la courbe de Fermat, il existe de nombreux anneaux d'entiers de corps de nombres qui ne sont pas principaux (il en existe une infinité). Cette remarque est à l'origine du concept d'idéal d'un anneau et de l'étude entreprise par Dedekind (1831-1916) des anneaux qui portent son nom [†].

3) L'anneau de coordonnées $\mathbb{C}[V]$ d'une courbe algébrique irréductible lisse V définie sur \mathbb{C} (cf. chap. I, IV, et le cor. 2.1 ci-dessous).

Voici une première caractérisation des anneaux de Dedekind :

Proposition 2.1. Soit A un anneau noethérien intègre. Les deux propriétés suivantes sont équivalentes :

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

Démonstration : L'implication $a) \implies b)$: on utilise le th. 1.1 du chapitre I. Soit \mathfrak{p} un idéal premier non nul de A . Puisque A est intègre et noethérien, il en est de même de l'anneau $A_{\mathfrak{p}}$. De plus, $\mathfrak{p}A_{\mathfrak{p}}$ est un idéal premier non nul de $A_{\mathfrak{p}}$ (on a $\mathfrak{p}A_{\mathfrak{p}} \cap A = \mathfrak{p}$) et c'est le seul. En effet, soit \mathfrak{P} un idéal premier non nul de $A_{\mathfrak{p}}$. L'anneau $A_{\mathfrak{p}}$ étant local, d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$, l'idéal \mathfrak{P} est contenu dans $\mathfrak{p}A_{\mathfrak{p}}$. Supposons que l'on ait $\mathfrak{P} \neq \mathfrak{p}A_{\mathfrak{p}}$. Dans ce cas $\mathfrak{P} \cap A$, qui est un idéal premier non nul de A , est strictement contenu dans \mathfrak{p} , ce qui conduit à une contradiction, car les idéaux premiers non nuls de A sont maximaux. D'où l'égalité $\mathfrak{P} = \mathfrak{p}A_{\mathfrak{p}}$, et notre assertion.

[†] 1) Montrer que le sous-anneau de \mathbb{C} engendré par \mathbb{Z} et $\sqrt{-6}$ n'est pas un anneau principal.

2) Montrer que l'anneau des entiers algébriques, i.e. l'ensemble des nombres complexes entiers sur \mathbb{Z} , n'est pas un anneau noethérien.

3) Soient K un corps et X une indéterminée. Montrer que $K[X^2, X^3]$ est un anneau noethérien intègre de dimension 1 qui n'est pas un anneau intégralement clos. Montrer que les anneaux $K[X, Y, \dots]$, avec au moins deux indéterminées, ne sont pas des anneaux de Dedekind.

Par ailleurs, $A_{\mathfrak{p}}$ est int gralement clos : en effet, soit x un  l ment du corps des fractions de $A_{\mathfrak{p}}$ (donc de A) entier sur $A_{\mathfrak{p}}$. En consid rant une  quation de d pendance int grale de x sur $A_{\mathfrak{p}}$ et un d nominateur commun aux coefficients de cette  quation, on constate qu'il existe des  l ments a_i de A et un  l ment s de $A \setminus \mathfrak{p}$ tels que l'on ait $sx^n + a_1x^{n-1} + \dots + a_n = 0$ (avec $n \geq 1$). En multipliant par s^{n-1} , on obtient une relation de d pendance int grale de sx sur A . Puisque A est int gralement clos, sx appartient   A , ce qui entra ne que x est dans $A_{\mathfrak{p}}$ (cette d monstration prouve que le localis  d'un anneau int gralement clos est int gralement clos). D'apr s le th. 1.1, $A_{\mathfrak{p}}$ est donc un anneau de valuation discr te.

L'implication $b) \implies a)$: consid rons deux id aux premiers non nuls \mathfrak{p} et \mathfrak{p}' de A tels que \mathfrak{p} soit contenu dans \mathfrak{p}' . Alors $\mathfrak{p}A_{\mathfrak{p}'}$ et $\mathfrak{p}'A_{\mathfrak{p}'}$ sont deux id aux premiers non nuls de l'anneau de valuation discr te $A_{\mathfrak{p}'}$. D'apr s la proposition 1.1, a) et c), on a donc $\mathfrak{p}A_{\mathfrak{p}'} = \mathfrak{p}'A_{\mathfrak{p}'}$. Il en r sulte l' galit  $\mathfrak{p} = \mathfrak{p}'$. Cela montre que tout id al premier non nul de A est maximal. Par ailleurs, A est int gralement clos : en effet, soit a un  l ment du corps des fractions de A , entier sur A . Pour tout id al premier non nul de A , a est en particulier entier sur $A_{\mathfrak{p}}$ qui, par hypoth se, est int gralement clos. Ainsi, a appartient   l'intersection des localis s $A_{\mathfrak{p}}$, o  \mathfrak{p} parcourt les id aux premiers (non nuls) de A , ce qui entra ne que a est dans A (cf. le lemme ci-dessous). D'o  l'implication.

Il reste   prouver le lemme suivant :

Lemme 2.1. *Soit A un anneau int gre. On a l' galit *

$$A = \bigcap_{\mathfrak{M}} A_{\mathfrak{M}},$$

o  \mathfrak{M} parcourt l'ensemble des id aux maximaux de A .

D monstration : Puisque A est int gre, A est contenu dans l'intersection des $A_{\mathfrak{M}}$ (aux identifications canoniques pr s). Inversement, soit α un  l ment de l'intersection de $A_{\mathfrak{M}}$. Soit I le sous-ensemble de A form  des  l ments x tels que $x\alpha$ appartienne   A . Alors, I est un id al de A . V rifions que I n'est contenu dans aucun id al maximal : soit \mathfrak{M} un id al maximal de A . Il existe d et e dans A tels que $\alpha = d/e$ et que e ne soit pas dans \mathfrak{M} . On a $e\alpha \in A$, i.e. $e \in I$, et donc I n'est pas contenu dans \mathfrak{M} . Cela entra ne $I = A$ et α est ainsi dans A . D'o  le lemme.

Corollaire 2.1. *Soit V une courbe alg brique d finie sur \mathbb{C} lisse et irr ductible. Alors, l'anneau de coordonn es de V est un anneau de Dedekind.*

D monstration : Soit $\mathbb{C}[V]$ l'anneau de coordonn es de V . Il est int gre (car V est irr ductible) et noeth rien. Par ailleurs, sa dimension est 1 : en effet, la dimension de $\mathbb{C}[V]$ est le degr  de transcendance sur \mathbb{C} de son corps des fractions, qui est 1 car V est une courbe (i.e. un ferm  alg brique de dimension 1). Ainsi, tous les id aux premiers non nuls de $\mathbb{C}[V]$ sont maximaux. Or un id al maximal de $\mathbb{C}[V]$ est associ    un point P de V , i.e.

est l'idéal \mathfrak{M}_P de $\mathbb{C}[V]$ formé des fonctions nulles en un point P (cf. le th. des zéros de Hilbert). Puisque V est lisse, les localisés de $\mathbb{C}[V]$ en les idéaux \mathfrak{M}_P sont des anneaux de valuation discrète (chap. I, th. 1.2). Il résulte de la prop. 2.1 que $\mathbb{C}[V]$ est un anneau de Dedekind.

II. Le groupe des classes d'idéaux d'un anneau de Dedekind

À tout anneau de Dedekind A , nous allons associer un groupe abélien, appelé le groupe des classes d'idéaux de A .

2.1. Idéaux fractionnaires d'un anneau

Considérons un anneau intègre A , de corps des fractions K .

Définition 2.2. On appelle idéal fractionnaire de A (ou de K par rapport à A) tout sous- A -module I de K pour lequel existe un élément non nul d de A tel que dI soit contenu dans A .

Un idéal de A est un idéal fractionnaire de A (avec $d = 1$). Un idéal de A est parfois appelé un idéal entier de A .

Lemme 2.2. Un sous- A -module de type fini de K est un idéal fractionnaire de A . Si A est noethérien, un idéal fractionnaire de A est un sous- A -module de type fini de K .

Démonstration : Soient I un sous- A -module de type fini de K et (x_1, \dots, x_n) un système générateur de I . En posant $x_i = a_i/d_i$ et en considérant le produit d des d_i (qui est non nul), on constate que dx_i est dans A et donc que dI est contenu dans A . Supposons de plus A noethérien. Il existe $d \in A$ non nul tel que I soit contenu dans $d^{-1}A$. Or $d^{-1}A$ est un A -module isomorphe à A , qui donc un A -module noethérien. Il en résulte que I est de type fini. D'où le lemme.

Soient I et I' deux idéaux fractionnaires de A . Les sous- A -modules de K , $I + I'$ et $I \cap I'$, sont aussi des idéaux fractionnaires de A . On définit le produit II' comme étant le sous-ensemble de K formé des sommes finies d'éléments $x_i y_i$ où $x_i \in I$ et $y_i \in I'$. C'est un idéal fractionnaire de A (si d (resp. d') est un dénominateur commun aux éléments de I (resp. de I'), dd' en est un aux éléments de II').

Notation. On désignera désormais par $\text{Id}(A)$ l'ensemble des idéaux fractionnaires non nuls de A .

La multiplication $(I, J) \mapsto IJ$, munit $\text{Id}(A)$ d'une structure de monoïde commutatif (un monoïde est un ensemble muni d'une loi de composition interne associative possédant un élément neutre). L'élément neutre pour cette loi de composition est l'idéal A . En particulier, un idéal fractionnaire I est inversible s'il existe un idéal fractionnaire J tel que $IJ = A$; on dit alors que J est l'inverse de I et on le note I^{-1} .

Exemple. Supposons que A soit un anneau principal. Alors $\text{Id}(A)$ est un groupe abélien. En effet, soit I un idéal fractionnaire non nul de A . Il existe d non nul dans A tel que dI soit un idéal de A . Puisque A est principal, il existe a non nul dans A tel que l'on ait $dI = a.A$, et l'on a ainsi $I = (a/d).A$. La partie $J = (d/a).A$ est un idéal fractionnaire de A et l'on a $IJ = A$, ce qui montre que I est inversible. D'où notre assertion.

Étant donnés deux éléments I et J de $\text{Id}(A)$, notons $(I : J)$ l'ensemble des $x \in K$ tels que xJ soit contenu dans I (on l'appelle le transporteur de J dans I). Alors $(I : J)$ appartient à $\text{Id}(A)$: en effet, on vérifie immédiatement que c'est un sous- A -module de K . Soient par ailleurs $d \in A$ non nul tel que $dI \subseteq A$, et b un élément non nul de J . On a alors $db \neq 0$, et l'inclusion $db(I : J) \subseteq A$. D'où l'assertion.

Lemme 2.3. *Soit I un idéal fractionnaire non nul de A . Si I est inversible, on a l'égalité $I^{-1} = (A : I)$. Autrement dit, I est inversible si et seulement si l'on a $(A : I)I = A$.*

Démonstration : Soit J un idéal fractionnaire de A tel que $IJ = A$. Par définition, J est contenu dans $(A : I)$. Inversement, on a l'inclusion $(A : I)I \subseteq A$. Cela entraîne que $(A : I)IJ \subseteq J$, et donc que $(A : I)$ est contenu dans J . D'où $J = (A : I)$ et le lemme.

Exercice. Montrer que si A est un anneau local intègre, les idéaux inversibles de A sont principaux.

2.2. Cas des anneaux de Dedekind

Considérons désormais un anneau de Dedekind A .

Théorème 2.1. *Supposons que A ne soit pas un corps. Alors, tout idéal maximal de A est inversible dans $\text{Id}(A)$.*

Démonstration : Soit \mathfrak{M} un idéal maximal de A ; puisque A n'est pas un corps, \mathfrak{M} n'est pas nul, autrement dit, \mathfrak{M} est dans $\text{Id}(A)$. Il s'agit de montrer que l'on a $(A : \mathfrak{M})\mathfrak{M} = A$ (lemme 2.3). Posons $\mathfrak{M}' = (A : \mathfrak{M})$. Par définition $\mathfrak{M}'\mathfrak{M}$ est un idéal de A . Puisque A est contenu dans \mathfrak{M}' , on a l'inclusion $\mathfrak{M} \subseteq \mathfrak{M}'\mathfrak{M}$. L'idéal \mathfrak{M} étant maximal, on a donc $\mathfrak{M}'\mathfrak{M} = \mathfrak{M}$ ou bien $\mathfrak{M}'\mathfrak{M} = A$.

Supposons que l'on ait $\mathfrak{M}'\mathfrak{M} = \mathfrak{M}$. Prouvons alors que

$$(1) \quad \mathfrak{M}' = A.$$

Considérons pour cela un élément x de \mathfrak{M}' . On a $x\mathfrak{M} \subseteq \mathfrak{M}$, et l'on en déduit que pour tout entier naturel n l'on a $x^n\mathfrak{M} \subseteq \mathfrak{M}$. Soit $A[x]$ le sous- A -module de K engendré par tous les x^k ($k \geq 0$). Si d est un élément non nul de \mathfrak{M} , on a donc l'inclusion $dA[x] \subseteq \mathfrak{M}$, ce qui entraîne en particulier que $A[x]$ est un idéal fractionnaire de A . Puisque A est noethérien, c'est un A -module de type fini, et x est donc entier sur A [†]. Or A étant intégralement

clos, x appartient donc à A . Cela prouve que \mathfrak{M}' est contenu dans A (l'autre inclusion est évidente). D'où l'égalité (1).

Il suffit maintenant de prouver que l'égalité (1) conduit à une contradiction. Soit a un élément non nul de \mathfrak{M} . Puisque A est noethérien, il existe un nombre fini d'idéaux premiers non nuls, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, tels que l'idéal $a.A$ contienne le produit des \mathfrak{p}_i ^{††}. Choisissons un entier n minimal tel que cette condition soit réalisée. Puisque \mathfrak{M} contient le produit des \mathfrak{p}_i , il contient l'un des \mathfrak{p}_i , qui n'est pas nul, et donc \mathfrak{M} est égal à l'un d'eux, disons \mathfrak{p}_1 . Soit I le produit des idéaux $\mathfrak{p}_2 \dots \mathfrak{p}_n$ (si $n = 1$ il s'agit du produit vide et $I = A$). D'après le caractère minimal de n , I n'est pas contenu dans $a.A$, et il existe un élément b de I tel que $b \notin a.A$. Puisque $\mathfrak{M}I$ est contenu dans $a.A$, $\mathfrak{M}ba^{-1}$ est contenu dans A , ce qui montre que ba^{-1} appartient à \mathfrak{M}' . Or puisque $b \notin a.A$, ba^{-1} n'est pas dans A . Par conséquent, \mathfrak{M}' est distinct de A , ce qui contredit l'égalité (1) et termine la démonstration du théorème.

On désigne par \mathbf{P} l'ensemble des idéaux premiers non nuls de A .

Théorème 2.2. *a) Tout élément I de $\text{Id}(A)$ s'écrit de manière unique sous la forme*

$$(2) \quad I = \prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{v_{\mathfrak{p}}(I)},$$

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

b) Le monoïde $\text{Id}(A)$ est un groupe.

Démonstration : Le théorème est vrai si A est un corps ; en effet, on a dans ce cas $\text{Id}(A) = \{A\}$, $\mathbf{P} = \emptyset$, et A est produit de la famille vide d'éléments de $\text{Id}(A)$.

Supposons désormais que A ne soit pas un corps.

1) Montrons d'abord l'existence d'une décomposition sous la forme (2). Soit I un élément de $\text{Id}(A)$. Il existe d non nul dans A tel que dI soit un idéal de A . L'égalité $(dA).I = (dI)$ permet de se ramener au cas où I est contenu dans A (cf. th. 2.1). Soit Φ l'ensemble des idéaux non nuls de A qui ne sont pas produit d'éléments de \mathbf{P} . Supposons que Φ ne soit pas vide. Puisque A est noethérien, Φ possède un élément maximal J . Nécessairement J est distinct de A , car A n'appartient pas à Φ (A est produit de la famille

[†] Soient B est un anneau contenant A et x un élément de B . Alors x est entier sur A si et seulement si $A[x]$ est un A -module de type fini (cf. par exemple [Sa], p. 33).

^{††} Dans un anneau noethérien, tout idéal non nul contient un produit d'idéaux premiers non nuls : on suppose que l'ensemble Φ des idéaux non nuls de A qui ne contiennent aucun produit d'idéaux premiers non nuls est non vide. Puisque A est noethérien, Φ possède un élément maximal I , qui n'est pas un idéal premier. On a $I \neq A$ car A est produit de la famille vide d'idéaux premiers. Il existe donc deux éléments x et y de $A - I$ tels que xy soit dans I . Les idéaux $I + x.A$ et $I + y.A$ ne sont pas dans Φ , et contiennent donc des produits d'idéaux premiers non nuls, ce qui conduit à une contradiction, et prouve que Φ est vide.

vide d'idéaux premiers). Ainsi J est contenu dans un idéal maximal \mathfrak{M} de A . D'après le th. 2.1, \mathfrak{M} possède un inverse \mathfrak{M}' : on a les inclusions

$$(3) \quad J \subseteq J\mathfrak{M}' \subseteq A.$$

En effet, on a $J\mathfrak{M}' \subseteq \mathfrak{M}\mathfrak{M}' = A$, et puisque A est contenu dans \mathfrak{M}' , on a $J \subseteq J\mathfrak{M}'$. On a en fait

$$(4) \quad J\mathfrak{M}' \neq J.$$

Dans le cas contraire, pour tout $x \in \mathfrak{M}'$, on aurait $xJ \subseteq J$, puis pour tout entier naturel n , $x^n J \subseteq J$, ce qui entraîne que x est entier sur A (comme dans le th. 2.1, cela entraîne que $A[x]$ est un A -module de type fini). Donc x est dans A (A est intégralement clos) et $\mathfrak{M}' = A$, ce qui n'est pas (car $\mathfrak{M}\mathfrak{M}' = A$) ; d'où (4). D'après le caractère maximal de J , $J\mathfrak{M}'$ étant un idéal non nul de A (cf. (3)), $J\mathfrak{M}'$ n'est pas dans Φ . Ainsi $J\mathfrak{M}'$ est un produit d'élément de \mathbf{P} . En multipliant par \mathfrak{M} , on constate qu'il en est de même de J , ce qui conduit à une contradiction. D'où l'assertion d'existence.

Montrons maintenant l'assertion d'unicité. Supposons que l'on ait

$$\prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{n_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

où $n_{\mathfrak{p}}$ et $m_{\mathfrak{p}}$ sont des entiers relatifs presque tous nuls. Il s'agit de montrer que l'on a $m_{\mathfrak{p}} = n_{\mathfrak{p}}$ pour tout \mathfrak{p} . Si tel n'était pas le cas, il existerait des entiers $r \geq 1$ et $n \geq 2$, et des idéaux maximaux \mathfrak{p}_i de A , deux à deux distincts, tels que

$$\prod_{1 \leq i \leq r} \mathfrak{p}_i^{t_{\mathfrak{p}_i}} = \prod_{r+1 \leq i \leq n} \mathfrak{p}_i^{t_{\mathfrak{p}_i}},$$

où les $t_{\mathfrak{p}_i}$ sont des entiers > 0 . Mais alors \mathfrak{p}_1 contiendrait l'un des idéaux \mathfrak{p}_i avec $i \geq r+1$ ce qui impliquerait l'égalité $\mathfrak{p}_1 = \mathfrak{p}_i$. D'où une contradiction et le résultat.

2) Soit I un élément de $\text{Id}(A)$. En écrivant I sous la forme (2), les éléments de \mathbf{P} étant inversibles dans $\text{Id}(A)$ (th. 2.1), on en déduit que I est inversible, d'inverse

$$I^{-1} = \prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{-v_{\mathfrak{p}}(I)}.$$

D'où le théorème.

Remarque. Soit I un idéal entier non nul de A . Soient $(\mathfrak{p}_i)_{1 \leq i \leq t}$ les idéaux premiers de A qui interviennent dans la décomposition de I en produit d'idéaux premiers (avec un exposant non nul). Il résulte de la démonstration du th. 2.2 que l'on a $v_{\mathfrak{p}_i}(I) > 0$. Par ailleurs, les \mathfrak{p}_i sont exactement les idéaux premiers de A qui contiennent I : cela provient

du fait qu'un idéal premier d'un anneau qui contient un produit d'idéaux contient l'un deux, et que tous les idéaux premiers non nuls de A sont maximaux. En particulier, si x est un élément non nul de A , il n'y a qu'un nombre fini d'idéaux premiers de A qui contiennent x .

On peut maintenant définir le groupe des classes d'idéaux de A :

Définition 2.2. Un élément de $\text{Id}(A)$ est dit *principal* s'il est de la forme Ax , où x est un élément non nul de K . Soit $\text{Pr}(A)$ l'ensemble des éléments de $\text{Id}(A)$ qui sont principaux. C'est un sous-groupe de $\text{Id}(A)$. Le groupe quotient

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

s'appelle le groupe des classes d'idéaux de A .

En fait, le groupe $\text{Cl}(A)$ mesure le défaut de principalité de A . Plus précisément, il résulte directement des définitions que l'on a l'énoncé suivant :

Lemme 2.4. Pour que A soit un anneau principal il faut et il suffit que le groupe $\text{Cl}(A)$ soit réduit à l'élément neutre.

Lorsque A est l'anneau d'entiers d'un corps de nombres, on peut démontrer que $\text{Cl}(A)$ est un groupe fini (cf. [Sa], p. 69-71).

III. La valuation discrète associée à un idéal maximal

Commençons par quelques remarques préliminaires. Étant donné I dans $\text{Id}(A)$ et \mathfrak{p} dans \mathbf{P} , on notera $v_{\mathfrak{p}}(I)$ l'exposant de \mathfrak{p} dans la décomposition de I en produit d'idéaux premiers (cf. th. 2.2). Si I et J sont dans $\text{Id}(A)$, on dit que I divise J (on note $I|J$) s'il existe un idéal I' de A tel que $J = II'$.

Lemme 2.5. Soient I et J deux éléments de $\text{Id}(A)$. On a

- a) $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$;
- b) $I \subseteq J \iff v_{\mathfrak{p}}(I) \geq v_{\mathfrak{p}}(J)$ pour tout $\mathfrak{p} \in \mathbf{P} \iff J|I$;
- c) $v_{\mathfrak{p}}(I + J) = \inf(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$;
- d) $v_{\mathfrak{p}}(I \cap J) = \max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$;
- e) $v_{\mathfrak{p}}(I \cap J) + v_{\mathfrak{p}}(I + J) = v_{\mathfrak{p}}(IJ)$;
- f) $v_{\mathfrak{p}}((I : J)) = v_{\mathfrak{p}}(IJ^{-1}) = v_{\mathfrak{p}}(I) - v_{\mathfrak{p}}(J)$.

Démonstration : L'assertion a) est immédiate. Pour la première équivalence de b), on peut supposer $J = A$. Si $I \subseteq A$, le fait que pour tout $\mathfrak{p} \in \mathbf{P}$ l'on ait $v_{\mathfrak{p}}(I) \geq 0$ résulte de la démonstration du th. 2.2. L'implication réciproque et l'autre équivalence sont immédiates. Démontrons c) : posons $n_{\mathfrak{p}} = \inf(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$. Puisque $n_{\mathfrak{p}}$ est plus petit que $v_{\mathfrak{p}}(I)$ et $v_{\mathfrak{p}}(J)$, on a (assertion b))

$$I + J \subseteq \prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

Par ailleurs, soit I' un idéal fractionnaire de A contenant I et J . On a $v_{\mathfrak{p}}(I) \geq v_{\mathfrak{p}}(I')$ et $v_{\mathfrak{p}}(J) \geq v_{\mathfrak{p}}(I')$. Il en résulte que $n_{\mathfrak{p}}$ est plus grand que $v_{\mathfrak{p}}(I')$ et donc que l'on a

$$\prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{n_{\mathfrak{p}}} \subseteq I'.$$

Cela prouve l'assertion c). Démontrons d) : posons $n_{\mathfrak{p}} = \text{Max}(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$. Puisque $I \cap J$ est contenu dans I et J , pour tout $\mathfrak{p} \in \mathbf{P}$, on a $v_{\mathfrak{p}}(I \cap J) \geq n_{\mathfrak{p}}$. Les inégalités $n_{\mathfrak{p}} \geq v_{\mathfrak{p}}(I)$ et $n_{\mathfrak{p}} \geq v_{\mathfrak{p}}(J)$ entraînent par ailleurs l'inclusion

$$\prod_{\mathfrak{p} \in \mathbf{P}} \mathfrak{p}^{n_{\mathfrak{p}}} \subseteq I \cap J.$$

D'où d). L'assertion e) provient directement de c) et d). Quant à l'assertion f), il suffit de remarquer que l'on a $(I : J) = IJ^{-1}$ (on a par définition $J(I : J) \subseteq I$ et $IJ^{-1} \subseteq (I : J)$). D'où le lemme.

Corollaire 2.2. *Soient I et J deux idéaux (entiers) de A . Les conditions suivantes sont équivalentes :*

- a) $I + J = A$;
- b) $I \cap J = IJ$;
- c) $v_{\mathfrak{p}}(I).v_{\mathfrak{p}}(J) = 0$ pour tout $\mathfrak{p} \in \mathbf{P}$.

Si l'une de ces conditions est réalisée, on dit que I et J sont comaximaux.

Démonstration : C'est une conséquence directe du lemme précédent.

Considérons maintenant un idéal premier non nul \mathfrak{p} de A , i.e. un idéal maximal de A . Notons

$$v_{\mathfrak{p}} : K^* \rightarrow \mathbb{Z},$$

l'application qui à un élément x de K^* associe l'exposant $v_{\mathfrak{p}}(Ax)$ de \mathfrak{p} , dans la décomposition de l'idéal fractionnaire Ax en produit d'idéaux premiers (cf. th. 2.2). On prolonge $v_{\mathfrak{p}}$ à K en posant $v_{\mathfrak{p}}(0) = +\infty$. Par définition, on a donc

$$(5) \quad v_{\mathfrak{p}}(Ax) = v_{\mathfrak{p}}(x).$$

Proposition 2.2. *L'application $v_{\mathfrak{p}}$ est une valuation discrète sur K . L'anneau de valuation correspondant est le localisé $A_{\mathfrak{p}}$, et le corps résiduel est isomorphe à A/\mathfrak{p} (on retrouve ainsi le fait que $A_{\mathfrak{p}}$ est un anneau de valuation discrète).*

Démonstration : Puisque l'idéal \mathfrak{p}^2 est strictement contenu dans \mathfrak{p} (d'après le th. 2.1, on aurait sinon $\mathfrak{p} = A$), il existe un élément x de \mathfrak{p} qui n'est pas dans \mathfrak{p}^2 . L'idéal xA est donc contenu dans \mathfrak{p} sans l'être dans \mathfrak{p}^2 , et l'on a donc $v_{\mathfrak{p}}(x) = 1$. Cela entraîne que l'application $v_{\mathfrak{p}}$ est une surjection de K^* sur \mathbb{Z} . Considérons alors deux éléments x et y de

K^* . L'égalité $Ax.Ay = A.xy$ implique que v_p est un homomorphisme de groupes. De plus, l'idéal fractionnaire $A(x+y)$ est contenu dans $Ax + Ay$, de sorte que l'on a (en utilisant le lemme 2.5)

$$v_p(x+y) \geq v_p(Ax + Ay) = \inf(v_p(Ax), v_p(Ay)) = \inf(v_p(x), v_p(y)).$$

Cela prouve que v_p est une valuation discrète sur K .

Par ailleurs, le localisé A_p est évidemment contenu dans l'anneau de valuation de v_p . Inversement, soit x un élément de K^* tel que $v_p(x)$ soit positif. En considérant la décomposition de l'idéal fractionnaire Ax en produit d'idéaux premiers, on constate qu'il existe deux idéaux entiers I et J de A tel que l'on ait $IAx = J$, et que $v_p(J) \geq 0$, $v_p(I) = 0$. On a $xI \subseteq J$. Soit β un élément de I qui n'est pas dans p . Alors $x\beta$ appartient à J , et x s'écrit donc sous la forme α/β où $\alpha \in J$, ce qui prouve que x est dans A_p . D'où le fait que A_p soit l'anneau de valuation de v_p . Compte-tenu de cette assertion, le fait que l'idéal de valuation de A_p soit pA_p , et que le corps résiduel soit isomorphe à A/p a déjà été démontré. D'où le lemme.

Terminons ce paragraphe par une propriété qui nous sera utile par la suite :

Lemme 2.6. *Soient i entier naturel et p un idéal premier non nul de A . Soit a un élément de p^i qui ne soit pas dans p^{i+1} . Alors, l'application $\varphi_i : A \rightarrow p^i/p^{i+1}$ définie par*

$$(5) \quad \varphi_i(x) = ax + p^{i+1},$$

est un homomorphisme de groupes surjectif de noyau p . Autrement dit, φ_i passée au quotient réalise un isomorphisme de groupes additifs de A/p sur p^i/p^{i+1} .

Démonstration : Par définition de a , il existe un idéal I de A tel que $a.A = p^iI$ et que $v_p(I) = 0$. L'application $A/p \rightarrow p^iI/p^{i+1}I$ qui à $x + p$ associe $ax + p^{i+1}I$ est un isomorphisme de groupes. Par ailleurs, l'application

$$\psi_i : p^iI \rightarrow p^i/p^{i+1},$$

définie par $\psi_i(y) = y + p^{i+1}$ est un homomorphisme de groupes surjectif de noyau $p^{i+1}I$: cela résulte des assertions c) et d) du lemme 2.5 : on a $p^{i+1} \cap p^iI = p^{i+1}I$ et $p^iI + p^{i+1} = p^i$. D'où le lemme.

Remarque. Le groupe quotient p^i/p^{i+1} est naturellement muni d'une structure de A/p -espace vectoriel. On déduit du lemme précédent que l'application φ_i passée au quotient est un isomorphisme de A/p -espaces vectoriels de A/p sur p^i/p^{i+1} , et en particulier que p^i/p^{i+1} est un A/p -espace vectoriel de dimension 1.

IV. Théorème d'approximation

Considérons toujours dans ce paragraphe un anneau de Dedekind A de corps des fractions K . Nous allons démontrer l'énoncé suivant, connu sous le nom de théorème, ou de lemme, d'approximation :

Théorème 2.3. *Soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$ des idéaux premiers non nuls de A distincts deux à deux, $(x_i)_{1 \leq i \leq n}$ des éléments de K , et $(n_i)_{1 \leq i \leq n}$ des entiers relatifs. Alors, il existe un élément x de K tel que l'on ait*

$$(6) \quad v_{\mathfrak{p}_i}(x - x_i) \geq n_i \text{ pour tout } i, \quad \text{et} \quad v_{\mathfrak{p}}(x) \geq 0 \text{ pour } \mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_n.$$

Démonstration : On suppose d'abord que les x_i appartiennent à A et l'on cherche une solution x dans A satisfaisant aux conditions (6). Quitte à augmenter les n_i , on peut supposer que ce sont des entiers naturels. Le résultat dans ce cas est une conséquence directe du théorème Chinois [†].

Dans le cas général, on écrit x_i sous la forme a_i/s , où a_i et s sont dans A et où $s \neq 0$. On cherche x sous la forme a/s , où a appartient à A . L'élément a doit alors vérifier les conditions

$$v_{\mathfrak{p}_i}(a - a_i) \geq n_i + v_{\mathfrak{p}_i}(s) \text{ pour tout } i \quad \text{et} \quad v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(s) \text{ pour } \mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_n.$$

Autrement dit, il s'agit de trouver un élément a de A tel que, pour tout i entre 1 et n , l'on ait $v_{\mathfrak{p}_i}(a - a_i) \geq n_i + v_{\mathfrak{p}_i}(s)$, pour tout idéal \mathfrak{p} tel que $v_{\mathfrak{p}}(s) > 0$ l'on ait $v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(s)$, et que $v_{\mathfrak{p}}(a) \geq 0$ pour les autres idéaux premiers non nuls de A . L'on se ramène ainsi à la situation considérée précédemment. Cela entraîne le lemme.

Corollaire 2.3. *Si A ne possède qu'un nombre fini d'idéaux premiers, A est un anneau principal.*

Démonstration : Soit $(\mathfrak{p}_i)_{1 \leq i \leq n}$ la famille des idéaux premiers de A . Il s'agit de montrer que tous les \mathfrak{p}_i sont principaux (cf. th. 2.2). Montrons que tel est le cas de \mathfrak{p}_1 . On choisit pour cela un élément x_1 qui est dans \mathfrak{p}_1 et qui n'est pas dans \mathfrak{p}_1^2 . D'après le théorème 2.3, il existe un élément x dans A tel que l'on ait

$$x \equiv x_1 \pmod{\mathfrak{p}_1^2} \quad \text{et} \quad x \equiv 1 \pmod{\mathfrak{p}_k} \text{ pour } k > 1.$$

[†] Il s'agit de l'énoncé suivant : soit A un anneau et (I_k) une famille finie d'idéaux de A comaximaux deux à deux. Alors l'application $A \rightarrow \prod (A/I_k)$, qui à un élément a associe le uplet $(a + I_k)$, est un homomorphisme surjectif d'anneaux.

Dans notre situation, on applique ce résultat au cas où les idéaux I_k sont des puissances d'idéaux premiers non nuls, compte tenu du fait que si n et m sont des entiers positifs et si \mathfrak{p}_1 et \mathfrak{p}_2 sont deux idéaux premiers non nuls de A , les idéaux \mathfrak{p}_1^n et \mathfrak{p}_2^m sont comaximaux dans A .

On a $v_{\mathfrak{p}_1}(x) = 1$ et $v_{\mathfrak{p}_k}(x) = 0$ pour $k > 1$. Cela entraîne l'égalité $xA = \mathfrak{p}_1$ (th. 2.2). D'où le fait que \mathfrak{p}_1 soit principal et le lemme.

Corollaire 2.4. *Soit I un idéal fractionnaire de A . Alors, le A -module I peut être engendré par au plus deux éléments (tel est en particulier le cas des idéaux entiers de A).*

Démonstration : On peut supposer que I est un idéal entier non nul de A . Soit a un élément non nul de I . D'après le th. 2.2 et le lemme 2.5 (assertion b)), puisque l'idéal aA est contenu dans I , il existe un entier t , des idéaux premiers \mathfrak{p}_i , et des entiers m_i et n_i , tels que $m_i \geq n_i$ et que

$$I = \prod_{i=1}^t \mathfrak{p}_i^{n_i} \quad \text{et} \quad aA = \prod_{i=1}^t \mathfrak{p}_i^{m_i}.$$

Pour tout i compris entre 1 et t , choisissons un élément b_i de A tel que b_i soit dans $\mathfrak{p}_i^{n_i}$ et pas dans $\mathfrak{p}_i^{n_i+1}$. D'après le th. 2.2, il existe b dans A tel que, pour tout i , l'on ait $b \equiv b_i \pmod{\mathfrak{p}_i^{n_i+1}}$. Pour tout idéal premier \mathfrak{p} de A , on a alors l'égalité

$$(7) \quad \text{Inf}(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)) = v_{\mathfrak{p}}(I).$$

En effet, si \mathfrak{p} est un idéal premier distinct des \mathfrak{p}_i , on a $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(I) = 0$. Par ailleurs, pour tout i , l'on a $v_{\mathfrak{p}_i}(b) = n_i = v_{\mathfrak{p}_i}(I)$. D'où l'égalité (7). Il résulte alors de l'assertion c) du lemme 2.5 que l'on a $I = aA + bA$. D'où le résultat.

Chapitre III — Extensions et ramification

Nous allons décrire dans ce chapitre le comportement des anneaux de Dedekind par passage aux extensions finies séparables. On introduira par ailleurs, la notion fondamentale de ramification dans les extensions de corps. On examinera la situation où les extensions considérées sont galoisiennes, et l'on définira ce que l'on appelle la substitution de Frobenius, qui joue un rôle crucial dans la théorie du corps de classes (cf. par exemple [Se1] et [Ne]).

I. La forme Trace et l'homomorphisme Norme

Partons d'un corps K et d'une extension finie L de K de degré n . Le corps L est naturellement muni d'une structure de K -espace vectoriel de dimension finie. Soit x un élément de L . Notons m_x l'endomorphisme de L donné par la multiplication par x : pour tout $y \in L$, on a $m_x(y) = xy$.

Définition 3.1. *La trace de x , relativement à L et K , est la trace de m_x . On la note $\text{Tr}_{L/K}(x)$. La norme de x , relativement à L et K , est le déterminant de m_x . On la note $\text{N}_{L/K}(x)$.*

Par définition, la trace et la norme de x sont des éléments de K . On obtient ainsi une forme K -linéaire $\text{Tr}_{L/K} : L \rightarrow K$ et un homomorphisme de groupes $\text{N}_{L/K} : L^* \rightarrow K^*$ (où l'exposant $*$ désigne le groupe multiplicatif des éléments non nuls du corps). Le polynôme caractéristique de m_x est à coefficients dans K . Il est unitaire de degré n . On notera $\text{Car}(x, L/K, X)$ ce polynôme (en l'indéterminée X). En posant

$$\text{Car}(x, L/K, X) = \sum_{k=0}^n a_k X^k,$$

on a

$$\text{Tr}_{L/K}(x) = -a_{n-1} \quad \text{et} \quad \text{N}_{L/K}(x) = (-1)^n a_0,$$

autrement dit, si $(x_i)_{1 \leq i \leq n}$ est la famille des racines de $\text{Car}(x, L/K, X)$ dans une extension convenable de K , l'on a

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

On obtient aussi par ces considérations une application

$$\varphi_{L/K} : L \times L \rightarrow K,$$

qui est donnée, pour tout x et y dans L , par l'égalité

$$\varphi_{L/K}(x, y) = \text{Tr}_{L/K}(xy).$$

C'est une forme K -bilinéaire symétrique sur L . Nous allons montrer l'énoncé suivant :

Théorème 3.1. *Supposons que L/K soit une extension séparable. Alors, la forme bilinéaire $\varphi_{L/K}$ est non dégénérée.*

Si $(e_i)_{1 \leq i \leq n}$ est une base de L sur K , il s'agit de montrer que la matrice qui représente $\varphi_{L/K}$ dans cette base, qui est celle dont l'élément de la i -ème ligne et la j -ième colonne est $\text{Tr}_{L/K}(e_i e_j)$, a un déterminant non nul.

1.1. Lemmes préliminaires

Commençons par démontrer quelques résultats préliminaires. Considérons une extension finie M du corps L : on a les inclusions $K \subseteq L \subseteq M$ (ci-dessous $[M : L]$ désigne le degré de M sur L).

Lemme 3.1. *Soit x un élément de L . On a l'égalité*

$$(2) \quad \text{Car}(x, M/K, X) = \text{Car}(x, L/K, X)^{[M:L]}.$$

En particulier, l'on a

$$(3) \quad \text{Tr}_{M/K}(x) = [M : L] \text{Tr}_{L/K}(x) \quad \text{et} \quad \text{N}_{M/K}(x) = \text{N}_{L/K}(x)^{[M:L]}.$$

Démonstration : Posons $[M : L] = s$. Soit $e = (e_i)_{1 \leq i \leq n}$ une base de L sur K et $(f_i)_{1 \leq i \leq s}$ une base de M sur L . Alors le système $g = (e_i f_j)_{i,j}$ est une base de M sur K . On ordonne cette base de façon lexicographique :

$$g = (e_1 f_1, \dots, e_n f_1, e_1 f_2, \dots, e_n f_2, \dots, e_1 f_s, \dots, e_n f_s).$$

Soit A la matrice de l'endomorphisme de L de multiplication par x dans la base e . On constate alors que la matrice de l'endomorphisme de M de multiplication par x dans la base g est formée de blocs diagonaux représentant la matrice A . D'où l'égalité (2). Les formules (3) résulte alors des égalités (1) et (2). D'où le lemme.

Considérons maintenant un élément x de L séparable sur K , et de degré m sur K . Soit $K(x)$ l'extension simple de K engendrée par x . Elle est séparable : soit $(\tau_k)_{1 \leq k \leq m}$ les m plongements de $K(x)$ dans une clôture algébrique \overline{K} de K , qui fixent les éléments de K .

Lemme 3.2. *On a les égalités*

$$(4) \quad \text{Tr}_{K(x)/K}(x) = \sum_{k=1}^m \tau_k(x) \quad \text{et} \quad \text{N}_{K(x)/K}(x) = \prod_{k=1}^m \tau_k(x).$$

Démonstration : Notons P le polynôme minimal de x . Les éléments $\tau_k(x)$ sont les racines de P . Par ailleurs, on a $P = \text{Car}(x, K(x)/K, X)$. En effet, P et $\text{Car}(x, K(x)/K, X)$ sont deux polynômes unitaires de degré m dont x est racine (cf. le théorème de Cayley-Hamilton). Les formules (1) entraînent alors le lemme.

Lemme 3.3. *Supposons que l'extension L/K soit séparable. Soient $(\sigma_i)_{1 \leq i \leq n}$ les n plongements de L dans \overline{K} égaux à l'identité sur K . Pour tout élément x de L , l'on a*

$$(5) \quad \text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x) \quad \text{et} \quad \text{N}_{L/K}(x) = \prod_{i=1}^n \sigma_i(x).$$

Démonstration : Soit x un élément de L . D'après les lemmes 3.1 et 3.2, l'on a

$$\text{Tr}_{L/K}(x) = [L : K(x)] \cdot \text{Tr}_{K(x)/K}(x) = [L : K(x)] \cdot \sum_{k=1}^m \tau_k(x),$$

où les τ_k désignent les $[K(x) : K]$ plongements de $K(x)$ dans \overline{K} qui fixent les éléments de K . Or chacun des τ_k se prolonge à L en un homomorphisme σ_i de $[L : K(x)]$ façons différentes. La première égalité de (5) en résulte. La deuxième se prouve en utilisant le même argument.

1.2. Démonstration du théorème

Choisissons une base $(e_i)_{1 \leq i \leq n}$ de L sur K . Soient $(\sigma_i)_{1 \leq i \leq n}$ les n plongements de L dans \overline{K} égaux à l'identité sur K . D'après (5), pour tout i et j compris entre 1 et n , l'on a

$$(6) \quad \text{Tr}_{L/K}(e_i e_j) = \sum_{k=1}^n \sigma_k(e_i e_j) = \sum_{k=1}^n \sigma_k(e_i) \sigma_k(e_j).$$

Soit M la matrice dont l'élément de la i -ème ligne et de la j -ième colonne est $\sigma_i(e_j)$. Il résulte de (6) que ${}^t M M$ est la matrice qui représente la forme bilinéaire $\varphi_{L/K}$ dans la base (e_i) (où ${}^t M$ désigne la matrice transposée de M). Tout revient donc à montrer que le déterminant de M n'est pas nul. Supposons que ce déterminant soit nul. Dans ce cas, il existe une famille d'éléments $(\lambda_i)_{1 \leq i \leq n}$ de \overline{K} , non tous nuls, tels que, pour tout x dans L , l'on ait

$$(7) \quad \sum_{i=1}^n \lambda_i \sigma_i(x) = 0.$$

D'après le lemme suivant, cela conduit à une contradiction :

Lemme 3.4. (Dedekind) *Soient G un groupe, M un corps, et $(\psi_i)_{1 \leq i \leq n}$ une famille d'homomorphismes de groupes distincts de G à valeurs dans le groupe multiplicatif M^* .*

Alors, la famille $(\psi_i)_{1 \leq i \leq n}$ est libre dans le M -espace vectoriel des fonctions de G à valeurs dans M .

Démonstration : On choisit une égalité de la forme $\sum u_i \psi_i = 0$, où le nombre q des éléments u_i de M non nuls est minimum et au moins 1. On a donc pour tout $g \in G$, une égalité de la forme

$$(8) \quad \sum_{i=1}^q u_i \psi_i(g) = 0,$$

où tous les u_i sont non nuls. Puisque les ψ_i ne sont pas nuls, on a $q \geq 2$. Par ailleurs, pour tout h et g dans G , l'on a

$$\sum_{i=1}^q u_i \psi_i(hg) = \sum_{i=1}^q u_i \psi_i(g) \psi_i(h) = 0,$$

En multipliant (8) par $\psi_1(h)$ et en soustrayant, l'on obtient pour tout $g \in G$,

$$\sum_{i=2}^q u_i (\psi_1(h) - \psi_i(h)) \psi_i(g) = 0.$$

D'après le choix de q , pour tout i tel que $2 \leq i \leq q$, et tout $h \in G$, on doit avoir l'égalité $\psi_1(h) = \psi_i(h)$. On a donc $\psi_i = \psi_1$ pour tout i compris entre 2 et q , ce qui contredit le fait que les ψ_i soient distincts. D'où le lemme.

Cela termine la démonstration du théorème 3.1.

Corollaire 3.1. *Supposons que L/K soit une extension séparable. Soit $(e_i)_{1 \leq i \leq n}$ une base de L sur K . Alors, il existe une K -base $(e'_i)_{1 \leq i \leq n}$ de L et une seule telle que l'on ait*

$$\mathrm{Tr}_{L/K}(e_i e'_j) = \delta_{i,j},$$

où $\delta_{i,j}$ vaut 1 si $i = j$ et 0 sinon. On dit que $(e'_i)_{1 \leq i \leq n}$ est la base duale de $(e_i)_{1 \leq i \leq n}$ relativement à la forme bilinéaire $\varphi_{L/K}$.

Démonstration : D'après le th. 3.1, l'application Ψ de L dans son dual, qui à un élément x associe la forme linéaire $y \mapsto \varphi_{L/K}(x, y)$ est un isomorphisme de K -espaces vectoriels. Soit $(e_i^*)_{1 \leq i \leq n}$ la base duale de $(e_i)_{1 \leq i \leq n}$. Pour tout i entre 1 et n , posons $e'_i = \Psi^{-1}(e_i^*)$. Alors $(e'_i)_{1 \leq i \leq n}$ est une base de L qui possède la propriété voulue. Considérons par ailleurs une base $(\alpha_i)_{1 \leq i \leq n}$ de L , telle que pour tout i et j l'on ait $\mathrm{Tr}_{L/K}(e_i \alpha_j) = \delta_{i,j}$. Pour tout j tel que $1 \leq j \leq n$, les formes linéaires $y \mapsto \varphi_{L/K}(\alpha_j, y)$ et $y \mapsto \varphi_{L/K}(e'_j, y)$ coïncident sur les e_i . Elles sont donc égales, ce qui entraîne $\alpha_j = e'_j$ et le résultat.

II. Anneaux de Dedekind et extensions

On considère un anneau intègre A de corps des fractions K et L une extension finie de degré n de K . On note B la fermeture intégrale de A dans L . On suppose dans tout ce paragraphe que les conditions suivantes sont réalisées :

- 1) l'extension L/K est séparable ;
- 2) l'anneau A est intégralement clos.

Remarquons que le corps des fractions de B est L . En effet, si y est un élément de L , il existe $d \in A$, $d \neq 0$, tel que dy soit entier sur A i.e. tel que dy soit dans B , ce qui entraîne notre assertion.

Lemme 3.5. *Soit x un élément de B . Les éléments $N_{L/K}(x)$ et $\text{Tr}_{L/K}(x)$ appartiennent à A .*

Démonstration : Pour tout K -plongement σ_i de L dans \overline{K} , $\sigma_i(x)$ est un élément de \overline{K} qui est entier sur A . D'après le lemme 3.3, $N_{L/K}(x)$ et $\text{Tr}_{L/K}(x)$ sont donc aussi entiers sur A . Puisque ce sont des éléments de K et que A est intégralement clos, ils sont dans A .

Proposition 3.1. *Supposons de plus que A soit noethérien. Alors, B est un A -module de type fini.*

Démonstration : Soit $(y_i)_{1 \leq i \leq n}$ une K -base de L . Il existe un élément d de A tel que, pour tout i , dy_i appartienne à B . Posons $z_i = dy_i$. On obtient ainsi une base $(z_i)_{1 \leq i \leq n}$ de L/K formée d'entiers. Soit $(z'_i)_{1 \leq i \leq n}$ la base duale de $(z_i)_{1 \leq i \leq n}$ relativement à la forme $\varphi_{L/K}$ (cf. le cor. 3.1). Montrons que l'on a l'inclusion de A -modules

$$(9) \quad B \subseteq \sum_{i=1}^n Az'_i.$$

Considérons pour cela un élément x de B . Il existe des éléments x_j de K tel que l'on ait

$$x = \sum_{j=1}^n x_j z'_j.$$

Pour tout i entre 1 et n , l'élément xz_i est dans B et donc $\text{Tr}_{L/K}(xz_i)$ appartient à A (lemme 3.5). Or, étant donné un indice i compris entre 1 et n , l'on a

$$\text{Tr}_{L/K}(xz_i) = \text{Tr}_{L/K}\left(\sum_{j=1}^n x_j z'_j z_i\right) = \sum_{j=1}^n \text{Tr}_{L/K}(x_j z'_j z_i) = \sum_{j=1}^n x_j \text{Tr}_{L/K}(z'_j z_i) = x_i.$$

Ainsi x_i est dans A , ce qui établit l'inclusion (9). On déduit de là que B est contenu dans un A -module de type fini. Puisque A est noethérien, B est donc aussi un A -module de type fini. D'où la proposition.

Corollaire 3.2. *Si A est un anneau noethérien, il en est de même de B .*

Démonstration : Puisque B est un module de type fini sur A , qui est noethérien, B est un A -module noethérien. En particulier, les idéaux de B , qui sont des A -modules, sont de type fini sur A , donc aussi sur B . D'où le résultat.

Corollaire 3.3. *Supposons que A soit un anneau principal. Alors, B est un A -module libre de rang n .*

Démonstration : L'inclusion (9) montre en fait que B est contenu dans un A -module libre de rang n . D'après l'hypothèse faite sur A , B est donc aussi un A -module libre, dont le rang est $\leq n$. Or comme on l'a constaté dans la démonstration de la prop. 3.1, B contient une base de L/K . Cela entraîne que le rang de B sur A est au moins n , et il est donc égal à n .

On notera qu'une K -base de L contenue dans B n'est pas nécessairement une A -base de B : considérer par exemple le cas où $K = L = \mathbb{Q}$, $A = B = \mathbb{Z}$ et remarquer que 2 n'est pas une base du \mathbb{Z} -module \mathbb{Z} .

On en arrive maintenant au résultat principal de ce paragraphe :

Théorème 3.2. *Supposons que A soit un anneau de Dedekind. Alors, B est aussi un anneau de Dedekind.*

Démonstration : On sait déjà que B est noethérien (cor. 3.2). Par ailleurs, B est intégralement clos : si $x \in L$ (rappelons que L est le corps des fractions de B) est entier sur B , x est aussi entier sur A , car B est entier sur A . Donc x est dans B . Il reste à montrer que tous les idéaux premiers non nuls de B sont maximaux. Soient \mathfrak{P} un idéal premier non nul de B et x un élément non nul de \mathfrak{P} . Considérons une équation de dépendance intégrale de la forme $x^n + a_1x^{n-1} + \dots + a_0 = 0$, pour laquelle on choisit n minimum. On a donc $a_0 \neq 0$ et a_0 appartient à $\mathfrak{P} \cap A := \mathfrak{p}$. Puisque \mathfrak{p} est un idéal premier non nul de A , et que A est de Dedekind, \mathfrak{p} est un idéal maximal. Par ailleurs, A/\mathfrak{p} est un sous-corps de B/\mathfrak{P} , et B/\mathfrak{P} est entier sur A/\mathfrak{p} . Il en résulte que B/\mathfrak{P} est aussi un corps [†], et \mathfrak{P} est donc un idéal maximal de B . D'où le théorème.

On déduit des résultats précédents l'énoncé fondamental suivant :

[†] C'est une propriété des extensions entières d'anneaux : soit B un anneau intègre entier sur un sous-anneau A . Alors, B est un corps si et seulement si tel est le cas de A . En effet, supposons que B soit un corps. Soit a un élément non nul de A . Alors, a possède une inverse dans B , et en écrivant une équation de dépendance intégrale pour a^{-1} , on constate que $a^{-1} \in A$. Inversement, soit b un élément non nul de B . Si A est un corps, l'anneau $A[b]$ est un A -espace vectoriel de dimension finie (b est entier sur A). Puisque l'application de $A[b]$ dans $A[b]$ qui à x associe bx est A -linéaire injective (B est intègre et $b \neq 0$), elle est aussi surjective, et b est donc inversible dans B . D'où l'assertion.

Corollaire 3.4. Soient L une extension finie de \mathbb{Q} et B son anneau d'entiers (B est l'ensemble des éléments de L qui sont entiers sur \mathbb{Z}). Alors, B est un anneau de Dedekind et est un \mathbb{Z} -module libre de rang le degré de L sur \mathbb{Q} .

Démonstration : Il suffit d'appliquer le cor. 3.3 et le th. 3.2 avec $A = \mathbb{Z}$ et $K = \mathbb{Q}$ pour obtenir le résultat.

III. Ramification

On considère un anneau de Dedekind A , de corps des fractions K et une extension finie séparable L de K . Soit B la fermeture intégrale de A dans L . D'après le th. 3.2, B est un anneau de Dedekind.

Définition 3.2. Soient \mathfrak{P} un idéal premier non nul de B et \mathfrak{p} un idéal premier de A . On dit que \mathfrak{P} est au-dessus de \mathfrak{p} , ou bien que \mathfrak{P} divise \mathfrak{p} , si $\mathfrak{p} = \mathfrak{P} \cap A$. On écrit parfois $\mathfrak{P}|\mathfrak{p}$.

On notera que si \mathfrak{P} est un idéal premier non nul de B , $\mathfrak{P} \cap A$ est un idéal premier non nul de A (cf. dém. du th. 3.2). Rappelons par ailleurs, que si \mathfrak{p} est un idéal premier non nul de A , il existe un idéal premier de B qui le divise (cf. [Ma], p. 50).

Considérons maintenant un idéal premier non nul \mathfrak{p} de A . On notera $\mathfrak{p}B$ l'idéal de B engendré par \mathfrak{p} .

Lemme 3.6. Les idéaux premiers de B qui contiennent \mathfrak{p} (ou $\mathfrak{p}B$) sont exactement ceux qui divisent \mathfrak{p} .

Démonstration : Par définition, si \mathfrak{P} divise \mathfrak{p} , alors \mathfrak{P} contient \mathfrak{p} . Inversement, soit \mathfrak{P} un idéal premier de B qui contient \mathfrak{p} . Alors \mathfrak{p} est contenu dans $\mathfrak{P} \cap A$, et ils sont donc égaux, car ce sont deux idéaux maximaux de A . D'où le lemme.

On déduit de là que les idéaux premiers de B qui interviennent dans la décomposition de $\mathfrak{p}B$ en produit d'idéaux premiers, sont exactement ceux qui sont au-dessus de \mathfrak{p} (cf. chap II, th. 2.2). Étant donné un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , on notera $e_{\mathfrak{P}}$, ou bien $e_{\mathfrak{P}|\mathfrak{p}}$ si l'on veut préciser le corps de base K , l'exposant de \mathfrak{P} dans $\mathfrak{p}B$: on a ainsi

$$(10) \quad e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B) \geq 1,$$

et l'égalité

$$(11) \quad \mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}.$$

Si \mathfrak{P} est un idéal premier de B qui divise \mathfrak{p} , le corps B/\mathfrak{P} est une extension finie de A/\mathfrak{p} (cf. la prop. 3.1). On notera $f_{\mathfrak{P}}$ le degré de cette extension, ou $f_{\mathfrak{P}|\mathfrak{p}}$ si l'on veut préciser le corps K .

Terminologie. L'entier $e_{\mathfrak{P}}$ est appelé l'indice de ramification de \mathfrak{P} dans l'extension L/K . L'entier $f_{\mathfrak{P}}$ est appelé le degré résiduel de \mathfrak{P} dans l'extension L/K . Si $e_{\mathfrak{P}} = 1$ et si B/\mathfrak{P} est une extension séparable de A/\mathfrak{p} , on dit que L/K est non ramifiée en \mathfrak{P} . S'il n'existe qu'un seul idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} et que $f_{\mathfrak{P}} = 1$, on dit que L/K est totalement ramifiée en \mathfrak{p} . On dit que l'idéal premier \mathfrak{p} de A se ramifie dans l'extension L/K s'il existe un idéal premier \mathfrak{P} de B ramifié au-dessus de \mathfrak{p} .

Soit \mathfrak{P} un idéal premier de B au-dessus de \mathfrak{p} . L'anneau $B/\mathfrak{p}B$ contient un sous-corps isomorphe à A/\mathfrak{p} . En effet, le morphisme d'anneaux naturel $A \rightarrow B/\mathfrak{p}B$ a pour noyau $A \cap \mathfrak{p}B$; or \mathfrak{p} est contenu dans $A \cap \mathfrak{p}B$ et $A \cap \mathfrak{p}B$ est contenu dans $A \cap \mathfrak{P} = \mathfrak{p}$, de sorte que l'on a $A \cap \mathfrak{p}B = \mathfrak{p}$. L'anneau $B/\mathfrak{p}B$ est ainsi muni d'une structure de A/\mathfrak{p} -algèbre, et sa dimension est finie car B est de type fini sur A (prop. 3.1). L'anneau $B/\mathfrak{P}^{e_{\mathfrak{P}}}$ possède la même propriété, comme on le constate en considérant la flèche naturelle $A \rightarrow B/\mathfrak{P}^{e_{\mathfrak{P}}}$ de noyau $\mathfrak{p} = A \cap \mathfrak{P}^{e_{\mathfrak{P}}} (\mathfrak{p} = A \cap \mathfrak{p}B \subseteq A \cap \mathfrak{P}^{e_{\mathfrak{P}}} \subseteq A \cap \mathfrak{P} = \mathfrak{p})$. (On peut aussi considérer l'homomorphisme canonique $A/\mathfrak{p} \rightarrow B/\mathfrak{p}B \rightarrow B/\mathfrak{P}^{e_{\mathfrak{P}}}$).

Notons alors n le degré de l'extension L/K .

Théorème 3.3. Soit \mathfrak{p} un idéal premier non nul de A . Alors, l'anneau $B/\mathfrak{p}B$ est une A/\mathfrak{p} -algèbre de dimension n , qui est isomorphe au produit $\prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$. On a l'égalité

$$(12) \quad n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Démonstration : On va utiliser le lemme suivant :

Lemme 3.7. Soient K_1 et K_2 deux corps, M_1 et M_2 deux anneaux et $\varphi_1 : K_1 \rightarrow M_1$, $\varphi_2 : K_2 \rightarrow M_2$, deux homomorphismes d'anneaux : M_1 (resp. M_2) est ainsi muni d'une structure d'algèbre sur K_1 (resp. sur K_2). On suppose qu'il existe des isomorphismes d'anneaux $f : K_1 \rightarrow K_2$ de K_1 sur K_2 , et $g : M_1 \rightarrow M_2$ de M_1 sur M_2 , tels que l'on ait $\varphi_2 \circ f = g \circ \varphi_1$. Alors, M_1 est de dimension finie sur K_1 si et seulement si tel est le cas de la K_2 -algèbre M_2 . De plus, leurs dimensions sont les mêmes.

Démonstration : On vérifie directement ce lemme par transport de structure au moyen de f et g .

1) Montrons que la dimension du A/\mathfrak{p} -espace $B/\mathfrak{p}B$ est n . L'idée est de se ramener, par localisation, à prouver cette assertion lorsque A est un anneau principal.

Posons pour cela $S = A \setminus \mathfrak{p}$: S est une partie multiplicative de B . On a l'inclusion $\mathfrak{p}B \subseteq \mathfrak{p}B.S^{-1}B \cap B$. On a ainsi un homomorphisme d'anneaux

$$g : B/\mathfrak{p}B \rightarrow S^{-1}B/\mathfrak{p}B.S^{-1}B,$$

défini par

$$g(x + \mathfrak{p}B) = \frac{x}{1} + \mathfrak{p}B.S^{-1}B.$$

Montrons que g est un isomorphisme. Prouvons d'abord qu'il est injectif, autrement dit que l'on a l'égalité

$$(6) \quad \mathfrak{p}B.S^{-1}B \cap B = \mathfrak{p}B.$$

Considérons un élément u de $\mathfrak{p}B.S^{-1}B \cap B$. On a $u = \alpha/s$, où $\alpha \in \mathfrak{p}B$ et $s \in S$: on a $\alpha = su$. Il s'agit de montrer que u appartient à $\mathfrak{p}B$. On remarque pour cela, que pour tout idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , l'exposant $v_{\mathfrak{P}}(s)$ de s dans \mathfrak{P} est nul (car s n'appartient pas à \mathfrak{p}). Ainsi, pour tout idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , l'on a $v_{\mathfrak{P}}(u) = v_{\mathfrak{P}}(\alpha)$, et cela entraîne que u est dans $\mathfrak{p}B$ (cf. Chap. II, lemme 2.5, assertion b)). D'où l'égalité (6).

Montrons maintenant que g est surjectif. Soit $x = b/s$ un élément de $S^{-1}B$. Les idéaux maximaux de l'anneau $B/\mathfrak{p}B$ correspondent aux idéaux maximaux de B qui contiennent $\mathfrak{p}B$, autrement dit, correspondent aux idéaux premiers de B au-dessus de \mathfrak{p} (lemme 3.6). Puisque s n'est pas dans \mathfrak{p} , s n'appartient à aucun de ces idéaux premiers, et s est donc inversible modulo $\mathfrak{p}B$. Il existe donc un élément c de B tel que l'on ait $cs \equiv 1 \pmod{\mathfrak{p}B}$. Ainsi $(b/s) - bc = (b/s)(1 - cs)$ appartient à $\mathfrak{p}B.S^{-1}B$. On a par conséquent l'égalité $g(bc + \mathfrak{p}B) = x + \mathfrak{p}B.S^{-1}B$. D'où notre assertion, et le fait que g soit un isomorphisme d'anneaux.

De même, on dispose d'un homomorphisme d'anneaux

$$f : A/\mathfrak{p} \rightarrow S^{-1}A/\mathfrak{p}.S^{-1}A,$$

qui à $a + \mathfrak{p}$ associe $(a/1) + \mathfrak{p}.S^{-1}A$. On a $\mathfrak{p}.S^{-1}A \cap A = \mathfrak{p}$ et l'on montre comme précédemment que f est surjectif, autrement dit que f est un isomorphisme.

Notons alors

$$i : A/\mathfrak{p} \rightarrow B/\mathfrak{p}B \quad \text{et} \quad j : S^{-1}A/\mathfrak{p}.S^{-1}A \rightarrow S^{-1}B/\mathfrak{p}B.S^{-1}B,$$

les applications naturelles qui munissent $B/\mathfrak{p}B$ (resp. $S^{-1}B/\mathfrak{p}B.S^{-1}B$) d'une structure de A/\mathfrak{p} -algèbre (resp. d'une structure de $S^{-1}A/\mathfrak{p}.S^{-1}A$ -algèbre). On vérifie immédiatement que l'on a

$$j \circ f = g \circ i.$$

D'après le lemme 3.7 tout revient donc à prouver que la dimension de $S^{-1}B/\mathfrak{p}B.S^{-1}B$ sur le corps $S^{-1}A/\mathfrak{p}.S^{-1}A$ est finie égale à n . On utilise pour cela le fait que $S^{-1}A$ est un anneau principal (prop. 2.1 du chap. II) et que $S^{-1}B$ est la fermeture intégrale de $S^{-1}A$ dans L . D'après le corollaire 3.3, $S^{-1}B$ est donc un $S^{-1}A$ -module libre de rang n , ce qui entraîne le résultat [†]. D'où l'assertion 1).

2) Démontrons maintenant l'égalité (12). Si \mathfrak{P} et \mathfrak{P}' sont deux idéaux premiers distincts de B au-dessus de \mathfrak{p} , les idéaux $\mathfrak{P}^{e_{\mathfrak{P}}}$ et $\mathfrak{P}'^{e_{\mathfrak{P}'}}$ sont comaximaux. Il en résulte que l'homomorphisme naturel

$$B \rightarrow \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}},$$

a pour noyau $\mathfrak{p}B$ (i.e. l'intersection des $\mathfrak{P}^{e_{\mathfrak{P}}}$). D'après le théorème Chinois, il est surjectif. On déduit de là que l'application

$$B/\mathfrak{p}B \rightarrow \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}},$$

qui à $x + \mathfrak{p}B$ associe l'élément $(x + \mathfrak{P}^{e_{\mathfrak{P}}})_{\mathfrak{P}|\mathfrak{p}}$ est un isomorphisme de A/\mathfrak{p} -algèbres.

Notons alors $n_{\mathfrak{P}}$ la dimension de la A/\mathfrak{p} -algèbre $B/\mathfrak{P}^{e_{\mathfrak{P}}}$. D'après l'assertion 1), on a l'égalité

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} n_{\mathfrak{P}}.$$

Par ailleurs, il résulte de la remarque qui suit le lemme 2.6 du chapitre II, que pour tout entier $i \geq 0$, les A/\mathfrak{p} -espaces vectoriels $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ et B/\mathfrak{P} sont isomorphes. Or pour tout $i \geq 1$ on a la suite exacte de A/\mathfrak{p} -algèbres

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

On déduit de là que l'on a

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

Cela termine la démonstration du théorème.

Corollaire 3.5. *Le nombre d'idéaux premiers de B au-dessus de \mathfrak{p} est compris entre 1 et n . En particulier, si A ne possède qu'un nombre fini d'idéaux premiers, il en est de même de B , qui est dans ce cas un anneau principal.*

Démonstration : C'est une conséquence directe du th. 3.3 et du cor. 2.3.

Étant donnés un élément x de K , un idéal premier non nul \mathfrak{p} de A et un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , on a

$$(13) \quad v_{\mathfrak{P}}(x) = e_{\mathfrak{P}} v_{\mathfrak{p}}(x).$$

[†] Soient B un anneau et A un sous-anneau de B , tels que B soit un A -module libre de rang n . Alors, si I un idéal de A , B/IB est un A/I -module libre de rang n . Si $(e_i)_{1 \leq i \leq n}$ est une A -base de B , on montre que $(e_i + IB)_{1 \leq i \leq n}$ est une A/I -base de B/IB : en effet, c'est clairement un système générateur. Par ailleurs, si l'on a une égalité de la forme $\sum (a_i + I)(e_i + IB) = 0$, la somme des $a_i e_i$ est dans IB . Il existe donc des éléments b_i de I tels que l'on ait $\sum a_i e_i = \sum b_i e_i$, et les a_i sont donc dans I . D'où notre assertion

On dit que la valuation $v_{\mathfrak{P}}$ prolonge $v_{\mathfrak{p}}$ avec l'indice (de ramification) $e_{\mathfrak{P}}$. On montrera plus loin que si w est une valuation discrète sur B qui prolonge $v_{\mathfrak{p}}$ avec l'indice e , il existe un diviseur premier \mathfrak{P} de B tel que $w = v_{\mathfrak{P}}$ et $e = e_{\mathfrak{P}}$.

IV. Cas des extensions galoisiennes

Conservons les notations du paragraphe III et les hypothèses faites sur A , K et L : A est un anneau de Dedekind de corps des fractions K et L/K est une extension finie séparable de degré n . On suppose de plus dans ce paragraphe que l'extension L/K est **galoisienne**. On notera $\text{Gal}(L/K)$ le groupe de Galois de cette extension.

Proposition 3.2. *Soit \mathfrak{p} un idéal premier de A . Le groupe $\text{Gal}(L/K)$ opère transitivement sur l'ensemble des idéaux premiers de B au-dessus de \mathfrak{p} .*

Démonstration : D'abord il est clair que $\text{Gal}(L/K)$ opère sur l'ensemble des idéaux premiers de B au-dessus de \mathfrak{p} : en effet, si \mathfrak{P} est l'un d'entre eux et si $\sigma \in \text{Gal}(L/K)$, $\sigma(\mathfrak{P})$ est aussi un idéal premier de B et l'on a $\sigma(\mathfrak{P}) \cap A = \mathfrak{p}$ (car $\mathfrak{p} = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{P}) \cap A$). Considérons maintenant un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , et supposons qu'il existe un idéal premier \mathfrak{P}' de B au-dessus de \mathfrak{p} , qui soit distinct de $\sigma(\mathfrak{P})$, pour tout σ dans $\text{Gal}(L/K)$. D'après le théorème d'approximation (th. 2.3), il existe un élément a dans \mathfrak{P}' qui n'est pas dans $\sigma(\mathfrak{P})$ pour tout σ dans $\text{Gal}(L/K)$. Posons alors $x = N_{L/K}(a)$. D'après le lemme 3.3, on a

$$x = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(a).$$

On déduit de là que x n'est pas dans \mathfrak{P} et que x appartient à \mathfrak{P}' . Cela conduit à une contradiction, car x est dans A et l'on a $\mathfrak{P} \cap A = \mathfrak{P}' \cap A$. D'où le résultat.

Corollaire 3.6. *Soit \mathfrak{p} un idéal premier non nul de A . Pour tout idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} , les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de \mathfrak{p} : on peut ainsi les noter $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$. Si $g_{\mathfrak{p}}$ désigne le nombre d'idéaux premiers de B au-dessus de \mathfrak{p} , on a l'égalité*

$$(14) \quad n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}.$$

Démonstration : Soient \mathfrak{P} un idéal premier de B au-dessus de \mathfrak{p} et σ un élément de $\text{Gal}(L/K)$. On remarque d'abord que $\sigma(\mathfrak{P})$ apparaît dans la décomposition de $\mathfrak{p}B$ en produit d'idéaux premiers avec l'exposant $e_{\mathfrak{P}}$. D'après la prop. 3.2, tous les exposants $e_{\mathfrak{P}}$ intervenant dans cette décomposition sont donc les mêmes. Par ailleurs, l'application

$$B/\mathfrak{P} \rightarrow B/\sigma(\mathfrak{P}),$$

qui à $x + \mathfrak{P}$ associe $\sigma(x) + \sigma(\mathfrak{P})$ est un isomorphisme de A/\mathfrak{p} -espaces vectoriels (cette application est bien définie car B est stable par $\text{Gal}(L/K)$). Là encore, on déduit de la

prop. 3.2 que les entiers $f_{\mathfrak{P}}$ ne dépendent que de \mathfrak{p} . L'égalité (14) résulte alors directement de la formule (12). D'où le résultat.

Définition 3.2. Soit \mathfrak{P} un idéal premier non nul de B . Le sous-ensemble de $\text{Gal}(L/K)$ formé des éléments σ tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$, est un sous-groupe de $\text{Gal}(L/K)$, et est appelé le sous-groupe de décomposition de \mathfrak{P} dans l'extension L/K . On le note souvent $D_{\mathfrak{P}}(L/K)$, ou D s'il n'y a pas d'ambiguïté.

Lemme 3.8. Soient \mathfrak{P} et \mathfrak{P}' deux idéaux premiers de B au-dessus d'un même idéal premier non nul de A . Alors, les sous-groupes de décomposition $D_{\mathfrak{P}}(L/K)$ et $D_{\mathfrak{P}'}(L/K)$ sont conjugués dans $\text{Gal}(L/K)$. En fait, si σ est un élément de $\text{Gal}(L/K)$ tel que $\sigma(\mathfrak{P}) = \mathfrak{P}'$, l'on a l'égalité

$$(15) \quad \sigma D_{\mathfrak{P}}(L/K) \sigma^{-1} = D_{\mathfrak{P}'}(L/K).$$

En particulier, si l'extension L/K est abélienne, on a $D_{\mathfrak{P}}(L/K) = D_{\mathfrak{P}'}(L/K)$, et le groupe de décomposition de \mathfrak{P} ne dépend que de $\mathfrak{P} \cap A$.

Démonstration : Il suffit de vérifier l'inclusion $\sigma D_{\mathfrak{P}}(L/K) \sigma^{-1} \subseteq D_{\mathfrak{P}'}(L/K)$, ce qui est immédiat.

Considérons maintenant un idéal premier non nul fixé \mathfrak{P} de B . Posons $\mathfrak{p} = \mathfrak{P} \cap A$. D'après le théorème de correspondance de Galois, le groupe de décomposition D de \mathfrak{P} correspond à une extension K_D de K contenue dans L (qui n'est en général pas une extension galoisienne de K).

Lemme 3.9. Avec les notations du corollaire 3.6, l'on a

$$(16) \quad [K_D : K] = g_{\mathfrak{p}} \quad \text{et} \quad |D| = e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Démonstration : On considère l'opération de $\text{Gal}(L/K)$ sur l'ensemble des idéaux premiers de B au-dessus de \mathfrak{p} . Pour cette action le stabilisateur de \mathfrak{P} est D . Par ailleurs, l'orbite de \mathfrak{P} est l'ensemble de tous les idéaux premiers au-dessus de \mathfrak{p} (prop. 3.2). Cette orbite est donc de cardinal $g_{\mathfrak{p}}$. On déduit de là l'égalité $n = g_{\mathfrak{p}} |D|$. Le lemme résulte alors de la formule (14) et de la théorie de Galois.

Posons alors $k = A/\mathfrak{p}$ et $l = B/\mathfrak{P}$. Ce sont les corps résiduels de A en \mathfrak{p} et de B en \mathfrak{P} . Puisque B est de type fini sur A (prop. 3.1), l est une extension finie de k de degré $f_{\mathfrak{p}}$, que l'on identifiera à un sur-corps de k (autrement dit, on identifie k et son image dans l). Cette extension n'est pas nécessairement galoisienne. Néanmoins :

Lemme 3.10. *L'extension l/k est normale (on dit aussi que l'extension l/k est quasi-galoisienne).*

Démonstration : Soit \overline{H} un polynôme irréductible à coefficients dans k possédant une racine $\alpha = a + \mathfrak{P}$ dans l . Il s'agit de montrer que toutes les racines de \overline{H} sont dans l . On considère pour cela le polynôme

$$P = \prod_{\sigma \in \text{Gal}(L/K)} (X - \sigma(a)).$$

C'est un polynôme à coefficients dans A dont a est racine. Soit \overline{P} le polynôme de $k[X]$ déduit de P en réduisant ses coefficients modulo \mathfrak{p} . On a $\overline{P}(\alpha) = 0$ et toutes les racines de \overline{P} sont dans l (ce sont les $\sigma(a) + \mathfrak{P}$, où σ parcourt $\text{Gal}(L/K)$). Or \overline{H} étant le polynôme minimal de α sur k , il doit diviser \overline{P} , ce qui entraîne notre assertion.

À chaque élément σ de D , on peut associer un homomorphisme de corps $\overline{\sigma}$ de l dans l défini, pour tout $x \in B$, par l'égalité

$$(17) \quad \overline{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}.$$

(B est stable par $\text{Gal}(L/K)$, et par définition de D , si $x \equiv y \pmod{\mathfrak{P}}$, l'on a la congruence $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{P}}$, de sorte que $\overline{\sigma}$ est bien une application). Puisque $\overline{\sigma}$ fixe les éléments de k , $\overline{\sigma}$ est un élément de $\text{Gal}(l/k)$. On obtient ainsi une application

$$\varepsilon : D \rightarrow \text{Gal}(l/k),$$

définie, pour tout σ de D , par l'égalité

$$(18) \quad \varepsilon(\sigma) = \overline{\sigma}.$$

L'application ε est un homomorphisme de groupes.

Définition 3.3. *Le noyau de ε est appelé le sous-groupe d'inertie de \mathfrak{P} dans l'extension L/K . On le note souvent $I_{\mathfrak{P}}(L/K)$, ou I s'il n'y a pas d'ambiguïté. C'est un sous-groupe distingué de D .*

D'après la théorie de Galois, il correspond à I une extension galoisienne K_I de K_D contenue dans L . On a $\text{Gal}(L/K_I) = I$ et le groupe de Galois de K_I sur K_D est isomorphe à D/I . On a de façon analogue au lemme 4.2 :

Lemme 3.11. *Soient \mathfrak{P}' un idéal premier de B au-dessus de \mathfrak{p} . Alors, les sous-groupes d'inertie $I_{\mathfrak{P}}(L/K)$ et $I_{\mathfrak{P}'}(L/K)$ sont conjugués dans $\text{Gal}(L/K)$. En fait, si σ est un élément de $\text{Gal}(L/K)$ tel que $\sigma(\mathfrak{P}) = \mathfrak{P}'$, l'on a l'égalité*

$$(19) \quad \sigma I_{\mathfrak{P}}(L/K) \sigma^{-1} = I_{\mathfrak{P}'}(L/K).$$

En particulier, si l'extension L/K est abélienne, l'on a $I_{\mathfrak{P}}(L/K) = I_{\mathfrak{P}'}(L/K)$, et le groupe d'inertie de \mathfrak{P} ne dépend que de \mathfrak{p} .

Proposition 3.3. *L'application $\varepsilon : D \rightarrow \text{Gal}(l/k)$ passée au quotient réalise un isomorphisme de groupes de D/I sur $\text{Gal}(l/k)$.*

Démonstration : Il s'agit de montrer que ε est surjective. Considérons pour cela un élément u de $\text{Gal}(l/k)$.

Supposons d'abord l'extension l/k séparable. Soit α un élément primitif non nul de l sur k : on a $l = k(\alpha)$. Il résulte du théorème d'approximation l'existence d'un représentant a de α qui appartienne à tous les $\sigma(\mathfrak{P})$ pour tout σ en dehors de D (on écrit $\alpha = b + \mathfrak{P}$ et il existe $a \in B$ tel que l'on ait $a \equiv b \pmod{\mathfrak{P}}$ et $a \equiv 0 \pmod{\sigma(\mathfrak{P})}$, pour $\sigma \notin D$). Considérons (comme dans le lemme 3.10) le polynôme

$$P = \prod_{\sigma \in \text{Gal}(L/K)} (X - \sigma(a)).$$

D'après le choix de a , les racines non nulles du polynôme \overline{P} déduit de P par réduction modulo \mathfrak{P} , sont les $\sigma(a) + \mathfrak{P} = \overline{\sigma}(a + \mathfrak{P})$ pour les éléments σ qui sont dans D (puisque a n'est pas dans \mathfrak{P} , on a $\sigma(a) + \mathfrak{P} = 0$ si et seulement si $\sigma \notin D$). En particulier, les racines du polynôme minimal de α sur k sont des éléments de la forme $\overline{\sigma}(a + \mathfrak{P})$, où σ est dans D . Il existe donc σ dans D tel que l'on ait $u(a + \mathfrak{P}) = \overline{\sigma}(a + \mathfrak{P})$. On a donc $u = \overline{\sigma}$, ce qui prouve que ε est surjective. D'où le résultat si l/k est séparable.

Si l'on ne suppose plus l/k séparable, on considère la fermeture séparable l_s de k dans l , i.e. la plus grande extension séparable de k contenue dans l . En choisissant ensuite un élément primitif de l'extension l_s/k , l'on montre, comme ci-dessus, l'existence d'un élément σ de D tel que $\overline{\sigma}$ coïncide avec u sur l_s . On utilise alors le fait que les restrictions de u et $\overline{\sigma}$ à l_s se prolongent de façon unique en un élément de $\text{Gal}(l/k)$. D'où $u = \overline{\sigma}$, et le résultat.

Corollaire 3.7. *Supposons l'extension l/k séparable. Avec les notations du corollaire 3.6, on a l'égalité*

$$(20) \quad |I| = e_{\mathfrak{p}}.$$

En particulier, l'extension L/K est non ramifiée en \mathfrak{P} (donc aussi en tous les idéaux premiers de B au-dessus de \mathfrak{p}) si et seulement si l'on a $|I| = 1$.

Démonstration : D'après l'hypothèse faite et le lemme 3.10, l'extension l/k est galoisienne. Il en résulte que l'ordre du groupe $\text{Gal}(l/k)$ est $f_{\mathfrak{p}}$. Le lemme 3.9 et la prop. 3.3 entraînent alors le résultat.

Terminons ce chapitre en définissant ce que l'on appelle la substitution de Frobenius en un idéal premier \mathfrak{P} de B non ramifié.

V. Substitution de Frobenius

On se place toujours dans la situation envisagée au début du paragraphe IV, et l'on conserve sans autre précision les notations déjà utilisées. On considère un idéal premier non nul \mathfrak{P} de B et l'on pose $\mathfrak{p} = \mathfrak{P} \cap A$. On suppose de plus dans la suite que les conditions suivantes sont réalisées :

$$(21) \quad \text{l'extension } L/K \text{ est non ramifiée en } \mathfrak{P} \quad \text{et} \quad A/\mathfrak{p} \text{ est un corps fini.}$$

Soit q le cardinal de A/\mathfrak{p} . D'après la prop. 3.3 et le cor. 3.7, le groupe d'inertie en \mathfrak{P} est réduit à l'élément neutre, et le groupe de décomposition $D_{\mathfrak{P}}(L/K)$ est isomorphe au groupe de Galois $\text{Gal}(l/k)$ des corps résiduels (rappelons que $l = B/\mathfrak{P}$ et $k = A/\mathfrak{p}$). Le corps l est fini de cardinal $q^{f_{\mathfrak{P}}}$, et le groupe de Galois $\text{Gal}(l/k)$ est cyclique, engendré par l'application $x \mapsto x^q$, qui est appelée, automorphisme de Frobenius de l'extension l/k . Il en résulte que le groupe $D_{\mathfrak{P}}(L/K)$ est aussi cyclique. Soit $s_{\mathfrak{P}}$ l'élément de $D_{\mathfrak{P}}(L/K)$ défini par l'égalité

$$(22) \quad \varepsilon(s_{\mathfrak{P}}) = \{x \mapsto x^q\}.$$

Alors, $s_{\mathfrak{P}}$ est un générateur de $D_{\mathfrak{P}}(L/K)$, et il est caractérisé [†] par la propriété suivante :

$$(23) \quad s_{\mathfrak{P}}(b) \equiv b^q \pmod{\mathfrak{P}} \quad \text{pour tout } b \in B.$$

Définition 3.4. L'élément $s_{\mathfrak{P}}$ est appelé la substitution de Frobenius en \mathfrak{P} (ou de \mathfrak{P}) de l'extension L/K . On le note parfois $(\mathfrak{P}, L/K)$.

Considérons une extension E de K contenue dans L (L est une extension galoisienne de E). Posons $\mathfrak{P}_E = \mathfrak{P} \cap E$. Soit $f_{\mathfrak{P}_E}$ le degré sur k du corps résiduel de E en l'idéal \mathfrak{P}_E . On notera que l'idéal \mathfrak{P} est non ramifié dans l'extension L/E . On peut ainsi considérer la substitution de Frobenius $(\mathfrak{P}, L/E)$ qui est un élément du groupe de décomposition $D_{\mathfrak{P}}(L/K)$.

Lemme 3.12. a) On a $(\mathfrak{P}, L/E) = (\mathfrak{P}, L/K)^{f_{\mathfrak{P}_E}}$.

[†] Si s_1 et s_2 sont deux éléments de $\text{Gal}(L/K)$ tels que pour tout $b \in B$, l'on ait la congruence $s_1(b) \equiv s_2(b) \pmod{\mathfrak{P}}$, alors $s_1 = s_2$. En effet, si $u \in s_1^{-1}(\mathfrak{P})$, on a $s_1(u) \in \mathfrak{P}$ et la congruence précédente entraîne que $u \in s_2^{-1}(\mathfrak{P})$. Par conséquent $s_2 s_1^{-1}$ appartient à $D_{\mathfrak{P}}(L/K)$. Par ailleurs, pour tout $b \in B$, $s_1^{-1}(b)$ est aussi dans B , et l'on a

$$s_2 s_1^{-1}(b) = s_2(s_1^{-1}(b)) \equiv s_1(s_1^{-1}(b)) \equiv b \pmod{\mathfrak{P}}.$$

La prop. 3.3 entraîne alors que $s_1 = s_2$.

b) Supposons que E soit une extension galoisienne de K . Alors, l'image de $(\mathfrak{P}, L/K)$ dans le groupe de Galois $\text{Gal}(E/K)$ (autrement dit la restriction de $(\mathfrak{P}, L/K)$ à E) est $(\mathfrak{P}_E, E/K)$.

c) Soit σ un élément de $\text{Gal}(L/K)$. On a

$$(24) \quad (\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}.$$

Démonstration : a) D'après (23), pour tout élément b de B , l'on a

$$(\mathfrak{P}, L/K)^{f_{\mathfrak{P}_E}}(b) \equiv b^{q^{f_{\mathfrak{P}_E}}} \equiv (\mathfrak{P}, L/E)(b) \pmod{\mathfrak{P}},$$

ce qui entraîne l'assertion a).

b) On remarque d'abord que la restriction de $(\mathfrak{P}, L/K)$ à E est un élément du sous-groupe de décomposition $D_{\mathfrak{P}_E}(E/K)$, en \mathfrak{P}_E , de $\text{Gal}(E/K)$. Pour tout c dans la fermeture intégrale de A dans E , on a

$$(\mathfrak{P}, L/K)(c) \equiv c^q \equiv (\mathfrak{P}_E, E/K)(c) \pmod{\mathfrak{P}_E},$$

ce qui prouve l'assertion b).

c) Pour tout $b \in B$, on a

$$(\mathfrak{P}, L/K)\sigma^{-1}(b) \equiv \sigma^{-1}(b)^q \pmod{\mathfrak{P}},$$

ce qui implique

$$\sigma(\mathfrak{P}, L/K)\sigma^{-1}(b) \equiv b^q \pmod{\sigma(\mathfrak{P})}.$$

D'où l'assertion c) et le lemme.

Supposons de plus l'extension L/K abélienne. D'après l'assertion c) du lemme 3.12, la substitution de Frobenius $(\mathfrak{P}, L/K)$ ne dépend en fait que de \mathfrak{p} . On la note alors $(\mathfrak{p}, L/K)$, et on l'appelle le symbole d'Artin de \mathfrak{p} . On étend par multiplicativité la définition du symbole d'Artin à tous les idéaux de A , dont la décomposition en produit d'idéaux premiers ne fait intervenir que des idéaux non ramifiés dans L . Signalons que si de plus K est un corps de nombres, l'on peut démontrer que tout élément de $\text{Gal}(L/K)$ est de la forme $(\mathfrak{p}, L/K)$ pour une infinité d'idéaux premiers \mathfrak{p} de A .

Exemple. Soit d un entier sans facteur carré. Prenons $A = \mathbb{Z}$ et $L = \mathbb{Q}(\sqrt{d})$. On a $K = \mathbb{Q}$ et B est ici l'anneau d'entiers de L , qui est un anneau de Dedekind. Soit p un nombre premier. Si pB est un idéal premier de B , ce qui correspond au cas où $e_p = g_p = 1$, la substitution de Frobenius $(p, L/K)$ est l'élément non trivial de $\text{Gal}(L/K)$. On dit dans ce cas que p est inerte dans L . Si l'on a $e_p = 1$ et $g_p = 2$, $(p, L/K)$ est l'automorphisme identité. On dit alors que p est décomposé (totalement) dans L .

Chapitre IV — Discriminant et ramification

Étant donné un anneau de Dedekind A de corps des fractions K , L une extension finie séparable de K et B la fermeture intégrale de A dans L , on a défini au chapitre III la notion d'indice de ramification d'un idéal premier \mathfrak{P} de B , qui est un entier $e_{\mathfrak{P}} \geq 1$. La question qui se pose est alors la suivante :

Question. *Quels sont les idéaux premiers \mathfrak{P} de B tels que $e_{\mathfrak{P}} > 1$? En particulier, quels sont les nombres premiers p de \mathbb{Z} qui se ramifient dans une extension finie donnée de \mathbb{Q} ?*

Comme on le constatera, il n'y en a en fait qu'un nombre fini. L'objectif de ce chapitre est l'étude de cette question. On va introduire pour cela la notion de discriminant $\delta_{B/A}$ de B sur A ou de l'extension L/K : $\delta_{B/A}$ est un idéal de A dont les diviseurs premiers \mathfrak{p} sont exactement ceux pour lesquels il existe un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} tel que $e_{\mathfrak{P}} > 1$.

I. Discriminant

On considère un anneau A (pas nécessairement de Dedekind) et un anneau B qui contient A . On suppose que B est un A -module libre de rang fini n . Étant donné un élément x de B , soit m_x l'homomorphisme du A -module B de multiplication par x . Comme dans le chapitre III, on définit la trace $\text{Tr}_{B/A}(x)$ et la norme $N_{B/A}(x)$ de x relativement à B et A , comme étant la trace et le déterminant de m_x . Ce sont des éléments de A .

Définition 4.1. *Soit $(x_i)_{1 \leq i \leq n}$ un élément de B^n . On appelle discriminant du système $(x_i)_{1 \leq i \leq n}$ l'élément $D(x_1, \dots, x_n)$ de A donné par la formule*

$$(1) \quad D(x_1, \dots, x_n) = \det \left((\text{Tr}_{B/A}(x_i x_j))_{i,j} \right).$$

Lemme 4.1. *Soient $(x_i)_{1 \leq i \leq n}$ et $(y_i)_{1 \leq i \leq n}$ deux éléments de B^n tels que, pour tout i compris entre 1 et n , l'on ait*

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

Alors, on a l'égalité

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

Démonstration : Soit M la matrice carrée (n, n) dont l'élément de la i -ème ligne et de la j -ième colonne est a_{ij} . Pour tout p et q on a

$$\text{Tr}_{B/A}(y_p y_q) = \sum_{i,j} a_{pi} a_{qj} \text{Tr}_{B/A}(x_i x_j).$$

On déduit de là l'égalité matricielle

$$(\mathrm{Tr}_{B/A}(y_p y_q))_{p,q} = M (\mathrm{Tr}_{B/A}(x_i x_j))_{i,j} {}^t M,$$

où ${}^t M$ est la matrice transposée de M . Cela entraîne le lemme.

On déduit du lemme 4.1 que les discriminants des bases de B sur A sont associées dans A (i.e. diffèrent multiplicativement par une unité de A). Cela permet de poser la définition suivante :

Définition 4.2. On appelle discriminant de B sur A , et on notera $\delta_{B/A}$, l'idéal principal de A engendré par le discriminant de n'importe quelle base de B sur A .

Le lemme 4.1 permet aussi de définir la notion de discriminant (absolu) d'un corps de nombres K , i.e. d'une extension finie de \mathbb{Q} : soit A l'anneau d'entiers de K . On a vu au chapitre III que A est un \mathbb{Z} -module libre de rang le degré de K sur \mathbb{Q} . Les discriminants des \mathbb{Z} -bases de A diffèrent multiplicativement par un carré inversible dans \mathbb{Z} , qui ne peut être que 1. Ces discriminants sont donc égaux.

Définition 4.3. On appelle discriminant de K , le discriminant de n'importe quelle base de A sur \mathbb{Z} (c'est en particulier un entier relatif).

Remarque. Les discriminants d'un système d'éléments de A , relativement à A et \mathbb{Z} , et relativement à K et \mathbb{Q} , sont égaux : cela provient du fait qu'une \mathbb{Z} -base de A est une \mathbb{Q} -base de K , et donc que pour tout $\alpha \in A$, l'on a $\mathrm{Tr}_{A/\mathbb{Z}}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.

II. Quelques propriétés de $\delta_{B/A}$

On considère, comme dans le paragraphe I, deux anneaux A et B tels que B contienne A et que B soit un A -module libre de rang n .

Lemme 4.2. Supposons que $\delta_{B/A}$ contienne un élément qui n'est pas diviseur de zéro. Pour qu'un élément $(x_i)_{1 \leq i \leq n}$ de B^n soit une base de B sur A il faut et il suffit que $D(x_1, \dots, x_n)$ soit un générateur de $\delta_{B/A}$.

Démonstration : Supposons que $d = D(x_1, \dots, x_n)$ soit un générateur de $\delta_{B/A}$. Soit $(e_i)_{1 \leq i \leq n}$ une base de B sur A . Il existe des éléments a_{ij} de A tels que l'on ait $x_i = \sum_j a_{ij} e_j$. En posant $d' = D(e_1, \dots, e_n)$, on a alors

$$d = \det(a_{ij})^2 d'.$$

Par hypothèse on a $Ad = Ad' = \delta_{B/A}$. Il existe donc $u \in A$ tel que $d' = ud$ et l'on a

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

Puisque d n'est pas un diviseur de zéro (sinon tous les éléments de $\delta_{B/A}$ seraient des diviseurs de zéro) on a donc $1 - \det(a_{ij})^2 u = 0$. Cela prouve que la matrice (a_{ij}) est inversible et donc que $(x_i)_{1 \leq i \leq n}$ est une base de B sur A . L'implication réciproque a été démontrée précédemment. D'où le lemme.

Lemme 4.3. *Soient $(x_i)_{1 \leq i \leq n}$ une base de B sur A et I un idéal de A . Posons $\bar{x}_i = x_i + IB$. Alors, $(\bar{x}_i)_{1 \leq i \leq n}$ est une A/I -base de B/IB et l'on a*

$$(3) \quad D(\bar{x}_1, \dots, \bar{x}_n) = D(x_1, \dots, x_n) + I.$$

Démonstration : Le fait que $(\bar{x}_i)_{1 \leq i \leq n}$ soit une A/I -base de B/IB a déjà été démontré (cf. chap. III, dém. du th. 3.2). Par ailleurs, si x est dans B , la matrice de l'endomorphisme $m_{\bar{x}}$ dans la base $(\bar{x}_i)_{1 \leq i \leq n}$ se déduit de celle de l'endomorphisme m_x dans la base $(x_i)_{1 \leq i \leq n}$ par réduction modulo I . Cela entraîne le lemme.

Lemme 4.4. *Soient $(C_i)_{1 \leq i \leq t}$ une famille d'anneaux contenant A et C l'anneau produit des C_i : A s'identifie diagonalement à un sous-anneau de C . Pour tout i , on suppose que C_i est un A -module libre de rang fini. Alors, C est aussi un A -module libre de rang fini, et l'on a l'égalité*

$$(4) \quad \delta_{C/A} = \prod_{i=1}^t \delta_{C_i/A}.$$

Démonstration : Par récurrence sur t , on peut supposer $t = 2$. Soient $(x_i)_{1 \leq i \leq m}$ et $(y_i)_{1 \leq i \leq n}$ des bases de C_1 et C_2 sur A . Alors $((x_1, 0), \dots, (x_m, 0), (0, y_1), \dots, (0, y_n))$ est une A -base de $C = C_1 \times C_2$. Par ailleurs, pour tout i et j entre 1 et m et tout l et k entre 1 et n , l'on a

$$\mathrm{Tr}_{C/A}(x_i x_j, 0) = \mathrm{Tr}_{C_1/A}(x_i x_j) \quad \text{et} \quad \mathrm{Tr}_{C/A}(0, y_l y_k) = \mathrm{Tr}_{C_2/A}(y_l y_k).$$

Le lemme résulte alors de ces égalités compte-tenu du fait que $(x_i, 0)(0, y_j) = (0, 0)$.

Soient K un corps et L une extension finie séparable de K de degré n . Soient $(\sigma_i)_{1 \leq i \leq n}$ les n plongements de L dans une clôture algébrique de K , qui fixent les éléments de K . La formule (6) du chapitre III, entraîne le résultat suivant :

Lemme 4.5. *Soit $(x_i)_{1 \leq i \leq n}$ une base de L sur K . On a*

$$D(x_1, \dots, x_n) = (\det(\sigma_i(x_j))_{i,j})^2 \neq 0.$$

En particulier, on a $\delta_{L/K} \neq (0)$.

Proposition 4.1. Soient K un corps parfait et L une K -algèbre de dimension finie sur K : K s'identifie à un sous-anneau de L . Pour que L soit réduite, il faut et il suffit que l'on ait $\delta_{L/K} \neq 0$, i.e. que le discriminant d'une base de L sur K ne soit pas nul.

Démonstration : Supposons que L ne soit pas réduite, autrement dit qu'il existe dans L un élément nilpotent x non nul. Soit n la dimension de L sur K et $(x_1 = x, x_2, \dots, x_n)$ une K -base de L . Pour tout j , l'élément $x_1 x_j$ est nilpotent, et donc l'endomorphisme $m_{x_1 x_j}$ de multiplication par $x_1 x_j$ est aussi nilpotent. Les valeurs propres de $m_{x_1 x_j}$ sont donc nulles. On déduit de là que l'on a $\text{Tr}_{L/K}(x_1 x_j) = 0$, et donc la première ligne de la matrice $(\text{Tr}(x_i x_j))_{i,j}$ est formée de 0. Son déterminant est donc nul et l'on a $\delta_{L/K} = 0$.

Inversement, supposons que L soit réduite. Il existe alors une famille d'idéaux premiers $(\mathfrak{p}_i)_{1 \leq i \leq t}$ de L telle que l'on ait [†]

$$(0) = \bigcap_{i=1}^t \mathfrak{p}_i.$$

Par ailleurs, L/\mathfrak{p}_i est une algèbre intègre de dimension finie sur K . C'est donc un corps et \mathfrak{p}_i est un idéal maximal. Pour tout i et j distincts, on a ainsi $\mathfrak{p}_i + \mathfrak{p}_j = L$, et d'après le théorème Chinois, L est donc K -isomorphe à l'algèbre produit des L/\mathfrak{p}_i . On déduit alors du lemme 4.4 l'égalité,

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

Puisque K est parfait, L/\mathfrak{p}_i est une extension finie séparable de K , et il résulte du lemme 4.5 que l'on a $\delta_{L/K} \neq 0$. D'où le résultat.

III. Lien avec la ramification

On considère dans ce paragraphe un anneau de Dedekind A , de corps des fractions K , une extension finie séparable L de degré n de K , et B la fermeture intégrale de A dans L . On ne suppose plus que B soit un A -module libre de rang fini. On va généraliser à cette situation la notion de discriminant de B sur A .

[†] Puisque L est une K -algèbre de type fini (car de dimension finie), L est un anneau noethérien. Or dans un anneau noethérien réduit, l'idéal nul est intersection finie d'idéaux premiers. En effet, tout idéal de A contient un produit fini d'idéaux premiers (cf. dém. du th. 2.1 du Chap. II). Il en résulte qu'il existe des idéaux premiers \mathfrak{p}_i de A et des entiers n_i tels que l'on ait

$$(0) = \prod_{i=1}^t \mathfrak{p}_i^{n_i}.$$

Si x est un élément appartenant à l'intersection des \mathfrak{p}_i , on a $x^{n_1 + \dots + n_t} = 0$. Puisque A est réduit, x est donc nul, et (0) est l'intersection des \mathfrak{p}_i . D'où l'assertion.

Soit $(x_i)_{1 \leq i \leq n}$ une base de L sur K contenue dans B . D'après le lemme 3.5, on a $\text{Tr}_{B/A}(x_i x_j) \in A$. Il en résulte que le discriminant $D(x_1, \dots, x_n)$ est dans A . Cela justifie la définition suivante :

Définition 4.4. On appelle discriminant de B sur A , et on notera encore $\delta_{B/A}$ (cf. la remarque 2) ci-dessous), l'idéal de A engendré par les discriminants des bases de L sur K qui sont contenues dans B .

Remarques

1) D'après le lemme 4.5, on a $\delta_{B/A} \neq (0)$.

2) Supposons que B soit un A -module libre de rang n (tel est par exemple le cas si A est un anneau principal). Alors, les notions de discriminant données dans les définitions 4.2 et 4.4 (mais pas 4.3) coïncident : cela résulte du lemme 4.1.

Le résultat suivant établit le lien entre les notions de discriminant et de ramification :

Théorème 4.1. Soit \mathfrak{p} un idéal premier non nul de A . Pour qu'il existe un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} tel que $e_{\mathfrak{P}} > 1$, il faut et il suffit que \mathfrak{p} divise le discriminant $\delta_{B/A}$. En particulier, il n'y a qu'un nombre fini d'idéaux premiers \mathfrak{P} de B tels que $e_{\mathfrak{P}} > 1$.

Démonstration : Il résulte du th. 3.3 qu'il existe un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} tel que $e_{\mathfrak{P}} > 1$ si et seulement si l'anneau $B/\mathfrak{p}B$ n'est pas réduit. Posons $S = A \setminus \mathfrak{p}$. Puisque A est de Dedekind, $S^{-1}A$ est un anneau principal et $S^{-1}B$ est un $S^{-1}A$ -module libre de rang n (cor. 3.3 du chap. III) : soit $(e_i)_{1 \leq i \leq n}$ une base de $S^{-1}B$ sur $S^{-1}A$. D'après le lemme 4.3, le système $(e_i + \mathfrak{p}B.S^{-1}B)_{1 \leq i \leq n}$ est une $S^{-1}A/\mathfrak{p}.S^{-1}A$ -base de $S^{-1}B/\mathfrak{p}B.S^{-1}B$, et l'on a

$$(5) \quad D(e_1, \dots, e_n) + \mathfrak{p}.S^{-1}A = D(e_1 + \mathfrak{p}B, \dots, e_n + \mathfrak{p}B).$$

Par ailleurs, comme on l'a constaté dans la démonstration du th. 3.3, les anneaux $B/\mathfrak{p}B$ et $S^{-1}B/\mathfrak{p}B.S^{-1}B$ sont isomorphes. Ainsi, $B/\mathfrak{p}B$ est réduit si et seulement si tel est le cas de $S^{-1}B/\mathfrak{p}B.S^{-1}B$. On déduit alors de la prop. 4.1 et de l'égalité (5) que l'on a l'équivalence (*) suivante :

(*) il existe un idéal premier \mathfrak{P} de B au-dessus de \mathfrak{p} tel que $e_{\mathfrak{P}} > 1$ si et seulement si le discriminant $D(e_1, \dots, e_n)$ appartient à $\mathfrak{p}.S^{-1}A$.

Supposons alors qu'il existe un idéal premier \mathfrak{P} de B tel que $\mathfrak{P}|\mathfrak{p}$ et que $e_{\mathfrak{P}} > 1$. Soit $(x_i)_{1 \leq i \leq n}$ une base de L sur K contenue dans B . Il existe des éléments a_{ij} de $S^{-1}A$ tels que l'on ait

$$x_i = \sum_{j=1}^n a_{ij} e_j.$$

D'après le lemme 4.1, on a $D(x_1, \dots, x_n) = \det(a_{ij})^2 D(e_1, \dots, e_n)$, et il résulte alors de (*) que $D(x_1, \dots, x_n)$ appartient à $\mathfrak{p}.S^{-1}A$. Puisque $D(x_1, \dots, x_n)$ est un élément de A , on a $D(x_1, \dots, x_n) \in A \cap \mathfrak{p}.S^{-1}A = \mathfrak{p}$. Cela entraîne que $\delta_{B/A}$ est contenu dans \mathfrak{p} , autrement dit que \mathfrak{p} divise $\delta_{B/A}$.

Inversement, supposons que \mathfrak{p} divise $\delta_{B/A}$. Il existe un élément $s \in S$ et des éléments $y_i \in B$ tels que l'on ait $e_i = y_i/s$. Le système $(y_i)_{1 \leq i \leq n}$ est une base de L sur K contenue dans B . On a

$$D(e_1, \dots, e_n) = \frac{1}{s^{2n}} D(y_1, \dots, y_n),$$

d'où l'on déduit que $D(e_1, \dots, e_n)$ appartient à l'idéal de $S^{-1}A$ engendré par $\delta_{B/A}$. Il résulte alors de l'hypothèse faite que $D(e_1, \dots, e_n)$ appartient à $\mathfrak{p}.S^{-1}A$. D'après (*) il existe donc un idéal premier de B au-dessus de \mathfrak{p} dont l'indice de ramification est au moins 2. Cela termine la démonstration du théorème.

IV. Exemples

Le calcul du discriminant d'un corps de nombres nécessite, à priori, la connaissance d'une \mathbb{Z} -base de son anneau d'entiers. De ce point de vue, le lemme suivant s'avère parfois utile en pratique :

Lemme 4.6. *Soit K un corps de nombres de degré n sur \mathbb{Q} . Soit $(x_i)_{1 \leq i \leq n}$ une base de K sur \mathbb{Q} telle que tous les x_i soient des entiers de K . Alors, si le discriminant $D(x_1, \dots, x_n)$ est sans facteur carré, $(x_i)_{1 \leq i \leq n}$ est une base sur \mathbb{Z} de l'anneau d'entiers de K .*

Démonstration : Soient A l'anneau d'entiers de K et $(e_i)_{1 \leq i \leq n}$ une \mathbb{Z} -base de A . On a $x_i = \sum_j a_{ij} e_j$ où les a_{ij} sont dans \mathbb{Z} , et $D(x_1, \dots, x_n) = \det(a_{ij})^2 D(e_1, \dots, e_n)$. Puisque $D(x_1, \dots, x_n)$ est sans facteur carré, on a $\det(a_{ij}) = \pm 1$, et cela entraîne que $(x_i)_{1 \leq i \leq n}$ est une base de A sur \mathbb{Z} . D'où le lemme.

Exercices

1) Soit α une racine dans \mathbb{C} du polynôme $X^3 - X + 1$. On pose $K = \mathbb{Q}(\alpha)$. Calculer le discriminant de K . Même question avec le polynôme $X^4 - X + 1$.

2) Soit F un polynôme irréductible unitaire de degré n à coefficients dans \mathbb{Z} . Soient α une racine de F dans \mathbb{C} , K le corps $\mathbb{Q}(\alpha)$ et A l'anneau d'entiers de K . On note $D(F)$ le discriminant de F et D_K le discriminant de K .

- Montrer que $D(F)$ est égal au discriminant de K sur \mathbb{Q} du système $(\alpha^i)_{0 \leq i \leq n-1}$.
- Montrer que $\mathbb{Z}[\alpha]$ est un sous-groupe d'indice fini de A .
- Soient f l'indice de $\mathbb{Z}[\alpha]$ dans A . Montrer que l'on a l'égalité

$$(6) \quad D(F) = D_K f^2.$$

En particulier, si $A = \mathbb{Z}[\alpha]$, l'on a $D(F) = D_K$.

Discriminant des corps quadratiques

Soit K un corps quadratique i.e. une extension de degré 2 de \mathbb{Q} . On a $K = \mathbb{Q}(\sqrt{d})$ où d est un entier relatif sans facteur carré. Soit A l'anneau des entiers de K . On montre qu'une \mathbb{Z} -base de A est $(1, \sqrt{d})$ si $d \equiv 2$ ou $3 \pmod{4}$, et est $(1, \frac{1+\sqrt{d}}{2})$ si $d \equiv 1 \pmod{4}$ (cf. [Sa], p. 41). On déduit de là (et on vérifiera à titre d'exercice) que si D_K est le discriminant de K , l'on a $D_K = d$ si $d \equiv 1 \pmod{4}$, et $D_K = 4d$ si $d \equiv 2$ ou $3 \pmod{4}$.

Discriminant de $\mathbb{Q}(\mu_p)$

Soient p un nombre premier et μ_p le groupe des racines p -ièmes de l'unité contenues dans \mathbb{C} . Soit ζ un générateur de μ_p . Posons $K = \mathbb{Q}(\mu_p)$. L'extension K/\mathbb{Q} est galoisienne de degré $p-1$ et son groupe de Galois est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$. Le polynôme minimal de ζ sur \mathbb{Q} est $\Phi_p = 1 + X + \dots + X^{p-1}$. Soit A l'anneau des entiers de K . On va déterminer une \mathbb{Z} -base de A et en déduire le discriminant D_K de K .

On va démontrer pour cela quelques lemmes préliminaires. Étant donné un élément x de K , on notera $\text{Tr}(x)$ et $N(x)$ respectivement la trace et la norme de x de K sur \mathbb{Q} .

Lemme 4.7. *On a les égalités suivantes :*

- a) $\text{Tr}(1) = p-1$ et $\text{Tr}(\zeta^j) = -1$ pour $1 \leq j \leq p-1$;
- b) $\text{Tr}(1 - \zeta^j) = p$ pour $1 \leq j \leq p-1$;
- c) $N(1 - \zeta) = p$ et

$$(7) \quad p = \prod_{j=1}^{p-1} (1 - \zeta^j);$$

- d) $(1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$;
- e) Pour tout $x \in A$, $\text{Tr}(x(1 - \zeta))$ appartient à $p\mathbb{Z}$.

Démonstration : a) On a $\text{Tr}(\zeta) = -1$ car Φ_p est le polynôme minimal de ζ sur \mathbb{Q} . Puisque les conjugués de ζ sur \mathbb{Q} (i.e. les racines de Φ_p sont les ζ^j , pour $1 \leq j \leq p-1$, il résulte du lemme 3.3 que l'on a $\text{Tr}(\zeta^j) = -1$. Le fait que $\text{Tr}(1) = p-1$ provient de ce que le degré de K sur \mathbb{Q} est $p-1$.

b) Cette assertion est une conséquence directe de a).

c) En posant $Y = X - 1$, on constate que le polynôme minimal F de $\zeta - 1$ est

$$F = Y^{p-1} + \sum_{j=1}^{p-1} C_p^j Y^{j-1}.$$

D'où $N(1 - \zeta) = p$. L'égalité (7) résulte alors du lemme 3.3 du chapitre III.

d) D'après (7), p appartient à $(1 - \zeta)A$. Ainsi $p\mathbb{Z}$ est contenu dans $(1 - \zeta)A \cap \mathbb{Z}$. Par ailleurs, $p\mathbb{Z}$ est un idéal maximal de \mathbb{Z} . Il en résulte que l'on a $(1 - \zeta)A \cap \mathbb{Z} = p\mathbb{Z}$ ou bien $(1 - \zeta)A \cap \mathbb{Z} = \mathbb{Z}$. Supposons que l'on ait $(1 - \zeta)A \cap \mathbb{Z} = \mathbb{Z}$. Dans ce cas, $1 - \zeta$, ainsi que

tous ses conjugués, doivent être inversibles dans A . D'après la formule (7), il est de même de p , et $1/p$ doit être entier sur \mathbb{Z} , ce qui conduit à une contradiction. D'où d).

e) Soit x un élément de A . Les conjugués de $x(1 - \zeta)$ sont multiples dans A de $1 - \zeta$. D'après le lemme 3.3, la trace de $x(1 - \zeta)$ appartient donc à $(1 - \zeta)A$. D'après le lemme 3.5, on a $\text{Tr}(x(1 - \zeta)) \in \mathbb{Z}$. L'assertion e) résulte alors de d). D'où le lemme.

On déduit de là le résultat suivant :

Proposition 4.2. *Le système $(\zeta^j)_{0 \leq j \leq p-2}$ est une base de A sur \mathbb{Z} .*

Démonstration : Il suffit de montrer que ce système engendre le \mathbb{Z} -module A . Considérons pour cela un élément x de A . Il existe des éléments a_j de \mathbb{Q} tels que l'on ait

$$(8) \quad x = \sum_{j=0}^{p-2} a_j \zeta^j.$$

Tout revient à démontrer que les a_j sont des entiers relatifs. D'après (8) on a

$$(9) \quad x(1 - \zeta) = \sum_{j=0}^{p-2} a_j (\zeta^j - \zeta^{j+1}).$$

D'après (9) et l'assertion a) du lemme 4.7, on a

$$(10) \quad \text{Tr}(x(1 - \zeta)) = a_0 p.$$

D'après l'assertion e) de ce lemme, l'égalité (10) entraîne alors que a_0 est dans \mathbb{Z} . L'élément ζ étant inversible dans A , on a d'après (8),

$$(x - a_0)\zeta^{-1} = \sum_{j=1}^{p-2} a_j \zeta^{j-1},$$

qui est un élément de A . En utilisant les arguments ci-dessus avec $(x - a_0)\zeta^{-1}$, on constate de nouveau que a_1 est un entier. En appliquant successivement ce procédé, on obtient alors le résultat.

Lemme 4.8. *Soit L une extension finie de degré n de \mathbb{Q} : il existe α dans L tel que $L = \mathbb{Q}(\alpha)$. Soient F le polynôme minimal de α sur \mathbb{Q} , et F' son polynôme dérivé. On a*

$$(11) \quad D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/\mathbb{Q}}(F'(\alpha)).$$

Démonstration : Soient $(\alpha_i)_{1 \leq i \leq n}$ les racines de F dans \mathbb{C} (i.e. les conjugués de α). D'après le lemme 4.5, on a

$$D(1, \alpha, \dots, \alpha^{n-1}) = (\det(\alpha_i^j)_{i,j})^2.$$

Par ailleurs, en utilisant le calcul classique d'un déterminant de Vandermonde, on a

$$(-1)^{\frac{n(n-1)}{2}} (\det(\alpha_i^j)_{i,j})^2 = \prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j).$$

On déduit de là que

$$(-1)^{\frac{n(n-1)}{2}} (\det(\alpha_i^j)_{i,j})^2 = \prod_{i=1}^n F'(\alpha_i),$$

qui n'est autre que $N_{L/\mathbb{Q}}(F'(\alpha))$. D'où le lemme.

On déduit alors le discriminant D_K de K :

Proposition 4.3. *Soit p un nombre premier impair. On a l'égalité*

$$(12) \quad D_K = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

En particulier, p est le seul nombre premier qui se ramifie dans K .

Démonstration : On a $(X-1)\Phi_p = X^p - 1$. On déduit de là que $(\zeta-1)\Phi'_p(\zeta) = p\zeta^{p-1}$. D'après le lemme 4.7, on a $N(\zeta-1) = p$, $N(p) = p^{p-1}$, et $N(\zeta) = 1$. On a ainsi l'égalité $N(\Phi'_p(\zeta)) = p^{p-2}$. Le lemme 4.8 et la prop. 4.2 entraînent le résultat.

En ce qui concerne la ramification de p , on a l'énoncé suivant :

Lemme 4.9. *L'idéal $(1-\zeta).A$ est premier. On a $pA = (1-\zeta)^{p-1}.A$ et p est donc totalement ramifié dans A .*

Démonstration : Soit $\varphi : \mathbb{Z} \rightarrow A/(1-\zeta).A$ l'homomorphisme qui à un entier associe sa classe modulo $(1-\zeta).A$. D'après l'assertion d) du lemme 4.7, le noyau de φ est $p\mathbb{Z}$. Étant donné un élément $\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$ de A (les a_i sont dans \mathbb{Z}), on a la congruence $\alpha \equiv a_0 + a_1 + \dots + a_{p-2} \pmod{(1-\zeta).A}$, ce qui prouve que φ est surjective. Ainsi, φ passée au quotient, réalise un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $A/(1-\zeta).A$, ce qui montre que $(1-\zeta).A$ est un idéal premier. Par ailleurs, il résulte de la formule (7) que pA est contenu dans $(1-\zeta)^{p-1}.A$, autrement dit, que l'indice de ramification de l'idéal $(1-\zeta).A$ est au moins $p-1$. Le corollaire 3.6 implique alors le résultat.

Exercices

- 1) Soient l et p deux nombres premiers distincts. Montrer que l'on a $\mathbb{Q}(\mu_p) \cap \mathbb{Q}(\mu_l) = \mathbb{Q}$.
- 2) Soient p un nombre premier impair et ζ une racine primitive p -ième de l'unité. On pose $L = \mathbb{Q}(\zeta + \zeta^{-1})$.
 - a) Montrer que le degré de L sur \mathbb{Q} est $(p-1)/2$.
 - b) Montrer que L est l'unique sous-corps réel maximal de $\mathbb{Q}(\zeta)$.

- c) (*) Soit B l'anneau d'entiers de L . En utilisant la prop. 4.2, montrer que l'on a l'égalité $B = \mathbb{Z}[\zeta + \zeta^{-1}]$.

Problème

On considère le polynôme $P = X^5 - 3X + 1 \in \mathbb{Z}[X]$. Soit α une racine de P dans \mathbb{C} . On pose $K = \mathbb{Q}(\alpha)$.

- 1) Montrer que le degré de K sur \mathbb{Q} est 5 et que le groupe de Galois de P est S_5 .
- 2) Soit A l'anneau des entiers de K . En utilisant les lemmes 4.6 et 4.8, montrer que la famille $(\alpha^i)_{0 \leq i \leq 4}$ est une \mathbb{Z} -base de A . Calculer le discriminant de K . En déduire que l'extension K/\mathbb{Q} est non ramifiée en dehors du nombre premier $p = 59083$.
- 3) (*) Montrer qu'il existe deux idéaux premiers \mathfrak{P}_1 et \mathfrak{P}_2 de A tels que $pA = \mathfrak{P}_1^2 \mathfrak{P}_2$, et que $f_{\mathfrak{P}_1} = 1$ et $f_{\mathfrak{P}_2} = 3$ [†] (l'usage d'un programme de factorisation des polynômes modulo p est indispensable pour cette question).
- 4) Montrer qu'il existe deux idéaux premiers \mathfrak{P} et \mathfrak{P}' de A tels que l'on ait $2A = \mathfrak{P}\mathfrak{P}'$.
- 5) Montrer que $7A$ est un idéal premier de A (on dit que 7 est inerte dans A).

Signalons que le logiciel de calcul PARI permet (entre autres) de traiter complètement ce type de questions (cf. [PA]).

[†] Soient K un corps de nombres et A son anneau d'entiers. Il existe un entier algébrique α tel que $K = \mathbb{Q}(\alpha)$. Considérons un nombre premier p . Une question qui se pose est de déterminer la décomposition de l'idéal pA en produit d'idéaux premiers de A . On pourra à ce sujet consulter [Co], 4.8 et 6.2. Signalons ici comment procéder dans le cas favorable où $A = \mathbb{Z}[\alpha]$, qui est celui intervenant dans l'exercice ci-dessus (il suffirait en fait pour ce qui suit que p ne divise pas l'indice de $\mathbb{Z}[\alpha]$ dans A). Soit F le polynôme minimal de α sur \mathbb{Q} : puisque α est entier, F appartient à $\mathbb{Z}[X]$. Notons \bar{F} le polynôme de $(\mathbb{Z}/p\mathbb{Z})[X]$ déduit de F en réduisant ses coefficients modulo p . Soit

$$\bar{F} = \prod_{i=1}^g f_i^{e_i},$$

la décomposition de \bar{F} en produit de facteurs irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$, où les f_i sont unitaires. Alors, la décomposition de pA en produit d'idéaux premiers de A est de la forme

$$pA = \prod_{i=1}^g \mathfrak{p}_i^{e_i},$$

avec $\mathfrak{p}_i = pA + F_i(\alpha)A$, où F_i est un représentant unitaire de f_i dans $\mathbb{Z}[X]$. De plus, le degré résiduel de \mathfrak{p}_i est le degré de f_i .

Chapitre V — Corps valués et complétion

Dans toute la suite, la lettre K désignera un corps commutatif.

I. Valeur absolue

1.1. Définition d'une valeur absolue

Définition 5.1. On appelle valeur absolue sur K , une application $|\cdot| : K \rightarrow \mathbb{R}_+$, de K à valeurs dans l'ensemble des nombres réels positifs telle que, pour tout x et y dans K , l'on ait :

- a) $|x| = 0$ si et seulement si $x = 0$;
- b) $|xy| = |x| \cdot |y|$;
- c) $|x + y| \leq |x| + |y|$.

On dit que cette valeur absolue est ultramétrique si l'on a de plus :

- d) $|x + y| \leq \max(|x|, |y|)$.

On a pour tout $x \in K$, $|x| = |1| \cdot |x|$. Puisqu'il existe un $x_0 \in K$ tel que $|x_0| \neq 0$ (par exemple $x_0 = 1$), on a donc

$$(1) \quad |1| = 1 \quad \text{et} \quad |-x| = |x| \quad (\text{cf. } |-1|^2 = 1, \text{ i.e. } |-1| = 1).$$

Par ailleurs, il résulte de b), que pour tout x non nul dans K , l'on a

$$(2) \quad |x^{-1}| = \frac{1}{|x|}.$$

De même, on vérifie que pour tout x et y dans K , l'on a

$$(3) \quad ||x| - |y||_\infty \leq |x - y|,$$

où $|\cdot|_\infty$ désigne la valeur absolue usuelle sur \mathbb{R} (voir ci-dessous l'alinéa 2)). On notera que l'application $|\cdot|$ est un homomorphisme du groupe multiplicatif K^* des éléments non nuls de K , dans le groupe multiplicatif \mathbb{R}_+^* des nombres réels > 0 .

Définition 5.2. On dit qu'une valeur absolue $|\cdot| : K \rightarrow \mathbb{R}_+$ est triviale, ou impropre, si, pour tout x non nul de K , on a $|x| = 1$.

1.2. Exemples

1) La seule valeur absolue sur un corps fini est la valeur absolue triviale. En effet, Si K est fini, ses éléments non nuls sont des racines de l'unité, et pour tout $x \neq 0$ dans K , on a $|x|^n = 1$, où n est l'ordre de K^* . D'où $|x| = 1$.

2) Si K est un sous-corps de \mathbb{R} , on dispose sur K de la valeur absolue usuelle, induite par celle de \mathbb{R} , définie par $|x| = \max(x, -x)$. On la notera $|\cdot|_\infty$.

3) Soit p un nombre premier. Pour tout x non nul de \mathbb{Q} , soit $v_p(x)$ l'exposant de p dans la décomposition de x en produit de nombres premiers. L'application

$$|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_+,$$

définie par les égalités

$$(4) \quad |0|_p = 0 \quad \text{et} \quad |x|_p = p^{-v_p(x)} \quad \text{pour} \quad x \neq 0,$$

est une valeur absolue ultramétrique sur \mathbb{Q} , et est appelée la valeur absolue p -adique sur \mathbb{Q} . Cette valeur absolue satisfait à ce que l'on appelle la formule du produit :

$$(5) \quad |x|_\infty \prod_p |x|_p = 1 \quad \text{pour tout} \quad x \in \mathbb{Q}^*.$$

On notera que le produit ci-dessus à un sens puisque l'on a $|x|_p = 1$ pour tous les nombres premiers sauf un nombre fini. Si x est un élément de \mathbb{Q}^* , on obtient directement la formule (5) en considérant la décomposition de x en facteurs premiers :

$$x = \varepsilon \prod_p p^{v_p(x)} \quad \text{où} \quad \varepsilon = \pm 1.$$

Considérons maintenant une indéterminée X et un corps fini k de cardinal q . Posons $K = k(X)$, le corps des fractions rationnelles en une variable sur k . C'est le corps des fractions de l'anneau $k[X]$ des polynômes à coefficients dans k .

4) Étant donné un élément non nul F de $k[X]$, notons $\deg(F)$ son degré. Considérons l'application $|\cdot| : k[X] \rightarrow \mathbb{N}$ définie par

$$|0| = 0 \quad \text{et} \quad |F| = q^{\deg(F)}.$$

En prolongeant cette application de façon naturelle à $k(X)$, à valeurs dans \mathbb{Z} , on obtient une valeur absolue sur $k(X)$ qui est ultramétrique. On la note aussi $|\cdot|_\infty$.

5) Soit P un polynôme irréductible unitaire de $k[X]$ de degré n . Étant donné un élément F non nul de $k(X)$, notons $v_P(F)$ l'exposant de P dans la décomposition de F en produit de polynômes irréductibles sur k . Posons

$$|0|_P = 0 \quad \text{et} \quad |F|_P = q^{-n \cdot v_P(F)}.$$

On obtient ainsi une autre valeur absolue ultramétrique sur $k(X)$.

Comme dans le cas où $K = \mathbb{Q}$, on vérifie que l'on a la formule du produit

$$(6) \quad |F|_\infty \prod_p |F|_p = 1 \quad \text{pour tout} \quad F \in k(X)^*.$$

1.3. Valeurs absolues ultramétriques

Énonçons d'abord une caractérisation des valeurs absolues sur K qui sont ultramétriques. Désignons ci-dessous par 1_K l'élément neutre de K^* .

Lemme 5.1. *Soit $|\cdot| : K \rightarrow \mathbb{R}_+$ une valeur absolue. Les conditions suivantes sont équivalentes :*

- a) *la valeur absolue $|\cdot|$ est ultramétrique ;*
- b) *il existe une constante N telle que, pour tout $n \in \mathbb{Z}$, l'on ait $|n.1_K| \leq N$;*
- c) *pour tout $n \in \mathbb{Z}$, l'on a $|n.1_K| \leq 1$.*

Démonstration : L'implication a) \implies c) (donc aussi a) \implies b)) résulte directement des formules (1) (et de la définition). Supposons que la condition b) soit réalisée. Soient n un entier relatif. Pour tout entier naturel k , l'on a $|n.1_K|^k = |n^k.1_K| \leq N$. D'où $|n.1_K| \leq 1$. Supposons maintenant la condition c) réalisée. Soient x et y deux éléments de K . Posons $M = \text{Max}(|x|, |y|)$. D'après la formule du binôme, pour entier naturel n , l'on a

$$|x + y|^n = |(x + y)^n| = \left| \sum_{i=0}^n C_n^i x^i y^{n-i} \right| \leq (n + 1)M^n.$$

On obtient ainsi

$$\left(\frac{|x + y|}{M} \right)^n \leq n + 1,$$

et cela entraîne l'inégalité $|x + y| \leq M$. D'où le lemme.

Corollaire 5.1. *Si la caractéristique de K est non nulle, toute valeur absolue sur K est ultramétrique.*

Signalons deux propriétés des valeurs absolues ultramétriques :

Lemme 5.2. *Soit $|\cdot|$ une valeur absolue ultramétrique sur K . Soient x et y deux éléments de K tels que $|x| \neq |y|$. On a $|x + y| = \text{Max}(|x|, |y|)$.*

Démonstration : Supposons par exemple que l'on ait $|x| < |y|$. On a alors $|x + y| \leq |y|$ et l'égalité $-y = x - (x + y)$ implique $|y| \leq \text{Max}(|x|, |x + y|)$ (cf. formule (1)). Cela entraîne le lemme.

Lemme 5.3. *Soit $|\cdot|$ une valeur absolue ultramétrique sur K . Soient A le sous-ensemble de K formé des éléments x tels que $|x| \leq 1$, et \mathfrak{M} l'ensemble des $x \in A$ tels que $|x| < 1$. Alors, A est un anneau local, intègre, dont le corps des fractions est K et dont l'idéal maximal est \mathfrak{M} .*

Démonstration : Le fait que A soit un sous-anneau de K résulte de la définition 5.1. Le corps des fractions de A est K , car si x est un élément de K^* , x ou bien x^{-1} est dans

A. Par ailleurs, le fait que A soit local d'idéal \mathfrak{M} , résulte de ce que les unités de A sont les éléments de valeur absolue égale à 1. D'où le résultat.

Terminologie. On dit aussi qu'une valeur absolue ultramétrique est non archimédienne.

II. Le théorème d'Ostrowski

Décrivons maintenant toutes les valeurs absolues que l'on peut construire sur \mathbb{Q} .

Théorème 5.1. (Ostrowski) Soit $|\cdot| : \mathbb{Q} \rightarrow \mathbb{R}_+$ une valeur absolue non triviale sur \mathbb{Q} .

1) Supposons qu'il existe un entier n tel que l'on ait $0 < |n| < 1$. Alors, il existe un nombre premier p et un nombre réel a tels que l'on ait $0 < a < 1$, et que pour tout x dans \mathbb{Q}^* ,

$$(7) \quad |x| = a^{v_p(x)}.$$

2) Supposons que pour tout entier n non nul l'on ait $|n| \geq 1$. Alors, il existe un nombre réel α tel que l'on ait $0 < \alpha \leq 1$, et que

$$(8) \quad |x| = |x|_\infty^\alpha.$$

Démonstration : Remarquons d'abord qu'il suffit de prouver les égalités (7) et (8) en se limitant aux entiers naturels : cela résulte des formules (1) et (2).

1) Supposons qu'il existe un entier n tel que l'on ait $0 < |n| < 1$. Il existe alors un diviseur premier p de n tel que l'on ait (cf. la condition b) de la déf. 1.1)

$$(9) \quad |p| < 1.$$

Lemme 5.4. Pour tout entier naturel b , l'on a $|b| \leq 1$.

Démonstration : Soit b et k deux entiers naturels non nuls. Il existe des entiers $b_i^{(k)}$ tels que $0 \leq b_i^{(k)} < p$ et que

$$b^k = \sum_{i=0}^{h_k} b_i^{(k)} p^i,$$

où $b_{h_k}^{(k)}$ n'est pas nul. Posons alors

$$M = \text{Max}(|1|, \dots, |p-1|).$$

D'après (9), on a l'inégalité

$$|b|^k \leq \sum_{i=0}^{h_k} |b_i^{(k)} p^i| \leq (1 + h_k)M.$$

Par ailleurs, on a $p^{h_k} \leq b^k$. En posant

$$B = \frac{\log b}{\log p},$$

on a donc $h_k \leq kB$. On déduit de là que

$$|b|^k \leq (1 + kB)M.$$

Pour tout $k \geq 1$, on a ainsi

$$|b| \leq (1 + kB)^{1/k} M^{1/k},$$

et en faisant tendre k vers $+\infty$, on obtient alors le lemme.

Lemme 5.5. *Pour tout entier naturel b non divisible par p , l'on a $|b| = 1$.*

Démonstration : Soient b un entier premier à p et k un entier naturel. Puisque p^k et b^k sont premiers entre eux, il existe u_k et v_k dans \mathbb{Z} tels que l'on ait $u_k p^k + v_k b^k = 1$. Supposons alors que l'on ait $|b| < 1$. D'après le lemme 5.2, l'on a $|u_k| \leq 1$ et $|v_k| \leq 1$. On déduit de là les inégalités

$$1 = |1| \leq |u_k p^k| + |v_k b^k| \leq |b|^k + |p|^k.$$

Les inégalités $|p| < 1$ et $|b| < 1$ conduisent alors à une contradiction dès que k est assez grand. D'où le lemme.

Terminons la démonstration de l'assertion 1) du théorème : Soit m un entier naturel non nul. Posons $a = |p|$: on a $0 < a < 1$. Il existe un entier m' premier à p tel que l'on ait $m = p^{v_p(m)} m'$. On a alors d'après le lemme 1.3,

$$|m| = a^{v_p(m)} |m'| = a^{v_p(m)}.$$

Cela prouve l'assertion 1) (après passage aux rationnels).

2) Supposons maintenant que pour tout entier n non nul l'on ait $|n| \geq 1$. Puisque la valeur absolue considérée sur K n'est pas triviale, il existe un entier naturel a tel que l'on ait $|a| > 1$. Posons

$$\alpha = \frac{\log |a|}{\log a}.$$

Il résulte de l'inégalité triangulaire c) de la def. 5.1, que $|a| \leq a$: d'où $0 < \alpha \leq 1$. Montrons alors que pour tout entier naturel non nul c l'on a

$$(10) \quad \frac{\log |c|}{\log c} \leq \alpha.$$

Soient c et k deux entier ≥ 1 . Soit

$$c^k = \sum_{i=0}^{h_k} c_i^{(k)} a^i,$$

où $c_{h_k}^{(k)}$ n'est pas nul, le développement de c^k en base a (on a $0 \leq c_{h_k}^{(k)} < a$). En posant

$$M = \text{Max}(|1|, \dots, |a-1|) \quad \text{et} \quad C = \frac{\log c}{\log a},$$

on obtient (en utilisant le fait que $a^{h_k} \leq c^k$)

$$|c|^k \leq M \frac{1 - |a|^{h_k+1}}{1 - |a|} \quad \text{avec} \quad h_k \leq kC.$$

On déduit de là l'inégalité

$$|c| \leq M^{1/k} \left(\frac{1 - |a|^{kC+1}}{1 - |a|} \right)^{1/k}.$$

En faisant alors tendre k vers $+\infty$, on obtient l'inégalité (10). Il en résulte que pour tout entier naturel c tel que $|c| > 1$, (en échangeant les rôles de a et c) l'on a

$$(11) \quad \frac{\log |c|}{\log c} = \alpha \quad \text{i.e. que} \quad |c| = c^\alpha (= |c|_\infty^\alpha).$$

Il reste à examiner l'égalité (11) pour les entiers naturels ≥ 2 tels que $|c| = 1$. En fait l'existence d'un tel entier entraîne l'inégalité $|n| \leq 1$ pour tout entier n (cf. la dém. du lemme 5.4), ce qui, compte-tenu de l'hypothèse faite, entraîne que la valeur absolue considérée est triviale, ce que l'on a exclu. On a donc $|c| = |c|_\infty^\alpha$ pour tout $c \in \mathbb{N}$, ce qui prouve l'assertion 2) du théorème.

On notera que le théorème d'Ostrowski fournit des conditions nécessaires pour qu'une application de \mathbb{Q} à valeurs dans \mathbb{R}_+^* soit une valeur absolue sur \mathbb{Q} . Inversement, on vérifie qu'une application $|\cdot| : \mathbb{Q} \rightarrow \mathbb{R}_+^*$ qui satisfait aux égalités (7) et (8) est une valeur absolue. On obtient ainsi la description de toutes les valeurs absolues sur \mathbb{Q} .

III. Valuation

Dans le premier chapitre nous avons défini les valuations discrètes sur un corps à valeurs dans $\mathbb{Z} \cup \{+\infty\}$. On va maintenant considérer, plus généralement, des valuations à valeurs dans le monoïde ordonné $\mathbb{R} \cup \{+\infty\}$.

Définition 5.3. Soit $v : K \rightarrow \mathbb{R} \cup \{+\infty\}$ une application. On dit que v est une valuation si, pour tout x et y dans K , les conditions suivantes sont réalisées :

- a) $v(x) = +\infty$ si et seulement si $x = 0$;
- b) $v(xy) = v(x) + v(y)$;
- c) $v(x + y) \geq \inf(v(x), v(y))$.

Définition 5.4. On dit qu'une valuation $v : K \rightarrow \mathbb{R} \cup \{+\infty\}$ est triviale, ou impropre, si, pour tout x non nul de K , l'on a $v(x) = 0$.

Une valuation sur K est en particulier un homomorphisme de K^* dans le groupe additif de \mathbb{R} . L'image $v(K^*)$ est donc un sous-groupe de $(\mathbb{R}, +)$. Par conséquent, muni de la topologie induite par la valeur absolue usuelle de \mathbb{R} , $v(K^*)$ est discret ou dense dans \mathbb{R} .

Définition 5.5. On dit que la valuation est discrète si $v(K^*)$ est discret, et dense dans le cas contraire.

Supposons que $v(K^*)$ soit *discrète*, et que v ne soit pas triviale. On retrouve alors, à isomorphisme près, la notion de valuation discrète introduite dans le chapitre I. En effet, il existe dans ce cas un nombre réel $a > 0$ tel que l'on ait $v(K^*) = a\mathbb{Z}$, qui est un groupe isomorphe à \mathbb{Z} . Un élément de K^* de valuation a est appelé une uniformisante de K . On dit que v est *normalisée* si l'on a $v(K^*) = \mathbb{Z}$. Si tel est le cas, une uniformisante est de valuation 1.

Il existe de nombreux exemples de valuations denses. Pour en expliciter, il suffit en fait de construire une valuation non triviale sur un corps algébriquement clos (nous en rencontrerons plus loin) :

Lemme 5.6. Supposons que K soit un corps algébriquement clos. Soit v une valuation non triviale sur K . Alors, le groupe $v(K^*)$ est divisible, autrement dit, étant donné un entier naturel non nul n et un élément x de K^* , il existe $y \in K^*$ tel que $nv(y) = v(x)$. En particulier, v n'est pas une valuation discrète sur K .

Démonstration : Soient x un élément de K^* et n un entier naturel non nul. Il suffit de remarquer qu'une racine y dans K du polynôme $X^n - x$ vérifie $nv(y) = v(x)$.

Nous allons maintenant définir la notion de valuations et de valeurs absolues équivalentes sur K .

Définition 5.6. a) Soient v_1 et v_2 deux valuations définies sur K . On dit que v_1 et v_2 sont équivalentes s'il existe un nombre réel $\rho > 0$ tel que, pour tout $x \in K$, l'on ait

$$(12) \quad v_2(x) = \rho v_1(x).$$

b) Soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues définies sur K . On dit que $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes s'il existe un nombre réel $b > 0$ tel que, pour tout $x \in K$, l'on ait

$$(13) \quad |x|_1 = |x|_2^b.$$

On notera que la classe d'équivalence d'une valeur absolue ultramétrique est formée de valeurs absolues qui sont aussi ultramétriques.

Lemme 5.7. a) Soit v une valuation sur K . Soit a un nombre réel tel que $0 < a < 1$. Alors, l'application $|\cdot| : K \rightarrow \mathbb{R}_+$ définie par

$$(14) \quad |0| = 0 \quad \text{et} \quad |x| = a^{v(x)} \quad \text{pour} \quad x \neq 0,$$

est une valeur absolue ultramétrique sur K . Si l'on remplace a par un nombre réel a' tel que $0 < a' < 1$, les valeurs absolues correspondantes définies par (14) sont équivalentes.

b) Soit $|\cdot|$ une valeur absolue ultramétrique sur K . Soit b un nombre réel strictement positif. Alors, l'application $v : K \rightarrow \mathbb{R} \cup \{+\infty\}$ définie par

$$(15) \quad v(0) = +\infty \quad \text{et} \quad v(x) = -b \log |x| \quad \text{pour} \quad x \neq 0,$$

est une valuation sur K . Si l'on remplace b par un nombre réel b' tel que $b' > 0$, les valuations correspondantes définies par (15) sont équivalentes.

Démonstration : La vérification de ce lemme est facile et est laissée à titre d'exercice.

Si v_1 et v_2 sont deux valuations équivalentes sur K et si a est un nombre réel tel que $0 < a < 1$, les valeurs absolues associées à v_1 et v_2 par l'égalité (14) sont équivalentes. De même, si $|\cdot|_1$ et $|\cdot|_2$ sont deux valeurs absolues ultramétriques équivalentes sur K , et si b est un nombre réel strictement positif, les valuations associées à $|\cdot|_1$ et $|\cdot|_2$ par l'égalité (15) sont équivalentes.

En fait la donnée d'une classe de valuations sur un corps K est équivalente à la donnée d'une classe de valeurs absolues ultramétriques sur ce corps. Plus précisément, notons \mathcal{V} l'ensemble des classes d'équivalence de valuations sur K et \mathcal{T} l'ensemble des classes d'équivalence de valeurs absolues ultramétriques sur K . On déduit de ce qui précède l'énoncé suivant :

Proposition 5.1. L'application $\Phi : \mathcal{V} \rightarrow \mathcal{T}$ qui à la classe de la valuation v sur K associe la classe d'équivalence de la valeur absolue ultramétrique définie par l'égalité (14), où a est n'importe quel nombre réel tel que $0 < a < 1$, est une bijection de \mathcal{V} sur \mathcal{T} . L'application réciproque de Φ associe à la classe de la valeur absolue ultramétrique $|\cdot|$ sur K , la classe d'équivalence de la valuation définie par l'égalité (15), où b est n'importe quel nombre réel strictement positif.

De façon analogue au cas des valuations discrètes, on a l'énoncé suivant :

Lemme 5.8. Soit v une valuation sur K . Soient A_v le sous-anneau de K formé des éléments x tels que $v(x) \geq 0$, et \mathfrak{M}_v l'ensemble des $x \in A_v$ tels que $v(x) > 0$. Alors, K est le corps des fractions de A_v , et \mathfrak{M}_v est l'unique idéal maximal de A_v . L'anneau A_v est

appelé l'anneau de valuation de v et \mathfrak{M}_v est l'idéal de valuation de v . Le corps A_v/\mathfrak{M}_v est le corps résiduel de v .

Dans le cas où v est une valuation discrète non triviale, A_v est un anneau de valuation discrète ; en particulier, A_v est un anneau local, principal, et ses idéaux non nuls sont des puissances de \mathfrak{M}_v . Si v est normalisée, v est la valuation définie à l'aide d'un générateur de \mathfrak{M}_v (cf. chap. I).

On prouvera dans le paragraphe suivant que si v_1 et v_2 sont deux valuations sur K , les anneaux A_{v_1} et A_{v_2} sont égaux si et seulement si v_1 et v_2 sont équivalentes.

Signalons l'énoncé suivant :

Lemme 5.9. *Soit A un anneau qui soit l'anneau de valuation d'un corps K (pour une valuation v). Alors, A est intégralement clos.*

Démonstration : Puisque pour tout $x \in K^*$, l'un des deux éléments x ou x^{-1} est dans A , K est le corps des fractions de A . Considérons un élément x de K entier sur A : on a une relation de dépendance intégrale $x^n + a_1x^{n-1} + \dots + a_n = 0$, où les a_i sont dans A et où $n \geq 1$. Si x n'est pas dans A , on a $v(x) < 0$ et par conséquent, pour tout i tel que $0 \leq i < n$, l'on a $v(x^n) < v(a_ix^{n-i})$. Il en résulte que l'on a $v(x^n) = v(x^n + a_1x^{n-1} + \dots + a_n)$. On a donc $nv(x) = +\infty$, et donc $x = 0$, ce qui contredit le fait que x n'est pas dans A . D'où le lemme.

IV. Topologie associée à une valeur absolue

Soit K un corps muni d'une valeur absolue $|\cdot|$. L'application

$$d : K \times K \rightarrow \mathbb{R}_+,$$

définie, pour tout x et y dans K , par l'égalité

$$(16) \quad d(x, y) = |y - x|,$$

est une distance sur K : le couple (K, d) est un espace métrique, et l'on dispose ainsi d'une topologie sur K définie par d . Une partie V de K est un voisinage d'un point $a \in K$, si V contient une boule ouverte de centre a et de rayon > 0 . Les ouverts de K sont les réunions de boules ouvertes. On munit l'ensemble $K \times K$ de la topologie produit.

Lemme 5.10. *Le corps K muni de sa distance d est un corps topologique.*

Démonstration : D'abord, le fait que l'application $(x, y) \mapsto x - y$ soit continue résulte directement de l'inégalité triangulaire. Montrons que l'application $(x, y) \mapsto xy$ est continue. Soit (x_0, y_0) un point de $K \times K$. On a $xy - x_0y_0 = (x - x_0)(y - y_0) + (x - x_0)y_0 + x_0(y - y_0)$. Il en résulte l'inégalité

$$|xy - x_0y_0| \leq |x - x_0| \cdot |y - y_0| + |x_0| \cdot |y - y_0| + |y_0| \cdot |x - x_0|,$$

ce qui entraîne l'assertion. De même, l'application $x \mapsto x^{-1}$ est continue en tout point $x_0 \neq 0$. En effet, pour tout $x \neq 0$, l'on a $x^{-1} - x_0^{-1} = x^{-1}(x_0 - x)x_0^{-1}$. On a ainsi

$$|x^{-1} - x_0^{-1}| = \frac{|x - x_0|}{|x_0| \cdot |x|}.$$

Soit alors ε un nombre réel > 0 . Choisissons un réel $\alpha > 0$ tel que

$$\alpha < \frac{\varepsilon |x_0|^2}{1 + \varepsilon |x_0|}.$$

Soit alors x un élément de K tel que $|x - x_0| < \alpha$. On a $|x_0| - \alpha < |x|$ et $\alpha < |x_0|$, ce qui entraîne

$$|x^{-1} - x_0^{-1}| < \frac{\alpha}{|x_0|} \cdot \frac{1}{|x_0| - \alpha} < \varepsilon.$$

D'où l'assertion et le lemme.

Deux valeurs absolues étant données sur K , énonçons maintenant un critère permettant de décider si elles définissent la même topologie.

Proposition 5.2. *Soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur K . Les conditions suivantes sont équivalentes :*

- a) *les topologies définies par $|\cdot|_1$ et $|\cdot|_2$ sont identiques ;*
- b) *les deux ensembles $\{x \in K ; |x|_1 < 1\}$ et $\{x \in K ; |x|_2 < 1\}$ sont égaux ;*
- c) *les valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes.*

Démonstration : L'implication a) \implies b) : les ensembles formés des éléments x de K tels que la suite $(x^n)_{n \in \mathbb{N}}$ soit convergente de limite 0, pour la topologie définie par $|\cdot|_1$ ou bien par $|\cdot|_2$, sont les mêmes. Or étant donné x dans K , la suite $(x^n)_{n \in \mathbb{N}}$ tend vers 0 si et seulement si sa valeur absolue, pour $|\cdot|_1$ ou $|\cdot|_2$, est < 1 . D'où l'implication.

L'implication b) \implies c) : supposons d'abord $\{x \in K ; |x|_1 < 1\} = \{0\}$. Les valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont alors égales à la valeur absolue triviale, ce qui prouve le résultat dans ce cas.

Considérons un élément a non nul fixé de $\{x \in K ; |x|_1 < 1\}$. Soit x un élément de K^* . Posons

$$b_1 = \frac{\log |x|_1}{\log |a|_1} \quad \text{et} \quad b_2 = \frac{\log |x|_2}{\log |a|_2},$$

et considérons l'ensemble

$$T_1 = \left\{ \frac{m}{n} \in \mathbb{Q}, n > 0 ; |a|_1^m < |x|_1^n \right\},$$

Alors b_1 est un minorant de T_1 , et en utilisant le fait que \mathbb{Q} est dense dans \mathbb{R} , l'on constate que b_1 est le plus grand minorant de T_1 . Soit T_2 l'analogue de T_1 en ce qui concerne la

valeur absolue $|\cdot|_2$. Il résulte de l'hypothèse faite que l'on a $T_1 = T_2$, ce qui implique l'égalité $b_1 = b_2$. Posons alors

$$b = \frac{\log |a|_1}{\log |a|_2}.$$

Par définition de a , b est strictement positif, et l'on a $|x|_1 = |x|_2^b$. Cela prouve l'implication.

L'implication $c) \implies a)$: Si la condition $c)$ est vérifiée, étant donné un élément a de K , la famille des boules ouvertes de centre a pour $|\cdot|_1$ est la même que celle définie par $|\cdot|_2$. Cela signifie que les topologies définies sur K par les valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sont les mêmes. D'où $a)$, et le résultat.

On notera que la condition $b)$ du lemme est encore équivalente à l'égalité

$$\{x \in K ; |x|_1 \leq 1\} = \{x \in K ; |x|_2 \leq 1\}.$$

Corollaire 5.2. *Les topologies que l'on peut définir sur \mathbb{Q} à partir d'une valeur absolue sont les suivantes :*

1. *la topologie discrète, qui est associée à la valeur absolue triviale ;*
2. *la topologie induite par la valeur absolue usuelle sur \mathbb{R} ;*
3. *pour tout nombre premier p , la topologie associée à la valeur absolue p -adique.*

Démonstration : C'est une conséquence du th. 5.1, du lemme 5.7 et de la prop. 5.2.

V. Le complété d'un corps valué

5.1. Théorème d'existence et d'unicité du complété

Définition 5.7. *On appelle corps valué un couple $(K, |\cdot|)$, où K est un corps et $|\cdot|$ est une valeur absolue ultramétrique définie sur K , ou bien un couple (K, v) , où K est un corps et v une valuation définie sur K . Lorsque la valeur absolue ultramétrique ou la valuation considérée est implicite, le corps valué sera simplement noté K .*

Considérons désormais un corps valué $(K, |\cdot|)$. On dispose d'une topologie sur K qui est celle définie par la classe de $|\cdot|$.

Rappelons qu'une suite d'éléments $(x_n)_{n \in \mathbb{N}}$ de K est dite de Cauchy si pour tout nombre réel ε , il existe un entier n_0 , tel que pour tous les entiers p et q plus grands que n_0 , l'on a $|x_p - x_q| \leq \varepsilon$. Par définition, le corps K est complet si toutes les suites de Cauchy d'éléments de K sont convergentes dans K . Une suite de Cauchy est bornée.

Définissons maintenant la notion de complétion d'un corps valué.

Définition 5.8. *Une complétion du corps valué $(K, |\cdot|)$ est un triplet $(L, \|\cdot\|, i)$, où $(L, \|\cdot\|)$ est un corps valué et $i : K \rightarrow L$ un homomorphisme de corps, qui satisfait aux deux conditions suivantes :*

a) Le corps $i(K)$ est dense dans L et l'on a

$$(17) \quad \|i(x)\| = |x| \quad \text{pour tout } x \in K;$$

b) le corps L est complet pour la topologie définie par $\|\cdot\|$.

On dit que deux complétions $(L_1, \|\cdot\|_1, i_1)$ et $(L_2, \|\cdot\|_2, i_2)$ de (K, v) sont isomorphes, s'il existe un isomorphisme de corps f de L_1 sur L_2 , tel que l'on ait

$$(18) \quad f \circ i_1 = i_2 \quad \text{et} \quad \|\cdot\|_2 \circ f = \|\cdot\|_1.$$

Théorème 5.2. *Le corps valué $(K, |\cdot|)$ possède une complétion, qui est unique à un isomorphisme unique près.*

Démonstration : Construisons une complétion $(\hat{K}, \|\cdot\|, i)$ de $(K, |\cdot|)$. Cette construction est analogue à celle du corps des réels comme complété de \mathbb{Q} pour la valeur absolue $|\cdot|_\infty$.

On considère l'anneau $K^\mathbb{N}$ des suites d'éléments de K . L'ensemble $C(K)$ formé des suites de Cauchy d'éléments de K est un sous-anneau de $K^\mathbb{N}$ (le fait que le produit de deux suites de Cauchy soit une suite de Cauchy provient du fait qu'elles sont bornées). Soit $I(K)$ le sous-ensemble de $C(K)$ formé des suites de Cauchy qui convergent vers 0. C'est un idéal de $C(K)$ car le produit d'une suite qui converge vers 0 et d'une suite de Cauchy, qui est bornée, converge aussi vers 0.

Lemme 5.11. *L'anneau quotient*

$$\hat{K} = C(K)/I(K)$$

est un corps.

Démonstration : Considérons une suite de Cauchy $(x_n)_{n \in \mathbb{N}}$ qui ne converge pas vers 0. Il s'agit de montrer que sa classe modulo $I(K)$ est inversible dans \hat{K} . Montrons pour cela qu'il existe un nombre réel $\alpha > 0$ tel que, dès que n est assez grand, l'on ait

$$(19) \quad |x_n| > \alpha.$$

Supposons le contraire. Alors, pour tout $\varepsilon > 0$ et tout entier N , il existe $k > N$ tel que $|x_k| < \varepsilon/2$. Quitte à augmenter N , on peut supposer que pour tous les entiers n et m plus grands que N , l'on a $|x_n - x_m| < \varepsilon/2$. Pour tout $n > N$ on a alors $|x_n| < |x_n - x_k| + |x_k| < \varepsilon$, ce qui entraîne que $(x_n)_{n \in \mathbb{N}}$ converge vers 0 et conduit à une contradiction. D'où (19). On considère alors la suite $(y_n)_{n \in \mathbb{N}} \in K^\mathbb{N}$ définie par $y_n = x_n^{-1}$ si $x_n \neq 0$ et $y_n = 1$ si $x_n = 0$. C'est un élément de $C(K)$. En effet, d'après (19), il existe un entier N , tel que, pour tous n et m plus grands que N , l'on ait $x_n x_m \neq 0$, et que

$$|y_n - y_m| = \frac{|x_n - x_m|}{|x_n x_m|} < \frac{1}{\alpha^2} |x_n - x_m|.$$

Par ailleurs, la suite $(x_n y_n - 1)_{n \in \mathbb{N}}$ étant nulle à partir d'un certain rang, elle appartient à $I(K)$, ce qui prouve le lemme.

L'on dispose alors d'un homomorphisme de corps $i : K \rightarrow \hat{K}$ qui à $x \in K$, associe la classe modulo $I(K)$ de la suite constante égale à x .

Définissons maintenant $\|\cdot\|$. Soit $\alpha = (x_n)_{n \in \mathbb{N}} + I(K)$ un élément de \hat{K} . Pour tout entier p et q l'on a

$$\left| |x_p| - |x_q| \right|_{\infty} \leq |x_p - x_q|.$$

On déduit de là que la suite de nombre réels $(|x_n|)_{n \in \mathbb{N}}$ est une suite de Cauchy. Puisque \mathbb{R} est complet pour la topologie associée à $|\cdot|_{\infty}$, cette suite est convergente dans \mathbb{R}^{\dagger} , et sa limite ne dépend pas du représentant choisi de α . Cela permet de poser par définition

$$(20) \quad \|\alpha\| = \lim_{n \rightarrow +\infty} (|x_n|)_{n \in \mathbb{N}}.$$

On vérifie alors que l'application $\|\cdot\| : \hat{K} \rightarrow \mathbb{R}_+$ est une valeur absolue ultramétrique sur \hat{K} qui satisfait à l'égalité (17).

On dispose ainsi de la topologie sur \hat{K} définie par $\|\cdot\|$. Vérifions que $i(K)$ est dense dans \hat{K} . Soit α un élément de \hat{K} . On a $\alpha = (x_n)_{n \in \mathbb{N}} + I(K)$, où $(x_n)_{n \in \mathbb{N}}$ est une suite de Cauchy d'éléments de K . Soit m un entier fixé. La suite $(x_n - x_m)_{n \in \mathbb{N}}$ d'éléments de K représente $\alpha - i(x_m)$. D'après (20), on a donc

$$(21) \quad \|\alpha - i(x_m)\| = \lim_{n \rightarrow +\infty} (|x_n - x_m|)_{n \in \mathbb{N}}.$$

Soit alors ε un nombre réel > 0 . Il existe un entier N tel que pour tout p et q plus grands que N on a $|x_p - x_q| \leq \varepsilon$. On déduit de là que si m est un entier $> N$ la limite quand n tend $+\infty$ de $(|x_n - x_m|)_{n \in \mathbb{N}}$ est $< \varepsilon$. D'après (21), cela prouve que

$$(22) \quad \alpha = \lim_{n \rightarrow +\infty} i(x_n).$$

D'où notre assertion.

Démontrons maintenant que \hat{K} est complet pour $\|\cdot\|$. Soit $(a_n)_{n \in \mathbb{N}}$ une suite de Cauchy d'éléments de \hat{K} . Puisque $i(K)$ est dense dans \hat{K} , pour tout entier n , il existe une suite $(b_{n,m})_{m \in \mathbb{N}}$ d'éléments de K telle que l'on ait

$$a_n = \lim_{m \rightarrow +\infty} i(b_{n,m}).$$

[†] On peut aussi évoquer le fait que si $(x_n)_{n \in \mathbb{N}}$ ne converge pas vers 0, la suite $(|x_n|)_{n \in \mathbb{N}}$ est stationnaire. En effet, d'après (19) il existe $\alpha > 0$ et un entier n_0 tel que si $n \geq n_0$ l'on ait $|x_n| > \alpha$. Par ailleurs, quitte à augmenter n_0 , si p et q sont plus grands que n_0 , l'on a $|x_p - x_q| < \alpha$. Il en résulte que si p et q sont plus grands que n_0 , l'on a, d'après l'inégalité ultramétrique, $|x_p| = |x_q|$.

Pour tout entier n , il existe donc un entier que l'on notera $m(n)$ tel que l'on ait

$$(23) \quad \|a_n - i(b_{n,m(n)})\| \leq \frac{1}{2^n}.$$

Posons $b(n) = b_{n,m(n)}$. Pour tout entier p et q l'on a

$$|b(p) - b(q)| = \|i(b(p)) - i(b(q))\| = \|a_p - i(b(p)) - (a_q - i(b(q)) - (a_p - a_q)\|,$$

et l'on déduit de là que

$$|b(p) - b(q)| \leq \frac{1}{2^p} + \frac{1}{2^q} + \|a_p - a_q\|.$$

Cela prouve que la suite $(b(n))_{n \in \mathbb{N}}$ est une suite de Cauchy de K . On pose alors

$$x = (b(n))_{n \in \mathbb{N}} + I(K).$$

D'après les formules (22) et (23), on a

$$x = \lim_{n \rightarrow +\infty} i(b(n)) \quad \text{et} \quad \lim_{n \rightarrow +\infty} a_n - i(b(n)) = 0.$$

Il en résulte que la suite $(a_n)_{n \in \mathbb{N}}$ est convergente de limite $x \in \hat{K}$. D'où le fait que $(\hat{K}, \|\cdot\|, i)$ soit une complétion de (K, v) , et l'assertion d'existence du th. 5.2.

Il reste à prouver l'assertion d'unicité. Considérons deux complétions $(L_1, \|\cdot\|_1, i_1)$ et $(L_2, \|\cdot\|_2, i_2)$ de (K, v) . Remarquons d'abord que pour tout y et z dans K l'on a

$$(24) \quad \|i_1(y) - i_1(z)\|_1 = \|i_1(y - z)\|_1 = |y - z| = \|i_2(y - z)\|_2 = \|i_2(y) - i_2(z)\|_2.$$

On définit alors une application $f : L_1 \rightarrow L_2$ de la façon suivante : soit x un élément de L_1 . Il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de K telle que l'on ait

$$\lim_{n \rightarrow +\infty} i_1(x_n) = x.$$

En utilisant (24), on constate que la suite $(i_2(x_n))_{n \in \mathbb{N}}$ est de Cauchy dans L_2 . Cette suite est donc convergente dans L_2 : soit $f(x)$ sa limite. Il résulte de (24) que $f(x)$ ne dépend pas de la suite $(x_n)_{n \in \mathbb{N}}$ choisie. On vérifie ensuite que l'application f ainsi définie est un isomorphisme de corps de L_1 sur L_2 , tel que $f \circ i_1 = i_2$.

Par ailleurs, on a $\|f(x)\|_2 = \|x\|_1$: cela résulte de la continuité des applications $\|\cdot\|_1$ et $\|\cdot\|_2$, du fait que $(i_2(x_n))_{n \in \mathbb{N}}$ converge vers $f(x)$, que $(i_1(x_n))_{n \in \mathbb{N}}$ converge vers x , et que pour tout n l'on a $\|i_1(x_n)\|_1 = \|i_2(x_n)\|_2$ (cf. l'égalité (24)).

Enfin, si g est un isomorphisme de corps de L_1 sur L_2 qui conserve les valeurs absolues, il est continu. Si de plus $g \circ i_1 = i_2$, f et g coïncident sur $i_1(K)$, et puisque $i_1(K)$ est dense dans L_1 , on a $f = g$ sur L_1 . Cela termine la démonstration du théorème.

Terminologie. On dit que le corps $\hat{K} = C(K)/I(K)$ est le complété de K pour la valeur absolue $|\cdot|$.

5.2. Traduction en termes de valuation

Signalons maintenant la traduction du th. 5.2 en termes de valuations. Supposons donc que K soit muni d'une valuation v . La topologie dont on dispose sur K est celle associée à la valeur absolue sur K , définie (par exemple) pour tout $x \in K$ par (cf. lemme 5.7 a)) avec $a = 1/e$,

$$(25) \quad |x| = \exp(-v(x)).$$

Autrement dit, il s'agit de la topologie associée à la distance d , définie pour tout x et y dans K , par l'égalité (cf. formule (16))

$$(26) \quad d(x, y) = \exp(-v(x - y)).$$

En particulier, une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de K est convergente de limite a si, pour tout $c > 0$, il existe un entier n_0 tel que pour tout $n \geq n_0$ l'on a $v(x_n - a) \geq c$. De même, $(x_n)_{n \in \mathbb{N}}$ est de Cauchy si pour tout $c > 0$, il existe un entier n_0 tel que si p et q sont plus grands que n_0 , l'on a $v(x_p - x_q) \geq c$.

Les traductions de la déf. 5.8 et du th. 5.2 en termes de valuations sont les suivantes :

Définition 5.8 bis. Une complétion du corps valué (K, v) est un triplet (L, v', i) , où (L, v') est un corps valué et $i : K \rightarrow L$ un homomorphisme de corps, qui satisfait aux deux conditions suivantes :

a) Le corps $i(K)$ est dense dans L et l'on a

$$(27) \quad v'(i(x)) = v(x) \quad \text{pour tout } x \in K;$$

b) le corps L est complet pour la topologie définie par v' .

On dit que deux complétions (L_1, v_1, i_1) et (L_2, v_2, i_2) de (K, v) sont isomorphes, s'il existe un isomorphisme de corps f de L_1 sur L_2 , tel que l'on ait

$$(28) \quad f \circ i_1 = i_2 \quad \text{et} \quad v_2 \circ f = v_1.$$

Théorème 5.2 bis. Le corps valué (K, v) possède une complétion, qui est unique à un isomorphisme unique près.

Signalons une complétion (\hat{K}, \hat{v}, i) de (K, v) : comme on l'a constaté dans la démonstration du th. 5.2, on peut prendre pour \hat{K} l'anneau quotient $C(K)/I(K)$. Par ailleurs, si

$\alpha = (x_n)_{n \in \mathbb{N}} + I(K)$ est un élément de \hat{K} , la suite d'éléments $(v(x_n))_{n \in \mathbb{N}}$ de $\mathbb{R} \cup \{+\infty\}$ est convergente [si $\alpha = 0$, la limite de $(v(x_n))_{n \in \mathbb{N}}$ est $+\infty$; si $\alpha \neq 0$, il existe un entier n_0 tel que dès que n et m sont plus grands que n_0 , l'on a $v(x_n) = v(x_m)$]. La valuation \hat{v} est alors définie par l'égalité

$$\hat{v}(\alpha) = \lim_{n \rightarrow +\infty} (v(x_n))_{n \in \mathbb{N}}.$$

On dit parfois que (\hat{K}, \hat{v}) est le complété de (K, v) . On identifie souvent K et son image par i dans son complété \hat{K} . Modulo cette identification, que l'on fera désormais, K est un sous-corps dense de \hat{K} et v est la restriction de \hat{v} à K .

5.3. Propriétés

Soient (K, v) un corps valué et (\hat{K}, \hat{v}) son complété. Désignons par $A_{\hat{v}}$ l'anneau de valuation, $\mathfrak{M}_{\hat{v}}$ l'idéal de valuation et $k_{\hat{v}}$ le corps résiduel de \hat{K} .

Proposition 5.3. a) On a $A_v = A_{\hat{v}} \cap K$ et $A_{\hat{v}}$ est l'adhérence de A_v dans \hat{K} .

b) On a $\mathfrak{M}_v = \mathfrak{M}_{\hat{v}} \cap K$ et $\mathfrak{M}_{\hat{v}}$ est l'adhérence de \mathfrak{M}_v dans \hat{K} .

c) L'application naturelle $k_v = A_v/\mathfrak{M}_v \rightarrow A_{\hat{v}}/\mathfrak{M}_{\hat{v}} = k_{\hat{v}}$ est un isomorphisme de corps de k_v sur $k_{\hat{v}}$.

d) On a $v(K) = \hat{v}(\hat{K})$. En particulier, si v est une valuation discrète sur K , il en est de même de \hat{v} sur \hat{K} .

Démonstration : Prouvons d'abord le lemme suivant :

Lemme 5.12. Soit $(x_n)_{n \in \mathbb{N}}$ une suite convergente d'éléments de (K, v) de limite x . Si l'on a $x \neq 0$, il existe un entier n_0 tel que, dès que n est plus grand que n_0 , l'on a $v(x_n) = v(x)$.

Démonstration : La suite $(x_n - x)_{n \in \mathbb{N}}$ tend vers 0 et donc la suite $(v(x_n - x))_{n \in \mathbb{N}}$ tend vers $+\infty$. Puisque x est non nul, on a $v(x) \neq +\infty$, et il existe ainsi un entier n_0 tel que pour tout $n \geq n_0$, l'on ait $v(x_n - x) > v(x)$. On déduit de là que pour tout $n \geq n_0$ l'on a $v(x_n) = \inf(v(x_n - x), v(x)) = v(x)$. D'où le lemme.

Démontrons maintenant la proposition 5.3. Les égalités $A_v = A_{\hat{v}} \cap K$ et $\mathfrak{M}_v = \mathfrak{M}_{\hat{v}} \cap K$ proviennent de ce que v est la restriction de \hat{v} à K . Puisque $A_{\hat{v}}$ est un fermé de \hat{K} , l'adhérence $\overline{A_v}$ de A_v dans \hat{K} est contenue dans $A_{\hat{v}}$. Inversement, soit x un élément non nul de $A_{\hat{v}}$. Puisque K est dense dans \hat{K} , il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de K qui converge vers x . D'après le lemme 5.12, dès que n est assez grand, l'on a $\hat{v}(x_n) = \hat{v}(x)$. Or $\hat{v}(x_n) = v(x_n)$ et $\hat{v}(x) \geq 0$. Il en résulte que x_n est dans A_v si n est assez grand, autrement dit, il existe une suite d'éléments de A_v qui converge vers x , ce qui prouve que x appartient à $\overline{A_v}$. D'où l'assertion a). L'assertion b) se démontre par le même argument.

Prouvons l'assertion c). Il résulte de a) et b) que l'application $A_v \rightarrow k_{\hat{v}}$ qui à $y \in A_v$ associe $y + \mathfrak{M}_{\hat{v}}$, est un homomorphisme d'anneaux de noyau \mathfrak{M}_v . Considérons par ailleurs un élément non nul $x + \mathfrak{M}_{\hat{v}}$ de $k_{\hat{v}}$. Il existe une suite d'éléments $(x_n)_{n \in \mathbb{N}}$ de A_v qui

converge vers x (cf. a)). Si n est assez grand, l'on a $\hat{v}(x_n) = \hat{v}(x) > 0$ (lemme 5.12), d'où $\hat{v}(x_n - x) \geq \hat{v}(x) > 0$. Pour un tel entier n , l'on a donc $x \equiv x_n \pmod{\mathfrak{M}_{\hat{v}}}$. Cela prouve que l'application précédente est surjective. D'où l'assertion.

Quant à l'assertion d), c'est une conséquence directe du lemme 5.12 : si $x \in \hat{K}^*$, on choisit une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de K qui converge vers x . Si n est assez grand, l'on a $v(x_n) = \hat{v}(x_n) = \hat{v}(x)$ et $\hat{v}(\hat{K})$ est donc contenu dans $v(K)$. D'où le résultat.

Terminons ce paragraphe par l'énoncé suivant :

Proposition 5.4. *Soit (K, v) un corps valué complet tel que v ne soit pas triviale. Alors K n'est pas dénombrable.*

Démonstration : D'après l'Appendice II tout espace métrique complet est un espace de Baire, autrement dit, si $(F_n)_{n \in \mathbb{N}}$ est une suite de fermés d'intérieur vide, la réunion des F_n est aussi d'intérieur vide. Si v n'est pas triviale, le singleton $\{x\}$ est un fermé d'intérieur vide. Si K est dénombrable, puisque K est un espace de Baire, l'intérieur de K , qui n'est autre que K , doit donc être vide, ce qui conduit à une contradiction.

On déduit de là que le corps valué (\mathbb{Q}, v_p) n'est pas complet.

5.4. Complétion de (\mathbb{Q}, v_p) : le corps \mathbb{Q}_p

Rappelons que si p est un nombre premier, v_p désigne la valuation p -adique de \mathbb{Q} qui à un nombre rationnel x associe l'exposant de p dans la décomposition de x en facteurs premiers.

Nous avons déjà défini au chapitre I l'anneau \mathbb{Z}_p des entiers p -adiques et son corps des fractions \mathbb{Q}_p . Rappelons que \mathbb{Z}_p est le sous-anneau de l'anneau produit

$$\prod_{n \geq 1} \mathbb{Z}/p^n \mathbb{Z},$$

formé des éléments $(\dots, x_n, x_{n-1}, \dots, x_1)$ tels que, pour tout entier $n \geq 2$, l'on ait

$$x_n \in \mathbb{Z}/p^n \mathbb{Z} \quad \text{et} \quad \varphi_n(x_n) = x_{n-1},$$

où $\varphi_n : \mathbb{Z}/p^n \mathbb{Z} \rightarrow \mathbb{Z}/p^{n-1} \mathbb{Z}$ est l'homomorphisme qui à la classe d'un entier modulo $p^n \mathbb{Z}$ associe sa classe modulo $p^{n-1} \mathbb{Z}$.

Tout élément non nul α de \mathbb{Q}_p s'écrit de façon unique sous la forme $p^n u$, où u est une unité p -adique et n un entier relatif. Cela permet de définir une valuation discrète \hat{v}_p sur \mathbb{Q}_p en posant

$$\hat{v}_p(\alpha) = n.$$

Si $\alpha = (\dots, x_n, x_{n-1}, \dots, x_1)$ est un élément non nul de \mathbb{Z}_p , $\hat{v}_p(\alpha)$ est le plus grand entier n tel que $\pi_n(\alpha) = x_n = 0$. Le couple $(\mathbb{Q}_p, \hat{v}_p)$ est ainsi un corps valué d'anneau de valuation

\mathbb{Z}_p et d'idéal de valuation $p\mathbb{Z}_p$. Soit $i : \mathbb{Z} \rightarrow \mathbb{Z}_p$ l'homomorphisme diagonal ; il se prolonge en un homomorphisme $j : \mathbb{Q} \rightarrow \mathbb{Q}_p$.

Proposition 5.5. *Le triplet $(\mathbb{Q}_p, \hat{v}_p, j)$ est une complétion de (\mathbb{Q}, v_p) .*

Démonstration : 1) Vérifions que $j(\mathbb{Q})$ est dense dans \mathbb{Q}_p . Soit α un élément de \mathbb{Q}_p . Il existe un entier s tel que $\alpha = p^s u$, où u est unite p -adique. On va prouver qu'il existe une suite de nombres rationnels dont l'image par j converge vers α . Quitte à remplacer α par $p^{-s}\alpha$, on peut supposer que α appartient à \mathbb{Z}_p . Pour tout $n \geq 1$, il existe un élément x_n de $\mathbb{Z}/p^n\mathbb{Z}$ tel que $\alpha = (\dots, x_n, x_{n-1}, \dots, x_1)$. Pour tout n choisissons un entier relatif y_n tel que

$$y_n + p^n\mathbb{Z} = x_n.$$

Alors la suite $(i(y_n))_{n \in \mathbb{N}}$ converge vers α . En effet, l'égalité précédente entraîne que $i(y_n) - \alpha$ appartient au noyau de la projection $\pi_n : \mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z}$, de sorte que $i(y_n) - \alpha$ est dans $p^n\mathbb{Z}_p$ (chap. I). D'où notre assertion.

Par ailleurs, si a est un entier relatif non nul, le plus grand entier n tel que $\pi_n(i(a))$ soit nul, est précisément l'exposant $v_p(a)$ de p dans la décomposition de a en facteurs premiers, qui par définition, n'est autre que $\hat{v}_p(i(a))$. On déduit de là l'égalité (27).

2) Prouvons maintenant que \mathbb{Q}_p est complet. On va montrer pour cela l'analogue du théorème de Bolzano-Weierstrass pour \mathbb{Q}_p :

Lemme 5.13. *De toute suite bornée d'éléments de \mathbb{Q}_p , on peut extraire une sous-suite convergente. En particulier, de toute suite d'éléments de \mathbb{Z}_p , on peut extraire une sous-suite convergente.*

Démonstration : Soit $(\alpha_n)_{n \geq 1}$ une suite d'éléments de \mathbb{Z}_p . Il existe une infinité de termes de cette suite dont l'image par la projection π_1 sur $\mathbb{Z}/p\mathbb{Z}$ soit la même. Il existe donc une sous-suite $(\alpha_n^{(1)})_{n \geq 1}$ de $(\alpha_n)_{n \geq 1}$ et un entier relatif x_1 tels que, pour tout $n \geq 1$, l'on ait $\pi_1(\alpha_n^{(1)}) = x_1 + p\mathbb{Z}$. De même, il existe une sous-suite $(\alpha_n^{(2)})_{n \geq 1}$ de $(\alpha_n^{(1)})_{n \geq 1}$ et un entier relatif x_2 tels que, pour tout $n \geq 1$, l'on ait $\pi_2(\alpha_n^{(2)}) = x_2 + p^2\mathbb{Z}$. Pour tout entier $k \geq 1$, on construit ainsi une suite $(\alpha_n^{(k)})_{n \geq 1}$ d'éléments de \mathbb{Z}_p et un entier x_k tels que l'on ait $\pi_k(\alpha_n^{(k)}) = x_k + p^k\mathbb{Z}$ et que $(\alpha_n^{(k+1)})_{n \geq 1}$ soit une sous-suite de $(\alpha_n^{(k)})_{n \geq 1}$. On obtient en particulier une suite d'entiers relatifs $(x_n)_{n \geq 1}$, et une suite de nombres p -adiques $(\alpha_n^{(n)})_{n \geq 1}$, telles que pour tout $n \geq 1$ l'on ait

$$x_{n+1} \equiv x_n \pmod{p^n\mathbb{Z}} \quad \text{et} \quad \pi_n(\alpha_n^{(n)}) = x_n + p^n\mathbb{Z}.$$

La suite $(x_n + p^n\mathbb{Z})_{n \geq 1}$ est un entier p -adique x . La suite $(\alpha_n^{(n)})_{n \geq 1}$, qui est extraite de $(\alpha_n)_{n \geq 1}$, est convergente de limite x : en effet, pour tout $n \geq 1$, on a $\pi_n(\alpha_n^{(n)} - x) = 0$, i.e. $\alpha_n^{(n)} - x$ appartient à $p^n\mathbb{Z}_p$.

Considérons maintenant une suite bornée $(\alpha_n)_{n \in \mathbb{N}}$ d'éléments de \mathbb{Q}_p . Par définition, il existe un entier $k \geq 0$ tel que l'on ait $\hat{v}_p(\alpha_n) \geq -k$. D'après l'alinéa précédent, on peut extraire de la suite $(p^k \alpha_n)_{n \in \mathbb{N}}$ une sous-suite convergente, ce qui entraîne le résultat.

Terminons la démonstration de la proposition : on considère une suite de Cauchy $(x_n)_{n \in \mathbb{N}}$ d'éléments de \mathbb{Q}_p . Elle est bornée. D'après le lemme 5.13, on peut en extraire une sous-suite convergente, et cela implique la convergence de la suite $(x_n)_{n \in \mathbb{N}}$. Cela prouve que le corps valué $(\mathbb{Q}_p, \hat{v}_p)$ est complet et le résultat.

VI. Développement de Hensel

Considérons un corps valué (K, v) . On suppose dans tout ce paragraphe que K est *complet* et que v est une valuation *discrète non triviale*. On notera A son anneau de valuation, \mathfrak{M} son idéal maximal et $k = A/\mathfrak{M}$ son corps résiduel. Soit π un générateur de \mathfrak{M} . On désignera par S un système de représentants de k dans A . Si $(s_n)_{n \in \mathbb{N}}$ est une suite d'éléments de S , la série de terme général $s_n \pi^n$ est convergente dans A , car K est complet, A est fermé, et la suite $(s_n \pi^n)_{n \in \mathbb{N}}$ tend vers 0[†]. On obtient en fait de cette façon tous les éléments de A :

Théorème 5.3. a) *Tout élément a de A s'écrit de façon unique sous la forme d'une série convergente*

$$(29) \quad a = \sum_{n \geq 0} s_n \pi^n, \quad \text{avec } s_n \in S.$$

b) *De même, tout élément x de K s'écrit sous la forme*

$$(30) \quad x = \sum_{n > -\infty} s_n \pi^n, \quad \text{avec } s_n \in S,$$

où la série ne comporte qu'un nombre fini de termes à exposants négatifs. On dit que l'égalité (30) est le *développement de Hensel* de x .

Démonstration : L'assertion b) résulte de a) par homothétie. Soit a un élément de A . Il existe un élément s_0 de S tel que l'on ait $a \equiv s_0 \pmod{\pi.A}$. Soit a_1 un élément de A tel que $a = s_0 + a_1 \pi$. De même, il existe $s_1 \in S$ tel que $a_1 \equiv s_1 \pmod{\pi.A}$, et il existe a_2 dans

[†] Pour qu'une série $\sum x_n$ d'éléments de K soit convergente dans K il faut et il suffit que la suite $(x_n)_{n \in \mathbb{N}}$ converge vers 0. En effet, soit $(S_n)_{n \in \mathbb{N}}$ la suite des sommes partielles. Si $(x_n)_{n \in \mathbb{N}}$ tend vers 0, pour tout $c > 0$, l'on a $v(S_{k+1} - S_k) > c$ dès que k est assez grand. Par ailleurs, étant donnés deux entiers m et n avec $m > n$, l'on a

$$v(S_m - S_n) \geq \inf(v(S_m - S_{m-1}), \dots, v(S_{n+1} - S_n)).$$

Il en résulte que si m et n sont assez grands, l'on a $v(S_m - S_n) > c$. Cela montre que la suite $(S_n)_{n \in \mathbb{N}}$ est de Cauchy. Puisque K est complet, elle est donc convergente. D'où l'assertion.

A tel que $a = s_0 + s_1\pi + a_2\pi^2$. En recommençant ce processus, on construit ainsi une série convergente de limite a . Supposons par ailleurs, que l'on ait

$$\sum_{n \geq 0} s_n \pi^n = \sum_{n \geq 0} s'_n \pi^n, \quad \text{avec } s_n \text{ et } s'_n \in S.$$

Les images de s_0 et s'_0 dans k sont égales, ce qui entraîne l'égalité $s_0 = s'_0$. Par récurrence, on déduit alors, par le même argument, que $s_n = s'_n$ pour tout n . D'où le résultat.

Exemple. Si $K = \mathbb{Q}_p$, on peut prendre pour S l'ensemble des entiers k tels que $0 \leq k < p$. On peut aussi prendre la réunion de $\{0\}$ et des racines $p - 1$ -ièmes de l'unité (cf. chap. VI).

Remarque. Soit $x = (\dots, x_{n+1}, x_n, \dots, x_2, x_1)$ un élément de \mathbb{Z}_p ($x_n \in \mathbb{Z}/p^n\mathbb{Z}$). Soit par ailleurs, $x = \sum_{k \geq 0} s_k p^k$ le développement de Hensel de x , où les s_k sont des entiers compris entre 0 et $p - 1$. Alors, pour tout $n \geq 1$ on a

$$(31) \quad x_n = \sum_{k=0}^{n-1} s_k p^k + p^n \mathbb{Z}.$$

En effet, il existe des entiers r_k compris entre 0 et $p - 1$ tels que l'on ait

$$x_n = \sum_{k=0}^{n-1} r_k p^k + p^n \mathbb{Z}.$$

Si $i : \mathbb{Z} \rightarrow \mathbb{Z}_p$ est le plongement canonique, on a donc pour tout $n \geq 1$ (cf. chap. I)

$$x - i\left(\sum_{k=0}^{n-1} r_k p^k\right) \in p^n \mathbb{Z}_p,$$

ce qui entraîne $x = \sum_k i(r_k p^k)$, i.e. $x = \sum_k r_k p^k$ (en identifiant \mathbb{Z} et $i(\mathbb{Z})$). L'unicité du développement de Hensel entraîne alors $r_k = s_k$, ce qui prouve l'égalité (31).

Exercices

- 1) Déterminer le développement de Hensel de $1/3$ dans le corps \mathbb{Q}_5 .
- 2) Soit x un élément de \mathbb{Z}_p . Connaissant le développement de Hensel de x , déterminer celui de $-x$.

VII. Caractérisation des corps valués localement compacts

On considère dans tout ce paragraphe un corps valué (K, v) tel v ne soit pas la valuation triviale. On notera A_v son anneau de valuation, \mathfrak{M}_v son idéal de valuation et k_v son corps résiduel. On va démontrer le résultat suivant :

Proposition 5.6. *Les conditions suivantes sont équivalentes :*

- a) *le corps K est localement compact ;*
- b) *l'anneau A_v est compact ;*
- c) *le corps K est complet, v est une valuation discrète, et k_v est un corps fini.*

Démonstration : Prouvons d'abord quelques résultats préliminaires. Dans ce qui suit, $(L, |\cdot|)$ désigne un corps valué tel que $|\cdot|$ ne soit pas la valeur absolue triviale.

Lemme 5.14. *Soient a et b deux points de L , et B_a, B_b deux boules fermées de centres a et b et de rayons r_a et r_b strictement positifs. Alors, il existe une boule fermée contenue dans B_a qui est homéomorphe à B_b . En particulier, s'il existe une boule fermée de L de rayon strictement positif qui est compacte, toutes les boules fermées de L sont aussi compactes.*

Démonstration : Par hypothèse, il existe $\lambda \in L^*$ tel que $|\lambda| \neq 1$. Il existe n dans \mathbb{Z} tel que l'on ait $|\lambda|^n r_b \leq r_a$. Posons $\mu = a - \lambda^n b$. L'application $x \mapsto \lambda^n x + \mu$, envoie homéomorphiquement la boule B_b sur la boule de centre a et de rayon $|\lambda|^n r_b$, et cette boule est contenue dans B_a . Cela prouve la première partie de l'énoncé. Considérons maintenant une boule fermée B_0 de L de rayon strictement positif qui soit compacte. Soit B une autre boule fermée de L de rayon strictement positif. Il existe une boule fermée B' contenue dans B_0 qui est homéomorphe à B . Puisque B_0 est compacte et que B' est fermée, B' est compacte, et donc B aussi. Par ailleurs, les boules fermées de rayon nul sont des singletons, et ce sont des parties compactes. D'où le lemme.

Lemme 5.15. *Les conditions suivantes sont équivalentes :*

- a) *le corps L est localement compact ;*
- b) *toutes les boules fermées de L sont compactes.*
- c) *toutes les boules ouvertes de L sont compactes.*

Démonstration : L'implication $a) \implies b)$: d'après le lemme 5.14, tout revient à prouver l'existence d'une boule fermée de rayon strictement positif qui soit compacte. On considère pour cela un voisinage compact V de 0. Il existe une boule fermée B de centre 0 et de rayon strictement positif contenue dans V , qui est donc compacte. D'où le résultat.

L'implication $b) \implies c)$: soit B une boule ouverte de L . C'est une partie fermée de L et elle est contenue dans une boule fermée, qui est compacte par hypothèse. Donc B est compacte.

L'implication $c) \implies a)$: l'ensemble des boules ouvertes de L de centre $a \in L$ forme un système fondamental de voisinages de a . Si ces boules sont compactes, L est donc localement compact. D'où le lemme.

Corollaire 5.3. *Supposons L localement compact. Alors, L est complet.*

Démonstration : Soit $(x_n)_{n \in \mathbb{N}}$ une suite de Cauchy de L . Puisque $(x_n)_{n \in \mathbb{N}}$ est bornée, tous les x_n appartiennent à une boule fermée B centrée en 0. Le corps L étant localement

compact, la boule B est compacte (lemme 5.15) et l'on peut donc extraire de la suite $(x_n)_{n \in \mathbb{N}}$ une suite convergente. Puisque $(x_n)_{n \in \mathbb{N}}$ est une suite de Cauchy, elle est donc convergente. D'où notre assertion.

Démontrons maintenant la proposition 5.6. L'équivalence des assertions a) et b) résulte directement des lemmes 5.14 et 5.15.

L'implication $b) \implies c)$: supposons que k_v soit infini. Il existe alors une famille infinie d'éléments $(x_n)_{n \in \mathbb{N}}$ de A_v deux à deux non congrus modulo \mathfrak{M}_v . Si m et n sont deux entiers distincts, l'on a donc $v(x_n - x_m) = 0$. On ne peut donc pas extraire de cette suite une sous-suite convergente, ce qui contredit la compacité de A_v . Supposons maintenant que $v(K^*)$ soit dense dans \mathbb{R} . Il existe alors une suite strictement croissante d'éléments de $v(K^*)$ qui sont tous strictement compris entre 0 et 1. Pour tout n , on choisit alors un élément x_n de K^* tel que $v(x_n) = r_n$. Puisque $r_n \geq 0$, les x_n sont dans A_v . De plus, si m et n sont deux entiers tels que $m > n$, l'on a $v(x_n - x_m) = \inf(v(x_n), v(x_m)) = r_n \leq 1$. Cela montre qu'il n'existe pas de sous-suite de (x_n) convergente, ce qui conduit de nouveau à une contradiction. Enfin, le fait que K soit complet résulte du cor. 5.3.

L'implication $c) \implies a)$: soit $(x_n)_{n \in \mathbb{N}}$ une suite infinie d'éléments de A_v . Montrons qu'elle possède une sous-suite convergente dans A_v . Soit q le cardinal de k_v . Il existe une infinité de termes de la suite $(x_n)_{n \in \mathbb{N}}$ qui appartiennent à une même classe modulo \mathfrak{M}_v . Soit y_1 l'un des éléments x_i de A_v qui soit dans cette classe résiduelle. On considère alors le groupe quotient $\mathfrak{M}_v / \mathfrak{M}_v^2$. Il est de cardinal q (cf. le lemme 2.6 du chap. II, appliqué avec l'anneau A_v , qui est de valuation discrète, et l'idéal \mathfrak{M}_v qui est premier non nul). Il existe donc une partition de l'ensemble $y_1 + \mathfrak{M}_v$ en q sous-ensembles disjoints. L'un d'entre eux contient donc une infinité de termes de la suite x_n . Soit y_2 l'un de ces termes. On construit ainsi par récurrence une sous-suite $(y_n)_{n \in \mathbb{N}}$ de la suite $(x_n)_{n \in \mathbb{N}}$ tel que, pour tout entier $n \geq 1$, l'ensemble $y_{n+1} + \mathfrak{M}_v^{n+1}$ soit contenu dans $y_n + \mathfrak{M}_v^n$. Pour tout $n \geq 1$, $y_{n+1} - y_n$ appartient donc à \mathfrak{M}_v^n . Par ailleurs, la valuation v étant discrète et non triviale, il existe un nombre réel $a > 0$ tel que l'on ait $v(K^*) = a\mathbb{Z}$. De plus, l'idéal \mathfrak{M}_v est principal et est engendré par un élément de valuation a . Il en résulte l'inégalité $v(y_{n+1} - y_n) \geq na$. Cela montre que la suite $(y_n)_{n \in \mathbb{N}}$ est une suite de Cauchy. Puisque K est supposé complet, elle est donc convergente. Or A_v étant une partie fermée, la limite est dans A_v , ce qui prouve que A_v est compact. D'où la proposition.

Remarque. Si v est triviale, les assertions a) et b) de la prop. 5.6 ne sont pas équivalentes. En effet, supposons que K soit infini. Puisque la topologie associée à v sur K est discrète, K est localement compact. Pour autant, on $A_v = K$, et pour que K soit compact, il faudrait qu'il soit fini.

On déduit de là :

Corollaire 5.4. *Le corps \mathbb{Q}_p est localement compact et l'anneau \mathbb{Z}_p est compact.*

Chapitre VI — Lemme de Hensel et applications

On considère dans les paragraphes I, II et III de ce chapitre un corps valué (K, v) **complet**. On notera respectivement A , \mathfrak{M} et k l'anneau de valuation, l'idéal de valuation et le corps résiduel de (K, v) .

Le lemme de Hensel est un critère de réductibilité des polynômes à coefficients dans A . On notera $A[X]$ (resp. $k[X]$) l'anneau des polynômes à coefficients dans A (resp. dans k). Si P est un élément de $A[X]$, on désignera par P' le polynôme dérivé de P et par \bar{P} son image dans $k[X]$ par la surjection canonique.

I. Première version du lemme de Hensel

Il existe en fait plusieurs versions du lemme de Hensel. Nous nous intéresserons ici à celle fournissant un critère très commode pour démontrer qu'un polynôme de $A[X]$ possède une racine dans A .

Théorème 6.1. *Soit P un polynôme de $A[X]$. Soit α un élément de A tel que l'on ait l'inégalité*

$$(1) \quad v(P(\alpha)) > 2v(P'(\alpha)).$$

Alors, il existe un unique élément a de A tel que $P(a) = 0$ et que $v(a - \alpha) > v(P'(\alpha))$.

Démonstration : Remarquons d'abord que l'inégalité (1) entraîne que $P'(\alpha)$ est non nul. On pose

$$\lambda = v(P(\alpha)) - 2v(P'(\alpha)) \quad \text{et} \quad \mu = v(P'(\alpha)).$$

On va construire une suite $(a_n)_{n \in \mathbb{N}}$ d'éléments de A telle que, pour tout $n \geq 0$, l'on ait

$$(*_n) \quad a_0 = \alpha, \quad a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)}, \quad v(P(a_n)) \geq 2^n \lambda + 2\mu \quad \text{et} \quad v(P'(a_n)) = \mu.$$

Posons

$$a_1 = a_0 - \frac{P(a_0)}{P'(a_0)}.$$

Il résulte de (1) que a_1 appartient à A . On vérifie alors que les formules $(*_0)$ sont satisfaites.

Supposons alors qu'il existe un entier naturel n , et une famille d'éléments $(a_k)_{0 \leq k \leq n+1}$ de A , telle que les formules $(*_k)$ soient vérifiées pour tout k tel que $0 \leq k \leq n$. Il existe des éléments c_k et b_k de A , avec $c_1 = P'(a_n)$, tels que l'on ait [†]

$$(2) \quad P(a_{n+1}) = P(a_n) + \sum_{k \geq 1} c_k (a_{n+1} - a_n)^k \quad \text{et} \quad P'(a_{n+1}) = P'(a_n) + \sum_{k \geq 1} b_k (a_{n+1} - a_n)^k.$$

On déduit alors des formules (2) que l'on a

$$v(P(a_{n+1})) \geq 2v(a_{n+1} - a_n) = 2\left(v(P(a_n)) - v(P'(a_n))\right) \geq 2^{n+1}\lambda + 2\mu,$$

puis les égalités

$$v(P'(a_{n+1})) = v(P'(a_n)) = \mu \text{ (on a } \lambda > 0).$$

Il en résulte que l'élément

$$a_{n+2} = a_{n+1} - \frac{P(a_{n+1})}{P'(a_{n+1})},$$

appartient A . D'où l'existence de a_{n+2} et le fait que les formules $(*)_{n+1}$ soient satisfaites. Cela démontre l'existence de la suite $(a_n)_{n \in \mathbb{N}}$.

Pour tout entier n , on a

$$(3) \quad v(a_{n+1} - a_n) \geq 2^n \lambda + \mu,$$

ce qui entraîne que la suite $(a_n)_{n \in \mathbb{N}}$ est de Cauchy. Le corps K étant complet, cette suite est convergente dans K de limite a . Puisque A est fermé, a est dans A . Par ailleurs, la suite $P(a_n)_{n \in \mathbb{N}}$ est convergente de limite 0, et P étant une fonction continue sur K , la suite $P(a_n)_{n \in \mathbb{N}}$ converge vers $P(a)$. D'où $P(a) = 0$.

Enfin, pour tout entier $n \geq 0$, on a

$$a_n - \alpha = \sum_{k=0}^{n-1} (a_{k+1} - a_k),$$

d'où il résulte l'inégalité $v(a_n - \alpha) \geq \lambda + \mu$ (cf. (3)), puis par passage à la limite, $v(a - \alpha) > \mu$ (cf. lemme 5.12). D'où l'existence de a .

Considérons maintenant deux éléments a et b dans A satisfaisant à la conclusion du théorème. Montrons que $a = b$. On remarque d'abord que l'on a $v(P'(b)) = v(P'(\alpha))$. En effet, d'après le rappel [†] ci-dessous, en substituant X par α et Y par $b - \alpha$, on a après dérivation par rapport à X ,

$$P'(b) = P'(\alpha) + P''(\alpha)(b - \alpha) + \sum_{k \geq 2} f'_k(\alpha)(b - \alpha)^k,$$

[†] Rappelons qu'étant donné un polynôme f à coefficients dans A , et deux indéterminées X et Y , il existe des polynômes f_k de $A[X]$ tels que l'on ait

$$f(X + Y) = \sum_{k \geq 0} f_k(X) Y^k \quad \text{avec} \quad k! f_k(X) = f^{(k)}(X),$$

où $f^{(k)}(X)$ est le polynôme dérivé d'ordre k de f .

et par hypothèse on a $v(b - \alpha) > v(P'(\alpha))$. Par ailleurs, on a

$$0 = (a - b) \left(P'(b) + \sum_{k \geq 2} f_k(b)(a - b)^{k-1} \right),$$

et $v(a - b) > v(P'(\alpha))$, i.e. $v(a - b) > v(P'(b))$. On en déduit alors que $a = b$. Cela termine la démonstration du théorème.

Corollaire 6.1. *Soit P un polynôme de $A[X]$. Soit α un élément de A tel que $\alpha + \mathfrak{M}$ soit une racine simple de \bar{P} . Alors, il existe un unique élément a dans A tel que $P(a) = 0$ et que $v(a - \alpha) > 0$.*

Démonstration : Par hypothèse, on a $v(P'(\alpha)) = 0$ et $v(P(\alpha)) > 0$. Le théorème 6.1 entraîne alors directement le résultat.

Remarque. L'hypothèse de complétude du corps valué (K, v) dans le th. 6.1 est indispensable. Par exemple, si l'on prend $(K, v) = (\mathbb{Q}, v_p)^\dagger$, où v_p est la valuation p -adique associée à un nombre premier p , le théorème ne s'applique pas ; en effet, le polynôme $P = X^2 + (2p + 1)X + p$ est irréductible sur \mathbb{Q} , bien que 0 soit racine simple de \bar{P} : on a $\bar{P} = X(X + 1)$.

II. Deuxième version du lemme de Hensel

Étant donnés trois polynômes P , F et G dans $A[X]$ tels que $P = FG$, on a par réduction dans $k[X]$ l'égalité $\bar{P} = \bar{F}\bar{G}$. Par conséquent, afin de factoriser un polynôme de $A[X]$, on peut chercher à le factoriser dans $k[X]$, puis ensuite essayer de trouver un relèvement de cette factorisation dans $A[X]$. Le corps K étant supposé complet, cela est possible dans de nombreuses situations :

Théorème 6.2. *Soit P un polynôme de $A[X]$ non nul modulo \mathfrak{M} (on dit qu'un tel polynôme est primitif). Soient f et g deux polynômes premiers entre eux de $k[X]$ tels que l'on ait $\bar{P} = fg$. Alors, il existe deux polynômes F et G de $A[X]$ possédant les propriétés suivantes :*

$$P = FG, \quad \bar{F} = f, \quad \bar{G} = g \quad \text{et} \quad \text{degré de } G = \text{degré de } g.$$

De plus, si g est unitaire, G peut aussi être choisi unitaire.

On admettra cet énoncé dont la démonstration est trop longue pour être donnée ici (cf. [Am], p. 58). Nous allons plutôt nous intéresser à une conséquence de ce résultat que l'on utilisera dans le chapitre suivant. Introduisons d'abord une notation :

[†] Une façon de prouver que le corps valué (\mathbb{Q}, v_p) n'est pas complet est de remarquer que \mathbb{Q} est dénombrable et d'utiliser la prop. 5.4.

Notation. Étant donné un polynôme $P = a_0 + a_1X + \dots + a_nX^n$ de $K[X]$, on notera

$$(4) \quad w(P) = \inf_i (v(a_i)).$$

Si $w(P) = 0$, les a_i sont alors tous dans A , et dans ce cas P est un polynôme primitif.

Proposition 6.1. *Soit $P = a_0 + a_1X + \dots + a_nX^n$ un polynôme irréductible de $K[X]$. On a l'égalité*

$$w(P) = \inf(v(a_0), v(a_n)).$$

Démonstration : On peut supposer que P est dans $A[X]$ et que $w(P) = 0$. En effet, si $v(a_i) = w(P)$, le polynôme a_iP est dans $A[X]$ et $w(a_i^{-1}P) = 0$. Par ailleurs, si la conclusion de l'énoncé est satisfaite pour $a_i^{-1}P$, on a $w(a_i^{-1}P) = \inf(v(a_i^{-1}a_0), v(a_i^{-1}a_n))$, ce qui entraîne le résultat.

Montrons alors que l'on a $\inf(v(a_0), v(a_n)) = 0$. Supposons le contraire. Puisque $P \in A[X]$, cela signifie que $\inf(v(a_0), v(a_n)) > 0$. Puisque $w(P) = 0$, il existe donc un entier s , $0 < s < n$, tel que l'on ait $v(a_i) > 0$ pour tout $i < s$, et que $v(a_s) = 0$. Le polynôme de $k[X]$ déduit de P par réduction est ainsi de la forme $X^s h$, où X ne divise pas h . D'après le théorème 6.2, il existe des polynômes F et G de $A[X]$ tels que l'on ait $P = FG$ et que le degré de G soit s . Cela contredit le fait que P soit irréductible car $0 < s < n$. D'où le résultat.

Corollaire 6.2. *Soit $P = a_0 + a_1X + \dots + a_nX^n$ un polynôme irréductible unitaire de $K[X]$ (on a $a_n = 1$). Alors, P appartient à $A[X]$ si et seulement si $P(0)$ est dans A .*

Démonstration : Si $P(0)$ est dans A , on a $\inf(v(a_0), v(a_n)) = 0$, ce qui d'après la prop. 6.1 entraîne que tous les coefficients de P sont dans A .

Corollaire 6.3. *Soit L une extension finie de K . Soit x un élément de L . Alors, la norme de L sur K de x appartient à A si et seulement si le polynôme minimal de x sur K appartient à $A[X]$.*

Démonstration : Le terme constant du polynôme caractéristique de x est par définition $(-1)^n N_{L/K}(x)$, où n est le degré de L sur K . Par ailleurs, le polynôme caractéristique de x est une puissance du polynôme minimal P de x (cf. le lemme 3.1 du Chap. III). Si P est dans $A[X]$, les puissances de son terme constant sont dans A et donc $N_{L/K}(x)$ aussi. Inversement, supposons que $N_{L/K}(x)$ soit dans A . Soit c le terme constant de P . D'après le corollaire 6.2, il suffit de montrer que c est dans A , ce qui provient du fait que l'on a $v(N_{L/K}(x)) = kv(c)$ pour un certain entier naturel k , et donc que $v(c)$ est positif. D'où le résultat.

Nous allons maintenant établir quelques conséquences du lemme de Hensel.

III. Structure du groupe des unités

Nous supposons de plus dans ce paragraphe que la condition suivante est réalisée :

le corps résiduel k de K est fini.

On notera q le cardinal de k et μ_{q-1} le groupe des racines $q-1$ -ièmes de l'unité contenues dans une clôture algébrique de K .

Proposition 6.2. *Soient n un entier premier à q et d le pgcd de n et $q-1$. Alors, le polynôme $X^n - 1$ possède exactement d racines distinctes dans K . En particulier, le corps K contient μ_{q-1} .*

Démonstration : Posons $F = X^d - 1$, $G = X^{q-1} - 1$ et $P = X^n - 1$. Montrons d'abord que P possède au moins d racines distinctes dans K . On remarque pour cela que le polynôme $\bar{F} \in k[X]$ a d racines distinctes dans k . En effet, \bar{G} a $q-1$ racines distinctes dans k (car tout élément x de k^* vérifie $x^{q-1} = 1$), et \bar{F} divise \bar{G} . D'après le corollaire 6.1, on peut alors relever les racines de \bar{F} en d racines $(a_i)_{1 \leq i \leq d}$ de F dans A non congrues deux à deux modulo \mathfrak{M} . Puisque P est divisible par F , les a_i sont donc d racines distinctes de P . D'où notre assertion.

Considérons alors une racine b de P dans K . On a $b^n = 1$ et $b + \mathfrak{M}$ est une racine de \bar{P} . C'est aussi une racine de \bar{F} : en effet, il existe deux entiers r et s tels que $d = nr + (q-1)s$, et cela entraîne $(b + \mathfrak{M})^d = 1$. L'un des éléments a_i , par exemple a_1 , est donc congru à b modulo \mathfrak{M} . Montrons alors que l'on a $b = a_1$. Supposons pour cela $b \neq a_1$. Puisque a_1 est inversible dans A (c'est une racine de l'unité), il existe z dans \mathfrak{M} , non nul, tel que l'on ait $b = a_1(1 + z)$. On a ainsi $(1 + z)^n = 1$. D'où l'égalité $z^{n-1} + \dots + C_n^2 z + n = 0$, ce qui conduit à une contradiction : en effet, on a $n \geq 2$ (car $z \neq 0$), et tous les termes de cette somme sont dans \mathfrak{M} , donc n doit être dans \mathfrak{M} , ce qui n'est pas, car n et q sont premiers entre eux. D'où le résultat.

Proposition 6.3. *Soient U le groupe des unités de A et U^1 le sous-ensemble de U formé des éléments x tels que $v(x-1) > 0$. Alors, U^1 est un sous-groupe de U et l'on a l'égalité*

$$(5) \quad U = \mu_{q-1} \times U^1.$$

Démonstration : Soit p la caractéristique de k : q est une puissance de p . On pose $v(p) = e$ (on a $e = +\infty$ si K est de caractéristique p). On va d'abord démontrer les lemmes suivants :

Lemme 6.1. *Soit u un élément de A . On a l'inégalité*

$$(6) \quad v((1+u)^q - 1) \geq \inf(e + v(u), qv(u)).$$

Démonstration : D'après la formule du binôme on a

$$(1+u)^q - 1 = u^q + \sum_{i=1}^{q-1} C_q^i u^i := u^q + t.$$

Par ailleurs, on a

$$iC_q^i = q C_{q-1}^{i-1}.$$

On déduit de là que $v(C_q^i) \geq v(q) - v(i)$. Puisque q est une puissance de p , pour tout i compris entre 1 et $q - 1$, on a $v(q) - v(i) \geq v(p) = e$. On a donc $v(t) \geq e + v(u)$, ce qui entraîne le lemme.

Lemme 6.2. *Soit a une unité de A . Alors, la suite $(a^{q^n})_{n \in \mathbb{N}}$ converge vers un élément $\omega(a)$ de μ_{q-1} . On a de plus la congruence $a \equiv \omega(a) \pmod{\mathfrak{M}}$.*

Démonstration : Pour tout $\alpha \in U$, on a $\alpha^{q-1} \equiv 1 \pmod{\mathfrak{M}}$, i.e. on a $v(\alpha^q - \alpha) > 0$. Ainsi, pour tout entier $n \geq 1$, on a $v(a^{q^n} - a^{q^{n-1}}) > 0$, et il existe un élément u_n de \mathfrak{M} tel que l'on ait $a^{q^n} = a^{q^{n-1}}(1 + u_n)$. On a alors $u_{n+1} = (1 + u_n)^q - 1$. D'après l'inégalité (6), on a

$$v(u_{n+1}) \geq \inf(e + v(u_n), qv(u_n)).$$

Le nombre $v(u_1)$ étant strictement positif, on déduit de là que pour tout c , $v(u_n)$ est plus grand que c dès que n est assez grand, autrement dit, que la suite $(u_n)_{n \in \mathbb{N}}$ converge vers 0. Or on a $v(a^{q^n} - a^{q^{n-1}}) = v(u_n)$ (car $v(a) = 0$), et donc la suite $(a^{q^n})_{n \in \mathbb{N}}$ est de Cauchy. Elle est donc convergente dans K : soit $\omega(a)$ sa limite.

De l'égalité $a^{q^n} = a^{q^{n-1}}(1 + u_n)$, on déduit alors que $\omega(a)^q = \omega(a)$ ainsi que les congruences $a^{q^n} \equiv a^{q^{n-1}} \equiv a \pmod{\mathfrak{M}}$. L'ensemble $a + \mathfrak{M}$ étant une partie fermée de K , $\omega(a) - a$ appartient à \mathfrak{M} . En particulier, $\omega(a)$ n'est pas nul et l'on a $\omega(a)^{q-1} = 1$. D'où le lemme.

Remarque. On déduit du lemme 6.2 un homomorphisme surjectif de groupes de U sur μ_{q-1} qui à x associe $\omega(x)$. En effet, si $(a_i)_{1 \leq i \leq q-1}$ est avec $\{0\}$ un système de représentants de k dans A , on a $\omega(a_i) \neq \omega(a_j)$ pour $i \neq j$ ($\omega(a_i)$ n'est pas congru à $\omega(a_j)$ modulo \mathfrak{M}).

Démontrons maintenant la proposition 6.3. Vérifions d'abord que U^1 est un sous-groupe de U . Il est clair que le produit de deux éléments de U^1 est dans U^1 . Soit x un élément de U^1 . Vérifions qu'il est inversible dans U^1 . On pose pour cela $x = 1 - z$, où z appartient à \mathfrak{M} . On a

$$(7) \quad 1 - z^n = (1 - z) \left(\sum_{i=0}^{n-1} z^i \right).$$

Puisque z est dans \mathfrak{M} , la suite $(z^n)_{n \in \mathbb{N}}$ converge vers 0, et ainsi la série de terme général z^n est aussi convergente. Soit l sa limite. Alors, l appartient à U^1 (car \mathfrak{M} est une partie fermée de K , donc U^1 aussi, et chaque somme partielle de la série $\sum z^n$ appartient à U^1), et d'après (7), on a $xl = 1$. D'où notre assertion.

Considérons alors un élément a de U . D'après la congruence $a \equiv \omega(a) \pmod{\mathfrak{M}}$ (lemme 6.2), il existe un élément z de \mathfrak{M} tel que l'on ait $a = \omega(a)(1 + z) \in \mu_{q-1} \times U^1$. Par ailleurs,

une telle écriture est unique. En effet, il s'agit de montrer que $\mu_{q-1} \cap U^1 = \{1\}$: soient ζ une racine $q-1$ -ième de l'unité autre que 1, et z un élément de \mathfrak{M} tels que $\zeta = 1 + z$. On a alors

$$1 = \zeta^{q-1} = 1 + z^{q-1} + \dots + (q-1)z.$$

Puisque z n'est pas nul et que $q-1$ n'est pas dans \mathfrak{M} , la valuation de $z^{q-1} + \dots + (q-1)z$ est $v(z)$, de sorte que cet élément ne peut être nul. D'où une contradiction et notre assertion. Cela termine la démonstration de la prop. 6.2.

Corollaire 6.4. *Supposons que la valuation v soit discrète et non triviale. Alors, le groupe multiplicatif de K est isomorphe au groupe produit $\mathbb{Z} \times \mu_{q-1} \times U^1$. Plus précisément, si π est une uniformisante de \mathfrak{M} , on a l'égalité*

$$K^* = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^1.$$

Démonstration : Soit x un élément de K^* . Posons $n = v(x)$. On a $x = \pi^n u$, où u est une unité de A , et d'après la prop. 6.2, u est le produit d'une racine $q-1$ -ième de l'unité et d'un élément de U^1 . Par ailleurs, 1 étant la seule puissance de π qui soit une unité, on a $\pi^{\mathbb{Z}} \cap (\mu_{q-1} \times U^1) = \{1\}$. D'où le résultat.

IV. Polynômes d'Eisenstein

Nous allons maintenant énoncer un critère très utile d'irréductibilité des polynômes à coefficients dans un anneau de valuation, dont le corps des fractions n'est pas nécessairement complet. Soient (K, v) un corps valué, A son anneau de valuation et \mathfrak{M} son idéal de valuation.

Proposition 6.4. *(Critère d'Eisenstein) Soit P un polynôme unitaire de degré $n \geq 1$ à coefficients dans A :*

$$P = X^n + a_1 X^{n-1} + \dots + a_n.$$

Si pour tout entier j tel que $1 \leq j \leq n$, l'on a $a_j \in \mathfrak{M}$ et si $a_n \notin \mathfrak{M}^2$, alors P est irréductible dans $K[X]$.

Démonstration : On prouve d'abord le lemme général suivant :

Lemme 6.3. *Soit B un anneau intégralement clos de corps des fractions L . Soient f et g deux polynômes unitaires à coefficients dans L tels que le polynôme fg soit dans $B[X]$. Alors, f et g sont dans $B[X]$.*

Démonstration : Soient (α_i) et (β_i) les racines respectivement de f et g dans une clôture algébrique de L . Soient M l'extension de L obtenue en adjoignant à L les α_i et les β_i et C la fermeture intégrale de B dans M . Puisque fg est unitaire à coefficients dans B , les α_i et β_i sont dans C . Les polynômes f et g étant unitaires, leurs coefficients

appartiennent donc à $L \cap C$, qui n'est autre que B d'après l'hypothèse faite sur B . D'où le lemme.

Démontrons maintenant la proposition. Supposons que P soit réductible. D'après le lemme 6.3, on a une égalité de la forme $P = P_1 P_2$, où P_1 et P_2 sont deux polynômes unitaires de $A[X]$ non constants. On écrit P_1 et P_2 sous la forme

$$P_1 = b_0 + b_1 X + \dots + b_{k-1} X^{k-1} + X^k \quad \text{et} \quad P_2 = c_0 + c_1 X + \dots + c_{h-1} X^{h-1} + X^h,$$

avec h et k non nuls. On a $b_0 c_0 = a_n$. Par exemple c_0 est dans \mathfrak{M} et pas b_0 . Par ailleurs, on a $a_{n-1} = c_0 b_1 + b_0 c_1$, d'où il résulte que c_1 est aussi dans \mathfrak{M} . On déduit de cette façon de proche en proche que c_i est dans \mathfrak{M} pour tout i tel que $1 \leq i \leq h-1$. On déduit de là que $\bar{P}_2 = X^h$. Puisque $\bar{P}_1 \bar{P}_2 = X^n$, on a donc $\bar{P}_1 = X^k$. Il en résulte que b_0 et c_0 sont dans \mathfrak{M} , et donc que $a_n = b_0 c_0$ appartient à \mathfrak{M}^2 , ce qui conduit à une contradiction. D'où la proposition.

Un polynôme qui satisfait au critère de la proposition est appelé un polynôme d'Eisenstein. On notera que la prop. 6.4 est encore valable en remplaçant A par un anneau principal et \mathfrak{M} par un idéal maximal de A .

V. Quelques applications au corps \mathbb{Q}_p

Proposition 6.5. *Soient l et p deux nombres premiers. Les corps \mathbb{Q}_p et \mathbb{Q}_l sont isomorphes si et seulement si $l = p$.*

Démonstration : Supposons $l \neq p$. Pour montrer que \mathbb{Q}_p et \mathbb{Q}_l ne sont pas isomorphes, il suffit de prouver qu'il existe un polynôme à coefficients dans \mathbb{Q} qui soit irréductible dans $\mathbb{Q}_p[X]$ et réductible dans $\mathbb{Q}_l[X]$ (si φ est un isomorphisme de \mathbb{Q}_p sur \mathbb{Q}_l , l'homomorphisme d'anneaux de $\mathbb{Q}_p[X]$ dans $\mathbb{Q}_l[X]$ qui à $\sum a_k X^k$ associe $\sum \varphi(a_k) X^k$ est un isomorphisme sur $\mathbb{Q}_l[X]$, qui fixe les polynômes à coefficients dans \mathbb{Q}). On considère un entier n tel que $n \equiv 0 \pmod{p}$ et $n \equiv 1 \pmod{l}$. Posons $F = X^2 + nX + pl$. D'après le critère d'Eisenstein, F est irréductible sur \mathbb{Q}_p . Par ailleurs, le polynôme déduit de F par réduction modulo l , à coefficients dans $\mathbb{Z}/l\mathbb{Z}$, est $X(X+1)$. Puisque \mathbb{Q}_l est complet, il résulte du lemme de Hensel que F est réductible sur \mathbb{Q}_l . D'où le résultat.

Proposition 6.6. *Le seul endomorphisme du corps \mathbb{Q}_p est l'identité.*

Démonstration : Soit $\varphi : \mathbb{Q}_p \rightarrow \mathbb{Q}_p$ un endomorphisme de corps. Montrons que φ est une application continue (pour la topologie associée à \hat{v}_p), ou ce qui revient au même que φ est continue en 0. Il suffit pour cela de montrer que pour tout $x \in \mathbb{Q}_p$, l'on a $\hat{v}_p(x) = \hat{v}_p(\varphi(x))$. Puisque φ fixe les éléments de \mathbb{Q} , il suffit donc de vérifier que l'image par φ d'une unité p -adique est aussi une unité p -adique. C'est une conséquence directe du lemme suivant :

Lemme 6.4. Soit u un élément non nul de \mathbb{Q}_p . Alors, u est une unité p -adique si et seulement si il existe une infinité d'entiers naturels n tels que u^{p-1} soit une puissance n -ième dans \mathbb{Q}_p .

Démonstration : Supposons qu'il existe une infinité d'entiers naturels n tels que u^{p-1} soit une puissance n -ième dans \mathbb{Q}_p . Dans ce cas $(p-1)\hat{v}_p(u)$ est divisible par une infinité d'entiers n et l'on doit avoir $\hat{v}_p(u) = 0$, i.e. u est une unité p -adique.

Inversement, supposons que u soit une unité p -adique. Puisque $\mathbb{Z}_p/p\mathbb{Z}_p$ est le corps à p éléments, et que u n'est pas nul modulo $p\mathbb{Z}_p$, on a $u^{p-1} \equiv 1 \pmod{p\mathbb{Z}_p}$. Pour tout entier $n \geq 1$, le polynôme déduit de $X^n - u^{p-1}$ par réduction modulo $p\mathbb{Z}_p$ est donc $X^n - 1$. Si n n'est pas multiple de p , 1 est une racine simple de $X^n - 1$ modulo $p\mathbb{Z}_p$. D'après le lemme de Hensel, pour les entiers n non multiples de p , u^{p-1} est donc une puissance n -ième dans \mathbb{Z}_p . D'où le lemme.

La proposition se déduit alors comme suit : l'application φ est continue sur \mathbb{Q}_p et vaut l'identité sur \mathbb{Q} . Puisque \mathbb{Q} est dense dans \mathbb{Q}_p , φ est donc l'identité sur \mathbb{Q}_p . D'où le résultat.

Nous allons maintenant déterminer les éléments de \mathbb{Q}_p qui sont des carrés.

Proposition 6.7. Supposons $p \neq 2$. Soit $x = p^n u$ un élément de \mathbb{Q}_p^* , où n est un entier, et u une unité p -adique. Alors, x est un carré dans \mathbb{Q}_p si et seulement si n est pair et l'image de u dans $\mathbb{Z}_p/p\mathbb{Z}_p$ est un carré.

Démonstration : Tout revient à déterminer les unités p -adiques qui sont des carrés. Supposons l'image de u dans $\mathbb{Z}_p/p\mathbb{Z}_p$ soit un carré. Posons $F = X^2 - u$. Il existe donc un élément $b \in \mathbb{Z}_p$ non divisible par p tel que l'on ait $F(b) \equiv 0 \pmod{p\mathbb{Z}_p}$. Puisque p est impair, on a $F'(b) = 2b \not\equiv 0 \pmod{p}$. D'après le lemme de Hensel, F possède donc une racine dans \mathbb{Z}_p , i.e. u est un carré dans \mathbb{Z}_p . L'implication réciproque est évidente. D'où le résultat.

Corollaire 6.5. Si p est impair, les unités p -adiques congrues à 1 modulo $p\mathbb{Z}_p$ sont des carrés dans \mathbb{Z}_p [†].

Corollaire 6.6. Si p est impair, le groupe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un système de représentants est $\{1, p, u, pu\}$, où u est une unité p -adique qui n'est pas un carré modulo $p\mathbb{Z}_p$.

Démonstration : Cela provient de la prop. 6.7 et du fait que le produit de deux entiers non carrés modulo p est un carré modulo p .

[†] Plus généralement, si n est un entier premier à p , toute unité p -adique u congrue à 1 modulo p est une puissance n -ième dans \mathbb{Q}_p . En effet, le polynôme déduit de $X^n - u$ par réduction modulo $p\mathbb{Z}_p$ est $X^n - 1$ et 1 est une racine simple de $X^n - 1$ modulo $p\mathbb{Z}_p$ (cf. la démonstration du lemme 6.4). D'où l'assertion.

Proposition 6.8. Soit $x = 2^n u$ un élément de \mathbb{Q}_2^* , où n est un entier, et u une unité 2-adique. Alors, x est un carré dans \mathbb{Q}_2 si et seulement si n est pair et $u \equiv 1 \pmod{8\mathbb{Z}_2}$.

Démonstration : Là encore tout revient à déterminer les unités 2-adiques qui sont des carrés. Si u est une unité de \mathbb{Z}_2 , on a $u \equiv 1 \pmod{2\mathbb{Z}_2}$ (cf. par exemple le développement de Hensel de u), d'où $u^2 \equiv 1 \pmod{8\mathbb{Z}_2}$ (car pour tout $a \in \mathbb{Z}_2$, $a(a+1)$ appartient à $2\mathbb{Z}_2$). Inversement, soit u une unité congrue à 1 modulo 8. Soit $F(X) = X^2 - u$. On a $F(1) \equiv 0 \pmod{8}$ et $F'(1) \not\equiv 0 \pmod{4}$. Le lemme de Hensel entraîne que F a une racine dans \mathbb{Z}_2 (congrue à 1 modulo 4). D'où le résultat.

On déduit de là :

Corollaire 6.7. Le groupe $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. Un système de représentants est $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Exercices

1) Soit f le polynôme de $\mathbb{Z}_2[X]$ défini par $f = X^3 - 2X - 3$. Montrer que f possède une unique racine α dans \mathbb{Z}_2 . Déterminer les premiers termes du développement de Hensel de α .

2) Soit a un entier. Trouver une condition nécessaire et suffisante pour que le polynôme $X^2 + X + a$ ait une racine dans \mathbb{Q}_2 .

3) Montrer que \mathbb{Q}_p^{*2} est un ouvert de \mathbb{Q}_p .

4) Soit p un nombre premier impair. Montrer que $(1 + p\mathbb{Z}_p)^p = 1 + p^2\mathbb{Z}_p$. En déduire que le groupe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*p}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

5) Montrer que, si p est impair, 1 est la seule racine p -ième de l'unité de \mathbb{Q}_p .

6) Soient p un nombre premier impair et F le polynôme $X^2 + (2/p)X - 1$. Montrer que F est irréductible sur \mathbb{Q} mais pas sur \mathbb{Q}_p .

Chapitre VII — Extensions d'un corps valué complet

On considère dans les paragraphes I et II de ce chapitre un corps valué **complet** (K, v) . On va d'abord démontrer l'existence et l'unicité d'un prolongement de v à n'importe quelle extension finie de K .

I. Théorème du prolongement

Étant donnés deux corps valués (K_1, v_1) et (K_2, v_2) , tels que K_2 contienne K_1 , nous dirons que v_2 prolonge v_1 si, pour tout x dans K_1 , l'on a $v_1(x) = v_2(x)$. Nous allons démontrer l'énoncé suivant :

Théorème 7.1. *Soit L une extension finie de degré n du corps valué complet (K, v) . Il existe une unique valuation w sur L qui prolonge v sur K . Pour tout élément x de L , la valuation w est définie par la formule :*

$$(1) \quad w(x) = \frac{1}{n}v(N_{L/K}(x)).$$

Démonstration : On désignera par A l'anneau de valuation de K et par B la fermeture intégrale de A dans L . Puisque A est intégralement clos, on a $A = B \cap K$.

On remarque d'abord que w est une fonction sur L qui prolonge v . En effet, si x est dans K , on a $N_{L/K}(x) = x^n$ et $w(x) = v(x)$.

1) Démontrons qu'il existe au plus une valuation sur L qui prolonge v .

Lemme 7.1. *Soit $P = a_0 + a_1X + \dots + X^d$ un polynôme de $A[X]$ tel que l'on ait $v(a_0) > 0$ et $\inf(v(a_1), \dots, v(a_{d-1})) = 0$. Alors, P est réductible dans l'anneau $A[X]$.*

Démonstration : La démonstration est analogue à celle de la prop. 6.1 : il existe un entier s tel que $0 < s < d$ et que $v(a_0) > 0, \dots, v(a_{s-1}) > 0, v(a_s) = 0$. On déduit de là que X^s divise le polynôme déduit de P par réduction modulo l'idéal de v , et il résulte du lemme de Hensel que P est réductible.

Lemme 7.2. *Soit v' une valuation de L prolongeant v . Alors, B est contenu dans l'anneau de valuation de v' .*

Démonstration : Soit x un élément de B . Il existe un entier $k \geq 1$ tel que l'on ait une relation de dépendance intégrale $x^k + a_1x^{k-1} + \dots + a_k = 0$, où les a_i sont dans A . Puisque v' prolonge v , on a $v'(a_i) \geq 0$. Si $v'(x) < 0$, on a alors $v'(x^k + a_1x^{k-1} + \dots + a_k) = kv'(x)$, ce qui conduit à une contradiction. D'où l'inégalité $v'(x) \geq 0$ et le résultat.

Lemme 7.3. *Soient v' une valuation de L prolongeant v et x un élément de B tel que x^{-1} ne soit pas dans B . On a alors $v'(x) > 0$.*

Démonstration : Soit $P = a_0 + a_1X + \dots + X^d$ le polynôme minimal de x sur K . Puisque x est dans B , le polynôme P est en fait dans $A[X]$. En effet, il existe un polynôme

unitaire F à coefficients dans A dont x soit racine. Ainsi P divise F , et le fait que A soit intégralement clos entraîne notre assertion (lemme 6.3). On a $v(a_0) > 0$: dans le cas contraire, a_0 serait une unité de A , et $Q = X^d a_0^{-1} P(1/X)$ serait le polynôme minimal de x^{-1} . Puisque Q est à coefficients dans A , cela impliquerait que x^{-1} est dans B , ce qui contredit l'hypothèse faite. D'où l'assertion. D'après le lemme 7.1, le fait que P soit irréductible entraîne alors $v(a_i) > 0$ pour tout i tel que $1 \leq i \leq d-1$. L'égalité $P(x) = 0$ entraîne alors le résultat.

Corollaire 7.1. *Soit v' une valuation prolongeant v . Alors, B est l'anneau de valuation de v' . En particulier, il existe au plus une valuation sur L qui prolonge v .*

Démonstration : Notons B' l'anneau de valuation de v' . D'après le lemme 7.2 B est contenu dans B' . Inversement, soit x un élément non nul de B' . Supposons que x ne soit pas dans B . Montrons alors que x^{-1} est dans B . On considère pour cela le polynôme minimal $P(X) = X^d + \dots + a_0$ de x sur K . Puisque x n'est pas dans B , a_0 n'est pas dans A (cf. cor. 6.2 du Chap. VI : si a_0 était dans A , P serait dans $A[X]$ et x serait entier sur A , i.e. x appartiendrait à B). Mais alors $Q(X) = a_0^{-1} X^d P(1/X)$, qui est le polynôme minimal de x^{-1} sur K , est tel que $Q(0) = a_0^{-1} \in A$. Cela prouve que Q est dans $A[X]$ et le fait que $x^{-1} \in B$. On applique maintenant le lemme 7.3 avec x^{-1} , et l'on constate que x ne peut être dans B' , ce qui conduit à une contradiction. D'où l'égalité $B = B'$.

Soient v' et v'' deux valuations sur L qui prolongent v sur K . Les anneaux de valuations de v' et v'' sont égaux (à B). cela entraîne que v' et v'' sont équivalentes, autrement dit qu'il existe $a > 0$ tel que $v' = av''$ (cf. prop. 5.2). Puisque l'on a $v'(x) = v''(x)$ si x est dans K , nécessairement $v' = v''$. D'où le résultat.

2) Il reste à démontrer que l'application w définie par l'égalité (1) est une valuation sur L .

2.1) Supposons $w(x) = +\infty$ pour $x \in L$. Dans ce cas la norme de x sur K est nulle, ce qui signifie que l'endomorphisme de L de multiplication par x n'est pas inversible, et cela entraîne $x = 0$. Inversement, si $x = 0$, il est clair que $w(x) = +\infty$.

2.2) Puisque pour tout x et y dans L l'on a $N_{L/K}(xy) = N_{L/K}(x) N_{L/K}(y)$, il en résulte que $w(xy) = w(x) + w(y)$.

2.3) Montrons l'inégalité triangulaire. Soient x et y deux éléments de L . Il s'agit de vérifier que $w(x+y) \geq \inf(w(x), w(y))$. On peut supposer que $xy \neq 0$ et que par exemple l'on a $w(y) \geq w(x)$. On a $w(x+y) = w(x) + w(1+y/x)$, de sorte qu'il suffit de démontrer que l'on a $w(1+y/x) \geq 0$. Posons pour cela $z = y/x$. Soit $P = X^d + \dots + a_0$ le polynôme minimal de z sur K . La norme de L sur K de z est une puissance positive de a_0 . Par ailleurs, les inégalités (1) et $w(y) \geq w(x)$, impliquent $v(N_{L/K}(y)) \geq v(N_{L/K}(x))$, et donc la norme de z appartient à A . On déduit de là que a_0 est dans A . Il en résulte que P est dans $A[X]$ (cor. 6.2) et donc z est dans B . On a ainsi $1+z \in B$ ce qui implique que la norme de $1+z$ sur K est dans A (cor. 6.3). D'après l'égalité (1), on a donc $w(1+z) \geq 0$, ce qui prouve notre assertion et termine la démonstration du théorème.

Remarque. Supposons que L soit une extension galoisienne de K . Il résulte de l'égalité (1) que deux éléments de L qui sont conjugués sur K ont la même valuation : en effet, si σ est un K -automorphisme de L , on a $N_{L/K}(x) = N_{L/K}(\sigma(x))$.

II. Cas où v est une valuation discrète

On considère dans ce paragraphe un corps valué *complet* (K, v) muni d'une valuation *discrète non triviale* v . On supposera que v est normalisée : on a $v(K^*) = \mathbb{Z}$. On notera A l'anneau de valuation de K , \mathfrak{M}_A l'idéal de valuation de A et $k_A = A/\mathfrak{M}_A$ le corps résiduel.

2.1. Généralités

Soient L une extension finie *séparable* de degré n de K et B la fermeture intégrale de A dans L . Soit w l'unique valuation de L qui prolonge v (cf. égalité (1)). D'après le corollaire 7.1, B est l'anneau de valuation de w .

Théorème 7.2. *La valuation w est discrète et le corps valué (L, w) est complet. En particulier, B est un anneau de valuation discrète. De plus, B est un A -module libre de rang n .*

Démonstration : Par définition de w , le groupe $w(L^*)$ est contenu dans $(1/n)\mathbb{Z}$, et il n'est donc pas dense dans \mathbb{R} . Par conséquent w est une valuation discrète sur L , et B est un anneau de valuation discrète. Par ailleurs, l'extension L/K étant séparable et A étant un anneau principal (car c'est un anneau de valuation discrète : cf. chap. I), B est un A -module libre de rang n (cor. 3.3). Le fait que (L, w) soit complet résulte directement de l'Appendice I. D'où le théorème.

Les anneaux A et B sont des anneaux de valuation discrète. Soit \mathfrak{M}_B l'idéal maximal de B et $k_B = B/\mathfrak{M}_B$ le corps résiduel. Notons π_A (resp. π_B) un générateur de \mathfrak{M}_A (resp. de \mathfrak{M}_B). Soit e l'indice de ramification de \mathfrak{M}_B et f son degré résiduel. Rappelons que f est le degré de l'extension k_B sur k_A . On a par définition

$$(2) \quad \mathfrak{M}_B^e = \mathfrak{M}_A \cdot B.$$

Il existe donc une unité u de B telle que l'on ait $\pi_A = \pi_B^e u$. On déduit de là que l'on a

$$(3) \quad w(L^*) = \frac{1}{e} \cdot \mathbb{Z}.$$

En particulier, le groupe $w(L^*)/v(K^*)$ est cyclique d'ordre e . Par ailleurs, puisque \mathfrak{M}_B est le seul idéal premier de B au-dessus de \mathfrak{M}_A , on a l'égalité (cf. th. 3.3)

$$(4) \quad n = ef.$$

Conformément à la terminologie utilisée dans le chapitre III, on dit que l'extension L/K est non ramifiée si l'on a $e = 1$ et si l'extension correspondante des corps résiduels est séparable, et que L/K est totalement ramifiée si $e = n$.

Signalons une description du A -module B lorsque k_A est un corps parfait, i.e. lorsque toute extension algébrique de k_A est séparable. On sait déjà que B est un A -module libre de rang n .

Proposition 7.1. *Supposons que k_A soit un corps parfait : soit x un élément de B dont la classe dans k_B soit un élément primitif de l'extension k_B/k_A . Alors, les produits $x^i \pi_B^j$ pour $0 \leq i < f$, $0 \leq j < e$, forment une base du A -module B .*

Démonstration : D'après la formule (4), il suffit de montrer que les produits $x^i \pi_B^j$ pour $0 \leq i < f$, $0 \leq j < e$, engendrent B comme A -module. D'après le lemme de Nakayama, cela revient à prouver que les classes de ces produits modulo $\pi_A.B$, engendrent $B/\pi_A.B$ comme espace vectoriel sur k_A . On a $\pi_A.B = \pi_B^e.B$. Considérons ainsi un élément α de $B/\pi_B^e.B$. On a $\alpha = \pi_B^t u + \pi_B^e.B$, où $0 \leq t < e$ et où u est une unité de B . Par ailleurs, il existe des éléments a_i de A tels que $u - \sum a_i x^i$ ($0 \leq i < f$), appartienne à $\pi_B.B$. Il existe donc un élément $v \in B$ tel que l'on ait

$$\alpha = \pi_B^t \sum_{i=0}^{f-1} a_i x^i + \pi_B^{t+1} v + \pi_B^e.B.$$

Si l'on a $t+1 \geq e$, l'assertion est démontrée ; sinon on recommence le procédé précédent avec l'élément $\pi_B^{t+1} v + \pi_B^e.B$, jusqu'à obtenir un exposant $t+1 \geq e$ et l'on obtient ainsi le résultat.

2.2. Description des extensions totalement ramifiées

Commençons par un exemple. Soit $\mathbb{Q}_p(\zeta)$ l'extension de \mathbb{Q}_p obtenue en adjoignant à \mathbb{Q}_p une racine primitive p -ième de l'unité ζ . C'est une extension totalement ramifiée de \mathbb{Q}_p de degré $p-1$. En effet, le polynôme cyclotomique $1 + X + \dots + X^{p-1}$ est le polynôme minimal de ζ sur \mathbb{Q}_p : en posant $Y = X - 1$, il s'écrit $Y^{p-1} + \dots + C_p^2 Y + p$ qui est un polynôme d'Eisenstein dont $\zeta - 1$ est racine. Si w est la valuation de $\mathbb{Q}_p(\zeta)$ prolongeant la valuation de \mathbb{Q}_p , on déduit de là que $w(1 - \zeta) = 1/(p-1)$ et, d'après la formule (3), que $p-1$ divise e . D'où $e = p-1$ et notre assertion.

L'exemple précédent se généralise comme suit :

Lemme 7.4. *Soit P un polynôme d'Eisenstein de $A[X]$ de degré m . Soit α une racine de P dans une clôture algébrique de K . Alors, l'extension $K(\alpha)/K$ est totalement ramifiée de degré m . De plus, α est une uniformisante de l'anneau de valuation de $K(\alpha)$.*

Démonstration : Posons $P = X^m + a_{m-1}X^{m-1} + \dots + a_0$. Puisque P est irréductible, m est le degré de $K(\alpha)$ sur K . Soit w l'extension de v à $K(\alpha)$. Par hypothèse, on a $v(a_0) = 1$ et $v(a_i) \geq 1$ pour tout i . L'égalité $P(\alpha) = 0$ entraîne alors $mw(\alpha) = 1$ (on peut aussi utiliser la formule (1) pour obtenir cette égalité). D'après la formule (3), on a donc $m = e$ et le résultat.

Ce lemme a une réciproque :

Lemme 7.5. *Soient L une extension finie totalement ramifiée de K et π une uniformisante de l'anneau de valuation de L . Alors, on a $L = K(\pi)$ et le polynôme minimal de π sur K est un polynôme d'Eisenstein.*

Démonstration : Posons $L' = K(\pi)$. Soient n' le degré de L' sur K et n le degré de L sur K . Soit w l'extension de v à L . La valuation $w(\pi)$ de π appartient à $w(L'^*)$ qui est contenue dans $v(K^*)/n'$. Par ailleurs, on a $w(\pi) = 1/n$ (cf. formule (2)). On déduit de là que n divise n' . Or n' divise aussi n , d'où $n = n'$ et $L' = L$.

Soit alors $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$ le polynôme minimal de π sur K . Puisque π est entier sur A , P appartient à $A[X]$ [†]. On a $P(\pi) = 0$ et $w(\pi) > 0$, ce qui implique $v(a_0) > 0$. Par ailleurs, P étant irréductible, on déduit du lemme 7.1 que $\inf(v(a_1), \dots, v(a_{n-1})) \geq 1$, puis que $v(a_0) = 1$ (car $w(\pi) = 1/n$). D'où le fait que P soit un polynôme d'Eisenstein.

2.3. Description des extensions non ramifiées

On va se placer sous l'hypothèse simplificatrice que le corps résiduel k_A est fini ; toutes les extensions algébriques de k_A sont ainsi séparables. D'après les hypothèses faites au début du paragraphe II, cela signifie que K est localement compact (prop. 5.6). Nous allons montrer le résultat suivant :

Proposition 7.2. *Soient m un entier naturel non nul et \overline{K} une clôture algébrique de K . Il existe une unique extension non ramifiée M de K de degré m contenue dans \overline{K} . De plus, M est une extension galoisienne de K et le groupe de Galois de M sur K est cyclique.*

Démonstration : Soit $\overline{k_A}$ une clôture algébrique de k_A . Étant donnée une extension finie de K de degré résiduel f , on identifiera son corps résiduel à l'unique extension de k_A de degré f contenue dans $\overline{k_A}$.

1) Construisons une extension de K de degré m non ramifiée. Puisque k_A est par hypothèse un corps fini, il existe un polynôme irréductible unitaire P de degré m à coefficients dans k_A . Posons $P = X^m + \alpha_{m-1}X^{m-1} + \dots + \alpha_0$. On considère des éléments a_i de A tels que $a_i \bmod \mathfrak{M}_A = \alpha_i$. Posons

$$\tilde{P} = X^m + \sum_{i=0}^{m-1} a_i X^i \in A[X].$$

Soit ξ une racine de \tilde{P} dans \overline{K} . Vérifions alors que l'extension $K(\xi)$ de K est non ramifiée de degré m . D'abord \tilde{P} est irréductible dans $K[X]$: sinon \tilde{P} serait produit dans $A[X]$ de

[†] En fait, soient M une extension finie de K , C la fermeture intégrale de A dans M et x un élément de M . Alors x est dans C si et seulement si le polynôme minimal de x sur K appartient à $A[X]$: cela provient du fait que l'on a une relation de dépendance intégrale à coefficients dans A , que A est intégralement clos et du lemme 6.3.

deux polynômes unitaires de degrés strictement inférieurs à m (A est factoriel), ce qui n'est pas car P est irréductible. Ainsi le degré de $K(\xi)$ sur K est m . Par ailleurs, ξ est entier sur A , donc appartient à l'anneau de valuation de $K(\xi)$: soit $\bar{\xi}$ l'image de ξ dans le corps résiduel de $K(\xi)$. En réduisant l'égalité $\tilde{P}(\xi) = 0$ modulo l'idéal de valuation de $K(\xi)$, on constate que $P(\bar{\xi}) = 0$. L'extension $k_A(\bar{\xi})/k_A$ est donc de degré m et est contenue dans le corps résiduel de $K(\xi)$. Il en résulte que le degré résiduel de $K(\xi)/K$ est m (et donc que le corps résiduel de $K(\xi)$ est $k_A(\bar{\xi})$), et que l'extension $K(\xi)/K$ est non ramifiée (cf. (4)). D'où l'assertion d'existence de la proposition.

2) Prouvons maintenant que $K(\xi)$ est une extension galoisienne de K . Il suffit pour cela de démontrer que le polynôme minimal de ξ , qui est \tilde{P} , possède toutes ses racines dans $K(\xi)$ et que ses racines sont simples. Soit C l'anneau de valuation de $K(\xi)$. D'après l'alinéa précédent, son corps résiduel est $k_A(\bar{\xi})$. Puisque k_A est fini, $k_A(\bar{\xi})$ est une extension galoisienne de k_A et le polynôme P se factorise dans $k_A(\bar{\xi})[X]$ en m polynômes distincts de degré 1. D'après le lemme de Hensel, les racines de P se relèvent dans C en m racines distinctes de \tilde{P} . Cela prouve notre assertion. Par ailleurs, le groupe de Galois de $k_A(\xi)$ sur k_A est cyclique. Il résulte alors de la prop. 3.3 et du cor. 3.7 que le groupe de Galois de $K(\xi)$ sur K (qui n'est autre que le groupe de décomposition de l'idéal de valuation de $K(\xi)$) est aussi cyclique.

3) Prouvons l'assertion d'unicité. Soient L_1 et L_2 deux extensions de K non ramifiées de degré m contenues dans \overline{K} . Soit $k_A(\alpha)$ leur corps résiduel dans $\overline{k_A}$. Soient Q le polynôme minimal de α sur k_A et \tilde{Q} un relèvement dans $A[X]$. D'après le lemme de Hensel, toutes les racines de \tilde{Q} dans \overline{K} sont dans $L_1 \cap L_2$. Le degré de Q , qui est aussi celui de \tilde{Q} , est m (car L_1 et L_2 sont non ramifiées). Par ailleurs, \tilde{Q} est irréductible dans $K[X]$ car il est irréductible modulo \mathfrak{M}_A . Si ξ est une racine de \tilde{Q} , le degré de $K(\xi)$ est donc m . Puisque $K(\xi)$ est contenu dans $L_1 \cap L_2$, cela implique $L_1 = L_2$. D'où le résultat.

Exercice. Soient p un nombre premier et $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p . Soit α une racine du polynôme $X^p - X - 1$ dans $\overline{\mathbb{Q}_p}$. Montrer que l'extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ est non ramifiée de degré p .

2.4. Corps valués algébriquement clos

Considérons une clôture algébrique \overline{K} de K .

Proposition 7.3. *Il existe sur \overline{K} une unique valuation qui prolonge la valuation v de K . On note encore v ce prolongement. Soient x un élément de \overline{K} et L une extension de degré n de K contenant x . On a alors*

$$(5) \quad v(x) = \frac{1}{n} v(N_{L/K}(x)).$$

Le groupe de valuation $v(\overline{K}^*)$ est \mathbb{Q} (qui est donc dense dans \mathbb{R}).

Démonstration : Puisque \overline{K} est réunion des extensions finies de K , il résulte du théorème 7.1 qu'il existe au plus une valuation sur \overline{K} qui prolonge v sur K . Vérifions

que l'égalité (5) définit une fonction v sur \overline{K} . Il suffit pour cela de vérifier qu'étant donné x dans \overline{K} , $v(x)$ ne dépend pas de l'extension L choisie contenant x . Soit n' le degré de $K(x)$ sur K . D'après la formule de transitivité des normes l'on a

$$N_{L/K}(x) = N_{K(x)/K}(N_{L/K(x)}(x)) = N_{K(x)/K}(x^{n/n'}).$$

On déduit de là l'égalité

$$\frac{1}{n}v(N_{L/K}(x)) = \frac{1}{n'}v(N_{K(x)/K}(x)),$$

et le fait que v est bien définie. On vérifie ensuite que v est une valuation sur \overline{K} (en considérant une extension finie contenant deux éléments donnés de \overline{K}). Enfin, $v(\overline{K}^*)$ est par définition contenu dans \mathbb{Q} . Inversement, soit a/b un élément de \mathbb{Q} ($b > 0$). Il existe un polynôme d'Eisenstein P dans $K[X]$ de degré b . Si π est une racine de ce polynôme, l'on a $v(\pi) = 1/b$, de sorte que $v(\pi^a) = a/b$. D'où l'égalité $v(\overline{K}^*) = \mathbb{Q}$ et le résultat.

Remarque. Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p . Alors $\overline{\mathbb{Q}_p}$ n'est pas complet. En effet, pour tout entier n , il n'existe qu'un nombre fini d'extensions de \mathbb{Q}_p de degré plus petit que n (cf. [Am], p. 74-75). Il en résulte que $\overline{\mathbb{Q}_p}$ est réunion dénombrable de sous- \mathbb{Q}_p -espaces vectoriels F_n de dimension finie. Les F_n sont des parties fermées de $\overline{\mathbb{Q}_p}$ (car ils sont complets) et ils sont d'intérieur vide[†]. D'après le théorème de Baire, $\overline{\mathbb{Q}_p}$ n'est donc pas complet. En particulier, $\overline{\mathbb{Q}_p}$ n'est pas localement compact (prop. 5.6). On montre que le complété de $\overline{\mathbb{Q}_p}$ est un corps algébriquement clos (cf. *loc. cit.*, p. 71-73).

Signalons le lemme suivant :

Lemme 7.6. *Le corps résiduel de \overline{K} est une clôture algébrique de k_A .*

Démonstration : Soient \overline{A} l'anneau de valuation de \overline{K} , $\overline{\mathfrak{M}}$ son idéal de valuation et $\overline{k} = \overline{A}/\overline{\mathfrak{M}}$ son corps résiduel. D'abord k_A est isomorphe à un sous-corps de \overline{k} . En effet, l'application naturelle $A \rightarrow \overline{A} \rightarrow \overline{k}$ est de noyau \mathfrak{M} . Identifions k_A et son image dans \overline{k} . Soit $\overline{x} = x + \overline{\mathfrak{M}}$ un élément de \overline{k} . Montrons que \overline{x} est algébrique sur k_A . Par définition, x est entier sur A , et il existe donc un polynôme unitaire P de $A[X]$ tel que $P(x) = 0$. Soit \overline{P} le polynôme déduit de P par réduction modulo l'idéal de valuation de A . On a $\overline{P}(\overline{x}) = 0$ et \overline{P} n'est pas nul (car P est unitaire). D'où le fait que \overline{k} soit une extension algébrique de k_A . Par ailleurs, soit \overline{H} un polynôme irréductible unitaire de $\overline{k}[X]$. Montrons que \overline{H} a une racine dans \overline{k} . On considère pour cela un relèvement unitaire H de \overline{P} dans $A[X]$. Alors H

[†] Soient K un corps valué, E un K -espace vectoriel normé, et B une boule ouverte de E de rayon strictement positif. Soit F le sous-espace vectoriel de E engendré par B . Supposons qu'il existe une suite d'éléments de K , convergente de limite nulle, dont les termes soient distincts deux à deux (à partir d'un certain rang). Alors, on a $F = E$. En particulier, les sous-espaces vectoriels de E , distincts de E , sont d'intérieur vide.

a une racine y dans \overline{K} , et puisque H est unitaire, y appartient à \overline{A} . On a alors l'égalité $\overline{H}(y + \overline{\mathfrak{M}}) = 0$, ce qui prouve notre assertion et le lemme.

III. Extension et complétion

On considère dans ce paragraphe un corps valué (K, v) , pas nécessairement complet, muni d'une valuation discrète non triviale v . On note A l'anneau de valuation de v et \mathfrak{M} l'idéal maximal de A . On suppose que v est normalisée : on a $v(K^*) = \mathbb{Z}$. Soit par ailleurs L une extension finie séparable de degré n de K . On note B la fermeture intégrale de A dans L . D'après le chapitre III : puisque A est un anneau de valuation discrète, c'est un anneau de Dedekind, et B est donc aussi un anneau de Dedekind. Soient $(\mathfrak{p}_k)_{1 \leq k \leq g}$ la famille des idéaux premiers de B au-dessus de \mathfrak{M} (on sait qu'il y en a un nombre fini). Soient e_k et f_k les indices ramifications et les degrés résiduels correspondant à \mathfrak{p}_k . Chaque \mathfrak{p}_k définit une valuation discrète w_k qui prolonge v , en posant

$$(6) \quad w_k(x) = \frac{1}{e_k} v_{\mathfrak{p}_k}(x), \quad (x \in L)$$

où $v_{\mathfrak{p}_k}(x)$ est l'exposant de l'idéal \mathfrak{p}_k dans la décomposition de l'idéal $x.B$ en produit d'idéaux premiers de B . Remarquons que si x est dans K on a bien $w_k(x) = v(x)$ (cela provient de l'égalité $\mathfrak{M}.B = \prod \mathfrak{p}_k^{e_k}$). Il résulte en particulier de (6) que l'on a

$$(7) \quad w_k(L^*) = \frac{1}{e_k} \mathbb{Z}.$$

Rappelons que l'anneau de valuation de w_k est le localisé de B en \mathfrak{p}_k . On obtient en fait de cette façon toutes les valuations sur L qui prolongent v :

Lemme 7.8. *Soit w une valuation sur L qui prolonge v . Alors, il existe un indice k tel que $w = w_k$.*

Démonstration : Soient W l'anneau de valuation de w et \mathfrak{P} son idéal maximal. Cet anneau contient B : en effet, soit x un élément de B . Il existe une relation de dépendance intégrale $x^d + a_{d-1}x^{d-1} + \dots + a_0 = 0$ à coefficients dans A . Puisque w prolonge v , on a $w(a_i) \geq 0$, d'où l'on déduit l'inégalité $w(x) \geq 0$, ce qui prouve que x appartient à W . Par ailleurs, $\mathfrak{P} \cap A$ est un idéal premier non nul de A : en effet, si x est un élément non nul de \mathfrak{M} , on a $v(x) = w(x) > 0$, de sorte que x appartient à $\mathfrak{P} \cap A$. On déduit de là que l'on a $\mathfrak{P} \cap A = \mathfrak{M}$. Par conséquent, \mathfrak{P} est au-dessus de \mathfrak{M} , et il existe k tel que $\mathfrak{P} = \mathfrak{p}_k$. Il en résulte que le localisé $B_{\mathfrak{p}_k}$ est contenu dans W : en effet, si α est un élément de B qui n'est pas dans \mathfrak{p}_k , il est inversible dans W , de sorte que l'inclusion $B \subseteq W$ se factorise à travers $B_{\mathfrak{p}_k}$ (et $B_{\mathfrak{p}_k}$ s'identifie à un sous-anneau de W). On a $W \neq L$ (car w n'est pas triviale), et $B_{\mathfrak{p}_k}$ étant un anneau de valuation, c'est un sous-anneau maximal de son corps

des fractions L^\dagger . Par suite, on a $W = B_{\mathfrak{p}_k}$. Il existe donc $a > 0$ tel que l'on ait $w = aw_k$, et comme w et w_k coïncident sur K , on a $w = w_k$. D'où le lemme.

Soient (\hat{K}, \hat{v}, i) une complétion de (K, v) et $(\hat{L}_k, \hat{w}_k, j_k)$ une complétion de (L, w_k) .

Proposition 7.4. *Le corps \hat{L}_k est une extension finie de \hat{K} . La valuation \hat{w}_k est l'unique valuation de \hat{L}_k qui prolonge \hat{v} . L'indice de ramification de l'extension \hat{L}_k/\hat{K} est e_k et son degré résiduel est f_k . En particulier, le degré de \hat{L}_k sur \hat{K} est $e_k f_k$.*

Démonstration : L'inclusion $K \subseteq L$ se prolonge par continuité en un homomorphisme de corps de \hat{K} dans \hat{L}_k . Plus précisément, soit x un élément de \hat{K} . Il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de K telle que la suite $(i(x_n))_{n \in \mathbb{N}}$ converge vers x . Par ailleurs, pour tout p et q , l'on a les égalités

$$\hat{w}_k(j_k(x_p) - j_k(x_q)) = \hat{w}_k(j_k(x_p - x_q)) = w_k(x_p - x_q) = v(x_p - x_q) = \hat{v}(i(x_p) - i(x_q)).$$

Puisque $(i(x_n))_{n \in \mathbb{N}}$ est convergente, elle est de Cauchy, et il en résulte que la suite d'éléments de \hat{L}_k , $(j_k(x_n))_{n \in \mathbb{N}}$, est aussi une suite de Cauchy. Elle est donc convergente de limite $y \in \hat{L}_k$. On vérifie que la définition de y ne dépend pas de la suite $(x_n)_{n \in \mathbb{N}}$ choisie, et l'on obtient ainsi une application ψ_k de \hat{K} dans \hat{L}_k qui est visiblement un homomorphisme de corps. Cela prouve que \hat{L}_k est une extension de \hat{K} . Nous identifierons désormais \hat{K} et son image dans \hat{L}_k .

Vérifions que \hat{L}_k est de degré fini sur \hat{K} . Soit θ un élément primitif de L sur K (L est par hypothèse une extension séparable de K). Alors $j_k(\theta)$ appartient à \hat{L}_k et $\hat{K}(j_k(\theta))$ est un sous-corps de \hat{L}_k de degré fini sur \hat{K} . D'après le lemme 5 de l'Appendice I, $\hat{K}(j_k(\theta))$ est un sous-espace vectoriel fermé de \hat{L}_k . Par ailleurs, $j_k(L)$ est contenu dans $\hat{K}(j_k(\theta))$ et est dense dans \hat{L}_k . Cela entraîne l'égalité $\hat{L}_k = \hat{K}(j_k(\theta))$ et notre assertion.

Vérifions que pour tout $x \in \hat{K}$, l'on a $\hat{w}_k(x) = \hat{v}(x)$. On considère pour cela une suite $(i(x_n))_{n \in \mathbb{N}}$ d'éléments de $i(K)$ qui converge vers x . On a $w_k(x_n) = \hat{w}_k(j_k(x_n))$ et $\hat{v}(i(x_n)) = v(x_n)$. Puisque $v(x_n) = w_k(x_n)$, on a donc $\hat{w}_k(j_k(x_n)) = \hat{v}(i(x_n))$, et par passage à la limite, on obtient que $\hat{w}_k(x) = \hat{v}(x)$. D'où le fait que \hat{w}_k soit l'unique prolongement de \hat{v} à \hat{L}_k .

Par ailleurs, si est \hat{e}_k l'indice de ramification de l'extension \hat{L}_k/\hat{K} , les égalités (3) et (7), et l'assertion d) de la prop. 5.3 entraînent directement que $\hat{e}_k = e_k$. Soit \hat{f}_k le degré résiduel de l'extension \hat{L}_k/\hat{K} . Montrons que $f_k = \hat{f}_k$. Soit k_v (resp. $k_{\hat{v}}$) le corps résiduel

[†] Soit A l'anneau d'une valuation v non triviale dans son corps des fractions K . Alors A est un sous-anneau maximal propre de K . D'abord on a $A \neq K$, car v n'est pas triviale. Soit B un sous-anneau de K contenant A distinct de A . Prouvons que $B = K$. Soit y un élément non nul de K . On considère un élément $x \in B$ qui ne soit pas dans A : on a $v(x^{-1}) > 0$. Il existe donc un entier $n > 0$ tel que l'on ait $nv(x^{-1}) \geq v(y^{-1})$; on a ainsi $v(y) \geq v(x^n)$, ce qui entraîne que y est dans Ax^n qui est contenu dans B . D'où notre assertion.

de K (resp. de \hat{K}). De même soit l_{w_k} (resp. $l_{\hat{w}_k}$) le corps résiduel de L en w_k (resp. celui de \hat{L}_k). On a vu que l'application $\gamma : k_v \rightarrow k_{\hat{v}}$ qui à la classe d'un élément $a + \mathfrak{M}$ de k_v associe la classe de $i(a)$ modulo l'idéal de \hat{v} est un isomorphisme de corps, et l'on a de même un isomorphisme analogue φ de l_{w_k} sur $l_{\hat{w}_k}$. Pour tout $x \in l_{w_k}$ et $\lambda \in k_v$, l'on a $\varphi(\lambda x) = \gamma(\lambda) \cdot \varphi(x)$. Autrement dit φ est compatible aux actions de k_v et $k_{\hat{v}}$, ce qui entraîne notre assertion.

La proposition résulte alors de la formule (4). D'où le résultat.

Remarque. On a constaté dans la démonstration précédente que si θ est un élément séparable de l'extension L/K , l'on a $\hat{L}_k = \hat{K}(j_k(\theta))$. En identifiant K , L et \hat{K} à des sous-corps de \hat{L}_k , on a alors $\hat{L}_k = L\hat{K}$. On déduit de là que l'extension \hat{L}_k/\hat{K} est aussi séparable.

Proposition 7.5. *Supposons que l'extension L/K soit galoisienne. Soit D_k le sous-groupe de décomposition de \mathfrak{p}_k du groupe de Galois $\text{Gal}(L/K)$. Alors, l'extension \hat{L}_k/\hat{K} est aussi galoisienne et le groupe de Galois $\text{Gal}(\hat{L}_k/\hat{K})$ est isomorphe à D_k .*

Démonstration : Soit σ un élément de D_k : on a $\sigma(\mathfrak{p}_k) = \mathfrak{p}_k$. L'automorphisme $\sigma : L \rightarrow L$ se prolonge en un automorphisme $\hat{\sigma}$ de \hat{L}_k que fixe \hat{K} : en effet, soient x un élément de \hat{L}_k et $(i_k(x_n))_{n \in \mathbb{N}}$ une suite d'éléments de $i_k(L)$ qui converge vers x . Alors la suite $(i_k(\sigma(x_n)))_{n \in \mathbb{N}}$ est convergente dans \hat{L}_k [cela vient du fait que pour tout n , l'exposant de $\sigma(\mathfrak{p}_k) = \mathfrak{p}_k$ dans la décomposition de $\sigma(x_n) \cdot B$ en produit d'idéaux premiers de B est celui de \mathfrak{p}_k dans celle de $x_n \cdot B$: on a $w_k(\sigma(x_n)) = (1/e_k)v_{\mathfrak{p}_k}(\sigma(x_n))$, et donc $w_k(\sigma(x_n)) = (1/e_k)v_{\sigma(\mathfrak{p}_k)}(\sigma(x_n)) = (1/e_k)v_{\mathfrak{p}_k}(x_n) = w_k(x_n)$. Par conséquent $\hat{w}_k(i_k(\sigma(x_n))) = w_k(i_k(x_n))$, ce qui entraîne l'assertion]. La limite $\hat{\sigma}(x)$ de cette suite ne dépend que de x , et l'on vérifie ensuite que $\hat{\sigma}$ est une application satisfaisant aux conditions annoncées. On déduit de là un homomorphisme injectif de groupes de D_k dans $\text{Gal}(\hat{L}_k/\hat{K})$ (car $\hat{\sigma}$ prolonge σ). L'ordre de $\text{Gal}(\hat{L}_k/\hat{K})$ est donc au moins $e_k f_k = |D_k|$. Comme cet ordre est plus petit que le degré de \hat{L}_k/\hat{K} qui est aussi $e_k f_k$, la flèche $\sigma \mapsto \hat{\sigma}$ est donc un isomorphisme. En particulier, l'ordre du groupe $\text{Gal}(\hat{L}_k/\hat{K})$ est égal au degré de \hat{L}_k/\hat{K} , ce qui prouve que cette extension est normale. Comme elle est séparable, elle est donc galoisienne. D'où le résultat.

Terminons ce paragraphe par une description du produit tensoriel $L \otimes_K \hat{K}$ en termes des complétés \hat{L}_k . On identifie pour cela K , L et \hat{K} à des sous-corps de \hat{L}_k . Remarquons que l'application naturelle

$$L \times \hat{K} \rightarrow \prod_{k=1}^g \hat{L}_k,$$

qui à un élément (a, λ) associe $(a\lambda)_{1 \leq k \leq g}$ est une application K -bilinéaire ; elle se factorise

donc à travers le produit tensoriel $L \otimes_K \hat{K}$. On obtient ainsi une application

$$\Phi : L \otimes_K \hat{K} \rightarrow \prod_{k=1}^g \hat{L}_k,$$

qui est, de façon naturelle, une application \hat{K} -linéaire.

Proposition 7.6. *L'application Φ est un isomorphisme de \hat{K} -espaces vectoriels.*

Démonstration : Soit F l'image de Φ . C'est un sous- \hat{K} -espace vectoriel du produit des \hat{L}_k qui est de dimension finie. Il résulte de l'Appendice I que F est une partie fermée. Par ailleurs, d'après le théorème d'approximation, l'image diagonale de L dans le produit des \hat{L}_k est dense : en effet, soient (y_1, \dots, y_g) un élément du produit des \hat{L}_k et N un entier strictement positif. Pour tout k entre 1 et g , il existe $x_k \in L_k$ tel que l'on ait l'inégalité $\hat{w}_k(x_k - y_k) > N$. D'après le théorème d'approximation, il existe $x \in L$ tel que pour tout k l'on ait $w_k(x - x_k) > N$. Il en résulte que pour tout k l'on a l'égalité $\hat{w}_k(x - y_k) = \hat{w}_k(x - x_k + x_k - y_k) > N$. D'où l'assertion. Cela entraîne en particulier que F est une partie dense, et donc que Φ est surjective. Par ailleurs, $L \otimes_K \hat{K}$ est \hat{K} -isomorphe à \hat{K}^n et la dimension sur \hat{K} du produit des \hat{L}_k est la somme des $e_k f_k$, qui est égale à n . On déduit de là que Φ est injective, ce qui prouve le résultat.

Chapitre VIII — Applications Diophantiennes

Soient K un corps et F un polynôme homogène dans $K[X, Y, Z]$ (en trois indéterminées X, Y et Z). Soit C la courbe projective plane définie sur K , d'équation

$$F(x, y, z) = 0.$$

Par définition, C est une sous-variété de dimension 1 du plan projectif \mathbb{P}^2 . Étant donnée une extension L de K , on note $C(L)$ l'ensemble des points de C rationnels sur L : par définition $C(L)$ est le sous-ensemble de \mathbb{P}^2 formé des points possédant un représentant (x_0, y_0, z_0) dans L^3 tel que $F(x_0, y_0, z_0) = 0$.

Un problème fondamental consiste en la détermination de l'ensemble $C(K)$. C'est en général un problème très difficile, ne serait-ce déjà que de décider si cet ensemble est vide ou non. Dans cette direction, lorsque K est muni d'une valuation discrète non triviale v , une méthode d'attaque consiste à étudier l'ensemble $C(K_v)$ des points de C rationnels sur le complété K_v de K en v . Par exemple, si $C(K_v)$ est vide, $C(K)$ l'est aussi. Cette remarque s'applique notamment lorsque K est une extension finie de \mathbb{Q} , en prenant pour v la valuation associée à un idéal maximal de l'anneau d'entiers de K . On se propose principalement dans ce chapitre d'illustrer cette situation dans des cas particuliers. Les deux ingrédients fondamentaux pour aborder cette étude sont le lemme de Hensel et les majorations obtenues par A. Weil vers 1950 sur le nombre de points rationnels des courbes algébriques sur les corps finis.

I. Énoncé des bornes de Weil sur les corps fini

Soient k un corps fini de cardinal q et \bar{k} une clôture algébrique de k . Considérons une courbe algébrique plane C définie sur k d'équation $F(x, y, z) = 0$, où $F \in k[X, Y, Z]$. On suppose que C est lisse, autrement dit, que pour tout point P de $C(\bar{k})$, l'une des dérivées partielles $\frac{\partial F}{\partial x}(P)$, $\frac{\partial F}{\partial y}(P)$ ou $\frac{\partial F}{\partial z}(P)$ n'est pas nulle. On suppose par ailleurs que C est absolument irréductible, i.e. que F est irréductible dans $\bar{k}[X, Y, Z]$.

Notons $N(C)$ le nombre de points de C rationnels sur k . On admettra le résultat suivant qui a été démontré par A. Weil vers 1950 (cf. par exemple [Mo], p. 48) :

Théorème 8.1. *Soit n le degré de F . On a l'inégalité*

$$(1) \quad |N(C) - (q + 1)| \leq (n - 1)(n - 2)\sqrt{q}.$$

Si l'on a $n \leq 3$, il résulte en particulier du th. que $N(C) \neq 0$, et que si q est assez grand par rapport au degré de F , l'on a $N(C) \neq 0$. On utilisera plus précisément l'énoncé suivant :

Corollaire 8.1. *On a l'implication*

$$(2) \quad q > ((n-1)(n-2))^2 \implies N(C) \neq 0.$$

Signalons qu'il existe des majorations plus fines de $|N(C) - (q+1)|$ que celle donnée par l'inégalité (1). Elles sont inutiles pour les applications que l'on a en vue.

II. Les quartiques de Fermat $x^4 + y^4 = cz^4$

Soient c un entier naturel non nul sans puissance quatrième et C la courbe algébrique d'équation

$$(3) \quad x^4 + y^4 = cz^4.$$

Comme le suggère J.-P. Serre dans [Se3], p. 67, on se propose de déterminer les nombres premiers p tels que $C(\mathbb{Q}_p)$ ne soit pas vide. On va démontrer l'énoncé suivant :

Proposition 8.1.

- a) *On a $C(\mathbb{Q}_2) \neq \emptyset \iff c \equiv 1$ ou $2 \pmod{16}$.*
- b) *Soit p un diviseur premier impair de c . On a $C(\mathbb{Q}_p) \neq \emptyset \iff p \equiv 1 \pmod{8}$.*
- c) *Soit p un nombre premier ne divisant pas c tel que $p \equiv 3 \pmod{4}$. Alors $C(\mathbb{Q}_p)$ n'est pas vide.*
- d) *Soit p un nombre premier ≥ 37 ne divisant pas c . Alors $C(\mathbb{Q}_p)$ n'est pas vide.*
- e) *On a $C(\mathbb{Q}_{17}) \neq \emptyset$.*
- f) *Supposons que l'on ait $p \in \{5, 13, 29\}$, et que p ne divise pas c . On a les équivalences suivantes :*

$$C(\mathbb{Q}_5) \neq \emptyset \iff c \not\equiv 3 \text{ ou } 4 \pmod{5},$$

$$C(\mathbb{Q}_{13}) \neq \emptyset \iff c \not\equiv 7, 8 \text{ ou } 11 \pmod{13},$$

$$C(\mathbb{Q}_{29}) \neq \emptyset \iff c \not\equiv 4, 5, 6, 9, 13, 22 \text{ ou } 28 \pmod{29}.$$

On déduit de là :

Corollaire 8.2. *Pour que la courbe C possède des points rationnels sur tous les corps \mathbb{Q}_p , il faut et il suffit que les conditions suivantes soient réalisées :*

- a) *on a $c \equiv 1$ ou $2 \pmod{16}$;*
- b) *tout diviseur premier impair de c est congru à 1 modulo 8 ;*
- c) *on a $c \not\equiv 3$ ou $4 \pmod{5}$;*
- d) *on a $c \not\equiv 7, 8$ ou $11 \pmod{13}$;*
- e) *on a $c \not\equiv 4, 5, 6, 9, 13, 22$ ou $28 \pmod{29}$.*

On notera que la condition e) signalée dans [Se3], p. 67 n'intervient pas.

Démonstration de la proposition

Étant donné un nombre premier p , on notera v_p la valuation p -adique de \mathbb{Q}_p . Remarquons que si $C(\mathbb{Q}_p)$ n'est pas vide, l'équation (3) possède une solution (x, y, z) dans \mathbb{Q}_p^3 vérifiant

$$(4) \quad \inf(v_p(x), v_p(y), v_p(z)) = 0.$$

Si p ne divise pas c , en réduisant l'équation (3) modulo p , on obtient une courbe projective plane sur \mathbb{F}_p que l'on notera \tilde{C} ; c'est une courbe lisse si p est impair. Si $[x, y, z]$ est un point de $C(\mathbb{Q}_p)$ satisfaisant (4), le triplet $[\bar{x}, \bar{y}, \bar{z}]$, déduit de $[x, y, z]$ par réduction modulo p , appartient à $\tilde{C}(\mathbb{F}_p)$.

a) Décrivons les unités de \mathbb{Z}_2 qui sont des puissances quatrièmes dans \mathbb{Q}_2 (ou dans \mathbb{Z}_2 cela revient au même). Soit u une unité de \mathbb{Z}_2 . Vérifions que l'on a

$$(5) \quad u \in \mathbb{Q}_2^4 \iff u \equiv 1 \pmod{16}.$$

On a $u \equiv 1 \pmod{2}$: posons $u = 1 + 2t$, où $t \in \mathbb{Z}_2$. On a $(1 + 2t)^4 \equiv 1 + 8t(t+1) \equiv 1 \pmod{16}$. Inversement, supposons $u \equiv 1 \pmod{16}$. On distingue alors deux cas.

a.1) Supposons $u \equiv 1 \pmod{32}$. Considérons le polynôme $F = X^4 - u$. On a les inégalités $v_2(F(1)) \geq 5$ et $v_2(F'(1)) = v_2(4) = 2$. D'après le lemme de Hensel, F possède donc une racine dans \mathbb{Q}_2 . D'où l'implication dans ce cas.

a.2) Supposons $u \equiv 17 \pmod{32}$. On a $F(5) = 625 - u \equiv 0 \pmod{32}$, d'où $v_2(F(5)) \geq 5$. Puisque $v_2(F'(5)) = 2$, le lemme de Hensel entraîne que F a une racine dans \mathbb{Q}_2 . D'où l'équivalence (5).

Cela étant, supposons $C(\mathbb{Q}_2)$ non vide. Soit (x, y, z) un élément de \mathbb{Z}_2^3 vérifiant les conditions (3) et (4). Puisque l'on a $v_2(c) \leq 3$, x ou y est une unité de \mathbb{Z}_2 . D'après (5), on a $x^4 \equiv 0$ ou $1 \pmod{16}$ et il en est de même pour y^4 . Par ailleurs, on a $v_2(z) = 0$. En effet, supposons $v_2(z) > 0$. Dans ce cas on a $x^4 + y^4 \equiv 0 \pmod{16}$, ce qui entraîne que x et y sont dans $2\mathbb{Z}_2$, et cela contredit alors (4). On a donc $z^4 \equiv 1 \pmod{16}$. On en déduit que $c \equiv x^4 + y^4 \pmod{16}$, i.e. $c \equiv 1$ ou $2 \pmod{16}$.

Inversement supposons $c \equiv 1$ ou $2 \pmod{16}$. Si $c \equiv 1 \pmod{16}$, il existe $t \in \mathbb{Z}_2$ tel que $c = t^4$ (cf. (5)). Le point $[t, 0, 1]$ appartient alors à $C(\mathbb{Q}_2)$. Si $c \equiv 2 \pmod{16}$, il existe $t \in \mathbb{Z}_2$ tel que $c - 1 = t^4$, et dans ce cas $[t, 1, 1]$ appartient à $C(\mathbb{Q}_2)$. Ainsi $C(\mathbb{Q}_2)$ n'est pas vide. D'où l'assertion a).

b) Soit p un diviseur premier impair de c .

Considérons un élément (x, y, z) de \mathbb{Z}_p^3 vérifiant (3) et (4). Nécessairement p ne divise pas xy (cf. la condition (4) et le fait que $v_p(c) \leq 3$). On déduit de là que -1 est une puissance quatrième dans \mathbb{F}_p , et cela implique $p \equiv 1 \pmod{8}$ (car \mathbb{F}_p^* possède alors un élément d'ordre 8).

Inversement, supposons $p \equiv 1 \pmod{8}$. Alors -1 est une puissance quatrième dans \mathbb{F}_p (si 8 divise $p-1$, \mathbb{F}_p^* possède un sous-groupe H d'ordre 8, et si a est un générateur de H , on a $a^4 = -1$). Il existe donc un entier x_0 tel que $x_0^4 \equiv -1 \pmod{p}$. Posons alors $F = X^4 + 1$. On a $v_p(F(x_0)) \geq 1$ et $v_p(F'(x_0)) = 0$ (car $p \neq 2$). D'après le lemme de Hensel, F a une racine dans \mathbb{Z}_p . Soit donc $x \in \mathbb{Z}_p$ tel que $x^4 = -1$. Le point $[x, 1, 0]$ appartient alors à $C(\mathbb{Q}_p)$. D'où l'assertion b).

Démontrons alors le lemme suivant :

Lemme 8.1. *Soit p un nombre premier qui ne divise pas $2c$. Alors, on a l'équivalence*

$$(6) \quad C(\mathbb{Q}_p) \neq \emptyset \iff \tilde{C}(\mathbb{F}_p) \neq \emptyset.$$

En particulier, si -1 n'est pas une puissance quatrième dans \mathbb{F}_p , on a

$$(7) \quad C(\mathbb{Q}_p) \neq \emptyset \iff c \pmod{p} \in \mathbb{F}_p^4 + \mathbb{F}_p^4.$$

Démonstration : Supposons $\tilde{C}(\mathbb{F}_p) \neq \emptyset$. Il existe alors un élément (x_0, y_0, z_0) de \mathbb{Z}^3 , non nul modulo p , tel que $x_0^4 + y_0^4 \equiv cz_0^4 \pmod{p}$. Puisque p ne divise pas c , on a $\text{Inf}(v_p(x_0), v_p(y_0)) = 0$. Supposons par exemple $v_p(x_0) = 0$. On pose $F = X^4 + y_0^4 - cz_0^4$. On a $v_p(F(x_0)) \geq 1$ et $v_p(F'(x_0)) = 0$ car $p \neq 2$. D'après le lemme de Hensel, F a donc une racine t dans \mathbb{Q}_p et le point $[t, y_0, z_0]$ appartient à $C(\mathbb{Q}_p)$. L'implication inverse a déjà été démontrée. D'où le lemme.

c) Soit p un nombre premier congru à 3 modulo 4 ne divisant pas c . Montrons qu'il existe u et v dans \mathbb{F}_p tels que l'on ait

$$(8) \quad u^4 + v^4 = c \pmod{p}.$$

On remarque pour cela qu'il existe un couple d'éléments $(\alpha, \beta) \neq (0, 0)$ dans \mathbb{F}_p tels que $\alpha^2 + \beta^2 = c \pmod{p}$ [†]. Par ailleurs, puisque $p-1$ est divisible par 2 et pas par 4, on a l'égalité $\mathbb{F}_p^{*2} = \mathbb{F}_p^{*4}$ [\mathbb{F}_p^{*4} est contenu dans \mathbb{F}_p^{*2} et le noyau du morphisme $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$ qui à x associe x^4 est $\{\pm 1\}$, de sorte que l'on a $|\mathbb{F}_p^{*4}| = |\mathbb{F}_p^{*2}| = (p-1)/2$]. D'où l'existence de u et v vérifiant (8). D'après le lemme 8.1, $C(\mathbb{Q}_p)$ n'est donc pas vide. D'où l'assertion.

d) Puisque p ne divise pas $2c$, la courbe \tilde{C} sur \mathbb{F}_p est lisse et absolument irréductible. D'après le cor. 8.1, l'ensemble $\tilde{C}(\mathbb{F}_p)$ n'est pas vide, et le lemme 8.1 entraîne le résultat.

[†] Dans un corps fini tout élément est somme de deux carrés. En effet, soient k un corps de cardinal $q = p^n$ (p premier) et a un élément de k . L'assertion est vraie si $p = 2$: dans ce cas, l'application de k dans k qui à x associe x^2 est un isomorphisme de corps, et donc tout élément de k est un carré. Supposons $p \geq 3$: soit A l'ensemble des éléments de k de la forme $a - x^2$. On a les égalités $|A| = |k^2| = (q+1)/2$, ce qui entraîne que $A \cap k^2$ n'est pas vide. D'où le résultat.

e) et f) Il reste à examiner les ensembles $C(\mathbb{Q}_p)$ lorsque p est un nombre premier qui ne divise pas c , tel que $5 \leq p \leq 31$ et $p \equiv 1 \pmod{4}$, autrement dit, lorsque

$$p \in \{5, 13, 17, 29\}.$$

Pour un tel p , on remarque d'abord que -1 est une puissance quatrième dans \mathbb{F}_p si et seulement si $p = 17$ (car $17 \equiv 1 \pmod{8}$). On déduit de là que $C(\mathbb{Q}_{17}) \neq \emptyset$: en effet, en appliquant le lemme de Hensel avec le polynôme $F = X^4 + 1$, on constate que -1 appartient à \mathbb{Q}_{17}^4 , ce qui entraîne l'assertion e) (si 17 divise c on a aussi $C(\mathbb{Q}_{17}) \neq \emptyset$ d'après b)). Par ailleurs, on a

$$\mathbb{F}_5^4 = \{0, 1\}, \quad \mathbb{F}_{13}^4 = \{0, 1, 3, 9\}, \quad \mathbb{F}_{29}^4 = \{0, 1, -9, -13, -6, -5, -4, 7\}.$$

Pour $p \in \{5, 13, 29\}$, on détermine alors la liste des éléments de \mathbb{F}_p^* qui s'écrivent comme somme de deux puissances quatrièmes, et en utilisant l'équivalence (7), on obtient alors l'assertion f) de la proposition. D'où le résultat.

Remarque. L'entier $c = 146$ vérifie les conditions du cor. 8.2. La courbe C d'équation $x^4 + y^4 = 146z^4$ possède ainsi des points rationnels dans tous les complétés de \mathbb{Q} . Cela suggère l'étude de l'ensemble $C(\mathbb{Q})$. En utilisant la théorie des courbes elliptiques, on peut en fait montrer que $C(\mathbb{Q})$ est vide. On dit alors que l'on a une contradiction au principe de Hasse. Ce phénomène ne se produit pas pour les courbes d'équation $F(x, y, z) = 0$, où F est un polynôme homogène de degré 2 (c'est le théorème de Hasse-Minkowski).

Exercice. Soient c un entier naturel non nul et C la courbe d'équation $x^8 + y^8 = cz^8$.

- 1) Montrer que l'on a $C(\mathbb{Q}_2) \neq \emptyset \iff c \equiv 1 \text{ ou } 2 \pmod{32}$.
- 2) Soit p un diviseur premier impair de c . Montrer que l'on a l'équivalence

$$C(\mathbb{Q}_p) \neq \emptyset \iff p \equiv 1 \pmod{16}.$$

- 3) Supposons $c = 97$. Montrer que $C(\mathbb{Q}_{41})$ est vide (en particulier $C(\mathbb{Q})$ est vide).

III. L'équation de Fermat locale

Considérons un nombre premier $p \geq 3$. Soit C la courbe de Fermat d'équation

$$(9) \quad x^p + y^p + z^p = 0.$$

Récemment A. Wiles a démontré que si $[x, y, z]$ appartient à $C(\mathbb{Q})$, alors $xyz = 0$ ([Wi]). On va montrer ici l'énoncé suivant :

Proposition 8.2. *Pour tout nombre premier l , il existe $(\alpha, \beta, \gamma) \in \mathbb{Z}_l^3$ tels que, $\alpha\beta\gamma \neq 0$, $\alpha\beta\gamma \equiv 0 \pmod{l}$ et $\alpha^p + \beta^p + \gamma^p = 0$.*

Démonstration : Posons $F = X^p + l^p + (-1)^p$. Supposons $l \neq p$. Soit \bar{F} le polynôme de $\mathbb{F}_l[X]$ déduit de F par réduction modulo l . On a $\bar{F} = X^p - 1 = (X - 1)(1 + \dots + X^{p-1})$.

Puisque l est distinct de p , 1 est racine simple de \bar{F} . D'après le lemme de Hensel, F possède donc une racine dans \mathbb{Z}_l . D'où le résultat dans ce cas. Supposons maintenant $l = p$. On a $v_l(F(1)) = p$, et $v_l(F'(1)) = 1$. Puisque l'on a $p \geq 3$, le lemme de Hensel entraîne de nouveau que F a une racine dans \mathbb{Z}_l . D'où la proposition.

Soit U_p le groupe des unités de \mathbb{Z}_p . Au vue de la prop. 8.2, une question naturelle est de demander s'il existe un triplet d'éléments (α, β, γ) dans U_p^3 tel que $\alpha^p + \beta^p + \gamma^p = 0$. La réponse est donnée par le résultat suivant :

Proposition 8.3. *Les conditions suivantes sont équivalentes :*

- (i) *il existe $(\alpha, \beta, \gamma) \in U_p^3$ tel que $\alpha^p + \beta^p + \gamma^p = 0$;*
- (ii) *il existe $(a, b, c) \in \mathbb{Z}^3$ tel que p ne divise pas abc et que $a^p + b^p + c^p \equiv 0 \pmod{p^2}$;*
- (iii) *il existe $a \in \mathbb{Z}$ tel que p ne divise pas $a(a+1)$ et que $(a+1)^p - a^p - 1 \equiv 0 \pmod{p^2}$.*

Démonstration : Supposons la condition (i) satisfaite. Dans ce cas, il existe des entiers a, b et c non divisibles par p tels que $\alpha \equiv a \pmod{p\mathbb{Z}_p}$, $\beta \equiv b \pmod{p\mathbb{Z}_p}$ et $\gamma \equiv c \pmod{p\mathbb{Z}_p}$, ce qui entraîne (ii). Inversement, supposons la condition (ii) vérifiée. Il existe $k \in \mathbb{Z}$ tel que $a^p + b^p + c^p = kp^2$. Posons $d = c - kp$. On a $d \not\equiv 0 \pmod{p}$, $d^p \equiv c^p - kp^2c^{p-1} \pmod{p^3}$, puis $a^p + b^p + d^p \equiv kp^2(1 - c^{p-1}) \pmod{p^3}$. Puisque p ne divise pas c , il en résulte que $a^p + b^p + d^p \equiv 0 \pmod{p^3}$. Le lemme de Hensel, appliqué avec le polynôme $X^p + b^p + d^p$, implique alors l'assertion (i). La preuve de l'équivalence des conditions (ii) et (iii) est laissée en exercice.

On peut vérifier que les nombres premiers impairs $p \leq 101$ qui ne satisfont pas à la condition (iii) sont

$$\{3, 5, 11, 17, 23, 29, 41, 47, 53, 71, 89, 101\}.$$

Cela prouve en particulier le *premier cas* du théorème de Fermat pour ces nombres premiers, autrement dit que l'équation (9) n'a pas de solution $(a, b, c) \in \mathbb{Z}^3$, avec abc non divisible par p .

Il résulte de la prop. 8.2 que des considérations locales ne permettent pas d'obtenir des informations sur non existence de points $[a, b, c] \in C(\mathbb{Q})$ tels que $abc \neq 0$ (cela est dû au fait qu'il existe des points triviaux de $C(\mathbb{Q})$: par exemple le point $[0, 1, -1]$). Il n'en va pas de même pour certaines variantes de l'équation (9). Considérons par exemple la courbe C d'équation

$$2x^7 + 5y^7 + 13z^7 = 0.$$

On a $C(\mathbb{Q}_{71}) = \emptyset$, et en particulier $C(\mathbb{Q})$ est vide. En effet, en utilisant le lemme de Hensel, on vérifie que si p est un nombre premier n'appartenant pas à $\{2, 5, 7, 13\}$, l'ensemble $C(\mathbb{Q}_p)$ est vide si et seulement si tel est le cas de $\tilde{C}(\mathbb{F}_p)$, où \tilde{C} est la courbe déduite de C par réduction modulo p . L'on vérifie ensuite que $\tilde{C}(\mathbb{F}_{71}) = \emptyset$ (cette égalité suffit d'ailleurs à prouver que $C(\mathbb{Q})$ est vide). D'où l'assertion. On notera que si p est un nombre premier

tel que $\tilde{C}(\mathbb{F}_p) = \emptyset$, on a nécessairement $p \equiv 1 \pmod{7}$ (car si $p \not\equiv 1 \pmod{7}$, on a $\mathbb{F}_p^* = \mathbb{F}_p^{*7}$). On peut en fait montrer à l'aide des bornes de Weil que 71 est le seul nombre premier p pour lequel $\tilde{C}(\mathbb{F}_p) = \emptyset$.

Exercice. Montrer que la courbe d'équation $2x^5 + 3y^5 + 7z^5 = 0$ n'a pas de point rationnel sur \mathbb{Q} .

IV. L'équation $x^2 + y^2 + z^2 = 0$

On notera C la courbe d'équation

$$(10) \quad x^2 + y^2 + z^2 = 0.$$

On se propose de démontrer le résultat suivant :

Proposition 8.4.

- a) On a $C(\mathbb{Q}_2) = \emptyset$;
- b) pour tout nombre premier impair, on a $C(\mathbb{Q}_p) \neq \emptyset$;
- c) si K une extension quadratique de \mathbb{Q}_2 , l'ensemble $C(K)$ n'est pas vide.

Démonstration : Notons v_2 la valuation 2-adique de \mathbb{Q}_2 .

L'assertion a) : on remarque que si $C(\mathbb{Q}_2)$ n'est pas vide, il existe un point $[x, y, z]$ de $C(\mathbb{Q}_2)$ tel que $v_2(x) = v_2(y) = 0$ et $v_2(z) \geq 0$. Ainsi x^2 et y^2 sont congrus à 1 modulo 4, de sorte que l'on a $v_2(x^2 + y^2) = 1$, ce qui conduit à une contradiction.

L'assertion b) : il existe deux éléments a et b dans \mathbb{F}_p tels que l'on ait $a^2 + b^2 = -1$. Il existe donc deux entiers x et y tels que $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. On peut supposer que x n'est pas divisible par p . Le polynôme $F = X^2 + y^2 + 1$ est alors tel que $F(x) \equiv 0 \pmod{p}$ et $F'(x) \not\equiv 0 \pmod{p}$. D'après le lemme de Hensel, F a une racine dans \mathbb{Q}_p . D'où l'assertion.

L'assertion c) : déterminons d'abord toutes les extensions quadratiques de \mathbb{Q}_2 . Une telle extension est de la forme $\mathbb{Q}_2(\sqrt{d})$, où d est un élément de \mathbb{Q}_2 qui n'est pas un carré. Elle ne dépend évidemment que de la classe de d modulo \mathbb{Q}_2^{*2} . Or $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ est un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$, dont un système de représentants est $S = \{\pm 1, \pm 2, \pm 3 \pm 6\}$ (cf. chap. VI). On déduit de là qu'il existe exactement sept extensions quadratiques de \mathbb{Q}_2 , qui sont précisément les $\mathbb{Q}_2(\sqrt{d})$, où $d \in S$ et $d \neq 1$.

1) Supposons $K = \mathbb{Q}(\sqrt{2})$. Montrons que $C(K) \neq \emptyset$. On remarque pour cela que l'on a $(1 - \sqrt{2})^2 + (\sqrt{2})^2 = 5 - 2\sqrt{2}$. On considère ensuite le polynôme $F = X^2 + 5 - 2\sqrt{2}$. On a $F(1 + \sqrt{2}) = 8$ et $F'(1 + \sqrt{2}) = 2(1 + \sqrt{2})$. Si v est la valuation de $\mathbb{Q}_2(\sqrt{d})$ qui prolonge v_2 , on a $v(F(1 + \sqrt{2})) = 3$ et $v(F'(1 + \sqrt{2})) = 1$. D'après le lemme de Hensel, F a donc une racine dans K , ce qui entraîne notre assertion.

2) En remarquant que -7 est un carré dans \mathbb{Q}_2 , que $\sqrt{-5} \in \mathbb{Q}_2(\sqrt{3})$, et enfin que $\sqrt{10} \in \mathbb{Q}_2(\sqrt{-6})$ (cf. chap. VI), on déduit alors le lemme des égalités suivantes :

$$(\sqrt{-1})^2 + 1 + 0 = 0, \quad (\sqrt{-2})^2 + 1 + 1 = 0, \quad (\sqrt{-5})^2 + 2^2 + 1 = 0,$$

$$(1 + \sqrt{-6})^2 + (1 - \sqrt{-6})^2 + (\sqrt{10})^2 = 0, \quad (\sqrt{6})^2 + 1 + (\sqrt{-7})^2 = 0,$$

$$(1 + \sqrt{-3})^2 + (1 - \sqrt{-3})^2 + 2^2 = 0.$$

V. Loi de réciprocité quadratique

On se propose dans ce paragraphe de donner une démonstration, utilisant la théorie de la ramification, de la loi de réciprocité quadratique. Soient p un nombre premier impair et d un entier premier à p . On définit le symbole de Legendre $\left(\frac{d}{p}\right)$ de la façon suivante :

$$\left(\frac{d}{p}\right) = 1 \quad \text{si } d \text{ est un carré modulo } p,$$

$$\left(\frac{d}{p}\right) = -1 \quad \text{si } d \text{ n'est pas un carré modulo } p.$$

Étant donnés deux entiers a et b premiers à p , on a l'égalité

$$(11) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

(Cela provient du fait que les groupes $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ et $\{\pm 1\}$ sont isomorphes) On dispose du critère suivant, dû à Euler :

Lemme 8.2. *Soit a un entier premier à p . On a l'égalité*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Démonstration : Le groupe \mathbb{F}_p^{*2} est d'ordre $(p-1)/2$. On déduit de là que \mathbb{F}_p^{*2} est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - 1$. Par ailleurs, on a

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Cela entraîne le lemme.

Démontrons maintenant la loi de réciprocité quadratique qui est due à Gauss. Il s'agit de l'énoncé suivant :

Théorème 8.2. *Soient p et q deux nombres premiers impairs distincts. On a l'égalité*

$$(12) \quad \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Démonstration : Montrons d'abord le lemme suivant :

Proposition 8.5. Soit F une extension de degré 2 de \mathbb{Q} : il existe un entier d sans facteur carré tel que l'on ait $F = \mathbb{Q}(\sqrt{d})$. Soient A l'anneau d'entiers de F et p un nombre premier impair qui ne divise pas d . Alors, l'idéal pA est premier si et seulement si l'on a $\left(\frac{d}{p}\right) = -1$. Si tel est le cas on dit que p est inerte dans F , et que p est décomposé dans le cas contraire.

Démonstration : Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique de \mathbb{Q}_p . Soit \mathfrak{p} un idéal premier de A au-dessus de p . Le complété $F_{\mathfrak{p}}$ de F en \mathfrak{p} s'identifie à une extension de \mathbb{Q}_p contenue dans $\overline{\mathbb{Q}_p}$, qui n'est autre que $\mathbb{Q}_p(\sqrt{d})$ (cf. prop. 7.4 et la remarque qui suit). Supposons $pA = \mathfrak{p}$. Dans ce cas $\mathbb{Q}_p(\sqrt{d})$ est une extension de degré 2 de \mathbb{Q}_p , et d n'est donc pas un carré dans \mathbb{Q}_p . D'après le lemme de Hensel, d modulo p n'est pas un carré dans \mathbb{F}_p , autrement dit, on a $\left(\frac{d}{p}\right) = -1$. Par ailleurs, p est non ramifié dans F (car p ne divise pas d). Par conséquent, si pA n'est pas un idéal premier, il y a deux idéaux premiers de A au-dessus de p , et l'on a $\mathbb{Q}_p(\sqrt{d}) = \mathbb{Q}_p$. Cela implique que d est un carré dans \mathbb{F}_p . D'où le résultat.

Démontrons maintenant le théorème. Soit ζ une racine primitive q -ième de l'unité. L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est cyclique de groupe de Galois isomorphe à $(\mathbb{Z}/q\mathbb{Z})^*$, via l'application j définie, pour tout $\sigma \in G$, par l'égalité

$$(13) \quad \sigma(\zeta) = \zeta^{j(\sigma)}.$$

Il existe en particulier une unique extension quadratique F contenue dans $\mathbb{Q}(\zeta)$, le groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta)/F)$ étant isomorphe via j au sous-groupe des carrés \mathbb{F}_q^{*2} de \mathbb{F}_q^* . Puisque p est distinct de q , p est non ramifié dans $\mathbb{Q}(\zeta)$ (cf. chap. IV) : soit σ_p la substitution de Frobenius en p de $\mathbb{Q}(\zeta)/\mathbb{Q}$ (cf. lemme 3.12 c)). Montrons que l'on l'équivalence suivante :

$$(14) \quad \sigma_p|_F = 1_F \iff \left(\frac{p}{q}\right) = 1.$$

D'abord la restriction de σ_p à F fixe les éléments de F si et seulement si $j(\sigma_p)$ est un carré dans \mathbb{F}_q . Par ailleurs, On a

$$(15) \quad \sigma_p(\zeta) = \zeta^p.$$

En effet, soit \mathfrak{P} un idéal premier de l'anneau d'entiers de $\mathbb{Q}(\zeta)$ au-dessus de p : on a $\sigma_p(\zeta) \equiv \zeta^p \pmod{\mathfrak{P}}$. Par ailleurs, il existe i tel que $\sigma_p(\zeta) = \zeta^i$. Il en résulte que si $i \neq p$, $1 - \zeta$ appartient à \mathfrak{P}^\dagger , ce qui n'est pas. D'où (15). On a ainsi $j(\sigma_p) = p \pmod{q}$, ce qui entraîne l'équivalence (14).

[†] Cette assertion se justifie de la façon suivante : soit j un entier tel que $1 \leq j \leq q-1$. On a $1 - \zeta^j = (1 - \zeta)u$, où u appartient à l'anneau d'entiers de $\mathbb{Q}(\zeta)$. En fait, u est une unité. En effet, les normes de $\mathbb{Q}(\zeta)$ sur \mathbb{Q} de $1 - \zeta^j$ et de $1 - \zeta$ sont égales, de sorte que u est un entier de norme 1. Or un entier d'un corps de nombres est une unité si et seulement si sa norme sur \mathbb{Q} est ± 1 (cf. [Sa], prop. 1., p. 72).

Cela étant, la restriction de σ_p à F est la substitution de Frobenius en p de l'extension F/\mathbb{Q} (cf. chap. III). Ainsi $\sigma_p|_F$ engendre le sous-groupe de décomposition en p du groupe de Galois $\text{Gal}(F/\mathbb{Q})$. On déduit de là que l'on a

$$(16) \quad \sigma_p|_F = 1_F \iff p \text{ est décomposé dans l'extension } F/\mathbb{Q}.$$

Par ailleurs, q est le seul nombre premier qui se ramifie dans F , car tel est le cas dans $\mathbb{Q}(\zeta)$. On a donc nécessairement (cf. chap. IV)

$$(17) \quad F = \mathbb{Q}(\sqrt{q^*}) \text{ où } q^* = (-1)^{\frac{q-1}{2}} q.$$

On déduit alors de (16), (17) et de la prop. 8.4 que l'on a

$$(18) \quad \sigma_p|_F = 1_F \iff \left(\frac{q^*}{p}\right) = 1.$$

D'après les équivalences (14) et (18), on a donc l'égalité

$$(19) \quad \left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

D'après la formule (11), on a

$$(20) \quad \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

et il résulte du lemme 8.2 que l'on a

$$(21) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Les égalités (19), (20) et (21) entraînent alors le théorème.

Appendice I — Espaces vectoriels topologiques et corps valués

On considère dans toute la suite un corps K , muni d'une valeur absolue *non triviale* (pas nécessairement ultramétrique), qui est *complet* : K est un corps muni d'une topologie séparée tel que les opérations d'addition, de multiplication et d'inversion soient continues.

Soit E un espace vectoriel de dimension finie n sur K . On suppose que E est muni d'une distance d invariante par translation (autrement dit que la distance de deux éléments x et y de E ne dépend que de $x - y$), et que les applications $E \times E \rightarrow E$ et $K \times E \rightarrow E$ définies par $(x, y) \mapsto x + y$ et $(\lambda, x) \mapsto \lambda x$ sont continues pour les topologies produits sur $E \times E$ et $K \times E$: E est ainsi muni d'une structure d'espace vectoriel topologique.

Nous allons démontrer le résultat suivant :

Théorème. *Tout isomorphisme d'espaces vectoriels de E sur K^n est aussi un homéomorphisme d'espaces topologiques.*

Démonstration

On montre d'abord quelques lemmes préliminaires. Commençons par donner (dans notre contexte) une caractérisation topologique des suites de Cauchy de E :

Lemme 1. *Soit $(x_n)_{n \in \mathbb{N}}$ une suite d'éléments de E . Elle est de Cauchy (pour d) si et seulement si la condition suivante est réalisée :*

(*) *pour tout voisinage V de 0 dans E , il existe un entier N , tel que dès que p et q sont plus grands que N , la différence $x_p - x_q$ appartient à V .*

Démonstration : Supposons que $(x_n)_{n \in \mathbb{N}}$ soit une suite de Cauchy. Soit V un voisinage de 0 dans E . Il existe un nombre $\epsilon > 0$ tel que la boule ouverte de centre 0 et de rayon ϵ soit contenue dans V . Il existe par ailleurs un entier N tel que pour tout p et q plus grands que N , l'on ait $d(x_p, x_q) < \epsilon$. Puisque d est invariante par translation, l'on a $d(x_p, x_q) = d(x_p - x_q, 0)$, de sorte que $x_p - x_q$ est dans V , ce qui prouve la condition (*). L'implication réciproque se prouve par le même argument.

Soit H un sous-espace vectoriel de E . Notons $\pi : E \rightarrow H$ une application de projection sur H (on choisit donc ici implicitement un supplémentaire de H dans E). Soit H' le noyau de π et $\varphi : E \rightarrow H \times H'$ l'application définie par

$$\varphi(x) = (\pi(x), x - \pi(x)).$$

Lemme 2. *L'application φ est un homéomorphisme de E sur $H \times H'$ si et seulement si π est continue.*

Démonstration : En composant φ avec la première projection $pr_1 : H \times H' \rightarrow H$, on constate que si φ est continue, π aussi. Inversement, supposons π continue. Alors, si pr_2 est

la deuxième projection $H \times H' \rightarrow H'$, les applications $pr_1 \circ \varphi$ et $pr_2 \circ \varphi$ sont continues, et il en résulte que φ est continue. Par ailleurs, l'application réciproque de φ , qui est donnée par $(x, y) \mapsto x + y$, est continue. D'où le fait que φ soit un homéomorphisme.

Lemme 3. *La topologie de K n'est pas discrète.*

Démonstration : Soit $|\cdot|$ la valeur absolue considérée sur K . Supposons que la topologie sur K associée à $|\cdot|$ soit discrète. Dans ce cas la valeur absolue triviale et $|\cdot|$ sont équivalentes, ce qui entraîne (par définition) que $|\cdot|$ est aussi triviale. D'où le lemme.

Lemme 4. *Soit F un espace vectoriel topologique sur K (pas nécessairement métrisable) et V un voisinage de 0 dans F . Alors, il existe un voisinage W de 0 contenu dans V possédant la propriété suivante : pour tout élément $b \in K$ tel que $|b| \leq 1$, l'ensemble bW est contenu dans W .*

Démonstration : L'application $K \times F \rightarrow F$ qui à (λ, x) associe λx est continue en $(0, 0)$. Il existe donc un nombre réel $\epsilon > 0$, et un voisinage U de 0 tels que, pour tout $a \in K$, dès que $|a| < \epsilon$, l'ensemble aU est contenu dans V . On pose alors

$$W = \bigcup_{|a| \leq \epsilon} aU.$$

Alors W est un voisinage de 0. En effet, puisque la valeur absolue $|\cdot|$ n'est pas triviale, il existe un $a \neq 0$ tel que $|a| < \epsilon$ (sinon $\{0\}$ serait un ouvert, donc par translation tous les points de F le seraient, et K serait discret, ce qui n'est pas d'après le lemme 3), et aU est un voisinage de 0. Soient alors b un élément de K tel que $|b| \leq 1$ et y un élément de W . Il existe $a \in K$ tel que $|a| < \epsilon$, et que y soit dans aU . Alors by appartient à baU qui est contenu dans W car $|ba| \leq |a| < \epsilon$. D'où le lemme.

Rappelons que, pour tout entier $r \geq 1$, l'espace topologique K^r muni de la topologie produit, est métrisable. Par exemple, la distance d' donnée par la formule

$$d'((x_i), (y_i)) = \sum_{i=1}^r |x_i - y_i|,$$

définit la topologie produit sur K^r . De plus d' est invariante par translation. Par ailleurs, K étant complet, le couple (K^r, d') est aussi complet.

Lemme 5. *Soit F un sous-espace vectoriel de E de dimension r . Supposons qu'il existe un isomorphisme linéaire et topologique de F sur K^r . Alors, F est complet. En particulier, F est une partie fermée de E .*

Démonstration : Soit $\varphi : F \simeq K^r$ un tel isomorphisme. Soit $(x_n)_{n \in \mathbb{N}}$ une suite de Cauchy de F . Il résulte du lemme 1 que $(\varphi(x_n))_{n \in \mathbb{N}}$ est une suite de Cauchy de K^r pour d' . Elle est convergente : soit x sa limite. On vérifie alors que $(x_n)_{n \in \mathbb{N}}$ converge vers $\varphi^{-1}(x)$,

ce qui prouve que F est complet. Par ailleurs, si $(x_n)_{n \in \mathbb{N}}$ est une suite d'éléments de F qui converge dans E , cette suite est de Cauchy, et comme F est complet, elle est convergente dans F . Cela montre que F est fermé.

Démontrons maintenant le théorème. On traite d'abord le cas où $n = 1$. Considérons un isomorphisme linéaire $\varphi : K \rightarrow E$ de K sur E . Il existe x non nul dans E tel que l'on ait $\varphi(a) = ax$ pour tout $a \in K$, et par conséquent φ est une application continue. Montrons que φ^{-1} est aussi continue. Il suffit pour cela de vérifier que l'application $\varphi^{-1} : E \rightarrow K$ qui à $y \in E$ associe $a \in K$, où $y = ax$, est continue en 0. Soit ϵ un nombre réel strictement positif. Puisque K n'est pas discret, il existe a_0 dans K tel que l'on ait $0 < |a_0| < \epsilon$. Comme a_0x n'est pas nul et que E est *séparé* (car métrisable), il existe un voisinage V de 0 tel que a_0x n'appartienne pas à V . Soit alors W un voisinage de 0 contenu dans V satisfaisant à la conclusion du lemme 4. Vérifions que $\varphi^{-1}(W)$ est contenu dans la boule ouverte centrée en 0 et de rayon ϵ , ce qui prouvera notre assertion. Soit y un élément de W . On a $\varphi^{-1}(y) = a$, où $y = ax$. Supposons $|a_0| \leq |a|$. On a alors $|a_0a^{-1}| \leq 1$, et cela entraîne $a_0x = (a_0a^{-1})(ax)$ appartient à $(a_0a^{-1})W$ qui est contenu dans W d'après le lemme 4, ce qui contredit le choix de V . Cela prouve l'inégalité $|a| < |a_0|$ et notre assertion. D'où le théorème si $n = 1$.

(*) On notera que cette démonstration vaut dès que E est séparé, qu'il soit métrisable ou pas.

On suppose alors le théorème vérifié pour tous les espaces vectoriels de dimension $\leq n - 1$, où n est un entier supérieur ou égal à 1. Soit $\psi : E \rightarrow K^n$ un isomorphisme linéaire de E sur K^n . Soient $(e_i)_{1 \leq i \leq n}$ la base canonique de K^n et $(x_i)_{1 \leq i \leq n}$ des éléments de E tels que $\psi(x_i) = e_i$. La famille $(x_i)_{1 \leq i \leq n}$ est une K -base de E .

Soit H' le sous-espace de E engendré par la famille $(x_i)_{1 \leq i \leq n-1}$. La restriction ψ' de ψ à H' induit un isomorphisme linéaire de H' sur $\psi(H') = K^{n-1}$. D'après l'hypothèse de récurrence, ψ' est un homéomorphisme de H' sur K^{n-1} . D'après le lemme 5, H' est une partie fermée de E .

Soit $\pi : E \rightarrow Kx_n$ l'application définie par

$$\pi\left(\sum_{i=1}^n a_i x_i\right) = a_n x_n.$$

C'est une application linéaire, qui vérifie $\pi \circ \pi = \pi$, $\pi(E) = Kx_n$ et $\pi^{-1}(0) = H'$. Montrons que π est continue. On remarque pour cela que l'application π induit un isomorphisme linéaire $\bar{\pi} : E/H' \rightarrow Kx_n$ de E/H' sur Kx_n . L'espace vectoriel E/H' , muni de la topologie quotient, est un espace vectoriel topologique, et puisque H' est fermé, E/H' est *séparé*. Par ailleurs, la dimension de E/H' sur K est égale à 1. On déduit de là que $\bar{\pi}$ est un homéomorphisme de E/H' sur Kx_n (cf. (*)). Par ailleurs, si $s : E \rightarrow E/H'$ est la surjection

canonique, on a $\pi = \bar{\pi} \circ s$, ce qui prouve que π est continue. On déduit alors du lemme 2 que l'application $\gamma : E \rightarrow H' \times Kx_n$ définie par

$$\sum_{i=1}^n a_i x_i \mapsto \left(\sum_{i=1}^{n-1} a_i x_i, a_n x_n \right)$$

est un homéomorphisme. Soit alors $\nu : H' \times Kx_n \rightarrow K^n$ l'application définie par

$$\left(\sum_{i=1}^{n-1} a_i x_i, a_n x_n \right) \mapsto (a_i)_{1 \leq i \leq n}.$$

C'est un homéomorphisme de $H' \times Kx_n$ sur K^n et l'on a $\nu \circ \gamma = \psi$ (car $\psi(x_i) = e_i$). Cela prouve que ψ est un homéomorphisme de E sur K^n . D'où le théorème.

On déduit en particulier du théorème et du lemme 5 le résultat suivant :

Corollaire. *L'espace métrique (E, d) est complet.*

Appendice II — Espaces de Baire

Soit E un espace topologique.

Définition. On dit que E est un espace de Baire si l'une des deux conditions équivalentes suivantes est réalisée :

- a) Toute réunion dénombrable d'ensembles fermés d'intérieur vide est d'intérieur vide.
- b) Toute intersection dénombrable d'ensembles ouverts denses dans E est dense dans E .

L'objectif de cet Appendice est de démontrer le résultat suivant :

Théorème. Supposons que l'une des conditions suivantes soit réalisées :

- a) l'espace E est localement compact ;
- b) il existe une distance d sur E , définissant la topologie de E , telle que l'espace métrique (E, d) soit complet.

Alors, E est un espace de Baire.

Démonstration

Considérons une suite $(F_n)_{n \in \mathbb{N}}$ de parties fermées de E . Posons

$$X = \bigcup_{n \in \mathbb{N}} F_n.$$

Soit Y l'intérieur de X . On suppose que Y n'est pas vide. Il s'agit de montrer l'existence d'un entier n tel que l'intérieur de F_n ne soit pas vide. Pour cela, on va procéder par l'absurde en supposant que tous les F_n sont d'intérieur vide.

1) Supposons que E soit localement compact.

On va construire une suite décroissante d'ouverts non vides $(U_n)_{n \in \mathbb{N}}$ de E , tels que pour tout entier n :

- (i) l'adhérence $\overline{U_0}$ de U_0 est contenu dans X ;
- (ii) $\overline{U_0}$ est compact ;
- (iii) $\overline{U_n} \cap F_n = \emptyset$.

D'après les hypothèses faites, il existe un point a de E qui appartienne à Y et pas à F_0 (sinon Y serait contenu dans F_0 , et il existerait un ouvert non vide contenu dans F_0 , ce qui n'est pas). L'ensemble $Z = Y \cap (E - F_0)$ est un ouvert de E qui contient a . Puisque E est localement compact, il existe un voisinage compact K de a contenu dans Z . Soit U_0 l'intérieur de K . Alors, l'ouvert U_0 satisfait aux conditions ci-dessus : U_0 n'est pas vide, car a appartient à U_0 (par définition K contient un ouvert contenant a), l'adhérence de U_0 est compacte car $\overline{U_0}$ est un fermé contenu dans K (qui est compact), $\overline{U_0}$ est contenu dans $Y \subseteq X$, et l'on a $\overline{U_0} \cap F_0 = \emptyset$ car K est contenu dans Z . Supposons alors qu'il existe un

entier $n \geq 0$ et un ouvert U_n satisfaisant aux conditions ci-dessus. Construisons un ouvert U_{n+1} satisfaisant à aussi à ces conditions. On remarque pour cela que U_n n'est pas contenu dans $\overline{U_n} \cap F_{n+1}$ (car F_{n+1} est d'intérieur vide et U_n n'est pas vide). L'ensemble

$$W = U_n \cap \left(E - (\overline{U_n} \cap F_{n+1}) \right)$$

est donc un ouvert non vide de E : soit b un point de W . Il existe un voisinage compact K' de b contenu dans W (E est localement compact), et l'ouvert U_{n+1} égal à l'intérieur de K' convient. D'où la construction d'une suite $(U_n)_{n \in \mathbb{N}}$ vérifiant les conditions demandées. Posons alors

$$U = \bigcap_{n \geq 0} \overline{U_n}.$$

Par définition, U est contenu dans $\overline{U_0}$ qui est compact, ce qui entraîne que U n'est pas vide (sinon il existerait une intersection finie de $\overline{U_n}$ qui serait vide, ce qui ne peut être, car la suite $(U_n)_{n \in \mathbb{N}}$ est décroissante et il en est de même de la suite $(\overline{U_n})_{n \in \mathbb{N}}$). Soit α un élément de U . Alors, α n'appartient pas à X (propriété (iii)), ce qui, d'après la propriété (i), conduit à une contradiction, car $\alpha \in \overline{U_0}$. D'où le théorème sous l'hypothèse envisagée.

2) Supposons maintenant que (E, d) soit un espace métrique complet. Démontrons d'abord le lemme suivant :

Lemme. Soit $(G_n)_{n \in \mathbb{N}}$ une suite décroissante de parties fermées bornées et non vides de E . Soit $\delta(G_n)$ le diamètre de G_n . Si la suite $(\delta(G_n))_{n \in \mathbb{N}}$ est convergente vers 0, on a

$$\bigcap_{n \in \mathbb{N}} G_n \neq \emptyset.$$

Démonstration : Pour chaque entier n , on choisit un élément x_n de G_n . Étant donné un entier n , pour tous les entiers p et q plus grands que n , les éléments x_p et x_q sont dans G_n . On a ainsi $d(x_p, x_q) \leq \delta(G_n)$. D'après l'hypothèse faite, cela entraîne que $(x_n)_{n \in \mathbb{N}}$ est une suite de Cauchy. Soit a la limite de cette suite. Alors a appartient à l'intersection des G_n . En effet, étant donné un entier n , puisque x_p est dans G_n si $n \geq p$ et que G_n est fermé, a appartient à G_n . D'où le lemme.

Démontrons l'assertion b) du théorème : Soit a un point de Y qui n'appartienne pas à F_0 (un tel point existe car F_0 est d'intérieur vide). L'ensemble $Z = Y \cap (E - F_0)$ est un ouvert de E qui contient a . Il existe donc un entier $\rho > 0$ tel que la boule ouverte de centre a et de rayon ρ soit contenue dans Z . Notons B_0 la boule fermée de centre a et de rayon $\rho/2$: B_0 est aussi contenu dans Z et l'on a $B_0 \cap F_0 = \emptyset$. On va alors construire une suite décroissante de boules fermées non vides $(B_n)_{n \in \mathbb{N}}$, telle que, si r_n est le rayon de B_n , la suite $(r_n)_{n \in \mathbb{N}}$ tende vers 0, et que pour tout n , l'on ait $B_n \cap F_n = \emptyset$.

L'existence d'une telle suite suffit pour obtenir le résultat : en effet, d'après le lemme, il existe un élément x dans l'intersection des B_n , et pour tout n , x n'appartient à F_n . Or x est dans B_0 et est donc contenu dans la réunion des F_n . D'où une contradiction et le résultat.

Reste à construire une suite $(B_n)_{n \in \mathbb{N}}$ satisfaisant les conditions demandées. On suppose pour cela qu'il existe un entier $n \geq 0$ et une boule fermée non vide B_n , telle que l'on ait $nr_n \leq 1$ et que $B_n \cap F_n = \emptyset$. Démontrons alors qu'il existe une boule fermée B_{n+1} vérifiant les conditions suivantes :

- (i) $B_{n+1} \subseteq B_n$;
- (ii) $(n+1)r_{n+1} \leq 1$;
- (iii) $B_{n+1} \cap F_{n+1} = \emptyset$.

Notons I_n l'intérieur de la boule B_n . Puisque l'intérieur de F_{n+1} est vide, I_n n'est pas contenu dans F_{n+1} . Par conséquent

$$A_n = I_n \cap (E - F_{n+1})$$

est un ouvert non vide : soit x un élément de A_n . Il existe un nombre réel $r > 0$ tel que la boule ouverte de centre x et de rayon r soit contenue dans A_n . Posons

$$R = \text{Min} \left(\frac{1}{n+1}, \frac{r}{2} \right).$$

La boule fermée B_{n+1} de centre x et de rayon R satisfait alors aux trois conditions ci-dessus. D'où le théorème.

On notera que les arguments utilisés dans les alinéas 1) et 2) sont tout à fait similaires. On pourra à titre d'exercice rédiger une seule démonstration du théorème, englobant à la fois le cas localement compact et le cas métrique complet.

Appendice III — Corps des séries de Puiseux

Soient K un corps et X une indéterminée. Soit $K(X)$ le corps des fractions rationnelles à coefficients dans K . Notons v la valuation de $K(X)$ associée à X : si F est un élément non nul de $K(X)$, $v(F)$ est l'exposant de X dans la décomposition de F en produit de facteurs irréductibles (on l'appelle la valuation X -adique sur $K(X)$).

Soient $K[[X]]$ l'anneau des séries formelles à coefficients dans K (cf. Chap. I, alinéa 2)). C'est un anneau de valuation discrète (*loc. cit.*), dont le corps des fractions $K((X))$ est le corps des séries formelles

$$\sum_{n \geq n_0} a_n X^n \quad \text{où } n_0 \in \mathbb{Z} \quad \text{et } a_n \in K.$$

La valuation discrète associée $\omega : K((X)) \rightarrow \mathbb{Z} \cup \{+\infty\}$, est décrite comme suit : pour tout élément $s = \sum a_n X^n$ non nul dans $K((X))$, $\omega(s)$ est le plus petit entier $n_0 \in \mathbb{Z}$ tel que $a_{n_0} \neq 0$.

On va décrire dans cet Appendice une complétion du corps valué $(K(X), v)$ et, dans le cas où K est algébriquement clos de caractéristique 0, déterminer une clôture algébrique de $K((X))$, que l'on appelle le corps des séries de Puiseux. Soit $i : K(X) \rightarrow K((X))$ le morphisme d'inclusion.

Théorème 1. *Le triplet $(K((X)), \omega, i)$ est une complétion de $(K(X), v)$.*

Démonstration : 1) Montrons que toute suite de Cauchy de $K((X))$ est convergente. Pour démontrer cette assertion, il suffit de se limiter aux suites de Cauchy d'éléments de $K[[X]]$. En effet, soit $(\sigma_n)_{n \in \mathbb{N}}$ une suite de Cauchy de $K((X))$. C'est une suite bornée. Autrement dit, il existe un entier N_0 (éventuellement négatif) qui minore la suite $(\omega(\sigma_n))_{n \in \mathbb{N}}$. Pour tout $n \in \mathbb{N}$, l'élément $X^{-N_0} \sigma_n$ appartient donc à $K[[X]]$, et la suite $(X^{-N_0} \sigma_n)_{n \in \mathbb{N}}$ est une suite Cauchy de $K[[X]]$. Si l'on suppose que cette suite est convergente de limite σ , alors la suite $(\sigma_n)_{n \in \mathbb{N}}$ est convergente de limite $X^{N_0} \sigma$. D'où notre assertion.

Considérons alors une suite de Cauchy $(\sigma_n)_{n \in \mathbb{N}}$ d'éléments de $K[[X]]$. Pour tout n , posons

$$\sigma_n = \sum_{k \geq 0} a_{n,k} X^k,$$

où les $a_{n,k}$ sont dans K . Pour tout entier M , il existe un entier N_M tel que, pour tous les entiers p et q , supérieurs ou égaux à N_M , l'on ait

$$a_{p,k} = a_{q,k} \quad \text{pour tout } k \leq M.$$

On déduit de là que pour tout entier $k \geq 0$ fixé, en prenant $M = k$, l'on a $a_{p,k} = a_{q,k}$ dès que p et q sont plus grands que N_k . Autrement dit, pour tout k , la suite $(a_{n,k})_{n \in \mathbb{N}}$ est

stationnaire. Notons a_k la limite de cette suite, et posons

$$\sigma = \sum_{k \geq 0} a_k X^k.$$

Alors la suite $(\sigma_n)_{n \in \mathbb{N}}$ est convergente de limite σ . En effet, pour tout M , dès que l'on a $n \geq N_M$, on a l'égalité $a_k = a_{n,k}$. Ainsi, pour tout $n \geq N_M$, la différence $\sigma_n - \sigma$ est multiple de X^M , i.e. on a $\omega(\sigma_n - \sigma) \geq M$ pour tout $n \geq N_M$. D'où l'assertion et le fait que le corps valué $(K((X)), \omega)$ soit complet.

2) La valuation ω prolonge v (par définition). Il reste à montrer que $K(X)$ est dense dans $K((X))$, autrement dit, que tout élément $t = \sum_{n \geq n_0} a_n X^n$ de $K((X))$ est limite d'une suite de fractions rationnelles. Comme précédemment, on peut supposer que t appartient à $K[[X]]$. Pour tout entier $n \geq n_0$, posons

$$\sigma_n = \sum_{k=n_0}^n a_k X^k.$$

Par définition σ_n est dans $K[X]$. Pour tout $n \geq n_0$, l'on a $\omega(t - \sigma_n) \geq n + 1$, ce qui prouve que la suite $(\sigma_n)_{n \in \mathbb{N}}$ converge vers t . D'où le résultat.

Supposons désormais que K soit algébriquement clos de caractéristique 0. Soit Ω une clôture algébrique de $K((X))$. Pour tout entier $n \geq 1$, on note L_n l'extension de $K((X))$, contenue dans Ω , obtenue en adjoignant à $K((X))$ une racine n -ième de X . Puisque K est algébriquement clos, L_n ne dépend pas de la racine n -ième de X choisie. En fait :

Lemme. *L'extension $L_n/K((X))$ est galoisienne totalement ramifiée de degré n .*

Démonstration : Le corps $K((X))$ étant de caractéristique 0 (car tel est le cas de K), l'extension $L_n/K((X))$ est séparable. Comme on l'a remarqué ci-dessus c'est une extension normale. Par ailleurs, le polynôme $Y^n - X$ est un polynôme d'Eisenstein de degré n (cf. le th. 1 et le Chap. VI). D'où le lemme.

Donnons maintenant une description de Ω .

Théorème 2. *Soit M une extension finie de $K((X))$ contenue dans Ω . Il existe un entier $n \geq 1$ tel que l'on ait $M = L_n$. En particulier, on a l'égalité*

$$(1) \quad \Omega = \bigcup_{n \geq 1} L_n.$$

Démonstration : Posons $A = K[[X]]$ et notons B la clôture intégrale de A dans M . Puisque A est un anneau de valuation discrète, il en est de même de B (cf. le th. 1 et Chap. VII, II). Soit π une uniformisante de B . Il existe un entier $n \geq 1$ tel que l'on ait $X = u\pi^n$, où u est une unité de B . Soit \bar{u} l'image de u dans $k_M = B/\pi.B$. Le corps k_M

est une extension finie de K : on a donc $k_M = K$. Il en résulte que le polynôme $Y^n - \bar{u}$ de $k_M[Y]$ a n racines distinctes dans k_M (K est de caractéristique 0). On déduit alors du lemme de Hensel, un relèvement v de l'une d'entre elles dans B , telle que l'on ait $v^n = u$. L'élément $\pi' = \pi v$ est une uniformisante de B (car v est une unité). L'extension $M/K((X))$ étant totalement ramifiée (car l'extension résiduelle correspondante est triviale), on a donc $M = K((X))(\pi')$ (lemme 7.5). Par construction, π' est une racine n -ième de X , et l'on a ainsi l'égalité $M = L_n$. D'où le théorème.

On peut en fait expliciter de façon intrinsèque, en termes de limite inductive, une clôture algébrique de $K((X))$ (sans faire appel à l'existence de Ω comme on l'a fait ci-dessus). On procède de la façon suivante : pour tout entier ≥ 1 , on pose $K_n = K((X))$, et pour tout couple d'entiers (n, m) tel que n divise m , on considère l'homomorphisme de corps

$$\varphi_{n,m} : K_n \rightarrow K_m,$$

défini par l'égalité

$$\varphi_{n,m}(X) = X^{\frac{m}{n}}.$$

Pour tous les entiers, n, m et p tels que n divise m et m divise p , l'on a

$$\varphi_{n,n} = 1_{K_n} \quad \text{et} \quad \varphi_{m,p} \circ \varphi_{n,m} = \varphi_{n,p}.$$

On obtient ainsi un système inductif filtrant $\{K_n; \varphi_{n,m}\}$ (cf. [Mat], p. 269). On peut considérer la limite inductive K_∞ de ce système, qui est l'ensemble quotient

$$K_\infty = \left(\coprod_{n \geq 1} K_n \right) / \mathcal{R},$$

où $\coprod K_n$ est la réunion disjointe des corps K_n et où \mathcal{R} est la relation d'équivalence définie comme suit : soient x et y deux éléments de $\coprod K_n$; il existe n et m tel que $x \in K_n$ et $y \in K_m$. Alors x est congru à y modulo \mathcal{R} s'il existe un entier p multiple de n et m tel que l'on ait $\varphi_{n,p}(x) = \varphi_{m,p}(y)$. Cela étant, puisque les K_n sont des corps, K_∞ est canoniquement muni d'une structure de corps, et pour tout $n \geq 1$, l'on dispose de l'homomorphisme de corps

$$i_n : K_n \rightarrow K_\infty,$$

qui à un élément x de K_n associe sa classe modulo \mathcal{R} dans K_∞ (cela permet par exemple d'identifier $K((X))$ via i_1 à un sous-corps de K_∞). Les homomorphismes de transition $\varphi_{n,m}$ étant injectifs, on a alors

$$K_\infty = \bigcup_{n \geq 1} i_n(K_n).$$

Par ailleurs, pour tout n , on a

$$i_n \circ \varphi_{1,n} = i_1,$$

de sorte que l'image de $X \in K_n$ dans K_∞ est une racine n -ième de $i_1(X)$. Ainsi $i_n(K_n)$ est l'extension de $i_1(K_1)$ obtenue par adjonction d'une racine n -ième de $i_1(X)$. La même démonstration que celle du théorème 2 entraîne alors que :

Théorème 2 bis. *Le corps K_∞ est une clôture algébrique de $K((X))$.*

Le corps K_∞ s'appelle le corps des séries de Puiseux.

Bibliographie

- [Am]. Y. Amice, les nombres p -adiques, PUF 1er édition, 1975.
- [At-Ma]. M. F. Atiyah et I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, 1969.
- [Bo-Ch]. Z. I. Borevitch et I. R. Chafarevitch, Théorie des nombres, Gauthier-Villars Paris, 1967.
- [Co]. H. Cohen, A Course in Computational Algebraic Number Theory, GTM 138, Springer-Verlag, 1993.
- [Fr-Ta]. A. Fröhlich et M. J. Taylor, Algebraic Number Theory, Cambridge University Press, 27, 1991.
- [Fu]. W. Fulton, Algebraic Curves, Mathematics Lecture Note Series, Advanced Book Program, Fifth printing, 1978.
- [Ha]. R. Hartshorne, Algebraic Geometry, Springer-Verlag, 52, 1983.
- [Mal]. M.-P. Malliavin, algèbre commutative, Masson, 1984.
- [Mar]. D. A. Marcus, Number Fields, Universitext, Springer-Verlag, 1977.
- [Mat]. H. Matsumura, Commutative ring theory, Cambridge studies in advanced mathematics, 8, 1986.
- [Mo]. C. J. Moreno, Algebraic curves over finite fields, Cambridge University Press, 1991.
- [Ne]. J. Neukirch, Class Field Theory, A Series of Comprehensive Studies in Mathematics, Springer-Verlag 280, 1985.
- [PA]. C. Batut, D. Bernardi, H. Cohen et M. Olivier, User's guide to PARI-GP (version 1.39.12).
- [Ri]. P. Ribenboim, The Theory of Classical Valuations, Springer-Verlag, 1999.
- [Sa]. P. Samuel, Théorie algébrique des nombres, deuxième édition, Hermann, Paris 1971.
- [Se1]. J.-P. Serre, Corps locaux, Hermann 3-ième édition 1980.
- [Se2]. J.-P. Serre, Cours d'Arithmétique, PUF 2-ième édition 1977.
- [Se3]. J.-P. Serre, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics, Vieweg 2nd edition 1990.
- [Wi]. A. Wiles, "Modular elliptic curves and Fermat's Last Theorem", *Ann. of Math.* **141** (1995), 443-551.