Arithmétique (M1)

J.-M. Fontaine

Orsay 2008-2009

Ce document est disponible en version PDF.

0 . −Rappels, conventions et notations

0.1 . −Notations

Pour un ensemble E on notera $\mathbb{P}(E)$ l'ensemble de ses parties.

Pour une application $f : E \to F$ et A une partie de E, on notera $f_{|A}$ la restriction de f à A.

0.2 . −Topologie

0.2.1 . −Espaces topologiques

Définition 0.2.1.1. Topologie Étant donné un ensemble E, une *topologie* sur E est une partie $\mathcal{T} \subset \mathbb{P}(E)$ de l'ensemble des parties de E satisfaisant aux axiomes :

TOP$_1$

$$E \in \mathcal{T} \text{ et } \emptyset \in \mathcal{T} .$$

TOP$_2$ Pour toute partie <u>finie</u> $\mathcal{U} \subset \mathcal{T}$, de $\mathcal{T}$,

$$\bigcap_{U \in \mathcal{U}} U \in \mathcal{T} .$$

TOP$_3$ Pour toute partie (quelconque) $\mathcal{U} \subset \mathcal{T}$ de $\mathcal{T}$,

$$\bigcup_{U \in \mathcal{U}} U \in \mathcal{T} .$$

On dit alors que $(E, \mathcal{T})$ est un *espace topologique*.

On appelle *ouvert* un élément de $\mathcal{T}$ et *fermé* un élément de $\mathbb{P}(E)$ dont le complémentaire appartient à $\mathcal{T}$.

Définition 0.2.1.2. Morphisme (application continue) Pour deux espaces topologiques $(E, \mathcal{T})$ et $(E', \mathcal{T}',)$ un *morphisme d'espaces topologiques* ou une *application continue*

$$f \ : \ (E, \mathcal{T}) \ \rightarrow \ (E', \mathcal{T}')$$

est une application $f \ : \ E \ \rightarrow \ E'$ telle que pour tout $U \ \in \ \mathcal{T}'$, $f^{-1}(U) \ \in \ \mathcal{T}$ c'est-à-dire une application telle que l'image réciproque de tout ouvert est un ouvert.

Définition 0.2.1.3. Topologie discrète Étant donné un ensemble E l'ensemble $\mathbb{P}(E)$ des parties de E est clairement une topologie sur E qu'on appelle la *topologie discrète* sur E. On peut montrer qu'on caractérise cette topologie par le fait que tous les singletons sont ouverts.

Définition 0.2.1.4. Séparation Un espace topologique $(E, \mathcal{T})$ est *séparé* si pour tout couple (x, y) d'éléments de E, $x \neq y$, il existe des ouverts U et V tels que

$$x \in U \ , \ y \in V \text{ et } U \cap V \ = \ \emptyset \ .$$

0.2.2 . –Espaces métriques

Définition 0.2.2.1. Distance Étant donné un ensemble E, une *distance* sur E est une application $\delta \ : \ E \times E \ \rightarrow \ \mathbb{R}^+$ (ou même à valeurs dans $\mathbb{Q}^+$ voire dans un groupe totalement ordonné) vérifiant les axiomes :

DIST$_1$

$$\delta(x, y) \ = \ \delta(y, x) \, \forall (x, y) \in E \times E \ ;$$

DIST$_2$

$$\delta(x, y) \ = \ 0 \ \Leftrightarrow \ x \ = \ y \ ;$$

DIST$_3$

$$\delta(x, z) \ \leq \ \delta(x, y) \ + \ \delta(y, z) \, \forall (x, y, z) \in E \times E \times E \ .$$

Si δ est un distance sur E, on dit que le couple (E, δ) est un *espace métrique*.

Définition 0.2.2.2. Boule ouverte/fermée Étant donné un espace métrique (E, δ), pour tout $x \ \in \ E$ et tout $\epsilon \ > \ 0$, on appelle *boule ouverte de centre x et de rayon ϵ* (resp. *boule fermée de centre x et de rayon ϵ* l'ensemble

$$B(x, \epsilon) \ := \ \{y \in E \mid \delta(x, y) < \epsilon\} \subset E \ ,$$

$$\text{(resp. } B^f(x, \epsilon) \ := \ \{y \in E \mid \delta(x, y) \leq \epsilon\} \subset E \ .\text{)}$$

Remarque 0.2.2.3. La notation $\overline{B}$ est usuelle pour les boules fermées mais peut prêter à confusion pour certaines topologie (discrète par exemple) pour lesquels une boule fermée n'est pas l'adhérence de la boule ouverte de même rayon.

Proposition 0.2.2.4. *Étant donné un espace métrique (E, δ), on note $\mathcal{T}_\delta \subset \mathbb{P}(E)$ l'ensemble des parties U de E telles que, pour tout $x \in U$, il existe $\epsilon > 0$ tel que la boule ouverte de centre x et de rayon ϵ $B(x, \epsilon)$ soit incluse dans U. Alors, $\mathcal{T}_\epsilon$ est une topologie sur E (cf. 0.2.1.1) et l'espace topologique $(E, \mathcal{T}_\delta)$ est un espace topologique séparé (cf. 0.2.1.4.)*

Définition 0.2.2.5. Suite de Cauchy Étant donné un espace métrique (E, δ), une *suite de Cauchy* à valeurs dans (E, δ) est une suite $(u_n)_{n\in\mathbb{N}}$ telle que, pour tout $\epsilon > 0$, il existe $n \in \mathbb{N}$ tel que pour tout $r \geq s \geq n$,

$$\delta(u_r, u_s) \ \leq \ \epsilon \ .$$

Une suite convergeante est de Cauchy en vertu de l'inégalité triangulaire (cf. 0.2.2.1(DIST$_3$).)

Définition 0.2.2.6. Espace métrique complet Un espace métrique (E, δ) est *complet* si toute suite de Cauchy à valeurs dans (E, δ) est convergeante.

Théorème 0.2.2.7. *Soit (E, δ) un espace métrique. On définit sur l'ensemble des suites de Cauchy de E la relation*

$$(x_n)_{n\in\mathbb{N}} \ \sim \ (y_n)_{n\in\mathbb{N}}$$

si, pour tout $\epsilon > 0$, il existe n_ϵ tel que pour tout $n \geq n_\epsilon$,

$$\delta(x_n, y_n) \ \leq \ \epsilon \ .$$

Alors :
i) Le quotient $\hat{E}$ de l'ensemble des suites de Cauchy de E par la relation $\sim$ a une structure naturelle d'espace métrique.
ii) L'application naturelle $E \ \to \ \hat{E}$ qui a un élément $x \in E$ associe la suite constante de terme général x est injective et continue. Son image est dense. Plus précisément si $\hat{\delta}$ désigne la distance naturelle sur $\hat{E}$, pour tout $(x, y) \in E \times E$,

$$\hat{\delta}(x, y) \ = \ \delta(x, y) \ .$$

iii) L'espace métrique $(\hat{E}, \hat{\delta})$ est complet.

Définition 0.2.2.8. Pour un espace métrique (E, δ), l'espace métrique $(\hat{E}, \hat{\delta})$ construit dans le théorème ci-dessus s'appelle le *séparé complété* de (E, δ).

0.3 . −Un bref aperçu du langage des catégories

0.3.1 . −Catégories

Définition 0.3.1.1. Catégorie Sans entrer dans les détails nous parlerons librement de catégories : Une *catégorie* $\mathbf{C}$ consiste en la donnée d'une *collection* d'*objets* $\mathrm{Ob}(\mathbf{C})$ et d'un ensemble de *flèches* ou *morphismes* (les deux termes risquent d'apparaître indifféremment) $\mathrm{Fl}(\mathbf{C})$ soumis aux axiomes suivants :

CAT_1 À tout couple (X, Y) d'objets de $\mathbf{C}$, on associe un ensemble de flèches

$$\mathrm{Hom}_{\mathbf{C}}(X, Y) \subset \mathrm{Fl}(\mathbf{C})$$

de sorte que $\mathrm{Fl}(\mathbf{C})$ apparaisse comme l'union disjointe des $\mathrm{Hom}_{\mathbf{C}}(X, Y)$ pour (x, Y) parcourant les couples d'objets de $\mathbf{C}$. En particulier, pour tout $f \in \mathrm{Fl}(\mathbf{C})$, il existe un unique couple (X, Y) d'objets de $\mathbf{C}$ tel que $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$. L'objet X est alors appelé la *source* de f et Y son *but*.

CAT_2 Sur l'ensemble $\mathrm{Fl}(\mathbf{C})$ on a une loi de composition partiellement définie, plus précisément, pour trois objets quelconques X, Y, Z de $\mathbf{C}$ on a une *loi de composition*

$$\begin{array}{rccc} \circ : & \mathrm{Hom}_{\mathbf{C}}(X, Y) \times \mathrm{Hom}_{\mathbf{C}}(Y, Z) & \to & \mathrm{Hom}_{\mathbf{C}}(X, Z) \\ & (f, g) & \mapsto & g \circ f \end{array}$$

telle que, pour quatre objets X, Y, Z, T de $\mathbf{C}$, et trois flèches

$$f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)\ ,\ g \in \mathrm{Hom}_{\mathbf{C}}(Y, Z) \text{ et } h \in \mathrm{Hom}_{\mathbf{C}}(Z, T)\ ,$$

on ait

$$h \circ (g \circ f) = (h \circ g) \circ f \in \mathrm{Hom}_{\mathbf{C}}(X, T)\ .$$

CAT_3 Pour tout objet $X \in \mathrm{Ob}(\mathbf{C})$ de $\mathbf{C}$ il existe un élément $\mathrm{Id}_X \in \mathrm{Hom}_{\mathbf{C}}(X, X)$ appelé *identité de* X et tel que pour tout

$$f \in \mathrm{Hom}_{\mathbf{C}}(X, Y) \text{ (resp. } \in \mathrm{Hom}_{\mathbf{C}}(Y, X)\ ,)$$

on ait

$$f \circ \mathrm{Id}_X = f \text{ (resp. } \mathrm{Id}_X \circ f = f\ .)$$

Définition 0.3.1.2. Isomorphisme Dans une catégorie $\mathbf{C}$, on dira qu'une flèche

$$f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$$

est un *isomorphisme* s'il existe $g \in \mathrm{Hom}_{\mathbf{C}}(Y, X)$ tel que

$$g \circ f = \mathrm{Id}_X \text{ et } f \circ g = \mathrm{Id}_Y\ .$$

Exemple 0.3.1.3.
a) Ainsi on pourra parler de la catégorie $\mathbf{Ens}$ des ensembles dont les objets sont les ensembles et les flèches les applications ; de la catégorie $\mathbf{Gr}$ des groupes dont les objets sont les groupes et les flèches les morphismes de groupes ; de la catégorie $\mathbf{Ab}$ dont les objets sont les groupes abéliens et les flèches les morphismes de groupes ; de la catégorie $\mathbf{Ann}$ des anneaux (commutatifs) dont les objets sont les anneaux et les flèches les morphismes d'anneaux ; de la catégorie $A - \mathbf{mod}$ des A-modules (pour A un anneau fixé,) dont les objets sont les A-modules et les flèches les morphismes de A-modules ; de la catégorie $\mathbf{Top}$ des espaces topologiques dont les objets sont les espaces topologiques et les flèches les applications continues (cf. 0.2.1.)

Dans les cas ci-dessus, les isomorphismes sont les bijections ensemblistes, (resp. les isomorphismes de groupes,) (resp. les isomorphismes de groupes,) (resp. les isomorphismes d'anneaux,) (resp. les isomorphismes de A-modules,) (resp. les homéomorphismes.)

b) On peut aussi donner des exemples de catégories qui paraissent moins naturels au premier abord : Si E est un ensemble, on peut considérer la catégorie $\mathbf{E}$ dont les objets sont les éléments de E et telle que pour tout $(x, y) \in E \times E$, $\mathrm{Hom}_{\mathbf{E}}(x, y)$ est vide pour $x \neq y$ et réduit à un élément (forcément l'identité Id_x) pour $x = y$.

c) Si $(I, \leq)$ est un ensemble ordonné, on peut lui associer une catégorie $\mathbf{I}$ dont les objets sont les éléments de I et telle que pour tout $(i, j) \in I \times I$ $\mathrm{Hom}_{\mathbf{I}}(j, i)$ est un singleton si $i \leq j$ et vide sinon.

0.3.2 . –Foncteurs

Définition 0.3.2.1. Foncteur Étant données deux catégories $\mathbf{C}$ et $\mathbf{D}$ on appellera *foncteur covariant* $F : \mathbf{C} \to \mathbf{D}$ un « procédé » qui à tout objet $X \in \mathrm{Ob}(\mathbf{C})$, associe un objet $F(X) \in \mathrm{Ob}(\mathbf{D})$ et, à toute flèche $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$ associe une flèche $F(f) \in \mathrm{Hom}_{\mathbf{D}}(F(X), F(Y))$ et tel que

$$\forall f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)\, \forall g \in \mathrm{Hom}_{\mathbf{C}}(Y, Z)\ ,$$

$$F(g \circ f) \ = \ F(g) \ \circ \ F(f) \ \in \ \mathrm{Hom}_{\mathbf{D}}(F(X), F(Z))$$

et

$$F(\mathrm{Id}_X) \ = \ \mathrm{Id}_{F(X)}\, \forall X \in \mathrm{Ob}(\mathbf{C})\ .$$

On a la notion duale de *foncteur contravariant* si pour tout $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y) n\ F(f) \in \mathrm{Hom}_{\mathbf{D}}(F(Y), F(X))$ et si $F(g \circ f) \ = \ F(f) \circ F(g)$.

Lemme 0.3.2.2. *Remarquons que la « compatibilité » d'un foncteur (aussi bien covariant que contravariant) F aux lois de composition $\circ$ sur $\mathrm{Fl}(\mathbf{C})$ et $\mathrm{Fl}(\mathbf{D})$ exprimée dans les deux identités ci-dessus implique en particulier que F transforme isomorphismes en isomorphismes.*

Exemple 0.3.2.3. [1].

[1] Quelques exemples rapides seraient sans doute les bienvenus ici.

0.3.3 . −Objets universels

Définition 0.3.3.1. Objet initial/final Un objet $U \in \mathrm{Ob}(\mathbf{C})$ d'une catégorie $\mathbf{C}$ est dit *final* (resp. *initial*) si pour tout objet $X \in \mathrm{Ob}(\mathbf{C}), \mathrm{Hom}_{\mathbf{C}}(X,U)$ (resp. $\mathrm{Hom}_{\mathbf{C}}(U,X)$) est un singleton autrement dit, il existe un unique morphisme de X dans U (resp. de U dans X.)

Un objet qui est initial ou final sera dit *universel*.

Lemme 0.3.3.2. *Dans une catégorie $\mathbf{C}$, un objet initial (resp. final) est unique à unique isomorphisme près c'est-à-dire que si U et U' sont deux objets initiaux (resp. finaux) il existe un unique isomorphisme (cf. 0.3.1.2,) de U dans U'.*

Preuve : On donne l'argument pour des objet initiaux, il est exactement identique pour des objets finaux.

Si U et U' sont deux objets initiaux dans une catégorie $\mathbf{C}$, il existe un unique morphisme $u : U \to U'$ (resp. $u' : U' \to U$.) Alors $u' \circ u$ est un morphisme de U dans lui-même qui ne peut être que Id_U puisque du fait que U est final, $\mathrm{Hom}_{\mathbf{C}}(U,U)$ est un singleton nécessairement égal à $\{\mathrm{Id}_U\}$ à cause de l'axiome 0.3.1.1(CAT$_3$).

De même, $u \circ u' = \mathrm{Id}_{U'}$ c'est-à-dire que u et u' sont des isomorphismes. *q.e.d*

I . −Rappels et compléments d'algèbre commutative

I.1 . −Anneaux, modules, idéaux

I.1.1 . −Anneaux A-modules

Définition I.1.1.1. Anneau Dans ce cours *anneau* signifiera *anneau commutatif unitaire*. Cependant on ne supposera pas nécessairement que $0 \neq 1$. Ainsi l'*anneau nul* est l'anneau dont l'ensemble sous-jacent est un singleton.

Définition I.1.1.2. Morphisme d'anneaux Un morphisme d'anneaux

$$f : (A,+,*) \to (B,+,*)$$

est un morphisme des groupes abéliens sous-jacents $(A,+) \to (B,+)$ tel que

$$f(x*y) = f(x)*f(y)\ \forall (x,y) \in A \times A \text{ et } f(1) = 1 .$$

Remarque I.1.1.3. Avec la définition de morphismes ci-dessus, si $\mathbf{Ann}$ désigne la catégorie (cf. 0.3.1.1) dont les objets sont les anneaux et les flèches (morphismes) les morphismes d'anneaux, l'anneau nul est final dans $\mathbf{Ann}$ mais pas initial (cf. 0.3.3.1.)

Définition I.1.1.4. Élément inversible Pour tout anneau A, on note $A^\times$ l'ensemble des *éléments inversibles* de A pour $*$ c'est-à-dire

$$A^\times = \{x \in A \mid \exists y \in A \mid x*y = 1\} .$$

Remarque I.1.1.5. On sait que, pour tout morphisme d'anneaux $f : A \to B$ et tout $x \in A^\times$, $f(x) \in B^\times$ c'est-à-dire que la restriction $f^\times$ de f à $A^\times$ est à valeurs dans $B^\times$.

Il est tout aussi clair que si A est un anneau (resp. un anneau commutatif,) $A^\times$ est un groupe (resp. un groupe abélien) et que pour tout morphisme d'anneaux

$$f : A \to B,$$

$$f^\times : A^\times \to B^\times$$

est un morphisme de groupe.

Il en résulte, moyennant de vérifier ce qui est immédiat, que pour tout anneau A ${\mathrm{Id}_A}^\times = \mathrm{Id}_{A^\times}$ et pour tous morphismes d'anneaux

$$A \xrightarrow{f} B \longrightarrow \xrightarrow{g} C\,,$$

$$(g \circ f)^\times = g^\times \circ f^\times\,,$$

que

$$\begin{array}{rcl} \mathbf{Ann} & \to & \mathbf{Gr} \\ A & \mapsto & A^\times \\ f & \mapsto & f^\times\,, \end{array}$$

est un foncteur covariant (cf. 0.3.2.1) de la catégorie des anneaux (commutatifs) dans la catégorie des groupes (abéliens.)

Définition I.1.1.6. Anneau intègre Un anneau *intègre* est un anneau non nul n'ayant pas de diviseurs de 0 autres que 0.

Définition I.1.1.7. Corps Un *corps* est un anneau A tel que $A^\times = A \setminus \{0\}$. C'est en particulier un anneau intègre.

Dans toute la fin du paragraphe, un anneau A est fixé.

Définition I.1.1.8. A-module Un *A-module* M, est un groupe abélien muni d'une loi de composition externe $\cdot : A \times M \to M$ vérifiant des axiomes bien connus.

De manière équivalente, un A-module M est un groupe abélien $(M, +)$ muni d'un morphisme d'anneaux $(A, +, *) \to \big(\mathrm{Hom}_{\mathbf{Gr}}(M, M), +, \circ\big)$.

Un *morphisme de A-module* $f : M \to N$ est une application de M dans N telle que

$$f(ax + by) = af(x) + bf(y)\ \forall (x, y) \in M \times M\ \forall (a, b) \in A \times A\,.$$

On notera $A - \mathbf{mod}$ la *catégorie des A-modules* dont les objets sont les A-modules et les flèches (morphismes) sont les morphismes de A-modules (cf. 0.3.1.1.)

On allégera souvent la notation en posant pour deux A-modules$P$ et Q,

$$\mathrm{Hom}_A(P, Q) := \mathrm{Hom}_{A-\mathbf{mod}}(P, Q)$$

l'ensemble des flèches de P dans Q dans $A-\mathbf{mod}$ c'est-à-dire l'ensemble des morphismes de A-modules de P dans Q.

On parlera souvent de *A-morphisme* au lieu de morphisme de A-modules.

Remarque I.1.1.9. Dans la catégorie $A-\mathbf{mod}$ des A-modules, le *module nul* dont l'ensemble sous(-jacent est un singleton est simultanément initial et final : on dira parfois que c'est un *objet zéro* et on le notera 0.

Remarque I.1.1.10. La catégorie $\mathbf{Ab}$ des groupes abéliens s'identifie canoniquement à la catégorie des $\mathbb{Z}$-modules.

Définition I.1.1.11. A-algèbre Si $f\ :\ A\ \to\ B$ est un morphisme d'anneaux, on dira que B (ou le couple (B,f) ou même f) est une *A-algèbre*. Le morphisme f sera appelé *morphisme structural*.

Un *morphisme de A-algèbres*

$$u\ :\ (B,f)\ \to\ (C,g)$$

est un morphisme d'anneaux $u\ :\ B\ \to\ C$ tel que $u\circ f\ =\ g$.

On peut ainsi définir la *catégorie des A-algèbres* $A-\mathbf{alg}$ dont les objets sont les A-algèbres et les flèches (morphismes) sont les morphismes de A-algèbres.

Proposition I.1.1.12.
i) Toute a-algèbre $f\ :\ A\ \to\ B$ possède une structure naturelle de A-module donnée par

$$a\cdot x\ :=\ f(a)*x\ \forall x\in B\ \forall a\in A\ .$$

ii) Tout morphisme de A-algèbres $u\ :\ (B,f)\ \to\ (C,g)$ donne un morphisme de A-modules pour les structures définies au point précédent si bien que l'opération qui consiste à « oublier » la structure de A-algèbre pour ne regarder que la structure de A-module définit un foncteur covariant (cf. 0.3.2.1) de la catégorie $A-\mathbf{alg}$ dans la catégorie $A-\mathbf{mod}$.

iii) La catégorie des anneaux s'identifie canoniquement à la catégorie des $\mathbb{Z}$-algèbres.

Corollaire I.1.1.13. *En particulier $\mathrm{Id}_A\ :\ A\ \to\ A$ est une A-algèbre et l'on peut donc voir A comme un A-module par la formule*

$$a\cdot x\ :=\ a*x\ \forall(a,x)\in A\times A\ .$$

Définition I.1.1.14. Noyau, image, conoyau Soit $f\ :\ P\ \to\ Q$ un morphisme de A-modules. On appelle *noyau* (resp. *image*) (resp. *conoyau*) l'ensemble

$$\mathrm{Ker}\, f\ :=\ \{x\in P\mid f(x)\ =\ 0\}$$

(resp.

$$\mathrm{Im}\, f\ :=\ \{f(x)\ ,\ x\in P\}\ \subset\ Q\ )$$

(resp.

$$\mathrm{Coker}\, f \ := \ Q/\mathrm{Im}\, f$$

(le dernier quotient étant pris au sens des groupes abéliens.)

Proposition I.1.1.15. *Pour tout morphisme de A-modules :*
i) Le noyau $\mathrm{Ker}\, f$ de f est un sous-A-modules de P c'est-à-dire un sous-ensemble de P qui est un A-module pour la structure induite par celle de P ou encore tel que l'inclusion naturelle $i : \mathrm{Ker}\, f \to P$ est un morphisme (nécessairement injectif) de A-modules.

Le couple $(\mathrm{Ker}\, f, i)$ a la propriété que, pour tout couple (M, g) où M est un A-module et $g : M \to P$ est un morphisme de A-modules, tel que $f \circ g = 0$, il existe un unique morphisme de A-modules $g' : M \to \mathrm{Ker}\, f$ tel que $g = g' \circ i$.

ii) Le conoyau $\mathrm{Coker}\, f$ possède une unique structure de A-module telle que la projection ensembliste $p : Q \to \mathrm{Coker}\, f$ soit un morphisme de A-modules.

iii) Le morphisme f est injectif (resp. surjectif) si et seulement si son noyau (resp. son conoyau) est nul.

Remarque I.1.1.16. On pourrait tout à fait regarder la catégorie **K** dont les objets sont les couples (M, g) comme ci-dessus et les flèches (morphismes) $\phi : (M_1, g_1) \to (M_2, g_2)$ sont les morphismes de A-modules ϕ tels que $g_1 = g_2 \circ \phi$. La propriété universelle du noyau énoncée ci-dessus s'exprime alors en disant que le couple $(\mathrm{Ker}\, f, i)$ est final (cf. 0.3.3.1) dans **K**.

On remarque que dualement de ce qu'on a dit pour le noyau le couple $(\mathrm{Coker}\, f, p)$ peut être vu comme un élément initiale bien choisie.

Définition I.1.1.17. Suite exacte Pour $f : P \to Q$ et $g : Q \to R$, des morphismes de A-modules la notation

$$0 \ \to \ P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \ \to \ 0$$

(on dit qu'on a une *suite exacte courte*) signifie que :
- f est injectif,
- $\mathrm{Im}\, f \ = \ \mathrm{Ker}\, g$,
- g est surjectif.

On note seulement

$$P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \ \to \ 0$$

(resp.

$$0 \ \to \ P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \,)$$

(resp.

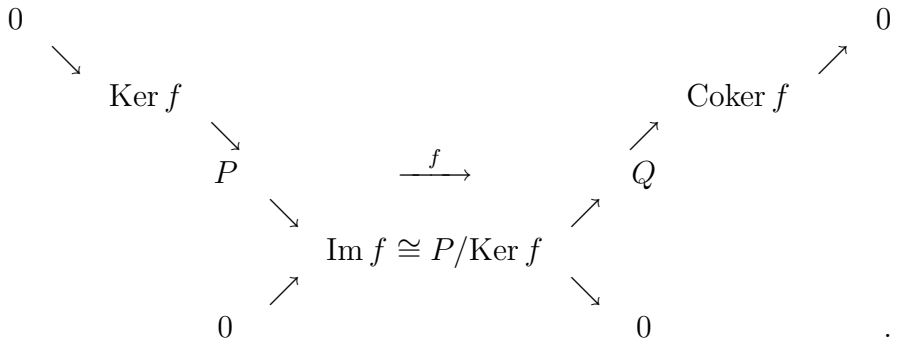
$$P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \,)$$

si l'on ne suppose pas que f est injectif (resp. si l'on ne suppose pas que g est surjectif) (resp. si l'on suppose simplement que $\mathrm{Im}\, f \ = \ \mathrm{Ker}\, g$.)

Proposition I.1.1.18. Factorisation des morphismes *Pour tout morphisme de A-modules*

$$f \ : \ P \ \to \ Q,$$

on a le diagramme commutatif suivant :



De plus, dès qu'on peut écrire un diagramme commutatif comme celui ci-dessus où des A-modules K, I, C occupent les places respectives de $\mathrm{Ker}\, f, \mathrm{Im}\, f$ *et* $\mathrm{Coker}\, f$*, il existe des isomorphismes uniques $K \cong \mathrm{Ker}\, f$, $I \cong \mathrm{Im}\, f$ et $C \cong \mathrm{Coker}\, f$. Autrement dit, le diagramme commutatif ci-dessus caractérise le noyau, le conoyau et l'image de f.*

Proposition I.1.1.19. *La suite*

$$0 \to P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R$$

(resp.

$$P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \to 0\ )$$

(resp.

$$0 \to P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \to 0\ )$$

est exacte si et seulement si $(P, f) = \mathrm{Ker}\, g$*, (resp.* $(Q, g) = \mathrm{Coker}\, f$*) (resp.*

$$(P, f) = \mathrm{Ker}\, g \text{ et } (Q, g) = \mathrm{Coker}\, f\ .)$$

I.1.2 . −Idéaux

Dans ce paragraphe, A est un anneau fixé.

Définition I.1.2.1. Idéal Un *idéal* $\mathfrak{I} \subset A$ de A est un sous-A-module de A (vu comme A-module sur lui-même par

$$a \cdot x := a * x \, \forall (a, x) \in A \times A$$

(cf. I.1.1.13.))

Il revient au même de demander que, pour tout $(x, y) \in \mathfrak{I} \times \mathfrak{I}$, et tout $a \in A$, $x + y \in \mathfrak{I}$, et $a * x \in \mathfrak{I}$.

Définition I.1.2.2. Idéal annulateur Étant donné un A-module M, l'ensemble

$$\mathrm{Ann}_A(M) := \{a \in A \mid ax = 0 \, \forall x \in M\}$$

est un idéal de A appelé *idéal annulateur* de M.

Pour tout $x \in M$, on notera

$$\mathrm{Ann}_A(x) \ := \ \mathrm{Ann}_A(Ax)$$

qu'on appellera l'idéal annulateur de x.

On a alors

$$\mathrm{Ann}_A(M) \ = \ \bigcap_{x \in M} \mathrm{Ann}_A(x) \ .$$

Un élément $x \in M$ est un *élément de torsion* si son idéal annulateur $\mathrm{Ann}_A(x)$ est différent de $\{0\}$.

Un A-module M est un *A-module de torsion* si tous ses éléments sont de torsion ; c'est un *A-module sans torsion* si pour tout $x \in M$,

$$\mathrm{Ann}_A(x) \ = \ \{0\} \ .$$

Proposition I.1.2.3. *Soit $f \ : \ A \ \to \ B$ un morphisme d'anneaux.*
i) Le noyau $\mathrm{Ker}\, f$ de f (vu comme morphisme de A-modules (cf. I.1.1.12)) est un idéal de A et son image $\mathrm{Im}\, f$ un sous-anneau de B.

ii) Il existe une unique structure d'anneaux sur le quotient (en tant que A-modules) $A/\mathrm{Ker}\, f$ tel que la projection naturel $A \ \to \ A/\mathrm{Ker}\, f$ soit un morphisme d'anneaux.

Proposition I.1.2.4. *Soit $f \ : \ A \ \to \ B$ une A-algèbre. Pour tout idéal $\mathfrak{J} \ \subset \ B$, $f^{-1}(\mathfrak{J})$ s'identifie naturellement au noyau du morphisme composée*

$$B \ \to \ B/\mathfrak{J} \ \circ \ f$$

et est donc un idéal. Le morphisme f induit donc une application naturelle de l'ensemble des idéaux de B dans celui des idéaux de A.

Proposition I.1.2.5. *Soit $\mathfrak{I}$ un idéal de A, $B \ := \ A/\mathfrak{I}$ et $f \ : \ A \ \to \ B$ le morphisme naturel. Alors le morphisme défini dans la proposition I.1.2.4 induit une bijection croissante (pour l'inclusion) de l'ensemble des idéaux de B dans l'ensemble des idéaux de A contenant $\mathfrak{I}$.*

Corollaire I.1.2.6. *Avec les notations ci-dessus, si A est noethérien, B l'est aussi.*

Définition I.1.2.7. Idéaux premiers, maximaux Un idéal $\mathfrak{p} \subset A$ est premier (resp. maximal,) si $A/\mathfrak{p}$ est intègre (resp. un corps.)

On notera $\mathrm{Spec}(A)$ (resp. $\mathrm{Spm}(A)$) l'ensemble des idéaux premiers de A (resp. l'ensemble des idéaux maximaux de A) qu'on appellera le *spectre* de A (resp. le *spectre maximal* de A.)

Proposition I.1.2.8. *Un anneau A est intègre si et seulement si $\{0\}$ est un idéal premier*

Remarque I.1.2.9. Le spectre d'un anneau
i) Pour tout morphisme d'anneaux $f \ : \ A \ \to \ B$, et tout idéal premier $\mathfrak{q} \ \subset \ B$, $\mathfrak{p} \ := \ f^{-1}(\mathfrak{q})$ est encore un idéal premier de A. Pour s'en convaincre, il suffit de remarquer que f induit un

morphisme injectif

$$\begin{array}{ccc} A/\mathfrak{p} & \to & B/\mathfrak{q} \\ \uparrow & & \uparrow \\ A & \xrightarrow{f} & B \end{array}$$

et donc, que si $B/\mathfrak{q}$ est intègre, $A/\mathfrak{p}$ l'est aussi.

Le morphisme f définit donc une application $\mathrm{Spec}(f) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ ce qui permet de montrer que $\mathrm{Spec}(\cdot)$ est un foncteur contravariant de la catégorie des anneaux commutatifs dans la catégorie des ensembles (cf. 0.3.2.1.)

On remarque qu'en revanche, si $\mathfrak{m} \subset B$ est un idéal maximal, $f^{-1}(\mathfrak{m})$ n'est pas nécessairement un idéal maximal. En particulier, si $f : \mathbb{Z} \to \mathbb{Q}$ est l'injection canonique $f^{-1}(\{0\}) = \{0\}$ qui est maximal dans $\mathbb{Q}$ qui est un corps mais ne l'est pas dans $\mathbb{Z}$. Il en résulte que $\mathrm{Spm}(\cdot)$ n'a pas d'aussi bonnes propriétés fonctorielles que $\mathrm{Spec}(\cdot)$.

ii) Pour tout idéal $\mathfrak{I} \subset A$, on note

$$V(\mathfrak{I}) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{I} \subset \mathfrak{p}\} .$$

On a alors les propriétés pour tout couple $(\mathfrak{I}, \mathfrak{J})$ d'idéaux de A,

$$V(\mathfrak{I}) \cup V(\mathfrak{J}) = V(\mathfrak{I}J) \text{ et } V(\mathfrak{I}) \cap V(\mathfrak{J}) = V(\mathfrak{I} + J) .$$

Ceci permet d'établir que si l'on note $\mathcal{T} \subset \mathcal{P}(\mathrm{Spec}(\mu A))$ l'ensemble des complémentaires des $V(\mathfrak{I})$ pour $\mathfrak{I}$ parcourant l'ensemble des idéaux de A, $\mathcal{T}$ est une topologie (cf. 0.2.1.1) sur $\mathrm{Spec}(A)$ qu'on appelle la *topologie de Zariski* sur $\mathrm{Spec}(A)$.

On peut alors montrer (et c'est assez élémentaire) que pour tout morphisme d'anneaux

$$f : A \to B,$$

l'application $\mathrm{Spec}(f) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est continue (ou encore est un morphisme d'espaces topologiques) (cf. 0.2.1.2,) pour peu que $\mathrm{Spec}(A)$ et $\mathrm{Spec}(B)$ soient munis de la topologie de Zariski c'est-à-dire que $\mathrm{Spec}(\cdot)$ est en fait un foncteur contravariant de la catégorie des anneaux dans la catégorie des espaces topologiques.

iii) Si A est un anneau intègre, l'adhérence de $\{0\}$ pour la topologie de Zariski est $\mathrm{Spec}(A)$ tout entier.

Les fermés de $\mathrm{Spec}(\mathbb{Z})$ sont les parties finies de $\mathrm{Spec}(\mathbb{Z})$.

Un corps a exactement deux idéaux 0 et lui-même et par voie de conséquence, le spectre d'un corps n'a qu'un élément qui correspond à l'idéal $\{0\}$.

I.1.3 . −Dimension d'un anneau

Définition I.1.3.1. Dans un ensemble ordonné $(I, \leq)$, un *chaîne* est une famille d'éléments

$$i_0 < i_1 < \ldots < i_n .$$

L'entier n est appellé la *longueur de la chaîne*.

Définition I.1.3.2. Soit A un anneau. L'ensemble $\mathrm{Spec}(A)$ des idéaux premiers de A (cf. I.1.2.7) peut être muni de la relation d'ordre donnée par l'inclusion. Une *chaîne d'idéaux premiers* est alors une famille

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n .$$

Si la longueur des chaînes d'idéaux premiers de A est majorée on dit que la *dimension de* A est le plus petit majorant des longueurs des chaînes d'idéaux premiers ; sinon on dit que la dimension de A est infinie.

Exemple I.1.3.3. Un corps (cf. I.1.1.7) est de dimension 0.

I.1.4 . −Quelques classes d'anneaux

Proposition I.1.4.1. *Pour un anneau A les conditions suivantes sont équivalentes :*
a) Étant donné un A-module M de type fini, toute suite croissante (pour l'inclusion) de sous-A-modules de M est stationnaire à partir d'un certain rang.

b) Étant donné un A-module de type fini M, toute famille non vide de sous-A-modules de M possède un élément maximal.

c) Tout sous-A-module d'un A-module de type fini est de type fini.

d) Toute suite croissante (au sens de l'inclusion) d'idéaux de A est stationnaire à partir d'un certain rang.

e) Tout idéal de A est de type fini.

Définition I.1.4.2. On dit qu'un anneau qui vérifie les conditions équivalentes de la proposition ci-dessus est *noethérien*.

Définition I.1.4.3. Un anneau *principal* est un anneau intègre A tel que tout idéal $\mathfrak{I}$ de A est engendré par un seul élément *i.e.*il existe $a \in A$ tel que $\mathfrak{I} = aA$.

Lemme I.1.4.4. *Un anneau principal est noethérien.*

Proposition I.1.4.5. *Dans un anneau principal tout idéal premier non nul (cf. I.1.2.7) est maximal autrement dit, un anneau principal est de dimension 1 (cf. I.1.3.2.)*

Proposition I.1.4.6. *Si A est un anneau principal, tout sous-A-module d'un A module libre de rang n est libre de rang plus petit que n.*

Proposition I.1.4.7. *Si a est un anneau principal, pour tout A-module M de type fini, il existe un A-module libre M_l et un A-module de torsion M_t (cf. I.1.2.2,) tels que*

$$M = M_l \oplus M_t .$$

I.1.5 . –Idéaux fractionnaires

Dans ce paragraphe, A est un anneau noethérien intègre et K est son corps des fractions.

Définition I.1.5.1. Idéal fractionnaire On appelle *idéal fractionnaire* de A tout sous-A-module non nul de type fini de K.

Proposition I.1.5.2. *Un idéal fractionnaire est un idéal si et seulement s'il est contenu dans A.*

Preuve : Un idéal fractionnaire contenu dans A est bien évidemment un idéal de A. Réciproquement, un idéal de A est de type fini puisque A est noethérien donc est un idéal fractionnaire de A contenu dans A. *q.e.d*

Proposition I.1.5.3. *Si $\mathfrak{I}$ est un idéal non nul de A et $s \in A$ non nul,*

$$\mathfrak{I}/s \ := \ \{s^{-1}x \ , \ x \in \mathfrak{I}\}$$

est un idéal fractionnaire.

Réciproquement, si $\mathfrak{J}$ est un idéal fractionnaire, il existe $s \in A$ non nul et $\mathfrak{I}$ un idéal de A tels que

$$\mathfrak{J} \ = \ \mathfrak{I}/s \ .$$

Preuve : Seule la partie réciproque de l'assertion nécessite un argument. Si $\mathfrak{J}$ est un idéal fractionnaire, notons $y_{i\ ,1\leq i\leq r}$ des générateurs de $\mathfrak{J}$. Puisque les y_i sont des élément de K, pour tout $1 \leq i \leq r$, il existe $(x_i, s_i) \in A \times (A \setminus 0)$ tel que $y_i \ = \ \frac{x_i}{s_i}$. Notons alors $s \ := \ \prod_{i=1}^{r} s_i$ et $\mathfrak{I}$ l'idéal de A engendré par les $x_{i\ ,1\leq i\leq r}$. Il est clair qu'alors

$$\mathfrak{J} \ = \ \mathfrak{I}/s \ .$$

q.e.d

Proposition I.1.5.4. *Pour $\mathfrak{I}$ et $\mathfrak{J}$ deux idéaux fractionaires, on note $\mathfrak{I}J$ le sous-A-module de K engendré par les xy $x \in \mathfrak{I}$, $y \in \mathfrak{J}$.*

$\mathfrak{I}J$ est encore un idéal fractionnaire. On définit ainsi une loi de composition sur l'ensemble des idéaux fractionnaires qui est associative, commutative et dont A est l'élément neutre.

Définition I.1.5.5. Pour tout idéal fractionnaire $\mathfrak{I}$, on note

$$\mathfrak{I}^{\perp} \ := \ \{x \in K \mid xy \in A \ \forall y \in \mathfrak{I}\} \ .$$

Proposition I.1.5.6. *Soit $\mathfrak{I}$ un idéal fractionnaire de A.*

i) $\mathfrak{I}^{\perp}$ est un idéal fractionnaire de A.

ii) Le produit (cf. I.1.5.4) $\mathfrak{I}\mathfrak{I}^{\perp}$ est un idéal de A.

iii) Si $\mathfrak{I}$ est un idéal, $\mathfrak{I}^{\perp}$ contient A et par conséquent, $\mathfrak{I}\mathfrak{I}^{\perp}$ contient $\mathfrak{I}$.

Preuve :

i) Pour tout $x \in \mathfrak{I}$ non nul, $x\mathfrak{I}^\perp$ est un idéal de A. Or

$$\mathfrak{I}^\perp \ = \ (x\mathfrak{I}^\perp)/x$$

qui est un idéal fractionnaire en vertu de I.1.5.3.

q.e.d

I.2 . −Produit tensoriel

I.2.1 . −Produit tensoriel de A-modules

Dans ce paragraphe, A est un anneau fixé.

Définition I.2.1.1. Application bilinéaire Étant donnés deux A-modules P et Q, on rappelle qu'une *application bilinéaire* $f \ : \ P \times Q \ \to \ M$ (où M est un A-module,) est une application f, A-linéaire par rapport à chacune des composantes *i.e.*

$$\begin{array}{rcl} f(ax+cz,by+dt) & = & \begin{array}{l} \forall (x,y),(z,t) \in P \times Q \\ \forall a,b,c,d \ \in A \ , \\ abf(x,y)+adf(x,t) \\ +bcf(z,y)+cdf(z,t) \ . \end{array} \end{array} \qquad \text{I.2.1.1.1}$$

On notera $L^2(P,Q,M)$ l'ensemble des applications bilinéaires de $P \times Q$ à valeurs dans M.

Lemme I.2.1.2. *Pour tout morphisme de A-modules $u \ : \ M \ \to \ N$, et toute application bilinéaire*

$$f \ : \ P \times Q \ \to \ M \ \in \ L^2(P,Q,M) \ ,$$
$$u \circ f \ : \ P \times Q \ \to \ N \ \in \ L^2(P,Q,N)$$

est une application bilinéaire de $P \times Q$ à valeurs dans N. Il est presque immédiat de constater alors que, pour P et Q deux A-modules fixés,

$$\begin{array}{rcl} L^2(P,Q,\cdot) : \quad A-\mathbf{mod} & \to & \mathbf{Ens} \\ M \in \mathrm{Ob}(\mathbf{A}-\mathbf{mod}) & \mapsto & L^2(P,Q,M) \\ u \in \mathrm{Hom}_{\mathbf{A}-\mathbf{mod}}(M,N) & \mapsto & u_* \ : \ L^2(P,Q,M) \ \to \ L^2(P,Q,N) \\ & & f \mapsto (u \circ f) \end{array}$$

est un foncteur covariant (cf. 0.3.2.1) de la catégorie des A-modules dans la catégorie des ensembles. On peut munir $L^2(P,Q,M)$ d'une structure de A-module (induite par celle de M) par la formule

$$(af+bg)(x,y) \ := \ af(x,y)+bg(x,y) \ , \ \forall a,b \in A \ , \ \forall f,g \in L^2(P,Q,M) \ , \ \forall (x,y) \in P \times Q \ .$$

On remarque qu'on peut de même munir $\mathrm{Hom}_A(X,Y)$ d'une structure de A-module (induite par celle de Y) par la formule

$$(af+bg)(x) \ = \ af(x)+bg(x)$$

et donc que l'écriture $\mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M))$ *a un sens.*

Il est ensuite facile de voir que l'application qui à tout élément $f \in L^2(P, Q, M)$ *associe l'application de* P *dans* $\mathrm{Hom}_A(Q, M)$ $x \mapsto f(x, \cdot)$, *définit un isomorphisme de* A*-modules*

$$L^2(P, Q, M) \cong \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) . \qquad \textit{I.2.1.2.1}$$

L'isomorphisme ci-dessus est même fonctoriel (on parle alors de transformation naturelle mais nous n'abuserons pas de cette notion dans le cadre de ce cours) au sens où : d'abord, $\mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, \cdot))$ *est un foncteur covariant de la catégorie* $A - \mathbf{mod}$ *des* A*-modules dans elle-même. On laisse le soin au lecteur d'établir que tout morphisme* $u : M \to N$ *induit un morphisme*

$$u_* : \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) \to \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, N)) .$$

Ensuite, pour tout morphisme $u : M \to N$ *le carré*

$$\begin{array}{ccc} L^2(P, Q, M) & \cong & \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) \\ {\scriptstyle u_*}\downarrow & & \downarrow{\scriptstyle u_*} \\ L^2(P, Q, N) & \cong & \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, N)) \end{array}$$

(où les flèches horizontales sont les isomorphismes I.2.1.2.1) est commutatif.

Proposition I.2.1.3. *Pour tous* A*-modules* P *et* Q :
i) Il existe un couple (T, τ) *satisfaisant :*

TENS$_1$ T *est un* A*-module.*

TENS$_2$ $\tau : P \times Q \to T$ *est une application bilinéaire.*

TENS$_3$ *Pour tout couple* (L, λ) *où* L *est un* A*-module et* $\lambda : P \times Q \to L$ *est une application bilinéaire, il existe un unique morphisme de* A*-modules* $\lambda' : T \to L$ *tel que*

$$\lambda = \lambda' \circ \tau .$$

ii) De plus, le couple (T, τ) *dépendant bien entendu des* A*-modules* P *et* Q *est unique à unique isomorphisme près c'est-à-dire que si* (T', τ') *est un autre couple satisfaisant I.2.1.3(TENS*$_1$*) à I.2.1.3(TENS*$_3$*), il existe un unique isomorphisme de* A*-modules* $\phi : T \cong T'$ *tel que*

$$\tau' = \phi \circ \tau .$$

Preuve :
i) **Existence** Notons $A^{(P\times Q)}$ le A-module libre de base $P \times Q$ et pour tout $(x, y) \in P \times Q$, $\epsilon_{x,y}$ l'élément de base correspondant à $(x, y) \in P \times Q$ dans $A^{(P\times Q)}$. Soit R le sous-A-module de $A^{(P\times Q)}$ engendré par les éléments de la forme

$$\forall (x, y), (z, t) \in P \times Q \, \forall a, b, c, d \in A , \epsilon_{ax+cz,by+dt} - \left(ab\epsilon_{x,y} + ad\epsilon_{x,t} + bc\epsilon_{z,y} + cd\epsilon_{z,t}\right) . \qquad \text{I.2.1.4}$$

Notons alors $T := A^{(P\times Q)}/R$ et $\tau : P\times Q \to T$ la composée de la projection naturelle $A^{(P\times Q)} \to T$ et de l'application

$$\begin{aligned} P\times Q &\to A^{(P\times Q)} \\ (x,y) &\mapsto \epsilon_{x,y}\ . \end{aligned}$$

Il suffit alors essentiellement de comparer les formules I.2.1.1.1 et I.2.1.4 pour constater que le couple (T,τ) satisfait I.2.1.3(TENS$_1$) à I.2.1.3(TENS$_3$).

i) **Unicité** Si (T,τ) et (T',τ) sont deux couples satisfaisant I.2.1.3(TENS$_1$) à I.2.1.3(TENS$_3$), en particulier, il existe un unique morphisme $\phi : T \to T'$ tel que $\phi\circ\tau = \tau'$ en appliquant I.2.1.3(TENS$_3$) pour (T,τ) à (T',τ') . En faisant l'inverse, on obtient l'existence d'un morphisme $\phi' : T' \to T$ tel que $\phi'\circ\tau' = \tau$.

Il s'ensuit que

$$\phi'\circ\phi\circ\tau = \phi'\circ\tau' = \tau\ .$$

En appliquant donc toujours I.2.1.3(TENS$_3$) à (T,τ) pour lui-même il résulte par unicité que Id_T est le seul morphisme ψ de T dans lui-même qui puisse vérifier $\psi\circ\tau = \tau$. Il en résulte que

$$\phi'\circ\phi = \mathrm{Id}_T\ .$$

L'argument étant exactement symétrique en T et T', on obtient aussi

$$\phi\circ\phi' = \mathrm{Id}_{T'}$$

ce qui prouve l'unicité à unique isomorphisme près.

q.e.d

Remarque I.2.1.5. Une lecture attentive des arguments ci-dessus comparés à ceux de la preuve du lemme 0.3.3.2, montrerait qu'ils ont l'air très semblables.

En effet, définissons une catégorie **T** dépendant des A-modules P et Q de la manière suivante : Les objets de **T** sont les couples (L,λ) où L est un A-module et $\lambda : P\times Q \to L$ une application bilinéaire. Les flèches de **T** $\phi : (L,\lambda) \to (L',\lambda')$ sont les morphismes de A-modules $\phi : L \to L'$ tels que $\phi\circ\lambda = \lambda'$.

Dès lors le produit tensoriel (T,τ) apparaît par définition comme un objet initial (cf. 0.3.3.1) dans la catégorie **T** et si son existence doit être prouvée indépendamment, son unicité (à unique isomorphisme près) est une conséquence du lemme 0.3.3.2.

Définition I.2.1.6. Produit tensoriel Pour deux A-modules P et Q, le couple (T,τ) défini (à unique isomorphisme près) par la proposition I.2.1.3, est appelé le *produit tensoriel* des A-modules P et Q.

Le module T est noté $P\otimes_A Q$ et l'application τ, $(x,y)\mapsto x\otimes y$.

Les éléments

$$x\otimes y \in P\otimes_A Q\ ,\ \forall (x,y)\in P\times Q$$

sont appelés *tenseurs décomposés*.

Remarque I.2.1.7.
i) Il découle de la description du produit tensoriel par générateurs et relations donnée dans la preuve de la proposition I.2.1.3, que les éléments

$$x \otimes y \ \in \ P \otimes_A Q \, \forall (x, y) \ \in \ P \times Q \ ,$$

sont des générateurs de $P \otimes_A Q$; puisque ce sont les images par un morphisme surjectif des générateurs $\epsilon_{x,y}$ de $A^{(P \times Q)}$.

Ainsi, si l'on dispose de deux morphismes

$$f \ , \ g \ : \ P \otimes_A Q \ \rightarrow \ M$$

où M est un A-modules,

$$f(x \otimes y) \ = \ g(x \otimes y) \, \forall (x, y) \in P \times Q, \qquad \text{I.2.1.7.1}$$

suffit à assurer que $f \ = \ g$.

ii) Si donc il paraît approprié de caractériser un morphisme par les images des tenseurs décomposés, en revanche il sera souvent mal commode, voire extrêmement délicat de le définir ainsi car il faudrait alors vérifier la compatibilité à l'identité I.2.1.4.

On constatera que, dans la pratique, on peut pratiquement oublier la description du produit tensoriel comme quotient donnée dans la preuve de la proposition I.2.1.3 et que l'on utilisera presque exclusivement la propriété universelle I.2.1.3(TENS$_3$). (Remarquer que l'identité I.2.1.7.1 ne signifie rien d'autre que $f \ \circ \ \tau \ = \ g \ \circ \ \tau$.)

Les preuves des résultats qui suivent sont une illustration de ceci.

Proposition I.2.1.8. Propriétés du produit tensoriel
i) ***Commutativité*** *Pour tous A-modules P et Q, il existe un unique isomorphisme de A-modules*

$$P \otimes_A Q \ \cong \ Q \otimes_A P$$

caractérisé par le fait que

$$x \otimes y \ \mapsto \ y \otimes x \, \forall (x, y) \in P \times Q \ .$$

ii) ***Associativité*** *Pour tous A-modules P, Q, R, il existe un unique isomorphisme*

$$(P \otimes_A Q) \otimes_A R \ \cong \ P \otimes_A (Q \otimes_A R)$$

tel que

$$(x \otimes y) \otimes z \ \mapsto \ x \otimes (y \otimes z) \ .$$

iii) ***Fonctorialité*** *Pour tous A-modules P_1 et Q_1 et tous morphismes de A-modules*

$$f \ : \ P_1 \ \rightarrow \ P_2 \text{ et } g \ : \ Q_1 \ \rightarrow \ Q_2 \ ,$$

il existe un unique morphisme

$$P_1 \otimes_A Q_1 \ \rightarrow \ P_2 \otimes_A Q_2$$

tel que

$$x \otimes y \ \mapsto \ f(x) \otimes g(y) \ .$$

On note $f \otimes_A g$ ce morphisme.

En particulier, si $Q_2 = Q_1$, et $g = \mathrm{Id}_{Q_1}$, le morphisme $f \otimes_A \mathrm{Id}_{Q_1}$ sera parfois noté $f \otimes_A Q_1$. Ainsi pour tout A-module Q,

$$\begin{array}{rrcl} \cdot \otimes_A Q : & A - \mathbf{mod} & \to & A - \mathbf{mod} \\ & P \in \mathrm{Ob}(\mathbf{A} - \mathbf{mod}) & \mapsto & P \otimes_A Q \\ & f \in \mathrm{Fl}(\mathbf{A} - \mathbf{mod}) & \mapsto & f \otimes_A Q \ := \ f \otimes_A \mathrm{Id}_Q \end{array}$$

est un foncteur covariant (cf. 0.3.2.1.)

iv) ***Distributivité par rapport à la somme directe*** *Pour tous A-modules P, Q, R, il existe un unique isomorphisme de A-modules*

$$P \otimes_A (Q \oplus R) \ \cong \ (P \otimes_A Q) \oplus (P \otimes_A R)$$

tel que

$$x \otimes (y + z) \ \mapsto \ (x \otimes y) \ + \ (x \otimes z) \ .$$

Corollaire I.2.1.9. *Pour tous A-modules P et Q, il découle de la proposition I.2.1.3, que*

$$f \ \mapsto \ f \circ \big((x, y) \mapsto x \otimes y\big) \ , \ \forall f \in \mathrm{Hom}_A(P \otimes_A Q, M)$$

M un A-module variable, induit un isomorphisme

$$\mathrm{Hom}_A(P \otimes_A Q, M) \ \cong \ L^2(P, Q, M)$$

qui, grâce à la remarque I.2.1.7, induit finalement un isomorphisme

$$\mathrm{Hom}_A(P \otimes_A Q, M) \ \cong \ \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) \qquad \textit{I.2.1.9.1}$$

lequel est encore fonctoriel en M à savoir que pour tout morphisme $u : M \to N$ les isomorphismes ci-dessus induisent un carré commutatif :

$$\begin{array}{ccc} \mathrm{Hom}_A(P \otimes_A Q, M) & \cong & \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) \\ {\scriptstyle u_*}\downarrow & & \downarrow{\scriptstyle u_*} \\ \mathrm{Hom}_A(P \otimes_A Q, M) & \cong & \mathrm{Hom}_A(P, \mathrm{Hom}_A(Q, M)) \ . \end{array}$$

Preuve de la proposition I.2.1.8 :

i) En vertu de I.2.1.3(TENS$_3$), pour définir un morphisme $P \otimes_A Q \ \to \ Q \otimes_A P$ il est nécessaire et suffisant de définir une application bilinéaire $P \times Q \ \to \ Q \otimes_A P$.

Posons donc

$$\phi(x, y) \ := \ y \otimes x \ \in \ Q \otimes_A P \ \forall (x, y) \in P \times Q \ .$$

Puisque

$$\tau \ : \ Q \times P \ \to \ Q \otimes_A P \ , \ (y,x) \ \mapsto \ y \otimes x$$

est bilinéaire, ϕ l'est aussi. Il existe donc un unique morphisme $\overline{\phi} \ : \ P \otimes_A Q \ \to \ Q \otimes_A P$ tel que $\overline{\phi}(x \otimes y) \ = \ y \circ x$.

Un argument exactement analogue permet de définir un unique morphisme

$$\overline{\psi} \ : \ Q \otimes_A P \ \to \ P \otimes_A Q$$

caractérisé par le fait que $\overline{\psi}(y \otimes x) \ = \ x \otimes y$.

Puisque, pour tout $(x,y) \in P \times Q$,

$$\overline{\psi}[\overline{\phi}(x \otimes y)] \ = \ \overline{\psi}(y \otimes x) \ = \ x \otimes y$$

il découle de la remarque I.2.1.7.i ou de I.2.1.3(TENS$_3$) (ce qui revient au même,) que

$$\overline{\psi} \ \circ \ \overline{\phi} \ = \ \mathrm{Id}_{P \otimes_A Q} \ .$$

Un argument exactement symétrique montre que

$$\overline{\phi} \ \circ \ \overline{\psi} \ = \ \mathrm{Id}_{Q \otimes_A P}$$

ce qui achève la preuve.

ii) L'argument est exactement du même type que ci-dessus et laissé en exercice.

iii) Ici encore, l'unicité de $f \otimes_A g$ est immédiate, dès l'instant où l'on impose $(f \otimes g)(x \otimes y) \ = \ f(x) \otimes g(y)$ et ce, toujours en vertu de I.2.1.3(TENS$_3$).

Reste donc uniquement à constater que l'application $P_1 \times Q_1 \ \to \ P_2 \otimes_A Q_2$ donnée par $(x,y) \ \mapsto \ f(x) \otimes g(y)$ est bien bilinéaire ; ce qui découle immédiatement de la linéarité de f et g, et de la bilinéarité de l'application

$$P_2 \times Q_2 \ \to \ P_2 \otimes_A Q_2 \ , \ (u,v) \mapsto u \otimes v \ .$$

iv) Laissé en exercice.

q.e.d

Proposition I.2.1.10. *Pour toute suite exacte*

$$P \xrightarrow{\ f \ } Q \longrightarrow \xrightarrow{\ g \ } R \ \to \ 0$$

(cf. I.1.1.17,) et tout A-module M, on a une suite exacte :

$$P \otimes_A M \xrightarrow{f \otimes_A M} Q \otimes_A M \longrightarrow \xrightarrow{g \otimes_A M} R \otimes_A M \ \to \ 0 \ .$$

Définition I.2.1.11. On traduit la proposition précédente en disant que le foncteur produit tensoriel (cf. I.2.1.8.iii) est *exact à droite*.

Preuve de la proposition I.2.1.10 : On doit en fait montrer que si $(R, g) = \mathrm{Coker}\, f$ alors pour tout M $\mathrm{Coker}\, f \otimes_A M = (R \otimes_A M, g \otimes_A M)$ (cf. I.1.1.19.)

On peut montrer que cela équivaut à montrer que, pour tout A-module N, la suite

$$0 \to \mathrm{Hom}_A(R \otimes_A M, N) \longrightarrow \mathrm{Hom}_A(Q \otimes_A M, N) \longrightarrow \xrightarrow{\mathrm{Hom}_A(P\otimes_A M,N)}$$

est exacte. Ceci revient finalement à montrer, en vertu du corollaire I.2.1.9, que la suite

$$0 \to \mathrm{Hom}_A(R, \mathrm{Hom}_A(M, N)) \longrightarrow \mathrm{Hom}_A(Q, \mathrm{Hom}_A(M, N)) \longrightarrow \mathrm{Hom}_A(P, \mathrm{Hom}_A(M, N))$$

est exacte, ce qui est laissé en exercice. *q.e.d*

Définition I.2.1.12. A**-module plat** Si M est un A-module tel que, pour toute suite exacte

$$0 \to P \longrightarrow Q \longrightarrow R \to 0\,,$$

la suite

$$0 \to M \otimes_A P \longrightarrow M \otimes_A Q \longrightarrow M \otimes_A R \to 0$$

est exacte, on dit que M est un *A-module plat* ou un module *A-plat*.

Lemme I.2.1.13. *Tout A-module libre est plat. En particulier, si A est un corps, tout A-module (A-espace vectoriel) est plat.*

Remarque I.2.1.14. Si le contexte est clair, on notera souvent $\mathrm{Hom}(P, Q)$ (resp. $P \otimes Q$) au lieu de $\mathrm{Hom}_A(P, Q)$ (resp. $P \otimes Q$.)

De même on notera $P \otimes Q = Q \otimes P$ et

$$P \otimes Q \otimes R := (P \otimes Q) \otimes R = P \otimes (Q \otimes R)$$

considérant que les isomorphismes I.2.1.8.i et I.2.1.8.ii sont suffisamment naturels.

Proposition I.2.1.15. *Soient*

$$P' \xrightarrow{f_1} P \longrightarrow \xrightarrow{g_1} P'' \to 0$$

et

$$Q' \xrightarrow{f_2} Q \longrightarrow \xrightarrow{g_2} Q'' \to 0\,.$$

Il résulte alors de la proposition I.2.1.10 qu'on a un diagramme commutatif

$$\begin{array}{ccccccc}
P' \otimes Q' & \to & P \otimes Q' & \to & P'' \otimes Q' & \to 0 \\
\downarrow & & \downarrow{\scriptstyle P\otimes f_2} & & \downarrow & \\
P' \otimes Q & \xrightarrow{f_1\otimes Q} & P \otimes Q & \xrightarrow{g_1\otimes Q} & P'' \otimes Q & \to 0 \\
\downarrow & & \downarrow{\scriptstyle P\otimes g_2} & & \downarrow{\scriptstyle P''\otimes g_2} & \\
P' \otimes Q'' & \to & P \otimes Q'' & \xrightarrow{g_1\otimes Q''} & P'' \otimes Q'' & \to 0 \\
\downarrow & & \downarrow & & \downarrow & \\
0 & & 0 & & 0 &
\end{array}$$

Notons

$$g \;:=\; (P'' \otimes g_2) \circ (g_1 \otimes Q) \;=\; (g_1 \otimes Q'') \circ (P \otimes g_2) \;:\; P \otimes Q \;\to\; P'' \otimes Q''$$

et

$$f \;:=\; (f_1 \otimes Q) + (P \otimes f_2) \;:\; (P' \otimes Q) \times (P \otimes Q') \;\to\; P \otimes Q\,.$$

Alors la suite

$$(P' \otimes Q) \times (P \otimes Q') \xrightarrow{\;f\;} P \otimes Q \longrightarrow \xrightarrow{\;g\;} P'' \otimes Q'' \;\to\; 0$$

est exacte.

Preuve :
i) On a

$$\begin{aligned} g \circ (P \otimes f_2) &= (g_1 \otimes Q'') \circ (P \otimes g_2) \circ (P \otimes f_2) \\ &= (g_1 \otimes Q'') \circ P \otimes (g_2 \circ f_2) \\ &= 0 \end{aligned}$$

et

$$\begin{aligned} g \circ f_1 \otimes Q &= (P'' \otimes g_2) \circ (g_1 \otimes Q) \circ (f_1 \otimes Q) \\ &= (P'' \otimes g_2) \circ (g_1 \circ f_1) \otimes Q \\ &= 0 \end{aligned}$$

d'où il découle que

$$g \;\circ\; f \;=\; 0\,.$$

ii) Soit $h \;:\; P \otimes Q \;\to\; M$ tel que $h \circ f \;=\; 0$. Ceci implique en particulier que $h \circ (f_1 \otimes Q) \;=\; 0$, donc, en vertu de I.1.1.15.ii, qu'il existe un unique $h' \;:\; P'' \otimes Q \;\to\; M$ tel que $h \;=\; h' \circ (g_1 \otimes Q)$.

Il en résulte puisque $h \circ f \;=\; 0$, que

$$\begin{aligned} h' \circ (P'' \otimes f_2) \circ (g_1 \otimes Q') &= h' \circ (g_1 \otimes Q) \circ (P \otimes f_2) \\ &= h \circ (P \otimes f_2) \\ &= 0 \end{aligned}$$

ce qui implique, puisque $g_1 \otimes Q'$ est surjectif que $h' \circ (P'' \otimes f_2) \;=\; 0$, ce qui implique encore qu'il existe un unique $h'' \;:\; P'' \otimes Q'' \;\to\; M$ tel que $h' \;=\; h'' \;\circ\; (P'' \otimes g_2)$. Il en découle que

$$h \;=\; h' \;\circ\; (g_1 \circ Q) \;=\; h'' \;\circ\; (P'' \otimes g_2) \circ (g_1 \otimes Q) \;=\; h'' \circ g\,.$$

iii) L'unicité de h'' factorisant h à travers $P'' \otimes Q''$ est alors conséquence du fait que g est surjectif comme composée de deux morphismes surjectifs. Ceci prouve finalement que

$$(P'' \otimes Q'', g) \;=\; \mathrm{Coker}\, f$$

donc le résultat (cf. I.1.1.19.)

q.e.d

Exemple I.2.1.16. Il résulte de la proposition précédente que, pour deux entiers naturels a et b et $a \wedge b$ leur PGCD, on a un isomorphisme

$$\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \ \cong \ \mathbb{Z}/a \wedge b\mathbb{Z} \ .$$

Proposition I.2.1.17. *Si P et Q sont des A-modules libres de bases respectives e_i ,$_{i\in I}$ et f_j ,$_{j\in J}$ alors, $P \otimes_A Q$ est un A-module libre de base $(e_i \otimes f_j)$,$_{(i,j)\in I\times J}$.*

Exemple I.2.1.18. Pour tout A-module M, on peut écrire une suite exacte

$$M_r \ \longrightarrow \ M_g \longrightarrow M \ \rightarrow \ 0$$

où M_r et M_g sont des A-modules libres. Il résulte alors de la proposition I.2.1.15 que pour deux modules P et Q, on a un isomorphisme

$$P \otimes Q \ \cong \ (P_g \otimes Q_g)/(P_r \otimes Q_g) + (P_g \otimes Q_r) \ .$$

I.2.2 . −Extension des scalaires

Dans ce paragraphe, $f \ : \ A \ \rightarrow \ B$ est une A-algèbre (cf. I.1.1.2.) On rappelle que B « hérite » alors d'une structure naturelle de A-module (cf. I.1.1.12.)

Lemme I.2.2.1. *Pour tout A-module M, on peut former le produit tensoriel $M \otimes_A B$ qui a naturellement une structure de A-module.*

L'application

$$B \times M \times B \ \rightarrow \ M \otimes_A B \ , \ (b, x, b') \ \mapsto \ x \otimes bb'$$

définit une application $\cdot \ : \ B \times (M \otimes_A B) \ \rightarrow \ M \otimes_A B$ caractérisée par le fait que

$$b \cdot (x \otimes b') \ = \ x \otimes bb'$$

et qui donne à $M \otimes_A B$ une structure de B-module.

La fonctorialité du produit tensoriel (cf. I.2.1.8.iii) assure que pour tout morphisme de A-modules $u \ : \ M \ \rightarrow \ N$ on a un unique morphisme de A-modules $u \otimes B \ : \ M \otimes B \ \rightarrow \ N \otimes B$ caractérisé par le fait que

$$(u \otimes B)(x \otimes b) \ = \ u(x) \otimes b \ .$$

Il est presque immédiat de vérifier sur la définition que $u \otimes B$ est en fait un morphisme de B-modules (pour les structures définies ci-dessus,) et que

$$M \ \mapsto \ M_b \ := \ M \otimes B \ , \ u \ \mapsto \ u_B \ := \ u \otimes B$$

est un foncteur covariant de la catégorie $A - \mathbf{mod}$ des A-modules dans la catégorie $B - \mathbf{mod}$ des B-modules.

Définition I.2.2.2. On appelle le foncteur

$$M \ \mapsto \ M_B$$

défini ci-dessus foncteur *extension des scalaires* ou *changement de base*.

Exemple I.2.2.3.
i) Si $\mathfrak{I} \ \subset \ A$ est un idéal et $B \ := \ A/\mathfrak{I}$, pour tout A-module M,

$$M_B \ = \ M \otimes_A B \ \cong \ M/\mathfrak{I}M \ .$$

ii) Soit $A \ \to \ B$ une A-algèbre. Il existe alors une unique application A-bilinéaire

$$B \times A[X] \ \to \ B[X]$$

caractérisée par le fait que

$$(b, X^k) \ \mapsto \ bX^k \ \forall b \in B \ \forall k \in \mathbb{N} \ .$$

Il n'est pas difficile de voir alors que cette application définit un morphisme de B-algèbres

$$B \otimes_A A[X] \ \to \ B[X]$$

caractérisé par

$$(b \otimes X) \mapsto bX \ \forall b \in B \ .$$

Réciproquement, il existe un unique morphisme de B-algèbres $B[X] \ \to \ B \otimes_A A[X]$ caractérisé par $X \mapsto 1 \otimes X$.

Il est tout à fait élémentaire désormais de vérifier que les deux morphismes de B-algèbres construits ci-dessus sont inverses l'un de l'autre et qu'en conséquence, on a un isomorphisme naturel

$$B \otimes_A A[X] \ \cong \ B[X] \ .$$

Proposition I.2.2.4. *Tout B-module peut être vu comme un A-module. Pour tout A-module P, tout B-module Q, et tout morphisme de A-modules*

$$f \ : \ P \ \to Q \ \in \ \mathrm{Hom}_A(P, Q) \ ,$$

il existe un unique morphisme de B-modules $\alpha(f) \ : \ P \otimes_A B \ \to \ Q$ caractérisé par le fait que

$$\alpha(f)(x \otimes b) \ = \ bf(x) \ .$$

On définit ainsi une application

$$\alpha \ : \ \mathrm{Hom}_A(P, Q) \ \to \ \mathrm{Hom}_B(P \otimes_A B, Q) \ .$$

L'application α est en fait un isomorphisme de A-modules.

Proposition I.2.2.5. *Étant donnés deux morphisme d'anneaux $f : A \to B$ et $g : B \to C$, pour tout A-module M, il existe un unique morphisme de C-modules*

$$(M \otimes_A B) \otimes_B C \to M \otimes_A C$$

caractérisé par

$$(x \otimes b) \otimes c \mapsto x \otimes g(b)c\,.$$

De plus, ce morphisme est un isomorphisme de C-modules.

I.2.3 . −Produit tensoriel de A-algèbres

Dans ce paragraphe, A est un anneau.

Lemme I.2.3.1. *Étant données deux A-algèbres*

$$f : A \to B \text{ et } g : A \to C\,,$$

on a, par fonctorialité du produit tensoriel (cf. I.2.1.8.iii,) un carré commutatif de A-modules :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle B\otimes_A g} \\ C & \xrightarrow{f\otimes_A C} & B \otimes_A C\,. \end{array} \qquad \textit{I.2.3.1.1}$$

On munit $B \otimes_A C$ de l'unique structure d'anneau donnée par

$$(b \otimes c) * (b' \otimes c') := bb' \otimes cc'\,.$$

Avec cette structure, les morphismes $B \otimes g$ et $f \otimes C$ deviennent des morphismes d'anneaux.

Définition I.2.3.2. Pour deux A-algèbres B et C, on appelle encore *produit tensoriel des algèbres B* et C le A-module $B \otimes_A C$ muni de la structure d'algèbre définie ci-dessus.

Lemme I.2.3.3. *Pour tout A-algèbre B et tout morphisme de A-algèbres $v : C \to D$, le morphisme*

$$v \otimes_A B : C \otimes_A B \to D \otimes_A B$$

est un morphisme de B-algèbres.

Lemme I.2.3.4. *Le carré I.2.3.1.1 est donc un carré commutatif d'anneaux. Il est même cocartésien c'est-à-dire que pour tout diagramme commutatif d'anneaux*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle g}\downarrow & \downarrow{\scriptstyle v} \\ C & \xrightarrow{u} & D \end{array}$$

il existe un unique morphisme d'anneaux $h : B \otimes_A C \to D$ tel que

$$v = h \circ (B \otimes g) \text{ et } u = h \circ (f \otimes C)\,.$$

I.3 . −Localisation

I.3.1 . −Localisation dans les modules

Définition I.3.1.1. Partie multiplicative Une *partie multiplicative* S d'un anneau A est une partie S contenant 1 et telle que pour tous s et t de S, $st \in S$.

Dans la suite du paragraphe, A est un anneau et S une partie multiplicative de A.

Proposition I.3.1.2.
i) Pour tout A-module M considérons la relation d'équivalence sur $M \times S$ donnée par $(x,t) \sim (y,t)$ s'il existe $u \in S$ tel que

$$u(tx - sy) \ = \ 0 \ \in \ M \ .$$

Alors le quotient $(M \times S)/\sim$ a une structure de groupe abélien donné par

$$(x,s) \ + \ (y,t) \ := \ (tx + sy, st) \ \forall (x,y) \in M \times M \ , \ \forall (s,t) \in S \times S$$

et une structure de A-module donnée par

$$a \cdot (x,s) \ := \ (ax, s) \ \forall x \in M \ , \ \forall a \in A \ , \ \forall s \in S \ .$$

ii) Pour tout morphisme de A-modules $f \ : \ P \ \to \ Q$ il existe un unique morphisme de A-modules

$$(P \times S)/\sim \ \to \ (Q \times S)/\sim$$

vérifiant

$$(x,s) \ \mapsto \ (f(x), s) \ \forall x \in P \ , \ \forall s \in S \ .$$

Définition I.3.1.3. Pour tout A-module M, le quotient $(M \times S)/\sim$ comme dans la proposition ci-dessus sera noté $S^{-1}M$ et appelé le *localisé de M en S*. La classe de $(x,s) \in M \times S$ dans $S^{-1}M$ est usuellement notée $\frac{x}{s}$.

Pour tout A-morphisme $f \ : \ P \ \to \ Q$ la morphisme induit $S^{-1}P \ \to \ S^{-1}Q$ par le procédé I.3.1.2.ii sera noté $S^{-1}f$ si bien qu'on a défini un foncteur covariant (cf. 0.3.2.1)

$$S^{-1}\cdot \ : \ A - \mathbf{mod} \ \to \ A - \mathbf{mod} \ .$$

Proposition I.3.1.4.
i) Si $f \ : \ A \ \to \ B$ est une A-algèbre (cf. I.1.1.11,) B a en particulier une structure de A-module (cf. I.1.1.12.i.) Le localisé $S^{-1}B$ de B en S a alors une structure de A-algèbre où le produit est donné par

$$(b,s) \ * \ (c,t) \ := \ (bc, st) \ \forall (b,c) \in B \times B \ , \ \forall (s,t) \in S \times S$$

et le morphisme structural par

$$a \ \mapsto \ (f(a), 1) \ .$$

ii) Pour tout morphisme de A-algèbres $u : (B, f) \to (C, g)$ le morphisme

$$S^{-1}u : S^{-1}B \to S^{-1}C$$

est un morphisme de A-algèbres pour la structure définie ci-dessus.

iii) En particulier, pour $\mathrm{Id}_A : A \to A$ l'anneau $S^{-1}A$ est une A-algèbre.

iv) Pour $f : A \to B$ une a-algèbre, $f(S)$ est encore une partie multiplicative de B et $S^{-1}B$ s'identifie à $f(S)^{-1}B$ si B est vu comme B-algèbre sur lui-même par l'identité Id_B.

Pour tout morphisme de A-algèbres $u : (B, f) \to (C, g)$ on a des isomorphismes canoniques

$$S^{-1}C \cong f(S)^{-1}C \cong (u \circ f)(S)^{-1}C \cong g(S)^{-1}C .$$

Proposition I.3.1.5. *La A-algèbre $\lambda_S : A \to S^{-1}A$ (cf. I.3.1.4.iii,) est telle que*

$$\lambda_S(S) \subset (S^{-1}A)^\times$$

et est universelle pour cette propriété.

Plus précisément, on peut considérer la catégorie (cf. 0.3.1.1) $\mathbf{S}$ définie de la manière suivante : Les objets de $\mathbf{S}$ sont les couples (B, f) où $f : A \to B$ est une A-algèbre telle que $f(S) \subset B^\times$ c'est-à-dire telle que pour tout $s \in S$, $f(s)$ est un inversible de B. Les morphismes

$$\phi : (B, f) \to (C, g)$$

sont les morphismes d'anneaux $\phi : B \to C$ tels que $g = \phi \circ f$. Le couple $(S^{-1}A, \lambda_S)$ est initial (cf. 0.3.3.1) dans $\mathbf{S}$ c'est-à-dire que pour toute A-algèbre $f : A \to B$ telle que $f(S) \subset B^\times$, il existe un unique morphisme d'anneaux $f' : S^{-1}A \to B$ tel que $f = f' \circ \lambda_S$.

Corollaire I.3.1.6.
i) Pour toute A-algèbre $f : A \to B$, il est clair que

$$f(S)subset\ (S^{-1}B)^\times = (f(S)^{-1}B)^\times$$

et donc que la morphisme naturel $A \to S^{-1}B$ (cf. I.3.1.4.i) se factorise à travers $S^{-1}A$ faisant naturellement de $S^{-1}B$ une $S^{-1}A$-algèbre.

ii) Pour tout morphisme de A-algèbres $u : B \to C$, le morphisme $S^{-1}u$ est un morphisme de $S^{-1}A$-algèbres.

Proposition I.3.1.7.
i) Pour tout A-module M, l'application

$$S^{-1}A \times S^{-1}M \to S^{-1}A\ ((a, s), (x, t)) \mapsto (ax, st)$$

définit une structure de $S^{-1}A$-module sur $S^{-1}M$ qui conïncide, dans le cas où M est une A-algèbre avec celle donnée par le corollaire I.3.1.6.i.

ii) Pour tout morphisme de A-modules $f : P \to Q$, le morphisme $S^{-1}f$ est naturellement un morphisme de $S^{-1}A$-modules pour la structure définie ci-dessus.

iii) Le foncteur $S^{-1}\cdot$ est finalement défini de la catégorie des A-modules (resp. A-algèbres) dans la catégorie des $S^{-1}A$-modules (resp. $S^{-1}A$-algèbres.)

Proposition I.3.1.8.
i) Pour tout A-module (resp. A-algèbre) X il existe un unique morphisme

$$X \otimes_A S^{-1}A \to S^{-1}X$$

caractérisé par

$$x \otimes \frac{a}{s} \mapsto \frac{ax}{s}$$

(le produit tensoriel étant pris au sens des A-modules (cf. I.2.1,) (resp. au sens des A-algèbres (cf. I.2.3.)))

Ce morphisme est un isomorphisme de $S^{-1}A$-modules (resp. $S^{-1}A$-algèbres.)

ii) Pour tout morphisme de A-modules, (resp. A-algèbres) $f : X \to Y$, le morphisme $S^{-1}f$ s'identifie au morphisme $f \otimes_A S^{-1}A$ (cf. I.2.1.8.iii,) à travers les isomorphismes du point précédent.

On peut alors identifier les foncteurs $S^{-1}\cdot$ et $\cdot \otimes_A S^{-1}A$ de $A - \mathbf{mod}$ (resp. $A - \mathbf{alg}$) dans $S^{-1}A - \mathbf{mod}$ (resp. $S^{-1}A - \mathbf{alg}$.)

Proposition I.3.1.9. *Si $S \subset T$ sont des partie multiplicatives de A, pour tout A-module (resp. A-algèbre) X, on a un morphisme naturel de $S^{-1}A$-modules (resp. $S^{-1}A$-algèbres) $S^{-1}X \to T^{-1}X$.*

Proposition I.3.1.10. *Si $f : X \to Y$ est un morphisme injectif dans $A - \mathbf{mod}$ (resp. $A - \mathbf{alg}$,) $S^{-1}f$ l'est aussi.*

Proposition I.3.1.11. *La A-algèbre $S^{-1}A$ est un A-module plat (cf. I.2.1.12.)*

Preuve : C'est une conséquence des énoncés I.3.1.10, I.3.1.8 et I.2.1.10. *q.e.d*

I.3.2 . −Propriétés des anneaux localisés

Dans ce paragraphe, A est un anneau et S une partie multiplicative.

i) Si S ne contient pas de diviseur de 0, le morphisme naturel

$$A \to S^{-1}A\,,\ a \mapsto \frac{a}{s}\,,$$

est injectif ; ce qui est en particulier le cas si A est intègre.

Proposition I.3.2.1. *Si A est un anneau intègre, son corps des fractions $\mathrm{Frac}(A)$ n'est autre que $(A \setminus \{0\})^{-1}A$ et dans ce cas, pour toute partie multiplicative S de A ne contenant pas 0, $S^{-1}A$ est un sous-anneau de $\mathrm{Frac}(A)$ donc en particulier intègre. De plus,*

$$K = \mathrm{Frac}(S^{-1}A)\,.$$

Proposition I.3.2.2. *Si M est un $S^{-1}A$-module on peut le voir (à travers le morphisme d'anneaux $A \to s^{-1}A$) comme un A-module on dit (par restriction des scalaires.) Alors l'unique morphisme*

$$M \otimes_A S^{-1}A \to M \ , \ x \otimes \frac{a}{s} \mapsto \frac{a}{s}x$$

est un isomorphisme de $S^{-1}A$-modules.

Proposition I.3.2.3. *Pour A un anneau et $S \subset A$ une partie multiplicative de A, posons $B := S^{-1}A$ et $f : A \to B$ le morphisme canonique.*

On rappelle qu'on a toujours une application $I(f)$ de l'ensemble des idéaux de B dans l'ensemble des idéaux de A donnée par

$$\mathfrak{J} \subset B \mapsto f^{-1}(\mathfrak{J}) \ .$$

Même si $f(\mathfrak{I})$ pour $\mathfrak{I} \subset A$ un idéal de A n'est pas nécessairement un idéal (c'en est un si f est surjectif néanmoins) on peut toujours poser $R(f)(\mathfrak{I}) := Bf(\mathfrak{I})$ l'idéal engendré par l'image de $\mathfrak{I}$ par f.

i) Pour tout idéal $\mathfrak{J} \subset B$, d'image réciproque $\mathfrak{I} = f^{-1}(\mathfrak{J}) \subset A$, l'inclusion naturelle $Bf(\mathfrak{I}) \subset \mathfrak{J}$ est bijective c'est-à-dire que $R(f) \circ I(f) = \mathrm{Id}$. Il en résulte que l'application $I(f)$ est injective.

ii) Comme $I(f)$ est également croissante pour l'inclusion, si A est noethérien, B l'est aussi.

iii) L'application $I(f)$ induit donc par restriction à $\mathrm{Spec}(S^{-1}A)$ (l'ensemble des idéaux premiers de $S^{-1}A$ (cf. I.1.2.9)) une application injective à valeurs dans $\mathrm{Spec}(A)$. Elle induit donc une bijection sur son image qui est la partie de $\mathrm{Spec}(A)$ formée des idéaux premiers de A qui ne rencontrent pas S. On peut montrer que cette bijection est bicontinue pour la topologie de Zariski (cf. I.1.2.9.)

Lemme I.3.2.4. *Soit $A \subset B$ des anneaux et S une partie multiplicative de A. Pour deux sous-A-modules $\mathfrak{I}$ et $\mathfrak{J}$ de B, on note $\mathfrak{I}\mathfrak{J}$ le sous-A-module de B engendré par les xy ,$_{x\in\mathfrak{I}}$, $_{y\in\mathfrak{J}}$. Alors les sou-$S^{-1}A$-modules $S^{-1}(\mathfrak{I}\mathfrak{J})$ et $(S^{-1}\mathfrak{I})(S^{-1}\mathfrak{J})$ de $S^{-1}B = B \otimes_A S^{-1}A$ sont égaux.*

Proposition I.3.2.5. *Soit A un anneau noethérien (cf. I.1.4.2) intègre (cf. I.1.1.6) de corps des fractions K. Pour toute partie multiplicative $S \subset A$ ne contenant pas 0, tout idéal fractionnaire (cf. I.1.5.1) $\mathfrak{I}$ de A, le $S^{-1}A$-module $S^{-1}\mathfrak{I} = \mathfrak{I} \otimes_A S^{-1}A$ est un idéal fractionnaire de $S^{-1}A$ qui est bien un anneau noethérien (cf. I.3.2.3.ii,) intègre de corps des fractions K.*

De plus, la localisation est « compatible » à la loi de composition définie en I.1.5.4, à savoir que, pour deux idéaux fractionnaires $\mathfrak{I}$ et $\mathfrak{J}$ de A, l'inclusion naturelle

$$S^{-1}\mathfrak{I}S^{-1}\mathfrak{J} \subset S^{-1}(\mathfrak{I}\mathfrak{J})$$

est bijective.

I.3.3 . −Anneaux locaux, localisé en un idéal

Définition I.3.3.1. Un *anneau local* est un anneau A n'ayant qu'un idéal maximal ou de manière équivalente pour lequel l'ensemble des éléments non inversibles $A \setminus A^\times$ est un idéal maximal ou de manière équivalente tel que $A \setminus A^\times$ est un idéal ou encore tel que $A \setminus A^\times$ est une partie stable par addition.

On note souvent $\mathfrak{m}_A$ l'idéal maximal d'un anneau local. Le quotient $A/\mathfrak{m}_A$ est un corps appelé le *corps résiduel* de A.

Proposition I.3.3.2. Lemme de Nakayama *Si A est un anneau local d'idéal maximal $\mathfrak{m}_A$ et M un A-module de type fini vérifiant*

$$M \;=\; \mathfrak{m}_A M$$

alors M est nul.

Définition I.3.3.3. Anneau de valuation Un *anneau de valuation* est un anneau intègre A, qui n'est pas un corps et tel que pour tout élément a de son corps des fractions $\mathrm{Frac}(A)$ si $a \notin A$, $a^{-1} \in A$.

Proposition I.3.3.4. *Un anneau de valuation est un anneau local.*

Preuve : Soit A un anneau de valuation, a et b des éléments de A. Supposons que $a+b$ est inversible. Si a est nul, b est inversible. Supposons donc que a et b sont non nuls. Il existe $c \in A$ tel que $c(a+b) = 1$. Des deux éléments de $\mathrm{Frac}(A)$ $\frac{a}{b}$ et $\frac{b}{a}$, l'un au moins est dans A puisque A est un anneau de valuation. Supposons que ce soit $\frac{a}{b}$. Alors

$$cb(\frac{a}{b}+1) \;=\; 1$$

et $c(1+\frac{a}{b}) \in A$ c'est-à-dire que b est inversible.

Il en résulte (par contraposée) que l'ensemble des éléments non inversibles de A est stable par addition, donc que A est local. *q.e.d*

Lemme I.3.3.5. *Soit A un anneau local intègre de dimension 1 ce qui équivaut à dire que ses seuls idéaux premiers sont $\{0\}$ et son idéal maximal $\mathfrak{m}_A$.*

Alors pour tous x et z dans $\mathfrak{m}$ non nuls, il existe n entier tel que x^n est dans l'idéal de A engendré par z.

Preuve : Soit S la partie multiplicative de A (cf. I.3.1.1) $\{1; x; \ldots; x^n; \ldots\}$ formée des puissances de x. Puisque A est intègre, S ne contient pas 0. Soit $B \;:=\; S^{-1}A$ (cf. I.3.1.3.) Comme A est intègre, on a les inclusions

$$A \;\subset\; B \;\subset\; \mathrm{Frac}(A)$$

(cf. I.3.2.i.) Les idéaux premiers de B correspondent bijectivement aux idéaux premiers de A qui ne rencontrent pas S (cf. I.3.2.3.iii.) Or A n'a, par hypothèses que deux idéaux premiers 0 et $\mathfrak{m}_A$ et $\mathfrak{m}_A \cap S \;\neq\; \emptyset$. Donc B n'a qu'un idéal premier, et comme il est intègre, (c'est un sous-anneau de $\mathrm{Frac}(A)$,) B est un corps qui est donc $\mathrm{Frac}(A)$.

Il en résulte que $1/z \in B$ donc s'écrit a/x^n pour $a \in A$, d'où $x^n = az$. *q.e.d*

Lemme I.3.3.6. *Un idéal $\mathfrak{p}$ d'un anneau A est premier si et seulement si son complémentaire $A \setminus \mathfrak{p}$ est une partie multiplicative.*

Définition I.3.3.7. Localisé en un idéal premier (fibre) Étant donné un idéal premier $\mathfrak{p}$ d'un anneau A, pour tout a-module (resp. A-algèbre) X, on note

$$X_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} X$$

qu'on appelle le *localisé de X en $\mathfrak{p}$* ou la *fibre de X en $\mathfrak{p}$*.

Proposition I.3.3.8. *Soit A un anneau.*
i) L'anneau $A_{\mathfrak{p}}$ pour $\mathfrak{p} \in \mathrm{Spec}(A)$ un idéal premier est local d'idéal maximal $A_{\mathfrak{p}}\mathfrak{p}$ (i.e.l'image par l'application $R(A \to A_{\mathfrak{p}})$ de la proposition I.3.2.3.) Son corps résiduel sera souvent noté $k(\mathfrak{p})$.
ii) Il découle de la proposition I.3.2.3.iii que $\mathrm{Spec}(A_{\mathfrak{p}})$ (l'ensemble des idéaux premiers de $A_{\mathfrak{p}}$) correspond bijectivement à l'ensemble des idéaux premiers de A contenus dans $\mathfrak{p}$.

Proposition I.3.3.9. *Soit A un anneau intègre de corps des fractions K et $\mathfrak{I}$ un sous-A-module de K.*
i) Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$, on a une suite d'inclusion

$$\mathfrak{I} \subset \mathfrak{I}_{\mathfrak{p}} \subset K\,.$$

ii) Pour deux idéaux premiers $\mathfrak{q} \subset \mathfrak{p}$ on a un isomorphisme canonique

$$\mathfrak{I}_{\mathfrak{q}} \cong \mathfrak{I}_{\mathfrak{p}_{A_{\mathfrak{p}}\mathfrak{q}}}$$

d'où une suite d'inclusions

$$\mathfrak{I} \subset \mathfrak{I}_{\mathfrak{p}} \subset \mathfrak{I}_{\mathfrak{q}}\, K\,.$$

iii) En particulier, tout idéal premier $\mathfrak{p}$ étant inclus dans un idéal maximal $\mathfrak{m}$ on a

$$\mathfrak{I} \subset \mathfrak{I}_{\mathfrak{m}} \subset \mathfrak{I}_{\mathfrak{p}} \subset K$$

d'où il résulte que

$$\mathfrak{I} \subset \bigcap_{\mathfrak{m}\in \mathrm{Spm}(A)} \mathfrak{I}_{\mathfrak{m}} = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A)} \mathfrak{I}_{\mathfrak{p}} \subset K\,.$$

Dans le cas où A est intègre, la première inclusion est bijective.

Preuve :
i) Est une conséquence immédiate de la proposition I.3.1.10.
ii) Est laissé en exercice.
iii) Notons

$$\mathfrak{I}' := \bigcap_{\mathfrak{m}\in \mathrm{Spm}(A)} \mathfrak{I}_{\mathfrak{m}}\,.$$

Pour tout $a \in \mathfrak{I}'$, notons

$$M := \{x \in A \mid ax \in \mathfrak{I}\} .$$

L'ensemble M est clairement un idéal de A.

Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, $a \in \mathfrak{I}_{\mathfrak{m}}$. Il existe donc $y \in \mathfrak{I}$ et $x \in A \setminus \mathfrak{m}$ tels que $a = \frac{y}{x}$ d'où il découle que $y = ax \in \mathfrak{I}$ d'où $x \in M$. Il en résulte que M est un idéal qui n'est contenu dans aucun des idéaux maximaux de A donc que $M = A$. En particulier, $1 \in M$ c'est-à-dire que $a \in \mathfrak{I}$.

On a donc montré que $\mathfrak{I}' \subset \mathfrak{I}$.

q.e.d

I.4 . −Extensions entières

I.4.1 . −Éléments entiers dans une extension

Dans ce paragraphe, A est un sous-anneau d'un corps E.

Proposition I.4.1.1. *Pour tout élément $\alpha \in E$, les conditions suivantes sont équivalentes :*

a) Il existe un polynôme unitaire $P \in A[X]$ tel que $P(\alpha) = 0$.

b) Il existe un sous A-module M de E non nul de type fini tel que

$$\alpha M = M .$$

Définition I.4.1.2. On dit qu'un élément $\alpha \in E$ est *entier sur* A s'il vérifie les conditions équivalentes de la proposition ci-dessus.

Si A est un corps, on dit que α est *algébrique sur* A.

Étant donné un sous-anneau B de E contenant A, on dit que B est *entier sur* A ou que $A \subset B$ est une *extension entière* si tous les éléments de B sont entiers sur A. Si A et B sont des corps, on parle d'*extension algébrique*.

Définition I.4.1.3. Si B est une A-algèbre (cf. I.1.1.11,) qui est un A-module de type fini, on dit que B est une *A-algèbre finie*. Si $A \subset B$, on parle aussi d'*extension finie*.

Corollaire I.4.1.4. *Une extension finie est entière.*

Remarque I.4.1.5. Il existe en revanche des extensions entières (ou algébriques) qui ne sont pas finies. Par exemple la clôture algébrique d'un corps n'est pas en général une extension finie. Cependant, la proposition suivante peut être vue comme une réciproque partielle au corollaire I.4.1.4 :

Proposition I.4.1.6. *Si $A \subset B$ est une extension entière et B est une A-algèbre de type fini (c'est-à-dire le quotient d'une algèbre de polynômes en un nombre fini d'indéterminées $A[X_1, \ldots, X_n]$,) alors B est un A-module de type fini, c'est-à-dire une A-algèbre finie.*

Proposition I.4.1.7. *Si $A \subset B \subset C$ sont des anneaux intègres, $A \subset C$ est une extension entière si et seulement si $A \subset B$ et $B \subset C$ sont des extensions entières.*

Proposition I.4.1.8. *Si A est un sous-anneau de B, l'ensemble des éléments de B entiers sur A est un anneau.*

Définition I.4.1.9. Pour B un anneau contenant A, l'anneau des éléments de B entiers sur A est appelé *fermeture intégrale* de A dans B ou *fermeture algébrique* si A est un corps.

Proposition I.4.1.10. *Soit K le corps des fractions de A. Si α est entier sur A alors il est algébrique sur K. Si α est algébrique sur K il existe $c \in A$ tel que $c\alpha$ est entier sur A.*

Définition I.4.1.11. Si A est égal à sa fermeture intégrale dans son corps des fractions, on dit que A est *intégralement clos* ou *algébriquement clos* si A est un corps.

Exemple I.4.1.12. Un *anneau factoriel* est intégralement clos : c'est une conséquence du lemme de Gauß.

I.4.2 . −Extensions entières et localisation

Soit A un anneau intègre (cf. I.1.1.6,), $K := \mathrm{Frac}(A)$ son corps des fractions et S une partie multiplicative de A ne contenant pas 0 (cf. I.3.1.1.)

On rappelle que $S^{-1}A$ (cf. I.3.1.3) est un sous-anneau de K (cf. I.3.2.1,) et que

$$K = \mathrm{Frac}(S^{-1}A)\,.$$

Proposition I.4.2.1. *Si A est intégralement clos, $S^{-1}A$ aussi.*

Proposition I.4.2.2. *Si B est un anneau intègre contenant A entier sur A, alors $S^{-1}B$ est entier sur $S^{-1}A$.*

Proposition I.4.2.3. *Si B est la fermeture intégrale de A dans un corps E contenant A, $S^{-1}B$ est la fermeture intégrale de $S^{-1}A$ dans E.*

I.4.3 . −Idéaux dans les extensions entières

Définition I.4.3.1. Soient $A \subset B \subset E$ où E est un corps A et B des sous-anneaux. Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$, et tout $\mathfrak{q} \in \mathrm{Spec}(B)$, on dit que $\mathfrak{q}$ est *au-dessus* de $\mathfrak{p}$ si $\mathfrak{q} \cap A = \mathfrak{p}$. Ceci revient encore à dire que $\mathfrak{p}$ est l'image de $\mathfrak{q}$ par l'application induite de $\mathrm{Spec}(B)$ vers $\mathrm{Spec}(A)$ par l'inclusion $A \subset B$ (cf. I.1.2.9.)

Dans la suite du paragraphe, $A \subset B \subset E$ sont des extensions d'anneaux, E est un corps, A et B des sous-anneaux tels que B est entier sur A.

Proposition I.4.3.2. *Si $\mathfrak{p}$ est un idéal premier de A, $\mathfrak{p}B$ est un idéal de B différent de B et il existe un idéal $\mathfrak{q}$ de B au dessus de $\mathfrak{p}$.*

Preuve : Rappelons que, pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, on a

$$B_{\mathfrak{p}} \;=\; B \otimes_A A_{\mathfrak{p}}$$

(cf. I.3.1.8.)

Par la proposition I.4.2.2, $B_{\mathfrak{p}}$ est entier sur $A_{\mathfrak{p}}$. Notons $\mathfrak{m} \;:=\; \mathfrak{m}_{A_{\mathfrak{p}}}$ l'idéal maximal de l'anneau local $A_{\mathfrak{p}}$ (cf. I.3.3.8.i.)

Si l'on suppose que $B\mathfrak{p} \;=\; B$, par localisation, $B_{\mathfrak{p}}\mathfrak{m} \;=\; B_{\mathfrak{p}}$. [2]

Si l'on suppose que $B_{\mathfrak{p}}\mathfrak{m} \;=\; B_{\mathfrak{p}}$, on peut écrire $1 = b_i x_i$ $1 \leq i \leq d$ avec $b_i \in B_{\mathfrak{p}}$ et $x_i \in \mathfrak{m}$. Si l'on pose $M \;:=\; A_{\mathfrak{p}}[b_1, \ldots, b_d]$, M est une $A_{\mathfrak{p}}$-algèbre de type fini engendrée par des éléments entiers donc M est un $A_{\mathfrak{p}}$-module de type fini. Or $\mathfrak{m}M \;=\; M$ ce qui entraîne, par le lemme de Nakayama (cf. I.3.3.2) que M est nul ce qui entraînerait que $B_{\mathfrak{p}}$ est nul puis finalement que B est nul.

Soit $\mathfrak{q}$ un idéal maximal de $B_{\mathfrak{p}}$ contenant $B_{\mathfrak{p}}\mathfrak{m}$. $\mathfrak{q} \cap A_{\mathfrak{p}}$, est un idéal premier de $A_{\mathfrak{p}}$ contenant $\mathfrak{m}$ qui est l'idéal maximal de $A_{\mathfrak{p}}$, donc $\mathfrak{q} \cap A_{\mathfrak{p}} \;=\; \mathfrak{m}$.

Enfin $\mathfrak{q} \cap B$ est un idéal premier de B et

$$\begin{aligned} \mathfrak{q} \cap B \cap A \;&=\; \mathfrak{q} \cap A \\ &=\; \mathfrak{q} \cap A_{\mathfrak{p}} \cap A \\ &=\; \mathfrak{m} \cap A \\ &=\; \mathfrak{p}\,. \end{aligned}$$

q.e.d

Proposition I.4.3.3. *Si $\mathfrak{q}$ est un idéal premier de B au-dessus de $\mathfrak{p}$, $\mathfrak{q}$ est maximal si et seulement si $\mathfrak{p}$ l'est.*

En particulier, A est un corps si et seulement si B en est un.

Preuve : Soit $\mathfrak{q}$ un idéal premier de B au-dessus d'un idéal premier $\mathfrak{p}$ de A. Ceci définit précisément un morphisme injectif $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$. Il faut encore remarquer que $B/\mathfrak{q}$ est entier sur $A/\mathfrak{p}$. Si $\mathfrak{p}$ est maximal $A/\mathfrak{p}$ est un corps ce qui entraîne que $B/\mathfrak{q}$ est un corps.

Réciproquement, si $\overline{B} \;:=\; B/\mathfrak{q}$ est un corps, supposons que $\overline{A} \;:=\; A/\mathfrak{p}$ ne soit pas un corps. Alors $\overline{A}$ contient un idéal premier non nul $\mathfrak{r}$ et d'après la proposition I.4.3.2, $\overline{B}\mathfrak{r} \neq \overline{B}$. Puisque $\overline{B}$ est un corps, ce ne peut être que 0 ce qui est contradictoire. *q.e.d*

Lemme I.4.3.4. *Soient $A \subset B \subset E$ où E est un corps A et B des sous-anneaux. Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$, tout idéal premier $\mathfrak{q} \in \mathrm{Spec}(B)$ au-dessus de $\mathfrak{p}$ et toute partie multiplicative S ne rencontrant pas $\mathfrak{p}$:*

[2] Si l'on savait ici que $B_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$-module de type fini, ce qui est le cas dans le cas d'une extension finie et pas simplement entière, on saurait immédiatement par Nakayama (cf. I.3.3.2) que $B_{\mathfrak{p}} \;=\; 0$ ce qui introduirait une contradiction.

i) On a un isomorphisme naturel

$$S^{-1}(B/\mathfrak{q}) \cong S^{-1}B/S^{-1}\mathfrak{q}\ .$$

ii) $S^{-1}\mathfrak{q} = \mathfrak{q} \otimes_A S^{-1}A$ *est un idéal premier de* $S^{-1}B = B \otimes_A S^{-1}A$ *au-dessus de l'idéal* $S^{-1}\mathfrak{p}$ *de* $S^{-1}A$.

iii) En particulier, si B *est entier sur* A, $\mathfrak{q}_\mathfrak{p}$ *est maximal. Si* $\mathfrak{q}$ *est déjà maximal dans* B, *on a un isomorphisme naturelle*

$$B/\mathfrak{q} \cong B_\mathfrak{p}/\mathfrak{q}_\mathfrak{p}\ .$$

Preuve :
i) La suite exacte de A-modules

$$0 \to \mathfrak{q} \longrightarrow B \longrightarrow B/\mathfrak{q} \to 0$$

donne, par localisation en S ou, ce qui revient au même, par tensorisation par $S^{-1}A$ (cf. I.3.1.8,) une suite exacte de $S^{-1}A$-modules

$$0 \to S^{-1}\mathfrak{q} \longrightarrow S^{-1}B \longrightarrow S^{-1}(B/\mathfrak{q}) \to 0$$

puisque $S^{-1}A$ est plat sur A (cf. I.3.1.11.) On en déduit un isomorphisme naturel

$$S^{-1}(B/\mathfrak{q}) \cong S^{-1}B/S^{-1}\mathfrak{q}\ .$$

ii) Or puisque $A \cap \mathfrak{q} = \mathfrak{p}$ $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$ donc $\mathfrak{q} \cap S = \emptyset$. Il en résulte que l'image de S dans $B/\mathfrak{q}$ est une partie multiplicative ne contenant pas 0. Comme $B/\mathfrak{q}$ est intègre par hypothèse, il résulte de la proposition I.3.2.1 que $S^{-1}(B/\mathfrak{q})$ est intègre ce qui prouve que $S^{-1}\mathfrak{q}$ est un idéal premier.

iii) Il résulte de la proposition I.4.2.2 que $B_\mathfrak{p}$ est encore entier sur $A_\mathfrak{p}$. Comme $\mathfrak{q}_\mathfrak{p}$ est au-dessus de $\mathfrak{m}_{A_\mathfrak{p}}$ d'après le point précédent, il découle de la proposition I.4.3.3 que $\mathfrak{q}_\mathfrak{p}$ est maximal.

Le quotient $B_\mathfrak{p}/\mathfrak{q}_\mathfrak{p}$ est donc un corps qui s'identifie à $(B/\mathfrak{q})_\mathfrak{p}$. Si $\mathfrak{q}$ est maximal $B/\mathfrak{q}$ donc égal à son corps des fractions. L'égalité souhaitée découle alors de la proposition I.3.2.1.

q.e.d

I.4.4 . −Clôture intégrale dans les extensions finies séparables

Dans ce paragraphe, A **est un anneau intègre (cf. I.1.1.6,) intégralement clos (cf. I.4.1.11) dans son corps des fractions** K, L **une extension finie séparable de** K **de degré** d **et** B **la fermeture intégrale (cf. I.4.1.9) de** A **dans** L.

Proposition I.4.4.1. *Il existe des sous-*A*-modules* M' *et* M'' *libres de rang* d, *de* L *tels que*

$$M' \subset B \subset M''\ .$$

Corollaire I.4.4.2. *Si A est noethérien, B est un A-module de type fini donc $A \subset B$ est une extension finie (cf. I.4.1.3.) L'anneau B est encore noethérien.*

Corollaire I.4.4.3. *Si A est principal B est un A-module libre de rang d.*

Exemple I.4.4.4. Si $A = \mathbb{Z}$, d'où $K = \mathbb{Q}$, n'importe quelle extension finie L de degré d est séparable. La clôture intégrale de $\mathbb{Z}$ dans L est un $\mathbb{Z}$-module libre de rang d.

Preuve de la proposition I.4.4.1 : On dispose d'une forme linéaire $\mathrm{Tr}_{L/K}(\cdot) : L \to K$ qu'on construit comme suit : On choisit E contenant K algébriquement clos, tel que l'ensemble des K-plongements de L dans E ait exactement d éléments. La trace de x $\mathrm{Tr}_{L/K}(x)$ est la somme des $\sigma(x)$ pour les plongements qui est indépendante du choix de E et à valeurs dans K.

D'après le lemme I.4.4.5, l'application trace est non nulle. Il existe donc $a \in L$ tel que $\mathrm{Tr}_{(/a}()) = 1$. On définit $f : L \times L \to K$ forme bilinéaire (symétrique) par $f(x,y) := \mathrm{Tr}_{(/x}(y))$ qui est non dégénérée. Pour tout $x \neq 0$ il existe y tel que $\mathrm{Tr}_{(/x}(y)) \neq 0$ (prendre $y = a/x$.)

On choisit une base $e_{i\ ,1\leq i\leq d}$ de L sur K. Il existe $c_{i\ ,1\leq i\leq d} \in A$ tels que $c_i e_i \in B$ (cf. I.4.1.10.) Quitte à remplacer les e_i par les $c_i e_i$ on peut supposer que les e_i sont dans B. On prend pour M' le sous-A-module de L engendré par les e_i.

On appelle e_i^* la base duale de e_i c'est-à-dire les éléments de L tels que $\mathrm{Tr}_{(/e}(\,)i^* e_j) = \delta_{ij}$. Et on note M'' le A-module engendré par les e_i^*.

Reste à vérifier que $B \subset M''$. Pour tout $b \in B$, on peut écrire

$$b \;=\; \sum_{i=1}^{d} \lambda_i e_i^*$$

avec les $\lambda_i \in K$. Et il ne reste donc plus qu'à montrer qu'ils sont dans A. Pour b et c dans B, bc dans B. Notons $u := bc$, qui est racine d'un polynôme unitaire à coefficients dans A ce qui entraîne que pour tout K-plongement σ, $\sigma(u)$ est entier sur A. Par conséquent, $\mathrm{Tr}_{(/u}())$ est entier sur A et est aussi un élément de K. Par conséquent $\mathrm{Tr}_{(/u}()) \in A$. On applique ce résultat à $c = e_{i\ ,1\leq i\leq n}$ ce qui permet de montrer que les coordonnées λ_i de b sont entières. *q.e.d*

Lemme I.4.4.5. *La trace définie dans la preuve de la proposition I.4.4.1 n'est pas nulle.*

Preuve : C'est une conséquence du lemme d'indépendance des caractères I.4.4.6. *q.e.d*

Lemme I.4.4.6. Lemme d'indépendance des caractères *Soit G un groupe, E un corps et $\xi_1, \ldots, \xi_d$ des caractères à valeurs dans E^*. S'ils sont deux à deux distincts alors ils sont linéairement indépendants sur E.*

Preuve :
i) Si $d = 1$ un caractère ξ à valeurs dans E^* est nécessairement non nul donc $\lambda\xi = 0,\ \lambda \in E$ implique $\lambda = 0$ c'est-à-dire que le résultat est établi pour $d = 1$.
ii) Pour $d \geq 1$, soient $d+1$ caractères $\xi_{i\ ,1\leq i\leq d+1}$ et $\lambda_{i\ ,1\leq i\leq d+1} \in E$ tels que

$$\sum_{i=1}^{d+1} \lambda_i \xi_i \;=\; 0\,.$$

Si les λ_i sont non tous nuls, on peut supposer quitte à renuméroter, que $\lambda_{d+1} \neq 0$ et même, quitte à diviser par λ_{d+1} que $\lambda_{d+1} = 1$. On a alors

$$\xi_{d+1} = -\sum_{i=1}^{d} \lambda_i \xi_i \, . \qquad \text{I.4.4.7}$$

Il en résulte que les $\lambda_{i\ ,1\leq i\leq d}$ ne peuvent être tous nuls sans quoi on aurait $\xi_{d+1} = 0$ ce qui n'est pas possible. Quitte à renuméroter encore, on peut supposer que $\lambda_d \neq 0$.

i) Il résulte de I.4.4.7 que

$$\xi_{d+1}(g) = -\sum_{i=1}^{d} \lambda_i \xi_i(g) \, \forall g \in G \qquad \text{I.4.4.8}$$

Qui donne, d'une part, par multiplication par $\xi_{d+1}(h)\ ,\ h \in G$:

$$\xi_{d+1}(gh) = -\sum_{i=1}^{d1} \lambda_i \xi_{d+1}(h) \xi_i(g) \, \forall g \in G \, \forall h \in G \, , \qquad \text{I.4.4.9}$$

et d'autre part, appliquée à $gh\ g \in G\ ,\ h \in G$:

$$\xi_{d+1}(gh) = -\sum_{i=1}^{d} \lambda_i \xi_i(gh) = -\sum_{i=1}^{d} \lambda_i \xi_i(g) \xi_i(h) \, \forall g \in G \, , \, \forall h \in G \, . \qquad \text{I.4.4.10}$$

Les identités I.4.4.9 et I.4.4.10 impliquent que :

$$\sum_{i=1}^{d} \lambda_i (\xi_{d+1}(h) - \xi_i(h)) \xi_i(g) = 0 \, \forall g \in G \, , \, \forall h \in G \, . \qquad \text{I.4.4.11}$$

i) Si l'on fait l'hypothèse de récurrence que le théorème st établi pour d caractères, l'identité I.4.4.11 implique que, pour tout $1 \leq i \leq d$,

$$\lambda_i (\xi_{d+1}(h) - \xi_i(h)) = 0 \, \forall h \in G \, .$$

En particulier, cela implique que

$$\lambda_d (\xi_{d+1}(h) - \xi_d(h)) = 0 \, \forall h \in G \, .$$

Or, puisque $\xi_{d+1} \neq \xi_d$ par hypothèse, il existe $h \in G$ tel que $\xi_{d+1}(h) \neq \xi_d(h)$. Il en résulte alors que nécessairement $\lambda_d = 0$ ce qui est contradictoire.

q.e.d

I.5 . −Anneaux de dimension 1

I.5.1 . −Anneaux de valuation discrète

Lemme I.5.1.1. *Soit A un anneau noethérien, intègre, intégralement clos et $\mathfrak{I}$ un idéal de A.*
L'inclusion naturelle

$$\mathfrak{I} \subset \mathfrak{I}\mathfrak{I}^{\perp}$$

(cf. I.1.5.6.iii) est bijective si et seulement si $\mathfrak{I}^{\perp} = A$.

Preuve : Si $\mathfrak{I}^{\perp} = A$ $\mathfrak{I}\mathfrak{I}^{\perp} = \mathfrak{I}$ bien entendu.

Réciproquement supposons que $\mathfrak{I}\mathfrak{I}^{\perp} = \mathfrak{I}$. On a vu ci-dessus que $A \subset \mathfrak{I}^{\perp}$. Pour tout $x \in \mathfrak{I}^{\perp}$, $x\mathfrak{I} \subset \mathfrak{I}$. Il en découle que pour tout $n \in \mathbb{N}$, $x^n\mathfrak{I} \subset \mathfrak{I}$ ce qui entraîne que $x^n \in \mathfrak{I}^{\perp}$. Notons alors A_n le sous-A-module de $\mathfrak{I}^{\perp}$ engendré par $1, x, \ldots, x^n$. La suite $(A_n)_{n\in\mathbb{N}}$ est une suite croissante de sous-A-modules de $\mathfrak{I}^{\perp}$ qui est un A-module de type fini donc noethérien (A est noethérien). Il s'ensuit que la suite $(A_n)_{n\in\mathbb{N}}$ est stationnaire à partir d'un certain rang c'est-à-dire qu'il existe $n \in \mathbb{N}$ tel que $A_{n+1} = A_n$, d'où il découle qu'il existe des éléments $\lambda_{i\ ,0\leq i\leq r} \in A$ tels que

$$x^{n+1} = \sum_{i=0}^{n} X^i$$

c'est-à-dire que x est entier sur A. Comme A est intégralement clos par hypothèse, $x \in A$ et donc

$$\mathfrak{I}^{\perp} \subset A\,.$$

q.e.d

Théorème I.5.1.2. *Pour un anneau A les conditions suivantes sont équivalentes :*
a) A est un anneau principal (cf. I.1.4.3,) local (cf. I.3.3.1,) qui n'est pas un corps.

b) A est local noethérien (cf. I.1.4.2) et l'idéal maximal de A est principal engendré par un élément π non nilpotent.

c) A est intègre n'est pas un corps et il existe un élément $\pi \in A$ non nilpotent tel que pour tout idéal non nul $\mathfrak{I} \neq A$ de A il existe un entier n tel que $\mathfrak{I} = \pi^n A$.

d) a est intègre, n'est pas un corps et il existe un élément π de A non nilpotent tel que pour tout idéal non nul $\mathfrak{I} \neq A$ de A, il existe un unique entier n tel que $\mathfrak{I} = \pi^n A$.

e) A est noethérien, intègre (cf. I.1.1.6,) intégralement clos (cf. I.4.1.11) et $\mathrm{Spec}(A)$ a exactement deux éléments.

f) A est noethérien, local intègre intégralement clos et de dimension 1 (cf. I.1.3.2.)

Définition I.5.1.3. Un anneau A est un *anneau de valuation discrète* s'il vérifie les conditions équivalentes du théorème ci-dessus. Le théorème II.1.3.3 donne d'autres caractérisations des anneaux de valuation discrète.

Preuve du théorème I.5.1.2 :

i) **(a) entraîne (b)** Un anneau principal est noethérien (cf. I.1.4.4.) L'idéal maximal de A est principal et son générateur n'est pas nilpotent puisque, par définition, un anneau principal est intègre.

ii) **(a) entraîne (e)** A est intègre puisque principal intégralement clos puisqu'un anneau principal est en particulier factoriel et qu'un aneau factoriel est intégralement clos (cf. I.4.1.12.) Par ailleurs puisque A est intègre, $\{0\}$ est un idéal premier de A (cf. I.1.2.8.) Tout idéal premier non nul de A est maximal puisque A est principal (cf. I.1.4.5.) Il en découle que $\mathrm{Spec}(A)$ a exactement deux éléments puisque A n'est pas un corps.

iii) **(e) équivaut à (f)** Laissé en exercice.

iv) **(c) équivaut à (d)** Soit $\mathfrak{I}$ un idéal de A et supposons donnés deux entiers $r \leq s$ tels que

$$\mathfrak{I} \;=\; \pi^r A \;=\; \pi^s A\,.$$

Il existe alors $x \in A$ tel que

$$\pi^s \;=\; x\pi^r$$

c'est-à-dire

$$\pi^r(x - \pi^{s-r})$$

ce qui implique que $r = s$ puisque A est intègre et π non nilpotent.

La réciproque est immédiate.

v) **(d) entraîne (a)** Le seul idéal maximal de A est πA donc A est local.

vi) **(b) entraîne (c)** Pour tout n $\pi^n \neq 0$. (en particulier π lui-même n'est pas 0, donc A n'est pas un corps).

Comme A est local noethérien d'idéal maximal $\mathfrak{m}$ l'intersection des $\mathfrak{m}^n$ est 0. Grâce au lemme de Nakayama (cf. I.3.3.2.) En effet, $M := \bigcap \mathfrak{m}^n$ est un A-module de type fini vérifiant $\mathfrak{m}M = M$.

Si $\mathfrak{I} \subset A$, est un idéal non nul différent de A, $\mathfrak{I} \subset \mathfrak{m}$. On a une suite décroissante d'idéaux de A donnée par les puissance $\mathfrak{m}^n \neq 0$, et leur intersection est nulle. On note $n_{\mathfrak{I}}$ le plus grand entier n tel que $\mathfrak{I} \subset \mathfrak{m}^n$.

Il existe au moins un élément $x \in \mathfrak{I}$ tel que $x \notin \mathfrak{m}^{n_{\mathfrak{I}}+1}$ c'est-à-dire que $x \;=\; u\pi^{n_{\mathfrak{I}}}$ avec $u \notin \mathfrak{m}$. Puisque A est local, u est inversible. Il en résulte que $\mathfrak{m}^{n_{\mathfrak{I}}} \subset \mathfrak{I}$ et donc que

$$\mathfrak{I} \;=\; \mathfrak{m}^{n_{\mathfrak{I}}} \;=\; \pi^{n_{\mathfrak{I}}}\,.$$

Pour tout couple (x, y) d'éléments non nuls de A il existe, d'après ce qui précède, des entiers n_x et n_y et des inversibles u_x et u_y tels que

$$x \;=\; u_x\pi^{n_x} \text{ et } y \;=\; u_y\pi^{n_y}\,.$$

Il en résulte que

$$xy \;=\; u_x u_y \pi^{n_x+n_y}$$

ne peut être nul puisque π n'est pas nilpotent. L'anneau A est donc intègre.

vii) **(e) entraîne (b)** L'anneau A étant intègre, 0 est un idéal premier. Puisque $\mathrm{Spec}(A)$ ne contient que deux éléments l'autre élément est un idéal $\mathfrak{m} \neq 0$ nécessairement maximal. Il en résulte que A est local d'idéal maximal $\mathfrak{m}$. L'idéal $\mathfrak{m}$ n'est pas nilpotent puisque A est intègre et $\mathfrak{m} \neq 0$.

Il découle de la proposition I.1.5.6.iii que les produit au sens des idéaux fractionnaires (cf. I.1.5.4,) $\mathfrak{n} := \mathfrak{m}\mathfrak{m}^{\perp}$ est un idéal de A contenant $\mathfrak{m}$. Puisque $\mathfrak{m}$ est maximal, soit $\mathfrak{n} = \mathfrak{m}$ soit $\mathfrak{n} = A$. Il découle du lemme I.5.1.1 que si $\mathfrak{n} = \mathfrak{m}$ alors $\mathfrak{m}^{\perp} = A$.

Or $\mathfrak{m}^{\perp} \neq A$: Soient en effet $z \in \mathfrak{m}$, $z \neq 0$ et x_i ,$1 \leq i \leq r$ des générateurs de $\mathfrak{m}$ qui comme idéal d'un anneau noethérien est de type fini. Pour tout $1 \leq i \leq r$, le lemme I.3.3.5 entraîne qu'il existe $n_i \in \mathbb{N}^*$ tel que $x_i^{n_i} \in (z)$. Il existe donc $n \in \mathbb{N}$ tel que $\mathfrak{m}^n \subset (z)$. Soit r le plus petit entier tel que $\mathfrak{m}^r \subset (z)$. On a nécessairement $r > 0$.

Soit $y \in \mathfrak{m}^{r-1}$, $y \notin (z)$. Il en résulte que $y/z \notin A$. Pour tout $x \in \mathfrak{m}$, $yx \in \mathfrak{m}^r$, donc dans (z), donc $xy/z \in A$, Ce qui montre que $y/z \in \mathfrak{m}^{\perp}$. Donc $\mathfrak{m}^{\perp} \neq A$.

Il s'ensuit que $\mathfrak{n} = A$. Par conséquent, $1 \in \mathfrak{n}$. Il existe donc x_i ,$1 \leq i \leq d \in \mathfrak{m}^{\perp}$ y_i ,$1 \leq i \leq d \in \mathfrak{m}$, tels que

$$1 = \sum_{i=1}^{d} x_i y_i \ .$$

Or $1 \notin \mathfrak{m}$ et pour tout $1 \leq i \leq d$ $x_i y_i \in A$. Il existe donc $1 \leq i_0 \leq d$ tel que $x_{i_0} y_{i_0} \notin \mathfrak{m}$. Comme A est local d'idéal maximal $\mathfrak{m}$, $x_{i_0} y_{i_0}$ est inversible dans A.

Pour tout $z \in \mathfrak{m}$, on a

$$z = (x_{i_0} y_{i_0})^{-1} x_{i_0} z y_{i_0} \ .$$

Or $z \in \mathfrak{m}$, $x_{i_0} \in \mathfrak{m}^{\perp}$ et par conséquent,

$$(x_{i_0} y_{i_0})^{-1} x_{i_0} z \in A \ .$$

Il en découle que y_{i_0} est un générateur de $\mathfrak{m}$ qui est donc principal

q.e.d

Proposition I.5.1.4. *Étant donné un anneau de valuation discrète A et π un générateur de son idéal maximal, l'application qui à tout entier relatif n associe l'idéal fractionnaire (cf. I.1.5.1) $\pi^n A$ est bijective et vérifie, pour tout $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,*

$$\pi^{m+n} A = (\pi^n A)(\pi^m A)$$

où le second produit est pris au sens de I.1.5.4 si bien que l'ensemble des idéaux fractionnaires de A est un groupe noté $\mathcal{I}(A)$ pour la loi de composition définie en I.1.5.4.

De plus, pour tout idéal fractionnaire $\mathfrak{I}$ de A, son inverse $\mathfrak{I}^{-1}$ s'identifie à l'idéal fractionnaire $\mathfrak{I}^{\perp}$ défini en I.1.5.5.

Preuve : C'est une conséquence immédiate de la caractérisation I.5.1.2.d et I.1.5.3. *q.e.d*

I.5.2 . −Anneaux de Dedekind

Théorème I.5.2.1. *Étant donné un anneau A qui n'est pas un corps, les assertions suivantes sont équivalentes :*
a) A est noethérien (cf. I.1.4.2,) intègre (cf. I.1.1.6,) intégralement clos (cf. I.4.1.11) et tel que tout idéal premier non nul est maximal autrement dit de dimension 1 (cf. I.1.3.2.)

b) A est un anneau noethérien, intègre, tel que pour tout idéal premier $\mathfrak{p}$ non nul, $A_{\mathfrak{p}}$ est un anneau de valuation discrète (cf. I.5.1.3.)

Preuve :
i) **(a) implique (b)** Pour tout idéal premier $\mathfrak{p}$ de A, l'anneau $A_{\mathfrak{p}}$ est local et n'a que deux idéaux premiers 0 et $\mathfrak{p}$. L'anneau $A_{\mathfrak{p}}$ est intégralement clos grâce à I.4.2.1. On peut donc utiliser la caractérisation I.5.1.2.e. On a donc montré que (a) implique (b).

ii) **(b) implique (a)** Réciproquement, reste à vérifier que A est intégralement clos et que tout idéal premier non nul est maximal.

Tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$ de A est contenu dans un idéal maximal $\mathfrak{m}$. Son image par localisation (cf. I.3.2.3) est donc un idéal premier $\mathfrak{q} \in \mathrm{Spec}(A_{\mathfrak{m}})$ de $A_{\mathfrak{m}}$ contenu dans l'idéal maximal $\mathfrak{m}_{A_{\mathfrak{m}}}$. L'anneau $A_{\mathfrak{m}}$ étant de valuation discrète,

$$\mathfrak{q} \;=\; 0 \; ou \; \mathfrak{q} \;=\; \mathfrak{m}_{A_{\mathfrak{m}}} \; .$$

On conclut grâce à la proposition I.3.2.3.iii.

q.e.d

Définition I.5.2.2. Anneau de Dedekind Un *anneau de Dedekind* est un anneau qui n'est pas un corps et vérifie les assertions équivalentes du théorème ci-dessus.

Remarque I.5.2.3. Le spectre d'un anneau de Dedekind A est comme le spectre de $\mathbb{Z}$. Les fermés sont $\mathrm{Spec}(A)$ tout entier et les ensembles finis de points.

Exemple I.5.2.4. L'anneau $\mathbb{Z}$ est un anneau de Dedekind, plus généralement un anneau principal qui n'est pas un corps est un anneau de Dedekind. En particulier, un anneau de valuation discrète (cf. I.5.1.3) est un anneau de Dedekind et réciproquement, un anneau de Dedekind local est un anneau de valuation discrète.

Proposition I.5.2.5. *Si A est de Dedekind, et si S est une partie multiplicative de A ne contenant pas 0. Si $S^{-1}A$ n'est pas un corps c'est un anneau de Dedekind.*

Proposition I.5.2.6. *Si A est un anneau de Dedekind, et L une extension finie séparable de son corps des fractions K, alors la fermeture intégrale B de A dans L est encore un anneau de Dedekind.*

Preuve :
i) B est encore noethérien. On a déjà vu ce résultat avec A noethérien intègre et intégralement clos (cf. I.4.4.2.)

ii) Si B était un corps il contiendrait le corps des fractions de A, ce qui impliquerait que A est égal à son corps des fractions mais A n'est pas un corps.

iii) Pour tout idéal premier $\mathfrak{q} \subset B$ non nul, on note $\mathfrak{p} := \mathfrak{q} \cap A$ qui est un idéal premier de A.
Pour tout $x \in L$, on pose

$$\nu(x) := \prod \sigma(x)$$

la norme de L à K de x où les σ sont les K-plongements de L dans une clôture algébrique de K.

Tout $x \in \mathfrak{q}$, $x \neq 0$, est entier sur A donc racine d'un polynôme unitaire $P_x \in A[X]$ dont $\sigma(x)$ est aussi racine. Les $\sigma(x)$ sont donc aussi entiers sur A. Parmi les plongements il y a l'identité donc $\nu(x) = x * y$ où $y \in L$ est un produit d'éléments entiers sur A ; y est donc entier sur A. Il en résulte que $y \in B$ et donc $x * y \in \mathfrak{q}$. Comme $x * y \in K$ et $x * y$ entier sur A, $x * y \in A$. Il s'ensuit donc finalement que $x * y \in \mathfrak{p}$. L'idéal $\mathfrak{p}$ est donc non nul donc maximal puisque A est de Dedekind.

iv) Le quotient $A/\mathfrak{p}$ est donc un corps et l'inclusion naturelle $A \subset B$ induit un morphisme injectif $A/\mathfrak{p} \to B/\mathfrak{q}$. Puisque $\mathfrak{q}$ est premier par hypothèse, $B/\mathfrak{q}$ est intègre. Par ailleurs B étant un A-module de type fini (cf. I.4.4.2,) $B/\mathfrak{q}$ est donc une $A/\mathfrak{p}$-algèbre intègre de dimension finie en tant que $A/\mathfrak{p}$-espace vectoriel donc un corps. L'idéal $\mathfrak{q}$ est donc maximal [3].

q.e.d

Exemple I.5.2.7. La proposition précédente permet de construire des exemples d'anneaux de Dedekind :
i) Soit L un corps de nombre (une extension finie de $\mathbb{Q}$, $\mathcal{O}_L$ est la fermeture intégrale de $\mathbb{Z}$ dans L. $\mathcal{O}_L$ est un anneau de Dedekind.

ii) Si L est une extension finie séparable de $k(X)$, la fermeture intégrale de $k[X]$ dans L est un anneau de Dedekind.

Remarque I.5.2.8. Le résultat de la proposition I.5.2.6 reste vrai même si on ne suppose pas l'extension $K \subset L$ séparable mais nous n'aurons pas besoin de cette généralisation.

I.6 . −Limites projectives

I.6.1 . −Généralités

Définition I.6.1.1. Système projectif Soit $\mathbf{C}$ une catégorie (cf. 0.3.1.1,) (ensembles, groupes, anneaux, A-modules etc). Pour $(I, \leq)$ un ensemble ordonné, on appelle *système projectif indexé par I à valeurs dans* $\mathbf{C}$ la donnée :
a) Pour tout $i \in I$, d'un objet $X_i \in \mathrm{Ob}(\mathbf{C})$ (*i.e.*d'un ensemble, groupe, anneau, A-module etc.)
b) Pour tout $(i, j) \in I \times I$ tel que $i \leq j$, d'un morphisme

$$x_{i,j} : X_j \to X_i \in \mathrm{Hom}_{\mathbf{C}}(X_j, X_i)$$

[3] On pourrait utiliser ici le résultat I.4.3.3 mais l'argument est plus facile ici dans la mesure où B est un A-module de type fini donc une A-algèbre finie (cf. I.4.1.3.)

(*i.e.*une application, un morphisme de groupes, un morphisme d'anneaux, un morphisme de A-modules etc.)

Ces données doivent satisfaire :

SysProj$_1$ Pour tout $i \in I$,
$$(x_{i,i} \ : \ X_i \ \to \ X_i) \ = \ \mathrm{Id}_{X_i} \ .$$

SysProj$_2$ Pour tout $(i,j,k) \in I \times I \times I$ tel que $i \leq j \leq k$,
$$x_{i,k} \ = \ x_{i,j} \ \circ \ x_{j,k} \ .$$

Les morphismes $x_{i,j}$,$_{(i,j)\in I\times I, i\leq j}$ sont appelés *morphismes de transition*. On notera
$$\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$$
le système projectif ainsi défini.

Si $\mathbf{C}$ est la catégorie des ensembles (resp. des groupes,) (resp. des anneaux etc,) on parlera de *système projectif d'ensembles* (resp. de *système projectif de groupes*,) (resp. de *système projectif d'anneaux* etc.)

Remarque I.6.1.2. On remarque que, si on muni $(I, \leq)$ de la structure de catégorie $\mathbf{I}$ de l'exemple 0.3.1.3.c,, un système projectif n'est rien d'autre qu'un foncteur covariant (cf. 0.3.2.1) de $\mathbf{I}$ à valeurs dans $\mathbf{C}$.

Définition I.6.1.3. Limite projective Étant donné un système projectif
$$\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$$
indexé par un ensemble ordonné $(I, \leq)$ et à valeurs dans une catégorie $\mathbf{C}$, une *limite projective* pour ce système est la donnée $\left(L, \{l_i \ : \ L \ \to \ X_i\}_{i\in I}\right)$ vérifiant :

LimProj$_1$ L est un objet de $\mathbf{C}$.

LimProj$_2$ Pour tout $i \in I$, $l_i \ : \ L \ \to \ X_i \in \mathrm{Fl}(\mathbf{C})$ est un morphisme de $\mathbf{C}$. Pour tout $(i,j) \in I^2$ tel que $i \leq j$,
$$l_i \ = \ x_{i,j} \ \circ \ l_j \ .$$

LimProj$_3$ Pour tout $\left(M, \{m_i \ : \ M \ \to \ X_i\}_{i\in I}\right)$ (qu'on appellera *diagrammes commutatif à valeurs dans* $\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$,) où M est un objet de $\mathbf{C}$, m_i un morphisme de $\mathbf{C}$ et pour tout $(i,j) \in I^2$ tel que $i \leq j$,
$$m_i \ = \ x_{i,j} \ \circ \ m_j \ ,$$
il existe un unique morphisme $\phi \ : \ M \ \to \ L \in \mathrm{Hom}_{\mathbf{C}}(M, L)$ de $\mathbf{C}$ tel que pour tout $i \in I$,
$$m_i \ = \ l_i \ \circ \ \phi \ .$$

On dira que le diagramme $\big(M, \{m_i \,:\, M \,\to\, X_i\}_{i\in I}\big)$ se *factorise à travers la limite projective*.

Remarque I.6.1.4. On peut réécrire la définition ci-dessus en introduisant la catégorie $\mathbf{X}$ dépendant du système projectif $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ définie de la manière suivante : Les objets de $\mathbf{X}$ sont les $\big(M, \{m_i \,:\, M \,\to\, X_i\}_{i\in I}\big)$ où les m_i sont des morphismes *compatibles aux morphismes de transition* (*i.e.*tels que pour tout $(i,j) \in I^2, i \leq j, m_i \,=\, x_{i,j} \circ m_j$.) En d'autres termes, les objets de $\mathbf{X}$ sont les diagrammes commutatifs à valeurs dans le système projectif $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$. Les flèches de $\mathbf{X}$

$$\phi \,:\, \big(M, \{m_i \,:\, M \,\to\, X_i\}_{i\in I}\big) \,\to\, \big(N, \{n_i \,:\, N \,\to\, X_i\}_{i\in I}\big)$$

de $\mathbf{X}$ sont les morphismes $\phi \,:\, M \,\to\, N \in \mathrm{Hom}_{\mathbf{C}}(M,N)$ de $\mathbf{C}$ tels que pour tout $i \in I$,

$$m_i \,=\, n_i \,\circ\, \phi\,.$$

La limite projective du système $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ est alors un objet final (cf. 0.3.3.1) dans $\mathbf{X}$. Ceci a les conséquence suivantes :

On fixe une catégorie $\mathbf{C}$ dans toute la suite du paragraphe.

Proposition I.6.1.5. *Étant donné un système projectif $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ indexé par un ensemble ordonné $(I, \leq)$ et à valeurs dans $\mathbf{C}$. S'il admet une limite projective, celle-ci est unique à unique isomorphisme près.*

Définition I.6.1.6. On parle alors de *la limite projective* d'un système projectif

$$\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$$

qu'on note

$$\varprojlim_{i\in I} X_i\,.$$

Proposition I.6.1.7. *Étant donné un système projectif $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$, à valeurs dans $\mathbf{C}$, dont on note*

$$\big(L, \{l_i \,:\, L \,\to\, X_i\}_{i\in I}\big) \,:=\, \varprojlim_{i\in I} X_i$$

la limite projective, pour deux morphismes

$$\phi \text{ et } \psi \,:\, M \,\to\, L\,,$$

$\phi \,=\, \psi$ *si et seulement si pour tout* $i \in I$,

$$l_i \,\circ\, \phi \,=\, l_i \,\circ\, \psi\,.$$

Proposition I.6.1.8. *Soient $(I, \leq)$ un ensemble ordonné et $(J, \leq) \,\subset\, (I, \leq)$ un sous-ensemble ordonné par la relation d'ordre induite. Soient*

$$\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big) \text{ et } \big(J, \{Y_i\}_{i\in J}, \{y_{i,j}\}_{(i,j)\in J^2, i\leq j}\big)$$

des systèmes projectifs à valeurs dans $\mathbf{C}$ *respectivement indexés par* I *et* J*. On note*

$$\left(X, \{x_i \, : \, X \, \rightarrow \, X_i\}_{i\in I}\right) \text{ et } \left(Y, \{y_j \, : \, Y \, \rightarrow \, Y_j\}_{j\in J}\right)$$

leurs limites projectives respectives (on suppose qu'elles existent.)

Alors pour tout ensemble de morphismes dans $\mathbf{C}$ $\{u_j \, : \, X_j \, \rightarrow \, Y_j\}_{j\in J}$ *tel que pour tout* $(i,j) \in J^2$, , $i \leq j$, *le carré*

$$\begin{array}{ccc} X_j & \xrightarrow{u_j} & Y_j \\ {\scriptstyle x_{i,;j}}\downarrow & & \downarrow{\scriptstyle y_{i,j}} \\ X_i & \xrightarrow{u_i} & Y_i \end{array}$$

est commutatif, il existe un unique morphisme $u \, : \, X \, \rightarrow \, Y$ *tel que, pour tout* $j \in J$,

$$y_j \, \circ \, u \, = \, u_j \, \circ \, x_j \, .$$

Définition I.6.1.9. Morphisme de systèmes projectifs On pourrait appeler la donnée d'un ensemble $\{u_j \, : \, X_j \, \rightarrow \, Y_j\}_{j\in J}$ comme ci-dessus un *morphisme de systèmes projectifs*. On dira alors que le morphisme $u \, : \, X \, \rightarrow \, Y$ *relève* le moàrphisme de systèmes projectifs.

Preuve de la proposition I.6.1.8 : Remarquons que $\left(X, \{u_j \circ x_j \, : \, X \, \rightarrow \, Y_j\}_{j\in J}\right)$ est un diagramme commutatif à valeurs dans le système projectif $\left(J, \{Y_i\}_{i\in J}, \{y_{i,j}\}_{(i,j)\in J^2, i\leq j}\right)$ et ce grâce à la condition

$$u_i \, \circ \, x_{i,j} \, = \, y_{i,j} \, \circ \, u_j \, \forall (i,j) \in J^2 \, , \, i \leq j \, .$$

L'existence et l'unicité d'un morphisme u factorisant ce diagramme découle alors immédiatement de la propriété I.6.1.3(LimProj$_3$) satisfaite par $\left(Y, \{y_j \, : \, Y \, \rightarrow \, Y_j\}_{j\in J}\right)$. *q.e.d*

Proposition I.6.1.10. *Avec les notations du point ci-dessus et dans le cas où* $I \, = \, J$, *si pour tout* $i \in I$, u_i *est un isomorphisme,* u *est un isomorphisme.*

Preuve : Il suffit de construire un inverse v au morphisme u construit grâce à la proposition I.6.1.8. Or pour tout $i \, \in \, I$, le morphisme $u_i \, : \, X_i \, \rightarrow \, Y_i$ possède, par hypothèse, un inverse $v_i \, : \, Y_i \, \rightarrow \, Y_i$. L'identité

$$u_i \, \circ \, x_{i,j} \, = \, y_{i,j} \, \circ \, u_j$$

implique que

$$u_i \, \circ \, x_{i,j} \, \circ \, v_j \, = \, y_{i,j}$$

ce qui implique encore que

$$x_{i,j} \, \circ \, v_j \, = \, v_i \, \circ \, y_{i,j}$$

ce qui établit l'existence d'un unique morphisme $v \, : \, Y \, \rightarrow \, X$ tel que pour tout $i \in I$,

$$x_i \, \circ \, v \, = \, v_i \, \circ \, y_i \, .$$

Il en résulte que, pour tout $i \in I$,

$$\begin{aligned} x_i \circ v \circ u &= v_i \circ y_i \circ u \\ &= v_i \circ u_i \circ x_i \\ &= x_i \end{aligned}$$

ce qui prouve, en vertu de la proposition I.6.1.7, que $v \circ u = \mathrm{Id}_X$. On prouve de manière exactement analogue que $u \circ v = \mathrm{Id}_Y$ c'est-à-dire que v est l'inverse de u. *q.e.d*

Définition I.6.1.11. On dit qu'on a une *limite projective filtrante* si I est un ensemble partiellement ordonné filtrant supérieurement c'est-à-dire que pour tout i et j dans I il existe $k \in I$ simultanément plus grand que i et j. C'est par exemple le cas de l'ensemble des entiers strictement positifs muni de la relation de divisibilité.

I.6.2 . −Construction de limites projectives dans certaines catégories

Proposition I.6.2.1. *Les limites projectives existent dans la catégorie des ensembles. Explicitement, cela signifie que, pour tout système projectif* $\big(I, \{E_i\}_{i\in I}, \{e_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ *où* $(I, \leq)$ *est un ensemble ordonné, les* $E_{i\ ,i\in I}$ *sont des ensembles, les* $e_{i,j}$ $_{,(i,j)\in I^2, i\leq j}$ *sont des applications, il existe un ensemble* L *et des applications* $l_i : L \to E_{i\ ,i\in I}$ *satisfaisant l'axiome I.6.1.3(LimProj*$_3$*).*

Preuve : Rappelons que, si I est un ensemble et si, pour tout $i \in I$, E_i est un ensemble, le produit cartésien des E_i se note $\prod_{i\in I} E_i$. Un élément x de cet ensemble consiste en la donnée pour tout $i \in I$ d'un élément x_i de E_i ; on écrit $x = (x_i)_{i\in I}$. Pour tout $i \in I$, on a une projection

$$p_i : \prod_{i\in I} E_i \to E_i\ ,\ x = (x_i)_{i\in I} \mapsto x_i\ .$$

La limite projective du système

$$\big(I, \{E_i\}_{i\in I}, \{e_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$$

est alors le sous-ensemble de $\prod_{i\in I} E_i$ formé des $x = (x_i)_{i\in I}$ tels que, pour tout couple i, j d'éléments de I vérifiant $i \leq j$, on a $e_{i,j}(x_j) = x_i$. Les applications $\varprojlim_{i\in I} E_i \to E_{i\ ,i\in I}$ sont les restrictions des p_i. *q.e.d*

Corollaire I.6.2.2. *Les limites projectives existent dans la catégorie des groupes, groupes abéliens, anneaux,* A*-modules etc.*

Preuve : En effet, si $\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ est un système projectif à valeurs dans l'une des catégories ci-dessus, le produit cartésien $\prod_{i\in I} X_i$ hérite de la structure correspondante, les lois de compositions étant définies composante à composante. Les projections

$$p_i : \prod_{i\in I} X_i \to X_{j\ ,j\in I}$$

sont naturellement des morphismes pour la structure correspondante. Il suffit de vérifier que la limite projective au sens des ensembles construite en I.6.2.1, hérite elle aussi de la structure correspondante et satisfait à I.6.1.3(LimProj$_3$). *q.e.d*

Corollaire I.6.2.3. *Soit $\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$ un système projectif à valeurs dans la catégorie des espaces topologiques (cf. 0.2.1.1,) c'est-à-dire que les $X_{i\ ,i\in I}$ sont des espaces topologiques et que les morphismes de transition sont des applications continues. La limite projective de ce système projectif (dans la catégorie des espaces topologiques) est alors la limite projective des ensembles sous-jacents (construite comme en I.6.2.1) muni de la topologie la moins fine telle que les projections $\varprojlim_{i\in I} X_i \ \rightarrow \ X_i$ soient continues c'est-à-dire la topologie engendrée par les images réciproques des ouverts des $X_{i\ ,i\in I}$.*

Exemple I.6.2.4.
i) Soit $(I, \leq)$ un ensemble ordonné tel que la relation d'ordre soit donnée par $i \leq j$ si et seulement si $i = j$. (Ceci revient à dire que la catégorie **I** de l'exemple 0.3.1.3.c a pour seules flèches les identités.) Alors pour un système projectif $\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$, la limite projective est simplement le produit cartésien.
ii) Soit $f \ : \ P \ \rightarrow \ Q$ un morphisme de A-modules. Notons

$$I \ := \ \{0; P; Q\}$$

muni de la relation d'ordre

$$Q \leq P \leq 0 \, .$$

On définit alors un système projectif de A-modules indexé par I $\left(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$ par :

$$X_0 \ := \ 0 \, , \ X_P \ := \ P \, , \ X_Q \ := \ Q$$

et

$$x_{P,0} \ := \ 0 \, , \ x_{Q,P} \ := \ f$$

ce qui implique que nécessairement

$$x_{Q,0} \ = \ f \ \circ \ 0 \ = \ 0 \, .$$

On vérifie alors que le noyau de f (cf. I.1.1.14) est la limite projective de ce système.

I.6.3 . −Limites projectives de A-modules

Dans ce paragraphe, A est un anneau.

Proposition I.6.3.1. *Soient $(I, \leq)$ un ensemble ordonné et*

$$\left(I, \{P_i\}_{i\in I}, \{p_{i,j}\}_{(i,j)\in I^2, i\leq j}\right) \, , \ \left(I, \{Q_i\}_{i\in I}, \{q_{i,j}\}_{(i,j)\in I^2, i\leq j}\right) \, , \ \left(I, \{R_i\}_{i\in I}, \{r_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$$

des systèmes projectifs de A-modules indexés par I. On note

$$\left(L, \{l_i \ : \ L \ \rightarrow \ P_i\}_{i\in I}\right) \, , \ \left(M, \{m_i \ : \ M \ \rightarrow \ Q_i\}_{i\in I}\right)$$

et $\big(N, \{n_i \,:\, N \,\to\, R_i\}_{i\in I}\big)$ *leurs limites projectives respectives.*

On suppose que, pour tout $(i,j) \in I^2$, $i \leq j$, *on a un diagramme commutatif de* A*-modules :*

$$\begin{array}{ccccccc} 0 \to & P_j & \xrightarrow{f_j} & Q_j & \xrightarrow{g_j} & R_j & \\ & {\scriptstyle p_{i,j}}\downarrow & & \downarrow{\scriptstyle q_{i,j}} & & \downarrow{\scriptstyle r_{i,j}} & \\ 0 \to & P_i & \xrightarrow{f_i} & Q_i & \xrightarrow{g_i} & R_i\,. & \end{array} \qquad \textit{I.6.3.2}$$

Alors la flèche $f \,:\, L \,\to\, M$ *(resp.* $g \,:\, M \,\to\, N$*) déduite des* $f_{i\,,i\in I}$ *(resp.* $g_{i\,,i\in I}$*) grâce à la proposition I.6.1.8 est telle que la suite*

$$0 \,\to\, L \xrightarrow{f} M \longrightarrow \xrightarrow{g} N$$

est exacte.

Preuve : Prouver que la suite ci-dessus est exacte revient à prouver (cf. I.1.1.19,) que $(L, f) = \mathrm{Ker}\, g$. On va pour cela utiliser la caractérisation du noyau donnée en I.1.1.15.i.

Tout d'abord, pour tout $i \in I$,

$$\begin{aligned} n_i \circ g \circ f \;&= g_i \circ m_i \circ f \\ &= \quad g_i \circ f_i \circ l_i \\ &= \quad 0 \end{aligned}$$

c'est-à-dire, en vertu de I.6.1.7, que $g \circ f \,=\, 0$.

Soit donc $h \,:\, X \,\to\, M$ tel que $g \circ h \,=\, 0$. Alors, pour tout $i \in I$, $n_i \,\circ\, g \,\circ\, h \,=\, 0$ c'est-à-dire, d'après I.6.1.8, que $g_i \,\circ\, m_i \,\circ\, h \,=\, 0$. Il existe donc un unique morphisme de A-modules $x_i \,:\, X \,\to\, P_i$ tel que $m_i \,\circ\, h \,=\, f_i \,\circ\, x_i$. Par unicité des x_i et commutativité du diagramme I.6.3.2, pour tout $(i,j) \in I^2$, $i \leq j$, $x_i \,=\, p_{i,j} \circ x_j$ c'est-à-dire que $\big(X, \{x_i \,:\, X \,\to\, P_i\}_{i\in I}\big)$ est un diagramme commutatif à valeurs dans le système projectif $\big(I, \{P_i\}_{i\in I}, \{p_{i,j}\}_{(i,j)\in I^2, i\leq j}\big)$ (cf. I.6.1.3.) Il résulte donc de I.6.1.3(LimProj$_3$) qu'il existe un unique morphisme $x \,:\, X \,\to\, L$ tel que, pour tout $i \in I$, $l_i \,\circ\, x \,=\, x_i$.

Il s'ensuit que, pour tout $i \in I$,

$$\begin{aligned} m_i \circ h \;&=\; f_i \circ x_i \\ &=\; f_i \circ l_i \circ x \\ &=\; m_i \circ f \circ x \end{aligned}$$

c'est-à-dire, en vertu de la proposition I.6.1.7 que

$$h \,=\, f \,\circ\, x\,.$$

Si

$$x \,\text{et}\, y \,:\, X \,\to\, L$$

sont deux morphismes vérifiant

$$h \,=\, f \,\circ\, x \,=\, f \,\circ\, y\,,$$

pour tout $i \in I$,

$$\begin{aligned} f_i \circ l_i \circ x &= m_i \circ f \circ x \\ &= m_i \circ f \circ y \\ &= f_i \circ l_i \circ y \ . \end{aligned}$$

Comme, pour tout $i \in I$, f_i est injectif, il en résulte que $l_i \circ x = l_i \circ y$ ce qui prouve, une fois encore grâce à I.6.1.7, que $x = y$. *q.e.d*

Remarque I.6.3.3.
i) Il faut prendre garde qu'on n'aura pas en général de résultat similaire avec un 0 à droite dans la suite exacte.

ii) On pourrait en fait tirer le résultat de la proposition I.6.3.1 d'un résultat plus général basé sur le fait que le noyau lui-même apparaît comme une limite projective (cf. I.6.2.4.ii.) On se bornera à mentionner un autre avatar de cet énoncé plus général :

Soient $\left(I, \{E_i^\alpha\}_{i\in I}, \{e_{i,j}^\alpha\}_{(i,j)\in I^2, i\leq j}\right)$ des systèmes projectifs indexés par un ensemble ordonné $(I, \leq)$, $\alpha \in A$ où A est un ensemble. On suppose que pour tout $\alpha \in A$, le système projectif $\left(I, \{E_i^\alpha\}_{i\in I}, \{e_{i,j}^\alpha\}_{(i,j)\in I^2, i\leq j}\right)$ admet une limite projective E^α. Notons

$$Q := \prod_{\alpha\in A} E^\alpha$$

et pour tout $i \in I$,

$$P_i := \prod_{\alpha\in A} E_i^\alpha \ .$$

Les morphismes de transition $e_{i,j}^\alpha$ permettent de définir naturellement des morphismes

$$p_{i,j} : P_j \to P_i$$

de sorte que $\left(I, \{P_i\}_{i\in I}, \{p_{i,j}\}_{(i,j)\in I^2, i\leq j}\right)$ est un système projectif dont on note P la limite projective (dont on suppose qu'elle existe.) On peut alors construire des applications naturelles $P \to Q$ et $Q \to P$ dont on montre qu'elles sont inverses l'une de l'autre.

En d'autres termes moins précis, la limite projective commute au produit cartésien qui est lui-même une limite projective (cf. I.6.2.4.i.)

On pourrait même constater que le fait que la limite projective dans les catégories de groupes, anneaux etc a pour ensemble sous-jacent la limite projective des ensembles sous-jacents est encore un résultat du même ordre.

II . −Corps Locaux

II.1 . −Valeurs absolues et valuations

II.1.1 . −Valeur absolue

Soit K un corps.

Définition II.1.1.1. Valeur absolue sur un corps Une *valeur absolue* sur K est une application $|\cdot| : K \to \mathbb{R}$ (ou même éventuellement à valeurs dans $\mathbb{Q}$) telle que pour tout couple (x, y) d'éléments de K :

ABS$_1$
$$|x| \geq 0 \, ;$$

ABS$_2$
$$|x| = 0 \Leftrightarrow x = 0 \, ;$$

ABS$_3$
$$|xy| = |x|.|y| \, ;$$

ABS$_4$
$$|x + y| \leq |x| + |y| \, .$$

Proposition II.1.1.2. *Si $|\cdot|$ est une valeur absolue sur K, l'application*

$$K \times K \to \mathbb{R}^+ \, , \, (x, y) \mapsto |y - x|$$

est une distance sur K (cf. 0.2.2.1.)

Définition II.1.1.3. Si $|\cdot|$ est une valeur absolue sur K, on dira que $(K, |\cdot|)$ est un espace métrique, la distance étant celle donnée par la proposition ci-dessus. On rappelle que c'est alors un espace topologique séparé (cf. 0.2.1.4.)

Définition II.1.1.4. Valeurs absolues équivalentes Deux valeurs absolues sur K sont *équivalentes* si elles définissent la même topologie sur K.

Définition II.1.1.5. Valeur absolue triviale La *valeur absolue triviale* est la valeur absolue telle que pour tout $x \neq 0$, $|x| = 1$.

Lemme II.1.1.6. *Une valeur absolue $|\cdot|$ sur K est la valeur absolue triviale si et seulement si la topologie qu'elle définie est la topologie discrète (cf. 0.2.1.3.)*

Corollaire II.1.1.7. *Toute valeur absolue équivalente à la valeur absolue triviale est la valeur absolue triviale elle-même.*

Théorème II.1.1.8. *Deux valeurs absolues $|\bullet|_1$ et $|\bullet|_2$ sont équivalentes si et seulement s'il existe un nombre réel $c > 0$ tel que,*

$$\forall x \in K \, , \, |x|_1 = |x|_2^c \, .$$

Preuve : S'il existe $c > 0$ tel que $|x|_1 = |x|_2^c$ pour tout $x \in K$, les topologie sont clairement équivalentes.

Réciproquement, supposons données deux valeurs absolues équivalentes $|\bullet|_1$ et $|\bullet|_2$. On peut supposer qu'elles ne sont pas triviales. Il existe $y \in K$, tel que $|y|_1 > 1$.

Pour tout $x \in K$ et tout $i \in \{1;2\}$, $|x|_i < 1$ équivaut à ce que la suite x^n tende vers 0 au sens de la topologie i. En conséquence, $|x|_1 < 1$ équivaut à $|x|_2 < 1$. On a également $|x|_1 > 1$ équivalent à $|x|_2 > 1$ et finalement $|x|_1 = 1$ équivalent à $|x|_2 = 1$.

Il existe donc $y \in K$ tel que $|y|_1 = a > 1$ et $|y|_2 = b > 1$.

Pour tout $x \in K$ tel que $|x|_i \geq 1$, il existe $\alpha \geq 0$ (resp. $\beta \geq 0$,) tel que

$$|x|_1 \ = \ a^\alpha \ (\text{resp. } |x|_2 \ = \ b^\beta \ .)$$

Si $\alpha \ = \ \beta$, il existe un $c > 0$ tel que $a \ = \ b^c$, ce qui entraîne que pour tout α, $a^\alpha \ = \ (b^\alpha)^c$.

Montrons donc finalement que $\alpha \ = \ \beta$: Pour tout couple d'entiers (m, n) tel que $\frac{m}{n} \geq \alpha$, et tout $x \in K$ tel que $|x|_1 \ = \ a^\alpha$,

$$|x|_1 \ = \ a^\alpha \ \leq \ a^{\frac{m}{n}} \ ,$$

ce qui implique que $|x|_1^n \leq a^m$ c'est-à-dire que $|x|_1^n \leq |y|_1^m$ ou encore

$$|\frac{x^n}{y^m}|_1 \leq 1 \ \Leftrightarrow \ |\frac{x^n}{y^m}|_2 \leq 1$$

c'est-à-dire encore

$$|x|_2^n \leq |y|_2^m$$

ou encore

$$|x|_2 \leq |y|_2^{\frac{m}{n}}$$

c'est-à-dire finalement

$$b^\beta \leq b^{\frac{m}{n}}$$

d'où il découle, par densité de $\mathbb{Q}$ dans $\mathbb{R}$ que $\beta \leq \alpha$. Par symétrie de l'argument, on obtiendrait de même que $\alpha \leq \beta$ et finalement l'égalité. ***q.e.d***

Définition II.1.1.9. Valeur absolue ultramétrique Une valeur absolue $|\cdot|$ sur un corps K, est *ultramétrique* (ou vérifie l'*inégalité ultramétrique* si pour tout couple (x, y) d'éléments de K

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

On dira aussi que la distance associée est *ultramétrique* et que la topologie associée est *ultramétrique*, ce qui est justifié par le lemme :

Lemme II.1.1.10. *Étant données deux valeurs absolues équivalentes, l'une est ultramétrique si et seulement si l'autre l'est.*

Définition II.1.1.11. Prolongement Si $K \subset L$ est une extension de corps, on dira qu'une valeur absolue $|\cdot|_L$ sur L *prolonge* une valeur absolue $|\cdot|_K$ sur K, si

$$(|\cdot|_L)_{|K} = \ |\cdot|_K \ .$$

II.1.2 . −Valuations

Définition II.1.2.1. Étant un groupe totalement ordonné $(G, +, \leq)$ (par exemple $(\mathbb{R}, +, \leq)$ ou $(\mathbb{Q}, +, \leq)$) on prolonge la relation d'ordre et l'addition sur G à l'ensemble $G \cup \{+\infty\}$ en posant

$$a \leq +\infty \text{ et } a + (+\infty) = +\infty \, \forall a \in G \, .$$

Définition II.1.2.2. Valuation Une *valuation à valeurs réelles,* sur un anneau A est une application $v : A \to \mathbb{R} \cup \{+\infty\}$ telle que pour tout couple (a, b) d'éléments de A,

VAL_1

$$v(a) = +\infty \Leftrightarrow a = 0 \, ;$$

VAL_2

$$v(ab) = v(a) + v(b) \, ;$$

VAL_3

$$v(a + b) \geq \min(v(a), v(b)) \, .$$

On dira que (A, v) est un *anneau à valuation.*

Lemme II.1.2.3. *Si (A, v) est un anneau à valuation A est intègre. Il a un corps des fractions K auquel la valuation v s'étend naturellement par la formule*

$$v(\frac{a}{s}) := v(a) - v(s) \, .$$

Lemme II.1.2.4. *Pour x et y des éléments de K, si $v(x) \neq v(y)$, $(vx + y) = \min(v(x), v(y))$.*

Preuve : Posons $z := x + y$. Supposons $v(x) < v(y)$. Si l'on suppose $v(z) > v(x)$, on aurait aussi $x = z - y$ ce qui imposerait $v(x) \geq v(z)$ et $v(x) \geq v(y)$ ce qui est contradictoire. *q.e.d*

Définition II.1.2.5. Corps valué On dira usuellement qu'un corps muni d'une valuation est un *corps valué.*

Définition II.1.2.6. Si $K \subset L$ est une extension de corps et K est muni d'une valuation v, on dit qu'une valuation w sur L *prolonge* v sir $w_{|K} = v$.

Proposition II.1.2.7. *Si K est un corps muni d'une valuation v, l'ensemble*

$$\mathcal{O}_K := \{x \in K \mid v(x) \geq 0\}$$

est un anneau de valuation (cf. I.3.3.3,) donc en particulier local (cf. I.3.3.4,) dont le corps des fractions est K et l'idéal maximal

$$\mathfrak{m}_K := \{x \in K \mid v(x) > 0\} \, .$$

Définition II.1.2.8. Pour un corps K muni d'une valuation v, l'anneau $\mathcal{O}_K$ défini ci-dessus s'appelle l'*anneau de la valuation*. On parlera indiféremment de l'*idéal maximal de* K ou de $\mathcal{O}_K$ et du *corps résiduel de* K ou de $\mathcal{O}_K$ (cf. I.3.3.1.)

Remarque II.1.2.9. Si $\mathcal{O}$ est un anneau de valuation (cf. I.3.3.3,) on peut montrer qu'il existe une valuation sur $\mathcal{O}$ qui s'étend à son corps des fractions et telle que $\mathcal{O}$ soit l'anneau de la valuation mais nous n'aurons en fait besoin de cette correspondance que dans le cas des anneaux de valuations discrète (cf. I.5.1.3,) pour lesquels nous allons donner d »d'autres caractérisations au paragraphe II.1.3.

Proposition II.1.2.10. *Soit K un corps.*
i) Un nombre réel $0 < \gamma < 1$ étant fixé, l'application qui à toute valuation v sur K associe l'application

$$x \mapsto |x| := \gamma^{v(x)}$$

est une bijection de l'ensemble des valuations de K dans l'ensemble des valeurs absolues ultramétriques sur K (cf. II.1.1.9.)

ii) Pour une valuation v fixée sur K, des réels

$$0 < \gamma_1 \leq \gamma_2 < 1$$

les valeurs absolues $\gamma_1^{v(\cdot)}$ et $\gamma_2^{v(\cdot)}$ sont équivalentes (cf. II.1.1.4.)

Définition II.1.2.11. Étant donnée une valuation v sur un corps K, on peut donc, grâce au point II.1.2.10.ii ci-dessus, de la *topologie définie par la valuation* sur K.

Définition II.1.2.12. On dira donc que deux valuations sont *équivalentes* si elles définissent la même topologie ou, ce qui revient au même si elle définissent des valeurs absolues équivalentes (cf. II.1.1.4.)

Proposition II.1.2.13. *Deux valuations à valeurs réelles v_1 et v_2 sur un corps K sont équivalentes si et seulement s'il existe un nombre réel $c > 0$ tel que*

$$v_1 = cv_2 .$$

Corollaire II.1.2.14. *Étant données deux valuations équivalentes v_1 et v_2 sur un corps K, l'anneau de v_1 est égal à l'anneau de v_2 (cf. II.1.2.8) et est la boule fermée de rayon 1 et de centre 0 (cf. 0.2.2.2) de l'espace métrique $(K, |\cdot|)$ pour n'importe quelle valeur absolue associée à v_1 ou à v_2.*

II.1.3 . −Valuations discrètes et anneaux de valuation discrète

Définition II.1.3.1. Valuation discrète Une valuation v sur un corps K est *discrète* si $v(K^\times)$ est un sous-groupe discret de $\mathbb{R}$ alors égal à $c\mathbb{Z}$.

Si $c = 1$ on dit que la valuation est *normalisée*.

Proposition II.1.3.2. *Étant donnée une valuation discrète sur un corps K, il existe toujours une valuation discrète normalisée qui lui est équivalente (cf. II.1.2.12.)*

Théorème II.1.3.3.
i) Si K est un corps muni d'une valuation discrète, alors l'anneau de la valuation $\mathcal{O}_K$ (cf. II.1.2.8) est un anneau de valuation discrète (cf. I.5.1.3.)

ii) Réciproquement, étant donné un anneau de valuation discrète A, et K son corps des fractions, il existe une unique valuation discrète normalisée sur K tel que A soit l'anneau de la valuation.

Preuve :
i) On sait déjà que $\mathcal{O}_K$ est intègre (comme sous-anneau de K,) et local (cf. II.1.2.7.)

La seul chose à montrer c'est que tout idéal est principal. On peut supposer la valuation normalisée (cf. II.1.2.14.)

Soit π un élément de valuation 1. Étant donné un idéal $\mathfrak{I} \subset \mathcal{O}_K$, on choisit un élément $x \in \mathfrak{I}$ de valuation minimal n. Il en résulte que $v(\frac{x}{\pi^n}) = 0$ et donc $\frac{x}{\pi^n}$ est inversible dans $\mathcal{O}_K$. On a donc $\mathfrak{I} = \pi^n \mathcal{O}_K$..

ii) Il suffit d'utiliser la caractérisation I.5.1.2.d et de poser $v(x)$ l'unique entier n tel que $Ax = A\pi^n$. On vérifie aisément qu'on définit ainsi une valuation.

q.e.d

Définition II.1.3.4. Pour K un corps muni d'une valuation discrète normalisée, v on appelle *uniformisante* de K relativement à v (ou de l'anneau $\mathcal{O}_K$ de la valuation) un élément de valuation 1 ou ce qui revient au même un générateur de l'idéal maximal $\mathfrak{m}_K$ de $\mathcal{O}_K$.

II.1.4 . −Topologie p-adique sur $\mathbb{Q}$

Soit p un nombre premier.

Lemme II.1.4.1. *Pour tout $q \in \mathbb{Q}^*$, il existe un unique triplet $(v_p(q), n(q), d(q) \in \mathbb{Z} \times \mathbb{Z}^* \times \mathbb{N}^*$ tel que*

$$q = p^{v_p(q)} \frac{n(q)}{d(q)},$$

$n(q)$ et $d(q)$ sont premiers entre eux et p ne divise ni $n(q)$ ni $d(q)$. En posant $v_p(0) := +\infty$, v_p devient une valuation discrète (cf. II.1.3.1.)

Définition II.1.4.2. On appelle la valuation v_p définie ci-dessus la *valuation p-adique*.

Il en résulte qu'un nombre réel $c > 1$ étant fixé,

$$|q|_p := c^{-v_p(q)} \, \forall q \in \mathbb{Q}\,,$$

est une valeur absolue ultramétrique (cf. II.1.1.9,) sur $\mathbb{Q}$ appelée *valeur absolue p-adique*.

On dit encore que la valeur absolue p-adique est *non archimédienne*.

La topologie définie par la valeurs absolue p-adique est appelée *topologie p-adique*.

Proposition II.1.4.3. *L'anneau de la valuation v_p sur $\mathbb{Q}$ est le localisé $\mathbb{Z}_{(p)}$ (cf. I.3.3.7) de $\mathbb{Z}$ en l'idéal (p).*

Lemme II.1.4.4. *Si p et ℓ sont deux nombres premiers distincts, la suite $(p_n^n)_{n\in\mathbb{N}}$ tend vers 0 pour la topologie p-adique mais pas pour la topologie ℓ-adique. Ces deux topologies ne sont donc pas équivalentes.*

Remarque II.1.4.5. Le *théorème d'Ostrowski* établit qu'une valeur absolue sur $\mathbb{Q}$ est soit équivalente à l'une des valeurs absolues p-adiques soit à la valeur absolue archimédienne

$$q \mapsto \max(q, -q) .$$

II.2 . −Corps valués

Dans cette section (K, v) est un corps valué (cf. II.1.2.5,) $\mathcal{O}_K$ est l'anneau de la valuation (cf. II.1.2.8,) $\mathfrak{m}_K$ son idéal maximal et $k := \mathcal{O}_K/\mathfrak{m}_K$ son corps résiduel (cf. I.3.3.1.)

Pour tout polynôme $P \in \mathcal{O}_K[X]$, on note $\tilde{P}$ son image dans $k[X]$.

II.2.1 . −Valuations et polynômes

Proposition II.2.1.1. *Soient $R := K[X]$ l'anneau des polynômes à une indéterminée sur K et $w : R \to \mathbb{R} \cup \{+\infty\}$ définie par $w(0) = +\infty$ et pour $P := \sum_{i=0}^{d} a_i X^i$, quelconque $w(P) := \min(v(a_i))$.*

Alors w est une valuation de R (cf. II.1.2.2.)

Preuve : La seule chose qui ne soit pas formelle à démontrer concernant w est

$$w(PQ) = w(P) + w(Q) \, \forall P \in R \, , \, \forall Q \in R \, .$$

Fixons les notations $P := \sum_{i=0}^{d} a_i X^i$, $Q := \sum_{i=0}^{e} b_i X^i$ et $PQ := \sum_{i=0}^{d+e} c_i X^i$.

On a alors $c_k = \sum_{i+j=k} a_i b_j$. On en déduit que

$$v(c_k) \geq v(a_i) + v(b_j) \geq w(P) + w(Q) \, .$$

Il existe un plus grand $0 \leq m \leq d$ (resp. $0 \leq n \leq e$) tel que $v(a_m) = w(P)$ (resp. $(v(b_n) = w(Q)$.)

On écrit alors

$$c_{m+n} = a_m b_n + \sum_{i=0}^{m-1} a_i b_{m+n-i} + \sum_{i=0}^{n-1} a_{m+n-i} b_i \, .$$

Dans cette somme, les deux derniers termes sont de valuation strictement supérieure à $w(P) + w(Q)$ alors que l'on a exactement $v(a_m b_n) = w(P) + w(Q)$. On obtient grâce au lemme II.1.2.4 que

$$v(c_{m+n}) \ = \ w(P) \ + \ w(Q) \, .$$

Ceci, combiné avec la minoration obtenue ci-dessus achève la preuve. *q.e.d*

Corollaire II.2.1.2. *Soit*

$$P \ := \ \sum_{i=0}^{d} a_i X^i \ \in \ \mathcal{O}_K[X]$$

un polynôme.
i) Si P n'est pas irréductible sur K alors P n'est pas irréductible sur $\mathcal{O}_K$.
ii) Si $v(a_d) = 0$ et P est irréductible sur k alors P est irréductible sur $\mathcal{O}_K$.

Preuve :
i) Si P n'est pas irréductible sur K, on peut écrire $P = QR$, avec $\deg(Q) > 0$ et $\deg(R) > 0$. Posons $\alpha \ := \ w(P) \geq 0$. Il existe un élément $a \in \mathcal{O}_K$ tel que $v(a) = \alpha$. Posons ensuite $\beta \ := \ w(Q)$ et $\gamma \ := \ w(R)$. Il existe des éléments b et c de $\mathcal{O}_K$ de valuations respectives β et γ. Et l'on a encore grâce à la proposition II.2.1.1 $\alpha \ = \ \beta + \gamma$. En posant $Q' \ := \ \frac{1}{b} Q$ et $R' \ := \ bR$, on obtient $w(Q') = 0$ et $w(R') = \beta + \gamma = \alpha \geq 0$. En d'autres termes Q' et R' sont dans $\mathcal{O}_K[X]$ et l'on a toujours $P \ = \ Q'R'$.

ii) C'est la démonstration standard du critère d'Eisenstein.

q.e.d

Remarque II.2.1.3. Il existe des polynômes P à coefficients dans $\mathbb{Z}$ unitaires, irréductibles et tels qu'il existe p, tel que leur image dans $\mathbb{F}_p[X]$ n'est pas irréductible. Par exemple $P = X^4 + 1$. P est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$, Si $p = 2$, $X^4 + 1 = (x+1)^4$. Les racines de P sont contenues dans la plus petite extension de $\mathbb{F}_p$ contenant des racines huitièmes de l'unité. Or le corps $\mathbb{F}_{p^2}$, contient les racines huitièmes de l'unité (c'est une conséquence immédiate du fait que le groupe multiplicatif d'un corps est un groupe cyclique et que $8 | p^2 - 1$.)

Soit la racine est dans $\mathbb{F}_p$ est un facteur de degré 1 divise $X^4 + 1$ soit dans $\mathbb{F}_{p^2}$ et là on a un polynôme de degré 2 qui divise $X^4 + 1$.

II.2.2 . −Approximations

Dans ce paragraphe, on suppose que K est complet (cf. 0.2.2.6,) pour une valeur absolue associée à sa valuation v (cf. II.1.2.10.) À noter qu'il l'est lors pour n'importe laquelle d'entre elles.

Lemme II.2.2.1. *L'anneau $\mathcal{O}_K$ est alors complet pour la métrique induite par celle de K.*

Preuve : On rappelle que $\mathcal{O}_K$ s'identifie à la boule unité fermée de K (cf. II.1.2.14) et est donc fermé dans un espace complet donc complet. *q.e.d*

Proposition II.2.2.2. Un cas particulier du lemme d'Hensel *Soit P un polynôme à coefficients dans $\mathcal{O}_K$. On note $\tilde{P}$ l'image de P dans $k[X]$ et a une racine simple de $\tilde{P}$.*

Alors il existe $\alpha \in \mathcal{O}_K$ unique vérifiant α relève a et $P(\alpha) = 0$.

Preuve :

i) Pour démontrer l'existence, on choisit α_0 un relèvement arbitraire de a dans $\mathcal{O}_K$.

Si $P(\alpha_0) = 0$ α_0 répond à la question.

Sinon $v(P(\alpha_0)) = r$ est un nombre réel strictement positif, puisque $P(\alpha_0) \in \mathfrak{m}_K$.

On cherche à construire une suite $(\alpha_n)_{n\in\mathbb{N}}$ convergeant vers une racine de P. Il suffit de construire α_n telle que $v(P(\alpha_n)) \geq r(n+1)$ et $v(\alpha_{n+1} - \alpha_n) \geq nr$.

Choisissons $\gamma \in \mathcal{O}_K$ tel que $v(\gamma) = r$. Supposons les n premiers termes de la suite construits et cherchons α_n sous la forme $\alpha_{n-1} + \gamma^n x$.

En remarquant que pour tout $s \leq n$,

$$\prod_{i=0}^{s+1} (n-i) \;=\; s! C_n^s$$

on montre que pour tout anneau A et tout polynôme $Q \in A[X]$, la quantité $Q^{[s]} := \frac{Q^{(s)}}{s!}$ est toujours un élément de $A[X]$. On peut, par conséquent, écrire une formule de Taylor :

$$Q(u+v) \;=\; \sum_{s=0}^{+\infty} Q^{[s]}(u) v^s \,.$$

On écrit alors

$$P(\alpha_n) \;=\; P(\alpha_{n-1} + \gamma^n x) \;=\; P(\alpha_{n-1}) \;+\; P'(\alpha_{n-1})\gamma^n x \;+\; C\gamma^{2n} \,.$$

On constate que

$$P'(\alpha_{n-1}) \;\equiv\; P'(\alpha_0)\ [\mathfrak{m}_K]$$

et donc que $P'(\alpha_{n-1})$ est inversible dans $\mathcal{O}_K$. Puisque, par hypothèse de récurrence,

$$v(P(\alpha_{n-1})) \;\geq\; nr,$$

on peut trouver $x \in \mathcal{O}_K$ tel que :

$$P(\alpha_{n-1}) \;+\; P'(\alpha_{n-1})\gamma^n x \;=\; 0 \,.$$

Reste à constater, ce qui est immédiat, que $\alpha_n := \alpha_{n-1} + \gamma^n x$ répond à la question.

ii) Pour prouver l'unicité, considérons α et β deux solutions, et notons $\gamma := \beta - \alpha$. En écrivant la formule de Taylor

$$0 \;=\; P(\beta) \;=\; P(\alpha) + \gamma P'(\alpha) + \gamma^2 R$$

avec $R \in \mathcal{O}_K$ d'où l'on tire que soit $v(\gamma) = 0$ ce qui est impossible puisque $\gamma \in \mathfrak{m}_K$, soit $v(\gamma) > v(\gamma)$ c'est-à-dire que $\gamma = 0$.

q.e.d

Proposition II.2.2.3. *Soit $P \in \mathcal{O}_K[X]$ un polynôme unitaire. S'il existe des polynômes unitaires $\chi, \rho \in k[X]$ premiers entre eux tels que $\tilde{P} = \chi\rho$, il existe un et un seul couple de polynômes unitaires $(Q, R) \in \mathcal{O}_K[X]$ tel que $P = QR$, $\tilde{Q}_1 = \chi$ et $\tilde{R} = \rho$.*

Preuve : On va construire de proche en proche des polynômes unitaires Q_n et R_n relevant χ et ρ et tels que $Q_n R_n \equiv P\ [\mathfrak{m}_K^n]$. Pour tout Q_1 et R_1 unitaires relevant respectivement χ et ρ, $Q_1 R_1 \equiv P\ [\mathfrak{m}_K]$. Pour $n \geq 1$, supposons construits les suites Q_s et R_s pour $s \leq n$. On suppose que $\deg(Q_s) = \deg(\chi)$, $\deg(R_s) = \deg(\rho)$ et $Q_s R_s \equiv P\ [\mathfrak{m}_K^s]$.

Si π désigne une uniformisante de K, il existe $S_n \in \mathcal{O}_K[X]$ tel que

$$P = Q_n R_n + \pi^n S_n .$$

L'unitarité de P, Q_n, R_n impose que $\deg(S_n) \leq \deg(P)$.

Cherchons $Q_{n+1} := Q_n + \pi^n A_n$ et $R_{n+1} := R_n + \pi^n B_n$. Alors nécessairement $P \equiv Q_{n+1} R_{n+1}\ [\mathfrak{m}_K^{n+1}]$ implique que

$$P \equiv Q_n R_n + (A_n R_n + B_n Q_n)\pi^n + A_n B_n \pi^{2n}\ [\mathfrak{m}_K^{n+1}] .$$

Il suffirait, pour cela, que

$$A_n R_n + B_n Q_n - S_n \equiv 0\ [\mathfrak{m}_K] .$$

Notons $\tilde{S}_n$ l'image de S_n dans $k[X]$, u et v des coefficients de Bézout pour χ et ρ c'est-à-dire que $u\chi + v\rho = 1$. Il en résulte que $\tilde{S}u\chi + \tilde{S}v\rho = \tilde{S}$. Pour tout relèvement A_n (resp. B_n) de $\tilde{S}v$ (resp. $\tilde{S}u,$) on a bien entendu $B_n Q_n + A_n R_n - S_n \equiv 0\ [\mathfrak{m}_K]$.

On rappelle qu'on sait, par des résultats élémentaires sur les équations de congruence, qu'étant donnée une solution (u_0, v_0) tel que $u_0\chi + v_0\rho = 1$, l'ensemble des (u, v) solutions de l'équation de Bézout est l'ensemble

$$\{(u_0 + z\rho, v_0 - z\chi)\ ,\ z \in k[X]\} .$$

On peut alors choisir u tel que $\deg(u) < \deg(\rho)$. On a alors $v\rho = 1 - u\chi$ ce qui implique

$$\deg(v) + \deg(\rho) \leq \deg(u) + \deg(\chi) < \deg(\rho) + \deg(\chi) = \deg(\tilde{P})$$

ce qui implique $\deg(v) < \deg(\chi)$.

On peut donc trouver A_n et B_n tels que

$$\deg(A_n) = \deg(v) + \deg(\tilde{S}) < \deg(\chi) + \deg(S_n) < \deg(\chi) + \deg(\tilde{P})$$

et de même, $\deg(B_n) < \deg(\rho) + \deg(\tilde{P})$. Ainsi la majoration sur les degrés passe du cran n au cran $n+1$ c'est-à-dire que les degrés des suites Q_n et R_n sont majorés indépendemment de n et donc que ces suites convergent vers des polynômes Q et R respectivement, qui répondent à la question. *q.e.d*

II.3 . −Extensions finies des corps locaux

II.3.1 . −Extensions de valuations

Proposition II.3.1.1. *Soit A un anneau de Dedekind (cf. I.5.2.2,) de corps des fractions K.*
i) Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, il existe une unique valuation discrète normalisée (cf. II.1.3.1,) $v_\mathfrak{p}$ sur K telle que $A_\mathfrak{p}$ soit l'anneau de la valuation.

On construit ainsi une application de l'ensemble des idéaux maximaux de A dans l'ensemble des valuations discrètes normalisées de K, telles que A est contenu dans l'anneau de la valuation.

ii) Réciproquement, étant donnée une valuation discrète normalisée v sur K dont l'anneau de la valuation

$$\mathcal{O}_v \ := \ \{x \in K \mid v(x) \geq 0\}$$

(cf. II.1.2.8,) contient A, notons

$$\mathfrak{m}_v \ := \ \{x \in K \mid v(x) > 0\}$$

l'idéal maximal de $\mathcal{O}_v$. Alors $\mathfrak{m}_v \ \cap \ A$ est un idéal maximal de A.

iii) Les applications

$$\mathfrak{p} \ \mapsto \ v_\mathfrak{p} \text{ et } v \ \mapsto \ \mathfrak{m}_v \cap A$$

sont inverses l'une de l'autre ; il en résulte que l'application $\mathfrak{p} \mapsto v_\mathfrak{p}$ est une bijection de $\mathrm{Spm}(A)$ dans l'ensemble des valuations discrètes normalisées sur K dont l'anneau contient A.

Preuve :
i) Pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, il résulte du théorème I.5.2.1 que $A_\mathfrak{p}$ est un anneau de valuation discrète de corps des fractions K. L'existence et l'unicité de $v_\mathfrak{p}$ (répondant à la question) sont alors assurées par la proposition II.1.3.2.

ii) Il est clair que $\mathfrak{m}_v \cap A$ est un idéal premier de A. On laisse le soin au lecteur de vérifier qu'il est non nul ; d'où il résulte, puisque A est un anneau de Dedekind, qu'il est maximal.

i) Laissé en exercice.

q.e.d

Théorème II.3.1.2. *Soit K un corps complet (cf. 0.2.2.6) pour une valuation discrète v (c'est-à-dire pour une valeur absolue qui lui est associée.) Notons v_K l'unique valuation discrète normalisée équivalente à v (cf. II.1.3.2.)*

Soit $K \subset L$ une extension finie séparable de degré d de K.
i) Il existe une valuation discrète w sur L qui prolonge v (cf. II.1.2.6.)
ii) La valuation w est la seule qui prolonge v et L est complet pour w.
iii) La fermeture intégrale $\mathcal{O}_L$ (cf. I.4.1.9) de $\mathcal{O}_K$ dans L est un anneau de valuation discrète qui est un $\mathcal{O}_K$-module libre de rang d.
iv) Si v_L désigne l'unique valuation discrète normalisée sur L équivalente à w et $\mathfrak{m}_L$ l'idéal maximal de L, il existe un entier $e_{L/K}$ tel que

$$(v_L)_{|K} \ = \ e v_K$$

et

$$\mathcal{O}_L \mathfrak{m}_K \ = \ \mathfrak{m}_L^e \ .$$

v) Si on note $\ell \ := \ \mathcal{O}_L/\mathfrak{m}_L$ *(resp.* $k \ := \ \mathcal{O}_K/\mathfrak{m}_K$*) le corps résiduel de* L *(resp.*K*) et*

$$f_{L/K} \ := \ [\ell : k]$$

on a l'identité

$$d \ = \ e_{L/K} f_{L/K} \ .$$

Preuve :
i) Rappelons d'abord que l'anneau $\mathcal{O}_K$ de la valuation v est un anneau de valuation discrète donc un anneau de Dedekind (cf. I.5.2.4.) La fermeture intégrale (cf. I.4.1.9,) $\mathcal{O}_L$ de $\mathcal{O}_K$ dans L est donc encore un anneau de Dedekind grâce à la proposition I.5.2.6.

L'anneau $\mathcal{O}_L$ a des idéaux maximaux qui sont tous au-dessus de l'idéal maximal $\mathfrak{m}_K$ de K (cf. I.4.3.2.) Pour $\mathfrak{p}$ un tel idéal il existe, en vertu de la proposition II.3.1.1, une unique valuation discrète normalisée $v_\mathfrak{p}$ sur $\mathcal{O}_L$ dont l'anneau de la valuation est $(\mathcal{O}_L)_\mathfrak{p}$.

Si π est une uniformisante pour v_K (cf. II.1.3.4,) il existe alors un entier e tel que $v_\mathfrak{p}(\pi) = e$ et il est clair que

$$\frac{1}{e} v_\mathfrak{p}$$

prolonge v_K.

ii) Montrons d'abord l'unicité du prolongement : La valuation v définit une valeur absolue $|\cdot|$ sur K (cf. II.1.2.10.) Choisissons $0 < \gamma < 1$ tel que $|\cdot| \ = \ \gamma^{v(\cdot)}$.

Pour toute valuation w sur L, $|\cdot|_L \ := \ \gamma^{w(\cdot)}$ est une norme sur le K-espace vectoriel L relativement à la valeur absolue $|\cdot|$ sur K.

Or sur un espace vectoriel de dimension finie sur un corps complet, toutes les normes sont équivalentes et l'espace vectoriel est complet pour l'une quelconque de ces normes. Ceci permet de conclure.

iii) Puisqu'on a vu qu'à tout idéal maximal de $\mathcal{O}_L$ on pouvait associer un prolongement de v, l'unicité du prolongement montre que $\mathcal{O}_L$ n'a qu'un idéal maximal c'est-à-dire est local. Comme c'est un anneau de Dedekind, c'est un anneau de valuation discrète. Comme $\mathcal{O}_K$ est principal, il découle du corollaire I.4.4.3 que $\mathcal{O}_L$ est un $\mathcal{O}_K$-module libre de rang d.

iv) Est clair.

v) Découle du point précédent et du lemme II.3.1.3.

q.e.d

Lemme II.3.1.3. [4]*. Soit* k *un corps,* B *un anneau,* $e \geq 1$ *un entier et* $\pi \in B$ *tel que* B/π^e *est une* k*-algèbre. Alors* B/π *se trouve aussi être une* k*-algèbre dont on note* f *la dimension en tant que* k*-espace vectoriel. Alors*

$$\dim_k B/\pi^e \ = \ ef \ .$$

[4]Ce lemme est en fait un lemme purement d'algèbre commutative qui n'a sans doute pas grand chose à faire ici mais on ne sait pas vraiment où le mettre.

Preuve : Pour tout $1 \leq j < e$, on a une suite exacte de k-espaces vectoriels

$$0 \ \rightarrow \ (\pi^j)/(\pi^{j+1}) \ \longrightarrow \ B/\pi^{j+1} \longrightarrow B/\pi^j \ \rightarrow \ 0 \, . \qquad \text{II.3.1.3.1}$$

La multiplication par π_i^j définit un isomorphisme de B-modules $B \ \rightarrow \ (\pi^j)$. L'image de (π^j) par cet isomorphisme est (π^{j+1}) d'où un isomorphisme

$$B/\pi \ \cong \ (\pi^j)/(\pi^{j+1})$$

ce qui prouve que

$$\dim_k (\pi^j)/(\pi^{j+1}) \ = \ \dim_k B/\pi \ = \ f \, .$$

En raisonnant par récurrence grâce à la suite exacte II.3.1.3.1, on établit que

$$\dim_k B/\pi^e \ = \ ef \, .$$

q.e.d

Définition II.3.1.4. Soit K un corps complet pour une valuation discrète et L une extension finie séparable. On appelle *indice de ramification* de l'extension l'entier $e_{L/K}$ défini par le point II.3.1.2.iv.

Le degré $f_{L/K}$ de l'extension

$$\mathcal{O}_K/\mathfrak{m}_K \subset \mathcal{O}_L/\mathfrak{m}_L$$

s'appelle le *degré résiduel* de l'extension L/K.

Définition II.3.1.5. On dit qu'une extension L d'un corps complet K est *non ramifiée*,si l'extension résiduelle est séparable et $e_{L/K} = 1$.

Ce qui signifie que le degré est le degré résiduel.

Définition II.3.1.6. Soit K un corps local. Une extensions finie L de K est *totalement ramifiée* si l'extension résiduelle est triviale.

Si l'extension L/K est séparable cela signifie que le degré $[L : K]$ est l'indice de ramification $e_{l/K}$.

Dans la suite de ce paragraphe, on suppose que K est un corps complet pour une valuation discrète. [5]. On Note v_K la valuation discrète normalisée sur K, $\mathcal{O}_K$ l'anneau de la valuation de k le corps résiduel.

Proposition II.3.1.7. *Pour E une extension algébrique quelconque de K. Il existe une et une seule valuation w sur E telle que $w(x) = v(x)$ pour tout $x \in K$.*

Preuve : Pour une extension finie on l'a vu. E est réunion d'extension finies. Sur chacune d'entre elles, on a une valuation unique, qui prolonge v. Si x est dans E, il est dans un L on doit avoir

[5]On pourrait même supposer K de caractéristique 0 pour éviter les questions de séparabilités puisque certains énoncés qui sont vrais dans un cadre plus général n'ont été établis que dans le cas des extensions séparables. En pratique, les corps locaux auxquels on en aura seront des extensions finies de $\mathbb{Q}_p$ donc de caractéristique 0.

$w(x) = w_L(x)$ ce qui démontre l'unicité du prolongement. L'existence se voit en utilisant le composé de deux extensions contenant x. *q.e.d*

Corollaire II.3.1.8. *En particulier si $K \subset L$ est une extension finie (séparable) et σ un K-plongement de L dans une extension algébrique (non nécessairement finie) E, notons w_L la valuation de L qui prolonge v, w_E la valuation de E qui prolonge v. Pour tout $a \in L$, $w_E(\sigma(a)) = w_L(a)$ par unicité.*

Corollaire II.3.1.9. *En particulier si $\overline{K}$ est une clôture algébrique de K, si on note encore v l'unique prolongement de v à $\overline{K}$ et si σ est un K-plongement de $\overline{K}$ dans lui-même, pour tout $\lambda \in \overline{K}$,*

$$v(\sigma(\lambda)) \; = \; v(\lambda) \; .$$

Remarque II.3.1.10. Par conséquent, si L/K est finie séparable, on note σ_i ,$1 \leq i \leq d$ des K-plongements distincts de L dans un corps E convenable. Alors pour $a \in L$,

$$\begin{aligned} v(\mathrm{N}_{L/K}(a)) &= w_L(\mathrm{N}_{L/K}(a)) \\ &= w_L(\prod_{i=1}^{d} \sigma_i(a)) \\ &= \sum_{i=1}^{d} w_L(\sigma_i(a)) \\ &= d w_L(a). \end{aligned}$$

Notations Pour K corps complet pour une valuation discrète v on note v_K la valuation de K normalisée, $v_K(K^\times) = \mathbb{Z}$. Si E est une extension algébrique de K quelconque, On notera encore v_K l'unique valuation de E qui prolonge v_K. (elle n'est plus nécessairement normalisée.) Si L finie séparable de degré d. On a deux valuation v_K et v_L, $v_K(x)$ $v_L(x) = e v_K(x)$. D'où

$$v_K(a) \; = \; \frac{1}{ef} v_K(\mathrm{N}_{L/K}(a)) \; .$$

II.3.2 . −Polygone de Newton, polynômes d'Eisenstein et extension totalement ramifiée

Définition II.3.2.1. Corps local Un *corps local* est un corps complet (cf. 0.2.2.6) pour une valuation discrète (cf. II.1.3.1) dont le corps résiduel est parfait.

Exemple II.3.2.2. On a vu au paragraphe II.1.4 que, pour tout nombre premier, p on peut munir le corps $\mathbb{Q}$ des rationnels de sa valeur absolue p-adique. Le résultat énoncé en 0.2.2.7 permet de constuitruire le complété de $\mathbb{Q}$ pour la topologie p-adique qu'on note $\mathbb{Q}_p$. C'est un exemple de corps local même si la justification du fait que la corps résiduel est parfait sera donnée plus tard.

Dans la suite de ce paragraphe, on suppose que K est un corps local de caractéristique 0 [6].

[6] Ces hypothèses sont peut-être trop restrictives mais il ne me semble pas qu'on ait besoin de plus.

On note v la valuation, $\mathcal{O}_K$ l'anneau de la valuation, $\mathfrak{m}_K$ l'idéal maximal et k le corps résiduel.

On fixe $\overline{K}$ une clôture algébrique de K, et on note encore v l'unique prolongement de v (cf. II.3.1.7) à $\overline{K}$.

Proposition II.3.2.3. *Soit*

$$P := \sum_{i=0}^{d-1} a_i X^i + X^d \in K[X]$$

un polynôme unitaire irréductible.

i) Toutes les racines de P dans $\overline{K}$ ont même valuation.

ii) Pour toute racine λ de P, $v(\lambda) \geq 0$, si et seulement si

$$v(a_i) \geq 0 \; \forall 0 \leq i \leq d-1 \text{ et } v(a_0) = 0 .$$

iii) $v(\lambda) = r$ pour toute racine λ de P si et seulement si

$$v(a_i) \geq r(d-i) \; \forall 0 \leq i \leq d-1 \; et \; v(a_0) = dr .$$

Preuve :

i) Il suffit de remarquer que P étant irréductible, les racines de P sont toutes conjuguées et d'appliquer le corollaire II.3.1.9.

ii) Il suffit d'utiliser les fonctions symétriques pour écrire les coefficients du polynôme en fonction des racines pour démontrer le sens direct.

Réciproquement, si

$$v(a_i) \geq 0 \; \forall 0 \leq i \leq d-1 \text{ et } v(a_0) = 0 ,$$

pour toute racine λ de P, en écrivant

$$\lambda^d = -\sum_{i=0}^{d-1} a_i \lambda^i ,$$

si on supposait $v(\lambda) < 0$, le membre de gauche aurait une valuation au plus $dv(\lambda)$ tandis que le membre de droite aurait une valuation au moins $(d-1)v(\lambda)$. De plus $v(\lambda) > 0$ entraîne $v(a_0) > 0$, on a donc $v(\lambda) = 0$.

iii) Supposons qu'il existe r tel que $v(\lambda_i) = r$ pour tout $1 \leq i \leq d$. Soit $\gamma \in \overline{K}$ tel que $v(\gamma) = r$. Posons $Q(X) := \frac{1}{\gamma^d} P(\gamma X)$. Le polynôme Q est unitaire, et λ est racine de P, si et seulement si $\gamma^{-1}\lambda$ est racine de Q. Or, alors, $v(\gamma^{-1}\lambda) = 0$, ce qui implique, en vertu du point précédent, que, pour tout $1 \leq i \leq d-1$, $v(\gamma^{i-d} a_i) \geq 0$ c'est-à-dire $v(a_i) \geq r(d-i)$ et $v(\gamma^{-d} a_0) = 0$ c'est-à-dire $v(a_0) = dr$.

q.e.d

Définition II.3.2.4. Polygone de Newton Étant donné un polynôme $P := \sum_{i=0}^{d} a_i X^i$, avec $a_0 \neq 0$, on appelle *polygone de Newton* du polynôme P, l'enveloppe convexe des points $(i, v(a_i))$. Le polygone de Newton est au-dessus du segment $[(0, rd), (d, 0)]$ (résultat non démontré.)

Proposition II.3.2.5. *Soit $P := \sum_{i=0}^{d} a_i X^i \in K[X]$ un polynôme de degré d. On note α_j ,$1 \leq j \leq s$ les pentes de son polygone de Newton, et d_j ,$1 \leq j \leq s$ la longueur de la projection horizontale du segment de pente α_j.*

Alors les α_j sont les valuations des racines de P dans $\overline{K}$ et d_j le nombre de racines de valuation α_j.

Preuve : En fait on a fait la démonstration dans le cas où il y a une seule pente en II.3.2.3. . La démonstration peut ensuite se faire par récurrence sur le nombre de pentes, *i.e.*le nombre de valeurs distinctes prises par les valuations des racines ou encore le nombre de facteurs irréductibles dans P. *q.e.d*

Définition II.3.2.6. Polynôme d'Eisenstein Un *polynôme d'Eisenstein* de degré d à coefficients dans K, est un polynôme unitaire $P := \sum_{i=0}^{d-1} a_i X^i + X^d$ tel que pour tout $0 \leq i \leq d-1$, $a_i \in \mathfrak{m}_K$ et $a_0 \notin \mathfrak{m}_K^2$.

Proposition II.3.2.7.

i) Un polynôme d'Eisenstein est irréductible.

ii) Un polynôme est d'Eisenstein si et seulement si son polygone de Newton est le segment $[(0, 1), (d, 0)]$ et donc qu'il n'y a qu'une seule pente égale à $\frac{1}{d}$.

Preuve :

i) Voir le critère d'irréductibilité II.2.1.2.ii.

q.e.d

Théorème II.3.2.8. Structure des extensions totalement ramifiées

i) Étant donné un polynôme d'Eisenstein $P \in K[X]$ de degré d, l'extension $L := K[X]/P$ de K est totalement ramifiée (cf. II.3.1.6) et X est une uniformisante de L (cf. II.1.3.4.)

ii) Réciproquement si L est une extension totalement ramifiée de K de degré d, dont π est une uniformisante, le polynôme minimal P de π est un polynôme d'Eisenstein.

Preuve :

i) On peut très bien ne pas supposer savoir que P est irréductible. Notons alors π une racine de P, et $L := K[\pi]$ qui est une extension de degré $n = ef \leq d$ (où e est son indice de ramification et f son degré résiduel.) (cf. II.3.1.4.) Si on note encore v l'unique prolongement de v à L, on a alors $v(L^\times) = \frac{1}{e}\mathbb{Z}$. D'après la proposition II.3.2.3, $v(\pi) = \frac{1}{d}$ donc $d|e$. Or $e|n \leq d$. Il en résulte que $n = d = e$ et $f = 1$ et que l'extension L/K est totalement ramifiée de degré d, que le polynôme P est irréductible et que π est une uniformisante puisque $v_L(\pi) = 1$.

ii) Soit π une uniformisante de L et P son polynôme minimal. Le polynôme P est unitaire de degré d dont toutes les racines sont de valuation $\frac{1}{d}$ donc un polynôme d'Eisenstein de degré d (cf. II.3.2.3.)

q.e.d

Corollaire II.3.2.9. Structure de la clôture intégrale dans une extension totalement ramifiée *Si L/K est une extension de degré d totalement ramifiée (cf. II.3.1.6,) et π une uniformisante (cf. II.1.3.4,) de L,*

$$1, \pi, \ldots, \pi^{d-1}$$

est une $\mathcal{O}_K$-base de la clôture intégrale $\mathcal{O}_L$ de $\mathcal{O}_K$ dans L.

Preuve : Le polynôme minimal de π est un polynôme d'Eisenstein de degré d et $L = K[\pi]$ On sait déjà que $1, \pi, \ldots, \pi^{d-1}$ est une K-base de L. Pour tout $\beta \in L$ il existe $\lambda_{i\ ,0\leq i\leq d-1} \in K$ tels que $\beta = \sum_{i=0}^{d-1} \lambda_i \pi^i$. Notons v_L la valuation normalisée sur L équivalente au prolongement de v. Pour tout $0 \leq i \leq d-1$,

$$v_L(\lambda_i \pi^i) = v_L(\lambda_i) + i = dv(\lambda_i) + i\ .$$

Les valuation des λ_i sont toutes différentes modulo d donc toutes différentes, donc

$$v_L(\beta) = \min_{i=0}^{d-1}(dv(\lambda_i) + i\ .$$

Si donc il existe i tel que $v(\lambda_i) < 0$, $v_L(\beta) < 0$. Autrement dit, $\beta \in \mathcal{O}_L$ si et seulement si pour tout $0 \leq i \leq d-1$, $v(\lambda_i) \geq 0$. Ceci prouve que $1, \ldots, \pi^{d-1}$ est une $\mathcal{O}_K$-base de $\mathcal{O}_L$. *q.e.d*

II.3.3 . −Extensions finies séparables de corps locaux

Dans ce paragraphe, on suppose que K est un corps local (cf. II.3.2.1) de caractéristique 0 [7].

On note v la valuation, $\mathcal{O}_K$ l'anneau de la valuation, $\mathfrak{m}_K$ l'idéal maximal, k le corps résiduel et v_K la valuation normalisée équivalente à v.

Soit $K \subset L$ une extension finie séparable de degré d dont on note $\mathcal{O}_L$ l'anneau de la valuation (ou ce qui revient au même la clôture intégrale de $\mathcal{O}_K$ dans L) $\mathfrak{m}_L$ l'idéal maximal et ℓ le corps résiduel. On note encore v_L l'unique valuation discrète normalisée sur L équivalente au prolongement de v.

On note $e_{L/K}$ l'indice de ramification de l'extension (cf. II.3.1.4) et $f_{L/K}$ son degré résiduel.

Proposition II.3.3.1. Structure de la fermeture intégrale dans une extension non ramifiée *Si l'extension L/K est non ramifiée (cf. II.3.1.5,) il existe un élément $\alpha \in \mathcal{O}_L$ tel que :*

[7] Ces hypothèses sont peut-être trop restrictives mais il ne me semble pas qu'on ait besoin de plus.

– *l'image de α dans ℓ est un générateur de l'extension ℓ/k,*
–
$$1, \alpha, \ldots, \alpha^{d-1}$$
est une $\mathcal{O}_K$-base du $\mathcal{O}_K$-modue libre de rang d (cf. II.3.1.2.iii.)

Preuve : Soit $a \in \ell$ un générateur de l'extension ℓ/k (ce qui existe puisque k est parfait.) Il existe un polynôme irréductible $P_a \in k[X]$ de degré d tel que $\ell = k[X]/P_a$. Soit $P \in \mathcal{O}_K[X]$ un polynôme irréductible qui relève P_a. D'après la proposition II.2.2.2 il existe une racine α de P au-dessus de a. On a alors $L = K[\alpha]$.

Tout $\beta \in L$ s'écrit donc $\beta = \sum_{i=0}^{d-1} \lambda_i \alpha^i$ avec les $\lambda_{i\ ,0\leq i\leq d-1} \in K$. Si $\beta \neq 0$, les λ_i ne sont pas tous nul et on note $s := \min_{i=0}^{d-1} v_K(\lambda_i)$. Si π est une uniformisante de K, il existe $\mu_{i\ ,0\leq i\leq d-1} \in K$ tels que $\lambda_i = \pi^s \mu_i$ avec $v_K(\mu_i) \geq 0$ et il existe i_0 tel que $v_K(\mu_{i_0}) = 0$. D'où $\beta = \pi^s \beta'$ avec $\beta' = \sum_{i=0}^{d-1} \mu_i \alpha^i$. Il en résulte que $\beta' \in \mathcal{O}_L$. Dans le corps résiduel ℓ, on a $\overline{\beta'} = \sum_{i=0}^{d-1} \overline{\mu_i} a^i$. Or $1, a, \ldots, a^{d-1}$ est une k-base de ℓ, et l'un au moins des μ_i étant de valuation 0, son image est non nul dans k, c'est-à-dire que β' n'est pas nul modulo $\mathfrak{m}_L$, et donc que $v_K(\beta) = s$. Il en résulte finalement, que $v_K(\beta) \geq 0$ implique que pour tout $0 \leq i \leq d-1$, $v_K(\lambda_i) \geq 0$. *q.e.d*

Théorème II.3.3.2. Structure des extensions finies séparables de corps locaux *Il existe une extension intermédiaire $K \subset L_0 \subset L$ telle que :*
i) Le corps résiduel de L_0 est ℓ est L_0/K est non ramifiée.
ii) L'extension L/L_0 est totalement ramifiée de degré $e_{L/K}$.
iii) Il existe un élément $\alpha \in \mathcal{O}_{L_0}$ dont l'image dans ℓ est un générateur de l'extension ℓ/k, et tel que pour toute uniformisante π de L,
$$\{\alpha^i \pi^j\}_{0\leq i\leq f_{L/K}-1\ ,\ 0\leq j\leq e_{L/K}-1}$$
est une $\mathcal{O}_K$-base de $\mathcal{O}_L$.
iv) Pour toute extension $K \subset E \subset L$, E/K est non ramifiée si et seulement si $E \subset L_0$.

Preuve :
i) Soit $a \in \ell$ un générateur de l'extension ℓ/k et $P_a \in k[X]$ son polyôme minimal. On peut grâce à la proposition II.2.2.2, trouver un polynôme irréductible $P \in \mathcal{O}_K[X]$ avec
$$\deg(P) = \deg(P_a) = [\ell : k] = f_{L/K}$$
et un élément $\alpha \in \mathcal{O}_L$ tel que $P(\alpha) = 0$. Posons alors $L_0 := K[\alpha]$. Le polynôme P est de degré $f_{L/K}$, ce qui implique que $L_0 = K[\alpha]$ est au plus de degré $f_{L/K}$. Mais, le corps résiduel ℓ_0

contient a et contient donc ℓ ce qui implique qu'il est au moins de degré $f_{L/K}$ sur k. Il en résulte que nécessairement

$$[L_0 : K] \;=\; [\ell_0 : k] \;=\; f_{L/K}$$

ce qui implique que L_0/K est non ramifiée et $\ell_0 \;=\; \ell$.

i) Est clair.

ii) On a $\mathcal{O}_L \;=\; \mathcal{O}_{L_0}[\pi]$ (cf. II.3.2.9) et $\mathcal{O}_{L_0} \;=\; \mathcal{O}_K[\alpha]$ (cf. II.3.3.1.)

ii) Soit E une extension finie non ramifiée de K contenue dans L. Son corps résiduel k_E est un sous-corps de ℓ qui contient k. L'extension k_E/k est donc finie séparable engendrée par un élément $b \in k_E$. Posons $\tilde{Q}$ le polynôme de b et, par la proposition II.2.2.2, il existe un polynôme $Q \in \mathcal{O}_K[X]$ relevant $\tilde{Q}$ et une unique racine β de Q relevant b. On peut appliquer le lemme aussi bien à E qu'à L_0 ce qui implique que β est simultanément dans E et dans L_0. Or pour des raisons de degré analogues à celles du point II.3.3.2.i, on montre que si E est non-ramifiée,

$$E \;=\; K[\beta] \;\subset\; L_0\,.$$

q.e.d

Définition II.3.3.3. Extension maximale non ramifiée Avec les notations du théorème II.3.3.2.iv, on appelle L_0 l'*extension maximale non-ramifiée* de K contenue dans L.

Remarque II.3.3.4. Plus généralement, si $\alpha \in \mathcal{O}_L$ relève un générateur de ℓ sur k (pas besoin qu'il soit dans $\mathcal{O}_{L_0}$) et si π est une uniformisante de L sur L_0, $\mathcal{O}_L = \mathcal{O}_K[\alpha, \pi]$ et les $\alpha_i\pi^j$ forment une$\mathcal{O}_K$- base.

Corollaire II.3.3.5. *Sous les mêmes hypothèses que dans le théorème II.3.3.2, il existe $\alpha \in \mathcal{O}_L$ tel que $1, \alpha, \ldots, \alpha^{d-1}$ est une $\mathcal{O}_K$-base de $\mathcal{O}_L$.*

Preuve : Soit $P \in \mathcal{O}_K[X]$ un polynôme unitaire relevant le polynôme minimal d'un générateur a de ℓ. Soit $\alpha_0 \in \mathcal{O}_L$ un relèvement de a (cf. II.2.2.2.) Notons v_L la valuation normalisée équivalente au prolongement de v à L. On a alors $v_L(P(\alpha_0)) > 0$.

i) Si $v_L(P(\alpha_0)) = 1$, $P(\alpha_0)$ est une uniformisante de $\mathcal{O}_L$. On a donc $\mathcal{O}_L \;=\; \mathcal{O}_{L_0}[P(\alpha_0)]$ et les puissances de $P(\alpha_0)$ sont une $\mathcal{O}_{L_0}$-base de $\mathcal{O}_L$. Il est clair qu'alors les puissances de α_0 forment une $\mathcal{O}_K$-base de $\mathcal{O}_L$.

ii) Sinon, $v_L(P(a_0)) \geq 2$. Soit alors π une uniformisante de $\mathcal{O}_L$. $\alpha \;:=\; \alpha_0 + \pi$ est encore un relèvement de a. On a alors

$$P(\alpha) \;=\; P(\alpha_0) \;+\; \pi P'(\alpha_0) \;+\; \pi^2 R\,.$$

Par séparabilité, $v(P'(\alpha_0)) \;=\; 0$ ce qui implique que $v(P(\alpha)) \;=\; 1$ et l'on a donc trouvé une uniformisante comme au point précédent.

q.e.d

Proposition II.3.3.6. Extensions Galoisiennes de corps local *On suppose que l'extension L/K est galoisienne. Soit L_0 l'extension maximale non ramifiée (cf. II.3.3.3.)*

iii) Les extensions L_0/K et ℓ/k Sont aussi galoisiennes.

iv) L'extension L/L_0 est aussi galoisienne et son groupe de Galois Gal_{L/L_0} est un sous-groupe normal du groupe de Galois $\mathrm{Gal}_{L/K}$ appelé groupe d'inertie de l'extension et noté $I_{L/K}$. Le quotient $\mathrm{Gal}_{L/K}/I_{L/K}$ est isomorphe au groupe de Galois $\mathrm{Gal}_{\ell/k}$ de l'extension résiduelle.

v) Si k est un corps fini, le groupe de Galois $\mathrm{Gal}_{\ell/k}$ est engendré par le Frobenius.

Si K^s est une clôture séparable de K, pour tout n, il existe une et une seule extension K_n contenue dans K^s de degré n non ramifiée.

Elle est cyclique avec pour générateur un relèvement de Frobenius encore appelé Frobenius.

Si on note encore ϕ le Frobenius en haut, pour tout $\beta \in \mathcal{O}_L$, $\phi(\beta) \equiv \beta^q$ [$\mathfrak{m}_L$.

Preuve : Soit $\alpha \in \mathcal{O}_{L_0}$ tel que $\mathcal{O}_{L_0} = \mathcal{O}_K[\alpha]$ et P un relèvement du polynôme minimal d'un générateur a de ℓ.
i) Le polynôme P se décompose dans L en polynômes du premier degré de racines α_i qui sont dans $\mathcal{O}_L$, puisque l'action du groupe de Galois ne change pas la valuation (cf. II.3.1.9.) Le corps $K[\alpha_i]$ est isomorphe à $K[\alpha]$ donc $K[\alpha_i]/K$ est non ramifiée contenu dans L, Donc $K[\alpha_i] \subset L_0$ (cf. II.3.3.2.iv ;) donc $K[\alpha_i] = L_0$.

q.e.d

Exemple II.3.3.7. Extensions cyclotomiques de $\mathbb{Q}_p$
i) Pour K un corps et $n \in \mathbb{N}^*$, si K est de caractéristique 0 ou si n est premier à la caractéristique p de K, le polynôme X^n-1 est séparable et son corps de décomposition L est donc une extension dite *extension cyclotomique* de K. Le groupe μ_n des racines de $X^n - 1$ dans L est un groupe cyclique (comme sous-groupe du groupe multiplicatif d'un corps,) isomorphe à $\mathbb{Z}/n$. Étant donné un générateur ϵ de μ_n, pour tout $g \in \mathrm{Gal}_{L/K}$ $g(\epsilon) \in \mu_n$ et s'écrit donc $\epsilon^{\chi(g)}$ qui est encore une racine primitive c'est-à-dire que $\chi(g) \in (\mathbb{Z}/n)^\times$. Le morphisme χ est appelé *caractère cyclotomique*. Il est clairement injectif.

ii) Si $K = \mathbb{Q}_p$ (cf. II.3.2.2,) et n un entier premier à p, $X^n - 1$ est séparable sur $\mathbb{F}_p$. Le corps k engendré par les racines de $X^n - 1$ sur $\mathbb{F}_p$ est une extension cyclique de degré f. Le degré f est le plus petit entier f tel que $n|p^f - 1$. Le polynôme $X^n - 1$ relève $X^n - 1$ dans $\mathbb{Z}_p[X]$ et l'on construit une extension L non ramifiée de degré f de $\mathbb{Q}_p$ grâce au lemme II.2.2.2 et aux procédés utilisés dans la proposition II.3.3.1. Si ϵ est une racine primitive $n^{\text{ième}}$ de l'unité dans L ϵ est dans $\mathcal{O}_L$ l'image de ϵ dans ℓ est un générateur du groupe des racines n ième de l'unité. En particulier $\mathcal{O}_L = \mathbb{Z}_p[\epsilon]$. et $1, \epsilon, \ldots, \epsilon^{f-1}$ est une $\mathbb{Z}_p$-base de $\mathcal{O}_L$.

Réciproquement, toute extension non ramifiée de $\mathbb{Q}_p$ est de ce type, c'est-à-dire est le corps engendré sur $\mathbb{Q}_p$ en rajoutant une racine primitive $n^{\text{ième}}$ quelconque de l'unité.

Il faut quand-même prendre garde au cas où $n = p-1$, parce que $\mathbb{Q}_p$ contient déjà les racines $p-1^{\text{ième}}$.

iii) Dans le cas où $n = p^r$, on commence par considérer le cas $n = p$. On pose $L = \mathbb{Q}_p[\epsilon]$ avec $\epsilon^p = 1$ et $\epsilon \neq 1$. On pose $\epsilon = 1 + \pi$. En fait ϵ est racine de $\frac{X^p-1}{X-1}$ ce qui entraîne que π est racine de $\frac{(1+X)^p-1}{X}$ c'est-à-dire que π est racine de $X^{p-1} + \sum_{k=1}^{p-1} C_p^k X^{k-1}$ qui est un polynôme

d'Eisenstein (cf. II.3.2.6.) Ce polynôme est irréductible (cf. II.3.2.7.i,) en particulier $L/\mathbb{Q}_p$ est de degré $p-1$ et totalement ramifiée (cf. II.3.2.8.i ;) $\pi = \epsilon - 1$ est une uniformisante de L, $\mathcal{O}_L$ est engendré par n'importe quelle uniformisante c'est donc $\mathbb{Z}_p[\epsilon - 1]$ qui est aussi $\mathbb{Z}_p[\epsilon]$.

Si maintenant $n = p^r$, pour $r \geq 1$, soit ϵ une racine primitive p^rième de l'unité dans une extension convenable de $\mathbb{Q}_p$. On pose $L_r := \mathbb{Q}_p(\epsilon)$ Alors $L_r/\mathbb{Q}_p$ est une extension abélienne totalement ramifiée de degré $(p-1)p^{r-1}$; $\epsilon - 1$ est une uniformisante de L_r et $\mathcal{O}_L = \mathbb{Z}_p[\epsilon]$.

On démontre ce fait par récurrence sur r. On vient de voir le cas $r = 1$. On peut considérer $L_{r-1} = \mathbb{Q}_p(\epsilon^p)$ L_{r-1} est totalement ramifiée de degré $(p-1)p^{r-2}$. On pose $\gamma := \epsilon^p - 1$ qui est une uniformisante de L_{r-1} et $\epsilon = 1 + \pi$ d'où la relation $(1+\pi)^p - 1 = \gamma$. Il en résulte que π est racine du polynôme $(1+X)^p - 1 - \gamma \in L_{r-1}[X]$ dont le terme constant γ est une uniformisante et les autres termes, à l'exception du terme dominant son tous divisibles par p ; c'est donc un polynôme d'Eisenstein sur L_{r-1}. Ce polynôme est irréductible de degré p, donc L_r/L_{r-1} est de degré p et π est une uniformisante pour cette extension totalement ramifiée.

Le groupe de Galois $\mathrm{Gal}_{L_r/\mathbb{Q}_p}$ s'injecte dans $(\mathbb{Z}/p^r)^\times$, cette injection étant en fait un isomorphisme.

iv) Soit $n \in \mathbb{N}^*$ un entier quelconque. On pose $L := \mathbb{Q}_p[\epsilon]$ avec ϵ une racine primitive $n$ième de l'unité et on écrit $n = n_0 p^r$ avec n_0 premier à p. Il en résulte que ϵ^{n_0} est une racine primitive p^rième de l'unité, on le note ϵ' et $\epsilon_0 := \epsilon^{p^r}$ est une racine primitive $n_0$ième de l'unité. On note $L_0 := \mathbb{Q}_p[\epsilon_0]$ et $L_1 := \mathbb{Q}_p[\epsilon']$. L_0 et L_1 sont contenues dans L et $L = L_0 L_1$.

v) Extensions cyclotomique du corps $\mathbb{F}_p((\pi))$ des séries formelles. Il est complet pour une valuation discrète, dont le corps résiduel est $\mathbb{F}_p$. Les racine $n$ième sont les racines $n_0$ième si $n = n_0 p^r$. Il n'y a que des extensions non ramifiées. On a $\mathbb{F}_p[\epsilon_0]$ est une extension finie de $\mathbb{F}_p$.

III . −Détermination de l'anneau des entiers d'un corps de nombres

III.1 . −Extensions d'anneaux de Dedekind

Définition III.1.0. Un *corps de nombres* est un corps K qui est une extension finie du corps $\mathbb{Q}$ des nombres rationnels. La fermeture intégrale (cf. I.4.1.9) de $\mathbb{Z}$ dans K est notée $\mathcal{O}_K$ et appelé l'*anneau des entiers* de K. C'est bien entendu un anneau de Dedekind (cf. I.5.2.2.)

III.1.1 . −Le groupe des idéaux fractionnaires d'un anneau de Dedekind

Dans ce paragraphe, A est un anneau de Dedekind (cf. I.5.2.2) de corps des fractions K. On note $\mathcal{I}(A)$ l'ensemble de ses idéaux fractionnaires (cf. I.1.5.1) muni de la loi de composition définie en (cf. I.1.5.4.)

Définition III.1.1.1. Valuation d'un idéal fractionnaire Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, notons $v_\mathfrak{p}$ l'unique valuation discrète normalisée sur K (cf. II.1.3.1,) dont l'anneau est $A_\mathfrak{p}$ (cf. II.3.1.1.i.)

Pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, Il résulte du corollaire I.5.1.4 que pour tout idéal fractionnaire $\mathfrak{i}$ de $A_{\mathfrak{p}}$ il existe un unique $n \in \mathbb{Z}$ tel que

$$\mathfrak{i} = \{x \in A_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) \geq n\} .$$

On notera encore $v_{\mathfrak{p}}(\mathfrak{i}) := n$.

Pour tout idéal fractionnaire $\mathfrak{I}$ de A, et tout $\mathfrak{p} \in \mathrm{Spm}(A)$, $\mathfrak{I}_{\mathfrak{p}}$ est un idéal fractionnaire de $A_{\mathfrak{p}}$ (cf. I.3.2.5.) On posera donc, par définition

$$v_{\mathfrak{p}}(\mathfrak{I}) := v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}})$$

qu'on appellera la *valuation en* $\mathfrak{p}$ *de* $\mathfrak{I}$.

Lemme III.1.1.2. *Pour tout couple* $(\mathfrak{I}, \mathfrak{J})$ *d'idéaux fractionnaires de* A *et tout* $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(\mathfrak{I}\mathfrak{p}) = v_{\mathfrak{p}}(\mathfrak{I}) + v_{\mathfrak{p}}(\mathfrak{J}) .$$

Preuve : Par définition, $v_{\mathfrak{p}}(\mathfrak{I}\mathfrak{J}) = v_{\mathfrak{p}}((\mathfrak{I}\mathfrak{J})_{\mathfrak{p}})$ qui est encore égal, en vertu de la proposition I.3.2.5, à $v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}}\mathfrak{J}_{\mathfrak{p}})$ qui vaut encore grâce à la proposition I.5.1.4, $v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}}) + v_{\mathfrak{p}}(\mathfrak{J}_{\mathfrak{p}})$ qui vaut, par définition

$$v_{\mathfrak{p}}(\mathfrak{I}) + v_{\mathfrak{p}}(\mathfrak{J}) .$$

q.e.d

Lemme III.1.1.3.

i) Pour tout idéal fractionnaire $\mathfrak{I}$ *de* A *et tout* $x \in K$, $x \in \mathfrak{I}$ *si et seulement si pour tout* $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{I}) .$$

De plus, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(\mathfrak{I}) = \inf_{x \in \mathfrak{I}}(v_{\mathfrak{p}}(x)) .$$

En particulier,

$$A = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \ \forall \mathfrak{p} \in \mathrm{Spm}(A)\} .$$

ii) Pour deux idéaux fractionnaires $\mathfrak{I}$ *et* $\mathfrak{J}$ *de* A, $\mathfrak{I} = \mathfrak{J}$ *si et seulement si pour tout* $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(\mathfrak{I}) = v_{\mathfrak{p}}(\mathfrak{J}) .$$

iii) Un idéal fractionnaire $\mathfrak{I}$ *de* A *est un idéal de* A *si et seulement si pour tout* $\mathfrak{p} \in \mathrm{Spm}(A)$, $v_{\mathfrak{p}}(\mathfrak{I}) \geq 0$.

Preuve :

i) Pour tout $x \in K$

$$v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{I}) = v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}}) \ \forall \mathfrak{p} \in \mathrm{Spm}(A)$$

équivaut à

$$x \in \bigcap_{\mathfrak{p}\in \mathrm{Spm}(A)} \mathfrak{I}_{\mathfrak{p}}$$

qui équivaut encore à $x \in \mathfrak{I}$ grâce à la proposition I.3.3.9.

Il en résulte que

$$v_{\mathfrak{p}}(\mathfrak{I}) \leq \inf_{x\in\mathfrak{I}}(v_{\mathfrak{p}}(x)) \; \forall \mathfrak{p} \in \mathrm{Spm}(A) \; .$$

Or, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$ $v_{\mathfrak{p}}(\mathfrak{I}) = v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}})$ et $\mathfrak{I}_{\mathfrak{p}}$ est un idéal fractionnaire de l'anneau de valuation discrète $A_{\mathfrak{p}}$. Il résulte alors de la proposition I.5.1.4 qu'il existe $\frac{x}{s} \in \mathfrak{I}_{\mathfrak{p}}$ tel que $v_{\mathfrak{p}}(\frac{x}{s}) = v_{\mathfrak{p}}(\mathfrak{I})$. Or s étant inversible dans $\mathfrak{I}_{\mathfrak{p}}$, $v_{\mathfrak{p}}(\frac{x}{s}) = v_{\mathfrak{p}}(x)$. Comme $x \in \mathfrak{I}$, on en déduit que

$$v_{\mathfrak{p}}(\mathfrak{I}) = \inf_{x\in\mathfrak{I}}(v_{\mathfrak{p}}(x)) \; .$$

ii) C'est une conséquence immédiate du point précédent.

iii) Si $\mathfrak{I}$ est un idéal de A, $\mathfrak{I} \subset A$. Cette inclusion induit, grâce à la proposition I.3.1.10,, un morphisme injectif de $A_{\mathfrak{p}}$-modules

$$\mathfrak{I}_{\mathfrak{p}} \hookrightarrow A_{\mathfrak{p}} \; .$$

Il résulte alors des points I.3.2.5 et I.1.5.2 que $\mathfrak{I}_{\mathfrak{p}}$ est un idéal de $A_{\mathfrak{p}}$. Ce dernier étant un anneau de valuation discrète,

$$v_{\mathfrak{p}}(\mathfrak{I}) = v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}}) \geq 0 \; .$$

Réciproquement, si pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, on a l'inégalité ci-dessus, $\mathfrak{I}_{\mathfrak{p}}$ est un idéal de $A_{\mathfrak{p}}$. Il résulte alors de la proposition I.3.3.9.iii

$$\mathfrak{I} = \bigcap_{\mathfrak{p}\in \mathrm{Spm}(A)} \mathfrak{I}_{\mathfrak{p}} \subset \bigcap_{\mathfrak{p}\in \mathrm{Spm}(A)} A_{\mathfrak{p}} = A$$

c'est-à-dire que $\mathfrak{I}$ est un idéal de A.

q.e.d

Proposition III.1.1.4. *Pour tout idéal fractionnaire $\mathfrak{I}$ de A,*

$$\mathfrak{I}^{\perp} := \{x \in K \mid xy \in A \; \forall y \in \mathfrak{I}\}$$

(cf. I.1.5.5,) est un idéal fractionnaire de A qui est l'inverse de $\mathfrak{I}$ pour la loi de composition définie en I.1.5.4.

On le notera $\mathfrak{I}^{-1}$.

Preuve : Puisque A est un anneau de Dedekind, A est en particulier noethérien et intègre. Il découle donc de la proposition I.1.5.6 que $\mathfrak{I}^{\perp}$ est un idéal fractionnaire de A.

On a une inclusion naturelle

$$\mathfrak{I}\mathfrak{I}^{\perp} \hookrightarrow A \; . \qquad \text{III.1.1.4.1}$$

Elle induit, grâce aux points I.3.1.10 et I.3.2.5 un morphisme injectif de $A_{\mathfrak{p}}$-modules

$$\mathfrak{I}_{\mathfrak{p}}\mathfrak{I}^{\perp}{}_{\mathfrak{p}} = (\mathfrak{I}\mathfrak{I}^{\perp})_{\mathfrak{p}} \hookrightarrow A_{\mathfrak{p}} \; . \qquad \text{III.1.1.4.2}$$

Puisque $A_{\mathfrak{p}}$ est un anneau de valuation discrète, l'idéal fractionnaire $(\mathfrak{I}_{\mathfrak{p}})^{-1}$ inverse de $\mathfrak{I}$ existe et s'identifie à l'ensemble

$$\{x \in K \mid xy \in A_{\mathfrak{p}} \, \forall y \in A_{\mathfrak{p}}\} \; = \; \{x \in K \mid v_{\mathfrak{p}}(x) \; \geq \; -v_{\mathfrak{p}}(\mathfrak{I}_{\mathfrak{p}})\}$$

grâce à la proposition I.5.1.4.

Soient y_i ,$1 \leq i \leq d$ des générateurs de $\mathfrak{I}$ en tant que A-module. Pour tout $\alpha \in (\mathfrak{I}_{\mathfrak{p}})^{-1}$, $\alpha y_i \in A_{\mathfrak{p}}$ c'est-à-dire qu'il existe $\frac{a_i}{s_i}$,$1 \leq i \leq d \in \; A_{\mathfrak{p}}$ tels que pour tout $1 \leq i \leq d$, $\alpha y_i \; = \; \frac{a_i}{s_i}$ c'est-à-dire puisque A est intègre

$$s_i \alpha y_i \; = \; a_i \; \in \; A \, \forall 1 \leq i \leq d \, .$$

Il en résulte que, pour tout $1 \leq i \leq d$,

$$\prod_{i=1}^{d} s_i \alpha y_i \; \in \; A$$

c'est-à-dire, puisque les y_i sont des générateurs de $\mathfrak{I}$, , que

$$\prod_{i=1}^{d} s_i \alpha \; \in \; \mathfrak{I}^{\perp}$$

ou encore que $\alpha \in \mathfrak{I}^{\perp}{}_{\mathfrak{p}}$.

Il en résulte que, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$(\mathfrak{I}_{\mathfrak{p}})^{-1} \; \subset \; \mathfrak{I}^{\perp}{}_{\mathfrak{p}} \, .$$

Il s'ensuit que

$$A_{\mathfrak{p}} \; = \; \mathfrak{I}_{\mathfrak{p}} (\mathfrak{I}_{\mathfrak{p}})^{-1} \; \subset \; \mathfrak{I}_{\mathfrak{p}} \mathfrak{I}^{\perp}{}_{\mathfrak{p}} \, .$$

Il en résulte que, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, le morphisme III.1.1.4.2 est bijectif.

Il en résulte finalement, grâce à la proposition I.3.3.9.iii que

$$\mathfrak{I}\mathfrak{I}^{\perp} \; = \; \bigcap_{\mathfrak{p} \in \mathrm{Spm}(A)} (\mathfrak{I}\mathfrak{I}^{\perp})_{\mathfrak{p}} \; = \; \bigcap_{\mathfrak{p} \in \mathrm{Spm}(A)} \mathfrak{I}_{\mathfrak{p}} \mathfrak{I}^{\perp}{}_{\mathfrak{p}} \; = \; \bigcap_{\mathfrak{p} \in \mathrm{Spm}(A)} A_{\mathfrak{p}} \; = \; A \, .$$

q.e.d

Corollaire III.1.1.5. *L'ensemble des idéaux fractionnaires d'un anneau de Dedekind A est un groupe abélien pour la loi de composition définie en I.1.5.4. On le notera $\mathcal{I}(A)$.*

Corollaire III.1.1.6. *L'inclusion ensembliste $\mathrm{Spm}(A) \; \hookrightarrow \; \mathcal{I}(A)$ induit donc naturellement un morphisme de groupe ϕ du groupe abélien libre $\mathbb{Z}^{(\mathrm{Spm}(A))}$ dans le groupe $\mathcal{I}(A)$.*

Preuve : C'est une conséquence du fait que $\mathcal{I}(A)$ est un groupe abélien et de la propriété universelle des groupes abéliens libres ($\mathbb{Z}$-modules libres)

$$\mathrm{Hom}_{\mathbf{Ens}}(\mathrm{Spm}(A), \mathcal{I}(A)) \; \cong \; \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(\mathrm{Spm}(a))}, \mathcal{I}(A)) \, .$$

q.e.d

Corollaire III.1.1.7. *Pour deux idéaux fractionnaires $\mathfrak{I}$ et $\mathfrak{J}$ de A,*

$$\mathfrak{I} \subset \mathfrak{J} \Leftrightarrow \mathfrak{J}^{-1} \subset \mathfrak{I}^{-1} .$$

Lemme III.1.1.8.
i) Pour tout $x \in A$, l'ensemble des idéaux $\mathfrak{p} \in \mathrm{Spm}(A)$, tels que $v_{\mathfrak{p}}(x) \neq 0$ est un ensemble fini.

ii) Pour tout $x \in K$, l'ensemble des idéaux $\mathfrak{p} \in \mathrm{Spm}(A)$, tels que $v_{\mathfrak{p}}(x) \neq 0$ est un ensemble fini.

iii) Pour tout idéal fractionnaire $\mathfrak{I}$ de A, l'ensemble des $\mathfrak{p} \in \mathrm{Spm}(A)$ tels que $v_{\mathfrak{p}}(\mathfrak{I}) \neq 0$ est fini.

iv) Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, et tout $n \in \mathbb{Z}$,

$$v_{\mathfrak{p}}(\mathfrak{p}^n) = n$$

et pour tout $\mathfrak{q} \in \mathrm{Spm}(A)$, $\mathfrak{q} \neq \mathfrak{p}$,

$$v_{\mathfrak{q}}(\mathfrak{p}^n) = 0$$

c'est-à-dire finalement que

$$\mathfrak{p}^n = \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{p}^n)} \; \forall \mathfrak{p} \in \mathrm{Spm}(A) \; \forall n \in \mathbb{Z} .$$

Preuve :
i) Soit $x \in A$, et supposons qu'il existe une infinité de $\mathfrak{p} \in \mathrm{Spm}(A)$ contenant x. En particulier, il existe une suite $(\mathfrak{p}_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathrm{Spm}(A)$ telle que, pour tout $n \in \mathbb{N}$, $x \in \mathfrak{p}_n$ et telle que pour tout $r \neq s$, $\mathfrak{p}_r \neq \mathfrak{p}_s$. Il en résulte que la suite

$$\{\bigcap_{i=0}^{n} \mathfrak{p}_i\}_{n\in\mathbb{N}}$$

est une suite décroissante d'idéaux de A. Notons, pour tout $n \in \mathbb{N}$, $\mathfrak{I}_n$ l'inverse de $\bigcap_{i=0}^{n} \mathfrak{p}_n$ (cf. III.1.1.4.) Il résulte du corollaire III.1.1.7, que la suite $(\mathfrak{I}_n)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux fractionnaires tous contenus dans $x^{-1}A$. Par noethérianité, la suite des $\mathfrak{I}_n$ est donc stationnaire *i.e.*il existe $n \in \mathbb{N}$ tel que $\mathfrak{I}_n = \mathfrak{I}_{n+1}$. Il s'ensuit que

$$\mathfrak{p}_{n+1} \cap \bigcap_{i=0}^{n} \mathfrak{p}_i = \bigcap_{i=0}^{n} \mathfrak{p}_i$$

ce qui implique que $\bigcap_{i=0}^{n} \mathfrak{p}_i \subset \mathfrak{p}_{n+1}$ qui implique encore que $\prod_{i=0}^{n} \mathfrak{p}_i \subset \mathfrak{p}_{n+1}$ ce qui implique, par primalité, que $\mathfrak{p}_{n+1}$ est égal à l'un des $\mathfrak{p}_{i\ ,0\leq i\leq n}$. Or on a construit la suite de sorte que tous les termes soient deux à deux distincts.

ii) Pour tout $x \in K$ il existe $a \in A$ et $s \in A \setminus 0$ tels que $x = \frac{a}{s}$. Dès lors, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(s)$. On conclut grâce au point précédent.
iii) Soit $\mathfrak{I}$ un idéal fractionnaire et notons x_i ,$1 \leq i \leq d$ des générateurs. Pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$ et tout

$$x = \sum_{i=1}^{d} a_i x_i \in \mathfrak{I} ,$$

$$v_{\mathfrak{p}}(x) \geq \min_{1 \leq i \leq d}(v_{\mathfrak{p}}(a_i x_i)) \geq \min_{1 \leq i \leq d}(v_{\mathfrak{p}}(x_i)) .$$

On déduit du lemme III.1.1.3.i que, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(\mathfrak{I}) = \inf_{x \in \mathfrak{I}}(v_{\mathfrak{p}}(x)) \geq \min_{1 \leq i \leq d}(v_{\mathfrak{p}}(x_i)) .$$

Or, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, il existe $1 \leq i(\mathfrak{p}) \leq d$ tel que

$$v_{\mathfrak{p}}(x_{i(\mathfrak{p})}) = \min_{1 \leq i \leq d}(v_{\mathfrak{p}}(x_i)) .$$

Or $x_{i(\mathfrak{p})} \in \mathfrak{I}$ d'où il découle que

$$v_{\mathfrak{p}}(\mathfrak{I}) = v_{\mathfrak{p}}(x_{i(\mathfrak{p})}) .$$

Il en résulte finalement que

$$\{\mathfrak{p} \in \mathrm{Spm}(A) \mid v_{\mathfrak{p}}(\mathfrak{I}) \neq 0\} \subset \bigcup_{i=1}^{d} \{\mathfrak{p} \in \mathrm{Spm}(A) \mid v_{\mathfrak{p}}(x_i) \neq 0\}$$

qui est fini grâce au point précédent.
iv) Il est clair que $x \in \mathfrak{p}$ si et seulement si $v_{\mathfrak{p}}(x) \geq 1$. Par ailleurs, $x \in \mathfrak{p}$ implique $x \in A$ donc pour tout $\mathfrak{q} \in \mathrm{Spm}(A)$ $v_{\mathfrak{q}}(x) \geq 0$. Or si $\mathfrak{q} \neq \mathfrak{p}$, il existe $x \in \mathfrak{p}$, $x \notin \mathfrak{q}$ et par conséquent, $v_{\mathfrak{q}}(x) = 0$, d'où il découle que

$$v_{\mathfrak{q}}(\mathfrak{p}) = \inf_{x \in \mathfrak{p}}(v_{\mathfrak{q}}(x)) = 0 .$$

Il découle ensuite du lemme III.1.1.2 que

$$v_{\mathfrak{q}}(\mathfrak{p}^n) = n v_{\mathfrak{q}}(\mathfrak{p}) \; \forall \mathfrak{q} \in \mathrm{Spm}(A) .$$

q.e.d

Proposition III.1.1.9. *Pour tout idéal fractionnaire $\mathfrak{I} \in \mathcal{I}(A)$,*

$$\mathfrak{I} = \prod_{\mathfrak{p} \in \mathrm{Spm}(A) \ , \ v_{\mathfrak{p}}(\mathfrak{I}) \neq 0} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{I})} = \prod_{\mathfrak{p} \in \mathrm{Spm}(A)} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{I})} .$$

Cette décomposition est unique.

Preuve : Notons

$$\mathfrak{J} := \prod_{\mathfrak{p}\in \mathrm{Spm}(A)\ ,\ v_{\mathfrak{p}}(\mathfrak{I})\neq 0} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{I})} .$$

Il découle alors de III.1.1.2 et III.1.1.8.iv que, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$,

$$v_{\mathfrak{p}}(\mathfrak{J}) \ = \ v_{\mathfrak{p}}(\mathfrak{I})$$

ce qui entraîne d'après le point III.1.1.3.ii, que

$$\mathfrak{I} \ = \ \mathfrak{J} .$$

Un argument analogue prouve l'unicité de cette décomposition. *q.e.d*

Remarque III.1.1.10. Cette proposition correspond à la décomposition en produit de facteurs premiers dans les anneaux principaux (voire factoriels).

Théorème III.1.1.11. Structure du groupe des idéaux fractionnaires d'un anneau de Dedekind *L'ensemble des idéaux fractionnaires d'un anneau de Dedekind muni de la loi de composition définie en I.1.5.4 est un groupe abélien $\mathcal{I}(A)$. Le morphisme*

$$\phi \ : \ \mathbb{Z}^{(\mathrm{Spm}(A))} \ \rightarrow \ \mathcal{I}(A)$$

défini en III.1.1.6 est un isomorphisme.

Proposition III.1.1.12. Lemme d'approximation *Soit A un anneau de Dedekind de corps des fractions K, $\mathfrak{p}_{i\ ,1\leq i\leq d}$ des idéaux maximaux deux à deux distincts de A, $n_{i\ ,1\leq i\leq d} \in \mathbb{Z}$ et des éléments $a_{i\ ,1\leq i\leq d} \in K$. Alors il existe $x \in K$ tel que pour tout $1 \leq i \leq d$,*

$$v_{\mathfrak{p}_i}(x - a_i) \ \geq \ n_i \text{ et } v_{\mathfrak{p}_i}(x) \ \geq \ 0 .$$

Preuve :
i) Si les a_i sont entiers c'est-à-dire les a_i sont dans A alors le résultat est une conséquence du théorème des restes chinois.

ii) Si les $a_{i\ ,1\leq i\leq d}$ ne sont pas dans A, comme ils sont en nombre fini et dans $K \ = \ \mathrm{Frac}(A)$, il existe $b_{i\ ,1\leq i\leq d} \in A$ et $s \in A \setminus 0$ tels que

$$a_i \ = \ \frac{b_i}{s} \ \forall 1 \leq i \leq d .$$

D'après le point précédent, il existe $y \in A$ tel que pour tout $1 \leq i \leq d$, $v_{\mathfrak{p}_i}(y - sa_i) \ \geq n_i + v_{\mathfrak{p}_i}(s)$ et $v_{\mathfrak{p}}(y) \geq v_{\mathfrak{p}}(s)$ si $\mathfrak{p}$ n'est pas l'un des $\mathfrak{p}_i$ et si $v_{\mathfrak{p}}(s) > 0$. Alors

$$x \ = \ \frac{y}{s}$$

répond à la question.

q.e.d

Corollaire III.1.1.13. *Un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux maximaux est principal.*

Preuve : Il suffit de démontrer que les idéaux maximaux $\mathfrak{p}_i$,$_{1\leq i\leq d}$ sont principaux.

Fixons $1 \leq j \leq d$. Pour tout $i \neq j$, posons $a_i := 1$ et prenons pour a_j un générateur de l'idéal maximal du localisé $A_{\mathfrak{p}_j}$ qui est bien un élément de K. D'après la proposition III.1.1.12 il existe $x_j \in K$ tel que $v_{\mathfrak{p}_i}(x_j - a_i) \geq 2$ pour tout $1 \leq i \leq d$. Ceci implique en particulier, que x_j n'est dans aucun des $\mathfrak{p}_i$ pour $i \neq j$, $x_j \in \mathfrak{p}_j$ et que $x_j \notin \mathfrak{p}_j^2$.

Reste à montrer que x_j est un générateur de $\mathfrak{p}_j$ ce qui est laissé en exercice. *q.e.d*

Définition III.1.1.14. Groupe de Picard ou groupe des classes d'idéaux Soit A un anneau de Dedekind, K son corps des fractions et $\mathcal{I}(A)$ le groupes des idéaux fractionnaires de A (cf. III.1.1.11.)

On a alors un morphisme de groupes

$$\begin{array}{rccc} \rho : & K^\times & \to & \mathcal{I}(A) \\ & c & \mapsto & cA\,. \end{array}$$

Le noyau de ρ est l'ensemble des $c \in K^\times$ tels que $cA = A$, qui est exactement $A^\times$.

L'image de ρ est, par définition, le *groupe des idéaux fractionnaires principaux*, et le groupe quotient est le *groupe de Picard* $\mathrm{Pic}(A)$ encore appelé *groupe des classes d'idéaux*.

On a une suite exacte

$$1 \to K^\times/A^\times \to \mathcal{I}(1) \to \mathrm{Pic}(A) \to 1$$

L'anneau est principal équivaut à dire que $\mathrm{Pic}(A)$ est le groupe trivial.

III.1.2 . −Décomposition des idéaux dans les extensions algébriques

Dans cette section A est un anneau de Dedekind (cf. I.5.2.2,) K son corps des fractions, L une extension finie séparable de degré d de K et B la fermeture intégrale (cf. I.4.1.9) de A dans L. On rappelle (cf. I.5.2.6,) que B est alors un anneau de Dedekind. On rappelle également que, pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, le localisé $A_\mathfrak{p}$ (cf. I.3.3.7) est un anneau de valuation discrète (cf. I.5.2.1.)

On notera $\mathcal{I}(A)$ (resp. $\mathcal{I}(B)$) le groupe des idéaux fractionnaires (cf. III.1.1.11) de A (resp. B.)

Lemme III.1.2.1. *Pour tout idéal fractionnaire $\mathfrak{I} \in \mathcal{I}(A)$, le sous-$B$-module de L $B\mathfrak{I}$ engendré par $\mathfrak{I}$ est un idéal fractionnaire de B ce qui définit une application*

$$\begin{array}{rccc} & \mathcal{I}(A) & \to & \mathcal{I}(B) \\ & \mathfrak{I} & \mapsto & B\mathfrak{I}\,. \end{array} \qquad \textit{III.1.2.2}$$

On a aussi une application

$$\begin{array}{rccc} & \mathcal{I}(B) & \to & \mathcal{I}(A) \\ & \mathfrak{J} & \mapsto & \mathfrak{J} \cap K\,. \end{array} \qquad \textit{III.1.2.3}$$

Preuve : La seule chose qui doive être justifiée est que l'application III.1.2.3 est à valeurs dans $\mathcal{I}(A)$ puisque a priori, pour $\mathfrak{J}$ un idéal fractionnaire de B, $\mathfrak{J} \cap K$ est un sous-A-module de K non nécessairement de type fini.

Pour tout idéal $\mathfrak{J} \subset B$, les éléments de $\mathfrak{J} \cap K$, sont à la fois dans B donc entiers sur A et dans K c'est-à-dire dans A puisque ce dernier est intégralement clos. $\mathfrak{J} \cap K$ est donc un idéal de A de type fini puisque A est noethérien.

On se ramène au cas d'un idéal pour un idéal fractionnaire quelconque. *q.e.d*

Proposition III.1.2.4. *Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, il existe un unique entier $g_\mathfrak{p} \geq 1$, un unique $g_\mathfrak{p}$-uplet $\mathfrak{q}_{i\ ,1\leq i\leq g_\mathfrak{p}} \in \mathrm{Spm}(B)$ et unique $g_\mathfrak{p}$-uplet $e_{\mathfrak{q}_i/\mathfrak{p}\ ,1\leq i\leq g_\mathfrak{p}} \in \mathbb{N}^*$ tels que :*
a) l'ensemble $\{\mathfrak{q}_i\}_{1\leq i\leq g_\mathfrak{p}}$ est l'ensemble des idéaux maximaux de B au-dessus de $\mathfrak{p}$ (cf. I.4.3.1,) c'est-à-dire que

$$\mathfrak{q}_i \cap K = \mathfrak{q}_i \cap A = \mathfrak{p}\ \forall 1 \leq i \leq g_\mathfrak{p}$$

et que les $\mathfrak{q}_i$ sont les seuls éléments de $\mathrm{Spm}(B)$ vérifiant cette propriété ;
b)

$$B\mathfrak{p} = \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}\ .$$

Preuve : Si $\mathfrak{p}$ est un idéal maximal de A, $B\mathfrak{p} \neq B$ (cf. I.4.3.2.) L'entier $g_\mathfrak{p}$, les éléments $\mathfrak{q}_{i\ ,1\leq i\leq g_\mathfrak{p}}$ et les entiers

$$e_{\mathfrak{q}_i/\mathfrak{p}} := v_{\mathfrak{q}_i}(B\mathfrak{p})$$

(cf. III.1.1.1) satisfaisant la condition (b) sont entièrement déterminés grâce à la proposition III.1.1.9. Par ailleurs, il résulte du lemme III.1.1.3.iii que, pour tout $1 \leq i \leq g_\mathfrak{p}$ $e_{\mathfrak{q}_i/\mathfrak{p}} \geq 1$.

Il résulte du point (b) que, pour tout $1 \leq i \leq g_\mathfrak{p}$,

$$B\mathfrak{p} \subset \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}} \subset \mathfrak{q}_i\ .$$

Il s'ensuit que $\mathfrak{p} \subset \mathfrak{q}_i \cap A$ d'où $\mathfrak{p} = \mathfrak{q}_i \cap A$ (puisque $\mathfrak{p}$ est maximal.) On a donc bien montré que $\mathfrak{q}_i$ est au-dessus de $\mathfrak{p}$.

Réciproquement, si $\mathfrak{q} \in \mathrm{Spm}(B)$ est au-dessus de $\mathfrak{p}$ $B\mathfrak{p} \subset \mathfrak{q}$ ce qui veut précisément dire que $v_\mathfrak{q}(B\mathfrak{p}) > 0$ c'est-à-dire que $\mathfrak{q}$ est l'un des $\mathfrak{q}_i$. *q.e.d*

Définition III.1.2.5. Les notations étant celle de la proposition III.1.2.4,
i) **Indice de ramification** l'entier

$$e_{\mathfrak{q}_i/\mathfrak{p}\ ,1\leq i\leq g_\mathfrak{p}} = v_{\mathfrak{q}_i}(B\mathfrak{p})$$

est appelé *indice de ramification* de $\mathfrak{q}_i$ par rapport à $\mathfrak{p}$.

ii) **Degré résiduel** Comme B est un A-module de type fini (cf. I.4.4.2,) pour tout $1 \leq i \leq g_\mathfrak{p}$, $B/\mathfrak{q}_i$ est une extension algébrique finie de $A/\mathfrak{p}$. On note $f_{\mathfrak{q}_i/\mathfrak{p}}$ son degré qu'on appelle *degré résiduel*.

Proposition III.1.2.6. *Si K est un corps local (cf. II.3.2.1,) l'anneau de la valuation $\mathcal{O}_K$ est alors un anneau de Dedekind (c'est un anneau de valuation discrète) et sa clôture intégrale $\mathcal{O}_L$ est aussi un anneau de valuation discrète. Alors*

$$e_{\mathfrak{m}_L/\mathfrak{m}_K} \;=\; e_{L/K} \text{ et } f_{\mathfrak{m}_L/\mathfrak{m}_K} \;=\; f_{L/K}$$

où les indice de ramification $e_{L/K}$ et degré résiduel $f_{L/K}$ sont ceux définis en II.3.1.4.

Preuve : Cela se déduit facilement du théorème II.3.1.2. *q.e.d*

Lemme III.1.2.7. *Soit M une extension finie séparable de L et C la clôture intégrale de B dans M, qui est aussi la clôture intégrale de A dans M.*

Pour tout idéal maximal $\mathfrak{r} \subset C$, notons $\mathfrak{q} \;:=\; B \cap \mathfrak{r}$, et

$$\mathfrak{p} \;:=\; A \cap \mathfrak{q} \;=\; A \cap \mathfrak{r}\,.$$

On a alors :

$$f_{\mathfrak{r}/\mathfrak{p}} \;=\; f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} \text{ et } e_{\mathfrak{r}/\mathfrak{p}} \;=\; e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}}\,.$$

Proposition III.1.2.8. *Avec les notations de la proposition III.1.2.4, Si A est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}$,*

$$\sum_{i=1}^{g_\mathfrak{p}} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}} \;=\; d\,.$$

Preuve : Si A est un anneau de valuation discrète, A est principal. Par conséquent, B est un A-module libre de rang d (cf. I.4.4.3.) Si l'on note $k \;:=\; A/\mathfrak{p}$ le corps résiduel, $\dim_k B/B\mathfrak{p} \;=\; \dim_k B \otimes_A k$ (cf. I.2.2.3,) qui est encore égale à

$$\dim_k A^d \otimes_A k \;=\; \dim_k k^d \;=\; d$$

(cf. I.2.1.8.iv.)

De plus, tous les idéaux maximaux de B sont au-dessus de l'unique idéal maximal de A. L'anneau de Dedekind B a donc $g_\mathfrak{p}$ idéaux maximaux ce qui entraîne qu'il est principal (cf. III.1.1.13.)

D'après la proposition III.1.2.4, il existe un unique

$$\left(g_\mathfrak{p}, \mathfrak{q}_i\,,1\leq i\leq g_\mathfrak{p} \in \mathrm{Spm}(B), e_{\mathfrak{q}_i/\mathfrak{p}}\,,1\leq i\leq g_\mathfrak{p} \in \mathbb{N}^*\right)$$

tel que

$$B\mathfrak{p} \;=\; \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}\,.$$

Il existe alors un isomorphisme naturel de B-modules

$$B/B\mathfrak{p} \;\cong\; \prod_{i=1}^{g_\mathfrak{p}} B/\mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$$

par le théorème chinois des restes. Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, $B/\mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$ acquiert dès lors une structure de $B/B\mathfrak{p}$-module. Ce dernier étant une k-algèbre chaque $B/\mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$ acquiert une structure de k-espace vectoriel si bien que l'isomorphisme ci-dessus est un isomorphisme de k-espaces vectoriels.

Il en résulte que ,

$$d \;=\; \dim_k B/B\mathfrak{p} \;=\; \sum_{i=1}^{g_{\mathfrak{p}}} \dim_k B/\mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}} \;. \qquad \text{III.1.2.8.1}$$

Or $\dim_k B/\mathfrak{q}_i \;=\; f_{\mathfrak{q}_i/\mathfrak{p}}$ par définition (cf. III.1.2.5.ii.)

Il suffit finalement d'appliquer le lemme II.3.1.3 et l'égalité III.1.2.8.1 pour conclure. *q.e.d*

Proposition III.1.2.9. *Avec les notations de la proposition III.1.2.4, pour tout* $\mathfrak{p} \in \mathrm{Spm}(A)$ *et toute partie multiplicative (cf. I.3.1.1)* S *telle que* $S \cap \mathfrak{p} \;=\; \emptyset$,

i) $S^{-1}A$ *(cf. I.3.1.3) est un anneau de Dedekind de corps des fractions* K, $S^{-1}B$ *est la clôture intégrale de* $S^{-1}A$ *dans* L.

ii) Pour tout idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$ *de* B *au-dessus de* A, $S^{-1}\mathfrak{q}$ *est un idéal maximal de* $S^{-1}B$ *au dessus de* $S^{-1}\mathfrak{p}$ *et*

iii)

$$e_{\mathfrak{q}/\mathfrak{p}} \;=\; e_{S^{-1}\mathfrak{q}/S^{-1}\mathfrak{p}}$$

et

$$f_{\mathfrak{q}/\mathfrak{p}} \;=\; f_{S^{-1}\mathfrak{q}/S^{-1}\mathfrak{p}} \,.$$

Preuve :

i) Découle des résultats des paragraphes I.4 et I.5.2.

Pour tout idéal maximal $\mathfrak{p}$ de A, écrivons

$$B\mathfrak{p} \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$$

grâce à la proposition III.1.2.4. Il en résulte que

$$S^{-1}(B\mathfrak{p}) \;=\; B\mathfrak{p} \otimes_A S^{-1}A \;=\; S^{-1}\big(\prod_{i=1}^{g_{\mathfrak{p}}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}\big) \,.$$

Il en résulte, grâce à la proposition I.3.2.5, que

$$S^{-1}(B\mathfrak{p}) \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} S^{-1}(\mathfrak{q}_i)^{e_{\mathfrak{q}_i/\mathfrak{p}}} \;. \qquad \text{III.1.2.9.1}$$

Par ailleurs

$$S^{-1}(B\mathfrak{p}) \;=\; S^{-1}BS^{-1}\mathfrak{p}$$

(cf. I.3.2.4.) L'égalité III.1.2.9.1 s'écrit donc désormais

$$S^{-1}BS^{-1}\mathfrak{p} \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} p^{-1}(\mathfrak{q}_i)^{e_{\mathfrak{q}_i/\mathfrak{S}}} \;. \qquad \text{III.1.2.9.2}$$

Il découle du lemme I.4.3.4.iii que pour tout $1 \leq i \leq g_{\mathfrak{p}}$,
– $S^{-1}(\mathfrak{q}_i)$ est un idéal maximal de $S^{-1}B$,
– et que

$$B/\mathfrak{q}_i \;\cong\; S^{-1}B/S^{-1}(\mathfrak{q}_i)\;.$$

Comme le même résultat appliqué à A lui-même donne

$$k \;:=\; A/\mathfrak{p} \;\cong\; S^{-1}A/S^{-1}\mathfrak{p}$$

le deuxième point ci-dessus donne

$$f_{\mathfrak{q}_i/\mathfrak{p}} \;=\; f_{S^{-1}(\mathfrak{q}_i)/S^{-1}\mathfrak{p}}\;.$$

Le premier point quant à lui montre que la décomposition III.1.2.9.2 est celle donnée par la proposition III.1.2.4 mais pour l'extension entière

$$S^{-1}A \;\subset\; S^{-1}B\;.$$

Ceci prouve que

$$e_{\mathfrak{q}_i/\mathfrak{p}} \;=\; e_{S^{-1}(\mathfrak{q}_i)/S^{-1}\mathfrak{p}}\;.$$

q.e.d

Proposition III.1.2.10. *Avec les notations de la proposition III.1.2.4, Si A est un anneau de Dedekind,*

$$\sum_{i=1}^{g_{\mathfrak{p}}} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}} \;=\; d\;\forall \mathfrak{p} \in \mathrm{Spm}(A)\;.$$

Preuve : Ce résultat est une conséquence immédiate des proposition III.1.2.8 et III.1.2.9 en se rappelant que pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, $A_{\mathfrak{p}}$ est un anneau de valuation discrète. *q.e.d*

Remarque III.1.2.11. Le résultat ci-dessus est l'exacte analogue du point II.3.1.2.v qui pourrait en être un corollaire.

III.2 . −Complétée d'une extension d'anneaux de Dedekind

III.2.0 . −Préliminaires

Lemme III.2.0.1. *On pourrait donner un énoncé un peu plus précis de la proposition I.6.1.10*[8] *: Soient $(I, \leq)$ un ensemble ordonné et $(J, \leq) \subset (I, \leq)$ un sous-ensemble ordonné par la relation d'ordre induite. Soient*

$$\big(I, \{X_i\}_{i\in I}, \{x_{i,j}\}_{(i,j)\in I^2, i\leq j}\big) \text{ et } \big(J, \{Y_i\}_{i\in J}, \{y_{i,j}\}_{(i,j)\in J^2, i\leq j}\big)$$

des systèmes projectifs à valeurs dans une C *respectivement indexés par I et J. On note*

$$\big(X, \{x_i \,:\, X \,\to\, X_i\}_{i\in I}\big) \text{ et } \big(Y, \{y_j \,:\, Y \,\to\, Y_j\}_{j\in J}\big)$$

leurs limites projectives respectives (on suppose qu'elles existent.)

Soit $\{u_j \,:\, X_j \,\to\, Y_j\}_{j\in J}$ un ensemble de morphismes dans C *tel que pour tout $(i, j) \in J^2, \ , \ i \leq j$, le carré*

$$\begin{array}{ccc} X_j & \xrightarrow{u_j} & Y_j \\ {\scriptstyle x_{i,j}}\downarrow & & \downarrow{\scriptstyle y_{i,j}} \\ X_i & \xrightarrow{u_i} & Y_i \end{array}$$

est commutatif. Alors, en vertu de la proposition I.6.1.8, il existe un unique morphisme

$$u \,:\, X \,\to\, Y$$

tel que, pour tout $j \in J$,

$$y_j \circ u \,=\, u_j \circ x_j \,.$$

Si de plus on suppose que :

a) I est filtrant (cf. I.6.1.11.)

b) Pour tout $i \in I$, il existe $j \in J$ tel que $i \leq j$ (on dit que J est cofinal dans I.)

c) Pour tout $j \in J$, u_j est un isomorphisme.

Alors u est un isomorphisme.

Preuve : Pour tout $i \in J$, le morphisme $u_i \,:\, X_i \,\to\, Y_i$ possède, par l'hypothèse (c), un inverse $v_i \,:\, Y_i \,\to\, X_i$. L'identité

$$u_i \circ x_{i,j} \,=\, y_{i,j} \circ u_j$$

implique que

$$u_i \circ x_{i,j} \circ v_j \,=\, y_{i,j}$$

ce qui implique encore que

$$x_{i,j} \circ v_j \,=\, v_i \circ y_{i,j} \,. \qquad \text{III.2.0.1.1}$$

[8] Cet énoncé remplacerait d'ailleurs avec profit la proposition I.6.1.10.

Remarquons ensuite que les hypothèses (a) et (b) entraînent que J lui-même est filtrant.

Pour tout $i \in I$ et tout $(j_1, j_2) \in J^2$ avec $i \leq j_1$ et $i \leq j_2$, il existe donc $j_3 \in J$ tel que $j_1 \leq j_3$ et $j_2 \leq j_3$.

Il existe alors des morphismes

$$v_{j_\alpha} \ : \ Y_{j_\alpha} \ \rightarrow \ X_{j_\alpha} \ ,\alpha\in\{1;2;3\}$$

inverses respectivement de $u_{j_\alpha} \ : \ X_{j_\alpha} \ \rightarrow \ Y_{j_\alpha}$ en vertu de l'hypothèse (c). On a alors

$$x_{i,j_1} \circ v_{j_1} \circ y_{j_1} \ = \ x_{i,j_1} \circ v_{j_1} \circ y_{j_1,j_3} \circ y_{j_3}$$

qui vaut encore grâce à III.2.0.1.1

$$\begin{aligned} x_{i,j_1} \circ x_{j_1,j_3} \circ v_{j_3} \circ y_{j_3} \ &= \ x_{i,j_3} \circ v_{j_3} \circ y_{j_3} \\ &= \ x_{i,j_2} \circ x_{j_2,j_3} \circ v_{j_3} \circ y_{j_3} \\ &= \ x_{i,j_2} \circ v_{j_2} \circ y_{j_2,j_3} \circ y_{j_3} \\ &= \ x_{i,j_2} \circ v_{j_2} \circ y_{j_2} \ . \end{aligned}$$

On peut donc poser, pour tout $i \in I$,

$$w_i \ := \ x_{i,j} \circ v_j \ : \ Y \ \rightarrow \ X_i \ \forall j \geq i$$

(puisque cette définition ne dépend pas du j choisi d'après ce qui précède. Pour tout $i \leq j$ dans I, on a bien entendu $w_i \ = \ x_{i,j} \circ w_j$. (À noter que pour tout $j \in J$, $w_j \ = \ v_j$ par construction.) La collection des $w_i \ ,i\in I$ se factorise donc en un unique morphisme

$$w \ : \ Y \ \rightarrow \ X \mid x_i \circ w \ = \ w_i \ \forall i \in I \ .$$

Pour tout $i \in I$, on a donc

$$x_i \circ w \circ u \ = \ w_i \circ u \ = \ x_{i,j} \circ v_j \circ y_j \circ u$$

pour « n'importeu quel » $j \in J$ $i \leq j$. Ceci vaut encore

$$x_{i,j} \circ v_j \circ u_j \circ x_j \ = \ x_{i,j} \circ x_j \ = \ x_i$$

ce qui prouve finalement que

$$w \circ u \ = \ \mathrm{Id}_X \ .$$

D'autre part, pour tout $j \in J$,

$$y_j \circ u \circ w \ = \ u_j \circ x_j \circ w \ = \ u_j \circ w_j \circ y_j \ = \ u_j \circ v_j \circ y_j \ = \ y_j$$

ce qui prouve finalement que

$$u \circ w \ = \ \mathrm{Id}_Y \ .$$

On a donc démontré que u et w étaient inverses l'un de l'autre. *q.e.d*

Corollaire III.2.0.2. *Soient P une partie infinie de $\mathbb{N}$, $X_{n\ ,n\in\mathbb{N}}$ et $Y_{n\ ,n\in P}$ des systèmes projectifs respectivement indexés par $\mathbb{N}$ et P*

$$u_i\ :\ X_i\ \cong\ Y_{i\ ,i\in P}$$

des isomorphismes compatibles aux morphismes de transition. Alors les u_i se factorisent en un isomorphisme $u\ :\ X\ \cong\ Y$. Les cas notamment où

$$P\ =\ [k;+\infty[\ k\in\mathbb{N}\ \text{ou}\ P\ =\ k\mathbb{N}\ k\in\mathbb{N}$$

seront utilisés dans la suite.

Lemme III.2.0.3. *Les hypothèses sont celles de la proposition I.6.3.1* [9]*. On suppose de plus que :*

- *$I\ =\ \mathbb{N}$ muni de sa relation d'ordre usuelle.*
- *Pour tout $i\in I$, la suite*

$$0\ \to\ P_i\xrightarrow{f_i}Q_i\longrightarrow\xrightarrow{g_i}R_i\ \to\ 0$$

  est exacte.
- *Pour tout $i\leq j$, la flèche $p_{i,j}\ :\ P_j\ \to\ P_i$ est surjective.*

Alors la suite

$$0\ \to\ L\xrightarrow{f}M\longrightarrow\xrightarrow{g}N\ \to\ 0$$

est exacte.

Preuve : En vertu de la proposition I.6.3.1 on sait déjà que la suite

$$0\ \to\ L\xrightarrow{f}M\longrightarrow\xrightarrow{g}N$$

est exacte, il ne reste donc plus qu'à montrer que g est surjective.

Pour tout $z\in N$, posons

$$z_{i\ ,i\in I}\ :=\ n_i(z)\ \in R_i\ .$$

- La flèche g_0 étant surjective, il existe $y_0\in Q_0$ tel que $g(y_0)\ =\ z_0$.
- Pour $k\in\mathbb{N}$, supposons construite une famille $y_{i\ ,0\leq i\leq k}\in Q_i$ telle que :

$$g_i(y_i)\ =\ z_i\forall 0\leq i\leq k,$$

$$q_{i,j}(y_j)\ =\ y_i\ \forall 0\leq i\leq j\leq k\ .$$

- Considérons alors un relèvement w de z_{k+1} dans Q_{k+1} qui existe en vertu de la surjectivité de g_{k+1}. On a alors

$$\begin{aligned} g_k[q_{k,k+1}(w)] &= r_{k,k+1}(z_{k+1})\\ &= z_k\\ &= g_k(y_k)\ . \end{aligned}$$

  Il s'ensuit que $y_k-q_{k,k+1}(w)\in\operatorname{Ker}g_k\ =\ \operatorname{Im}f_k$.

[9] D'ailleurs ce lemme mériterait d'être inséré comme un ajout à la proposition I.6.3.1.

– Il existe donc $x_k \in P_k$ tel que $y_k - q_{k,k+1}(w) = f_k(x_k)$. Puisque $p_{k,k+1}$ est surjective il existe $x_{k+1} \in P_{k+1}$ tel que $p_{k,k+1}(x_{k+1}) = x_k$.
– Posons alors $y_{k+1} := w + f_{k+1}(x_{k+1})$. Il s'ensuit que

$$g_{k+1}(y_{k+1}) = g_{k+1}(w) + g_{k+1}[f_{k+1}(x_{k+1})] = z_{k+1}$$

et que

$$\begin{aligned} q_{k,k+1}(y_{k+1}) &= q_{k,k+1}(w + f_{k+1}(x_{k+1})) \\ &= q_{k,k+1}(w) + f_k[p_{k,k+1}(x_{k+1})] \\ &= q_{k,k+1}(w) + f_k(x_k) \\ &= q_{k,k+1}(w) + y_k - q_{k,k+1}(w) \\ &= y_k \ . \end{aligned}$$

– Par récurrence, il existe donc une suite $y_k \ ,_{k\in\mathbb{N}} \in Q_k$ telle que

$$g_k(y_k) = z_k \ \forall k \in \mathbb{N}$$

et

$$q_{i,j}(y_j) = y_i \ \forall i \leq j \ .$$

Cette suite définit donc un élément $y \in M$ vérifiant

$$m_k(y) = y_k \ \forall k \in \mathbb{N} \ .$$

De plus, pour tout $k \in \mathbb{N}$,

$$\begin{aligned} n_k[g(y)] &= g_k[m_k(y)] \\ &= z_k \\ &= n_k(z) \end{aligned}$$

ce qui signifie exactement que

$$g(y) = z \ .$$

q.e.d

Définition III.2.0.4. On pourrait synthétiser les hypothèses de la proposition I.6.3.1 et notamment la donnée des diagrammes I.6.3.2 en disant qu'on a un *système projectif de suites exactes*. Cette dénomination n'est pas abusive au sens où l'on peut appeler *morphisme de suites exactes* un diagramme commutatif à lignes exactes comme en I.6.3.2. Ces morphismes satisfont aux axiomes des catégories (cf. 0.3.1.1,) ce qui autorise à les appeler ainsi.

Lemme III.2.0.5. Lemme d'Artin-Rees *Soit A un anneau noethérien, $\mathfrak{I} \subset A$ un idéal, M un A-module de type fini et R un sous-A-module de M. Alors il existe $k \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$,*

$$R \cap \mathfrak{I}^{n+k} M = \mathfrak{I}^n (R \cap \mathfrak{I}^k M) \ .$$

Définition III.2.0.6. Étant donnés deux foncteurs covariants (cf. 0.3.2.1)

$$F \text{ et } G \ : \ \mathbf{C} \ \to \ \mathbf{D},$$

on appelle *transformation naturelle* $u^{\cdot} \ : \ F(\cdot) \ \to \ G(\cdot)$ de F dans G la donnée, pour tout objet X de $\mathbf{C}$ d'un morphisme $u^X \ : \ F(X) \ \to \ G(X)$ dans $\mathbf{D}$ tel que pour tout morphisme

$$f \ : \ X \ \to \ Y$$

dans $\mathbf{C}$, le carré de morphismes dans $\mathbf{D}$

$$\begin{array}{ccc} F(X) & \xrightarrow{u^X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{u^Y} & G(Y) \end{array}$$

soit commutatif.

Remarque III.2.0.7. La définition ci-dessus peut paraître très formelle mais elle n'est donnée qu'en vue de s'éviter de devoir écrire d'innombrables diagrammes commutatifs comme en III.2.1.3.ii.

III.2.1 . −Complétions $\mathfrak{I}$-adiques

Dans la suite de ce numéro (III.2.1,) A est un anneau et $\mathfrak{I} \subset A$ un idéal.

Lemme III.2.1.1. *Soit M un A-module. Pour tout $n \in \mathbb{N}$, on note*

$$M_n \ := \ M \otimes_A A/\mathfrak{I}^n \ = \ M/\mathfrak{I}^n M$$

$\pi_n^M \ : \ M \ \to \ M_n$ la projection naturelle. Pour tout $r \leq s$ dans $\mathbb{N}$, on note $\rho_{r,s}^M \ : \ M_s \ \to \ M_r$ le morphisme de A-modules induit par l'inclusion naturelle $\mathfrak{I}^s M \subset \mathfrak{I}^r M$.
i)

$$\big(\mathbb{N}, \{M_r\}_{r\in\mathbb{N}}, \{\rho_{\cdot\ r,s}^{M}\}_{(r,s)\in\mathbb{N}^2, r\leq s}\big)$$

est un système projectif (cf. I.6.1.1.) Sa limite projective (cf. I.6.1.3)

$$\hat{M} \ := \ \big(\hat{M}, \{\pi^{\hat{M}}{}_n \ : \ \hat{M} \ \to \ M_n\}_{n\in\mathbb{N}}\big) \ := \ \varprojlim_{n\in\mathbb{N}} M_n$$

existe dans la catégorie des A-modules.
ii)

$$\big(M, \{\pi^M{}_n \ : \ M \ \to \ M_n\}_{n\in\mathbb{N}}\big)$$

est un diagramme commutatif qui se factorise de manière unique en un morphisme de A-modules

$$\lambda^M \ : \ M \ \to \ \hat{M} \ := \ \varprojlim_{n\in\mathbb{N}} M_n \ .$$

iii) On note

$$\mathcal{S}(M) \;:=\; M/\mathrm{Ker}\,\lambda^M \;=\; M/\big(\bigcap_{n\in\mathbb{N}}(\mathfrak{I}^n M)\big)\;.$$

Le morphisme λ^M se factorise à travers $\mathcal{S}(M)$:

$$\begin{array}{ccc} M & \xrightarrow{\pi^M} & \mathcal{S}(M) \\ & {\scriptstyle\lambda^M}\searrow & \big\downarrow{\scriptstyle\theta^M} \\ & & \hat{M} \end{array}$$

où π^M est surjectif et θ^M est injectif.

Pour tout $n \in \mathbb{N}$, on note

$$\pi_n^{\mathcal{S}(M)} \;:=\; \pi_n^{\hat{M}} \circ \theta^M \;:\; \mathcal{S}(M) \;\to\; M_n\;.$$

On a alors un diagramme commutatif

$$\begin{array}{ccc} M & & \\ {\scriptstyle\pi^M}\big\downarrow & \searrow^{\pi_n^M} & \\ \mathcal{S}(M) & \xrightarrow[\pi_n^{\mathcal{S}(M)}]{} & M_n \\ {\scriptstyle\theta^M}\big\downarrow & \nearrow_{\pi_n^{\hat{M}}} & \\ \hat{M} & & \end{array} \qquad \textit{III.2.1.1.1}$$

d'où il résulte que les morphismes $\pi_n^{\hat{M}}$ et $\pi_n^{\mathcal{S}(M)}$ sont surjectifs pour tout $n \in \mathbb{N}$.

Preuve : Cette démonstration très formelle est laissée comme exercice d'application du paragraphe I.6. *q.e.d*

Définition III.2.1.2. Étant donné un anneau A et un idéal $\mathfrak{I} \subset A$, pour tout A-module M, on notera

$$\hat{M} \;:=\; \big(\hat{M}, \{\pi^{\hat{M}}{}_n \;:\; \hat{M} \;\to\; M_n\}_{n\in\mathbb{N}}\big) \;:=\; \varprojlim_{n\in\mathbb{N}} M_n$$

la limite projective construite en III.2.1.1.i. On notera $\mathcal{S}(M)$ le A-module construit en III.2.1.1.iii. On conservera dans la suite les notations $\lambda^M, \pi^M, \ldots$ du lemme III.2.1.1.

Lemme III.2.1.3.

i) Les procédés,

$$\cdot \;\mapsto\; \cdot_n\,,_{n\in\mathbb{N}}\,,$$

$\cdot \mapsto \hat{\cdot}$ et $\cdot \mapsto \mathcal{S}(\cdot)$ sont des foncteurs covariants (cf. 0.3.2.1) de la catégorie des A-modules dans elle-même.

ii)

$$\begin{array}{lrcl}
\lambda^{\cdot}: & \mathrm{Id.} & \to & \hat{\cdot} \\
\pi^{\cdot}: & \mathrm{Id.} & \to & \mathcal{S}(\cdot) \\
\theta^{\cdot}: & \mathcal{S}(\cdot) & \to & \hat{\cdot} \\
\pi^{\cdot}_{n,n\in\mathbb{N}}: & \mathrm{Id.} & \to & \cdot_n \\
\pi^{\hat{\cdot}}_{nn\in\mathbb{N}}: & \hat{\cdot} & \to & \cdot_n \\
\pi_n^{\mathcal{S}(\cdot)}{}_{n\in\mathbb{N}}: & \mathcal{S}(\cdot) & \to & \cdot_n
\end{array}$$

sont des transformations naturelles (cf. III.2.0.6.)

Cela signifie par exemple, pour la première ligne ci-dessus, que pour tout morphisme de A-modules $u : M \to P$, que le carré

$$\begin{array}{ccc}
M & \xrightarrow{u} & P \\
{\scriptstyle \lambda^M}\downarrow & & \downarrow{\scriptstyle \lambda^P} \\
\hat{M} & \xrightarrow{\hat{u}} & \hat{P}
\end{array}$$

est commutatif, où bien, pour la dernière ligne, que le carré

$$\begin{array}{ccc}
\mathcal{S}(M) & \xrightarrow{\mathcal{S}(u)} & \mathcal{S}(P) \\
{\scriptstyle \pi_n^{\mathcal{S}(M)}}\downarrow & & \downarrow{\scriptstyle \pi_n^{\mathcal{S}(P)}} \\
M_n & \xrightarrow{u_n} & P_n
\end{array}$$

est commutatif pour tout $n \in \mathbb{N}$.

Preuve : La démonstration de ces faits est très formelle. *q.e.d*

Lemme III.2.1.4. *Dans ce lemme (III.2.1.4,) F désigne l'un des trois foncteurs de III.2.1.3.i et T l'une des transformation naturelles de III.2.1.3.ii.*
i) Dans le cas où le A-module M est l'anneau A lui-même, $F(A)$ a une structure de A-algèbre et T^A est un morphisme de A-algèbres.

ii) Pour tout A-module (resp. A-algèbre) X $F(X)$ a une structure naturel de $F(A)-$module (resp. $F(A)$-algèbre.)

Pour tout morphisme $u : X \to Y$ de A-modules, (resp. A-algèbres,) le morphisme

$$F(u) : F(X) \to F(Y)$$

est un morphisme de $F(A)$-module (resp. de $F(A)$-algèbre.)

En résumé, le foncteur F sur la catégorie des A-modules (resp. A-algèbres) est à valeurs dans la catégorie des $F(A)$-modules (resp. $F(A)$-algèbres.)

Preuve : Le seul point peut-être un peu délicat consiste à donner une structure d'anneaux à $\hat{A}$: Il suffit en fait de remarquer qu'une structure d'anneau sur $\hat{A}$ est essentiellement donnée par un certain nombre de morphismes $* : \hat{A} \times \hat{A} \to \hat{A}$ vérifiant un certain nombre de compatibilités. Or la structure d'anneau sur A définit les morphismes correspondants

$$*_n : A_n \times A_n \to A_n \mid \forall n \in \mathbb{N} .$$

Il suffit ensuite d'utiliser la remarque I.6.3.3.ii pour en déduire une structure d'anneau sur $\hat{A}$. *q.e.d*

Lemme III.2.1.5.
i) Soit M un A-module, puisque $\hat{M}$ (resp. $\mathcal{S}(M)$) est un $\hat{A}$-module (resp. $\mathcal{S}(A)$-module,) le morphisme de A-modules

$$\lambda^M \ : \ M \ \rightarrow \ \hat{M} \ (\textit{resp.}\ \pi^M \ : \ M \ \rightarrow \ \mathcal{S}(M) \ )$$

donne par adjonction (cf. I.2.2.4,) un morphisme de $\hat{A}$-module (resp. $\mathcal{S}(A)$-module)

$$\lambda^{M,*} \ : \ M \otimes_A \hat{A} \ \rightarrow \ \hat{M} \ (\textit{resp.}\ \pi^{M,*} \ : \ M \otimes_A \mathcal{S}(A) \ \rightarrow \ \mathcal{S}(M) \ .)$$

ii)

$$\lambda^{\cdot,*} \ : \ \cdot \otimes_A \hat{A} \ \rightarrow \ \hat{\cdot} \ \text{et} \ \pi^{\cdot,*} \ : \ \cdot \otimes_A \mathcal{S}(A) \ \rightarrow \ \mathcal{S}(\cdot)$$

sont des transformations naturelles et l'on a les relations :

$$\hat{\pi^{\cdot}_n} \ \circ \ \lambda^{\cdot,*} \ = \ \mathrm{Id.} \otimes_A \pi^{\hat{A}}_n \ \forall n \in \mathbb{N} \ ; \qquad \textit{III.2.1.5.1}$$

$$\pi^{\mathcal{S}(\cdot)}_n \ \circ \ \pi^{\cdot,*} \ = \ \mathrm{Id.} \otimes_A \pi^{\mathcal{S}(A)}_n \ \forall n \in \mathbb{N} \ . \qquad \textit{III.2.1.5.2}$$

Preuve : Cette démonstration est encore fastidieuse mais sans diffficulté. *q.e.d*

Lemme III.2.1.6.
i) On a $\mathcal{S}(\mathfrak{I}) \ = \ \mathfrak{I}/[\bigcap_{n\in\mathbb{N}} \mathfrak{I}^n]$ *et*

$$\mathrm{Ker}\, \pi^{\mathcal{S}(A)}_n \ \cong \ \mathcal{S}(\mathfrak{I})^n \ \forall n \in \mathbb{N} \qquad \textit{III.2.1.6.1}$$

si bien que le morphisme π^A induit des isomorphismes

$$A_n \ = \ A/\mathfrak{I}^n \ \cong \ \mathcal{S}(A)_n \ := \ \mathcal{S}(A)/[\mathcal{S}(\mathfrak{I})^n] \ \forall n \in \mathbb{N} \ . \qquad \textit{III.2.1.6.2}$$

On en déduit finalement un isomorphisme

$$\hat{A} \ \cong \ \widehat{\mathcal{S}(A)} \ := \ \varprojlim_{n\in\mathbb{N}} \mathcal{S}(A)/[\mathcal{S}(\mathfrak{I})^n] \ . \qquad \textit{III.2.1.6.3}$$

ii) Pour tout A-module M et $n \in \mathbb{N}$,

$$M_n \ = \ M/\mathfrak{I}^n M \ = \ M \otimes_A A_n \ = \ (M \otimes_A \mathcal{S}(A)) \otimes_{\mathcal{S}(A)} A_n$$

d'où il résulte un isomorphisme :

$$\hat{M} \ \cong \ M \ \widehat{\otimes_A \mathcal{S}}(A) \ = \ \varprojlim_{n\in\mathbb{N}} (M \otimes_A \mathcal{S}(A))/(\mathcal{S}(\mathfrak{I})^n (M \otimes_A \mathcal{S}(A))) \ . \qquad \textit{III.2.1.6.4}$$

Lemme III.2.1.7.
i) Pour tout $k \in \mathbb{N}$,

$$\mathrm{Ker}\, \pi_k^{\hat{A}} \;=\; \widehat{\mathfrak{I}^k} \;=\; \varprojlim_{n\in\mathbb{N}} \mathfrak{I}^k/\mathfrak{I}^n \;.$$

Il en résulte en particulier que $\hat{\mathfrak{I}}^k \;=\; \mathrm{Ker}\, \pi_k^{\hat{A}}$ *est un idéal de* $\hat{A}$ *pour tout* $k \in \mathbb{N}$.
ii) On a en fait

$$\mathrm{Ker}\, \pi_k^{\hat{A}} \;=\; \hat{\mathfrak{I}}^k \;\forall k \in \mathbb{N}\;.$$

iii) On en déduit des isomorphismes naturels

$$A_n \;\cong\; \hat{A}/\hat{\mathfrak{I}}^n \,{}_{,n\in\mathbb{N}}$$

qui induisent un isomorphisme naturel

$$\hat{A} \;\cong\; \widehat{\hat{A}} \;=\; \varprojlim_{n\in\mathbb{N}} \hat{A}/\hat{\mathfrak{I}}^n \;.$$

Preuve :
i) Pour tout $k \in \mathbb{N}$ et $n \in \mathbb{N}$ $n \geq k$, on a une suite exacte

$$0 \;\to\; \mathfrak{I}^k/\mathfrak{I}^n \;\longrightarrow\; A/\mathfrak{I}^n \longrightarrow \xrightarrow{\rho_{k,n}^A} A/\mathfrak{I}^k \;\to\; 0\;.$$

L'ensemble de ces suites exactes forme un système projectif de suites exactes, c'est-à-dire que les morphismes sont compatibles aux applications de transition. De plus il satisfait aux hypothèses du lemme III.2.0.3, si bien qu'on a une suite exacte de $\hat{A}$-modules

$$0 \;\to\; \varprojlim_{n\in\mathbb{N}} \mathfrak{I}^k/\mathfrak{I}^{n+k} \;\longrightarrow\; \varprojlim_{n\in\mathbb{N}} A/\mathfrak{I}^{n+k} \longrightarrow A/\mathfrak{I}^k \;\to\; 0\;.$$

Elle donne, grâce au lemme III.2.0.2, la suite exacte

$$0 \;\to\; \widehat{\mathfrak{I}^k} \;\longrightarrow\; \hat{A} \longrightarrow \xrightarrow{\pi_k^{\hat{A}}} A/\mathfrak{I}^k \;\to\; 0\;.$$

ii) Par naturalité des différents morphismes (cf. III.2.1.3.ii,) pour tout $k \in \mathbb{N}$, le carré

$$\begin{array}{ccc} \hat{\mathfrak{I}} & \to & \hat{A} \\ {\scriptstyle \pi_k^{\hat{\mathfrak{I}}}}\downarrow & & \downarrow{\scriptstyle \pi_k^{\hat{A}}} \\ \mathfrak{I}/\mathfrak{I}^k & \to & A_k \end{array}$$

est comutatif. On en déduit que $\pi_k^{\hat{\hat{\mathfrak{I}}}} \;=\; 0$ c'est-à-dire que

$$\hat{\mathfrak{I}}^k \subset \mathrm{Ker}\, \pi_k^{\hat{A}} \;=\; \widehat{\mathfrak{I}^k}\;.$$

Par ailleurs, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} \pi_n^{\hat{A}}(\hat{\mathfrak{J}}^k) &= \pi_n^{\hat{\mathfrak{J}}}(\hat{\mathfrak{J}}^k) \\ &= [\pi_n^{\hat{\mathfrak{J}}}(\hat{\mathfrak{J}})^k] \\ &= \mathfrak{J}^k/\mathfrak{J}^n \\ &= \pi_n^{\widehat{\mathfrak{J}^k}}(\widehat{\mathfrak{J}^k}) \\ &= \pi_n^{\hat{A}}(\widehat{\mathfrak{J}^k}) \end{aligned}$$

d'où il résulte que

$$\hat{\mathfrak{J}}^k = \widehat{\mathfrak{J}^k} .$$

iii) Découle immédiatement du point précédent.

q.e.d

Proposition III.2.1.8. Propriétés algébriques de $\hat{A}$

i) Pour tout $a \in \hat{A}$, les propriétés suivantes sont équivalentes :

a) a est inversible.

b) Pour tout $n \in \mathbb{N}$, $\pi_n^{\hat{A}}(a)$ est inversible dans $\hat{A}/\hat{\mathfrak{J}}^n$.

c) $\pi_1^{\hat{A}}(a)$ est inversible dans $\hat{A}/\hat{\mathfrak{J}}$.

ii) Si $A/\mathfrak{J}$ est un corps c'est-à-dire si $\mathfrak{J}$ est un idéal maximal, $\hat{A}$ est local (cf. I.3.3.1,) d'idéal maximal $\hat{\mathfrak{J}}$ et de corps résiduel

$$\hat{A}/\hat{\mathfrak{J}} = \mathcal{S}(A)/\mathcal{S}(\mathfrak{J}) = A/\mathfrak{J} .$$

Il en résulte que si l'on note

$$A_{(\mathfrak{J})} := (A \setminus \mathfrak{J})^{-1}A \text{ et } \mathcal{S}(A)_{(\mathcal{S}(\mathfrak{J}))} := (\mathcal{S}(A) \setminus \mathcal{S}(\mathfrak{J}))^{-1}\mathcal{S}(A)$$

les morphismes λ^A et θ^A se factorisent de manière qu'on ait le diagramme commutatif suivant :

$$\begin{array}{ccc} A & \xrightarrow{\lambda^A{}_{\mathfrak{J}}} & A_{(\mathfrak{J})} \\ & \searrow \lambda^A & \downarrow \\ {\scriptstyle \pi^A}\downarrow & & \hat{A} \\ & \overset{\theta^A}{\nearrow}\ {\scriptstyle \theta^A{}_{(\mathcal{S}(\mathfrak{J}))}} & \uparrow \\ \mathcal{S}(A) & \xrightarrow{\qquad} & \mathcal{S}(A)_{(\mathcal{S}(\mathfrak{J}))} . \end{array}$$

De plus,

$$\hat{A} = \varprojlim_{n\in\mathbb{N}} A_{(\mathfrak{J})}/\mathfrak{J}^n = \varprojlim_{n\in\mathbb{N}} \mathcal{S}(A)_{(\mathcal{S}(\mathfrak{J}))}/\mathcal{S}(\mathfrak{J})^n .$$

Preuve :

i)

– (a) implique (b) implique (c) résulte simplement du fait qu'un morphisme d'anneaux envoie inversibles sur inversibles.
– Supposons (b). Notons alors $S := \{1\} \cup \{a^n\}_{n\in\mathbb{N}^*}$ qui est une partie multiplicative (cf. I.3.1.1.) On note alors $a^{-1}\hat{A} := S^{-1}\hat{A}$ le localisé de $\hat{A}$ en S (cf. I.3.1.3) et

$$\lambda_a^A : \hat{A} \to a^{-1}\hat{A}$$

le morphisme naturel. Pour tout $n \in \mathbb{N}$,

$$\pi_n^{\hat{A}}(S) \subset (\hat{A}/\hat{\mathfrak{J}}^n)^\times ;$$

il existe donc un unique morphisme $\lambda_{a,n}^A : a^{-1}\hat{A} \to \hat{A}/\hat{\mathfrak{J}}^n$ tel que

$$\pi_n^{\hat{A}} = \lambda_{a,n}^A \circ \lambda_a^A .$$

Il résulte de cette identité et de l'unicité des $\lambda_{a,n}^A$ que, pour tout $(r,s) \in \mathbb{N}^2$, $r \leq s$,

$$\lambda_{a,r}^A = \rho_{r,s}^A \circ \lambda_{a,s}^A .$$

Il en résulte que $\left(a^{-1}\hat{A}, \{\lambda^A{}_n : a^{-1}\hat{A} \to A_n\}_{n\in\mathbb{N}}\right)$ est un diagramme commutatif à valeurs dans le système projectif des A_n ,$_{n\in\mathbb{N}}$; il existe donc un unique morphisme

$$\mu : a^{-1}\hat{A} \to \hat{A}$$

tel que pour tout $n \in \mathbb{N}$, $\lambda_{a,n}^A = \pi_n^{\hat{A}} \circ \mu$ (cf. I.6.1.3(LimProj$_3$).)
En particulier, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} \pi_n^{\hat{A}}[\mu(\lambda_a^A(a))] &= \lambda_{a,n}^A[\lambda_a^A(a)] \\ &= \pi_n^{\hat{A}}(a) \end{aligned}$$

c'est-à-dire que $\mu[\lambda_a^A(a)] = a$. Or $\lambda_a^A(a)$ est inversible dans $a^{-1}\hat{A}$ donc $a = \mu(a)$ l'est aussi dans $\hat{A}$. On a ainsi démontré que (b) implique (a).
– Soit $a \in \hat{A}$. Si a n'est pas inversible, il résulte du point précédent qu'il existe $n \in \mathbb{N}$ tel que $\pi_n^{\hat{A}}(a)$ n'est pas inversible dans $\hat{A}/\hat{\mathfrak{J}}^n$. La projection naturelle $\rho_{n-1,n} : \hat{A}/\hat{\mathfrak{J}}^n \to \hat{A}/\hat{\mathfrak{J}}^{n-1}$ a pour noyau $\hat{\mathfrak{J}}^{n-1}\hat{A}/\hat{\mathfrak{J}}^n$ qui vérifie

$$(\hat{\mathfrak{J}}^{n-1}\hat{A}/\hat{\mathfrak{J}}^n)^2 = 0 \in \hat{A}/\hat{\mathfrak{J}}^n .$$

Il en résulte que, pour tout $\alpha \in \hat{A}/\hat{\mathfrak{J}}^n$, si $\rho_{n-1,n}(\alpha)$ est inversible, alors α est inversible.
C'est en effet un résultat général : Soit $\rho : R \to R/\mathfrak{J}$ un morphisme surjectif d'anneaux tel que $\mathfrak{J}^2 = 0$. Pour tout $\alpha \in R$, si $\rho(\alpha)$ est inversible, il existe $\beta \in R$ tel que $1-\alpha\beta \in \mathfrak{J}$. D'où il résulte que

$$1 - 2\alpha\beta + \alpha^2\beta^2 \in \mathfrak{J}^2$$

donc est nul d'où résulte finalement que

$$\alpha(2\beta - \alpha\beta^2) = 1$$

c'est-à-dire que α est inversible. (On pourrait en fait voir ce résultat dans un cadre plus général, puisqu'il s'agit en fait d'une question de convergence pour la topologie $\mathfrak{J}$-adique.) Si donc $\pi_n^{\hat{A}}(a)$ n'est pas inversible il résulte du fait ci-dessus que pour tout $l \leq n$, $\pi_l^{\hat{A}}(a)$ n'est pas inversible et en particulier, $\pi_1^{\hat{A}}(a)$ n'est pas inversible. On a donc démontré par contraposée que (c) implique (a).

ii) En utilisant la caractérisation III.2.1.8.c des inversibles de $\hat{A}$ $a \in \hat{A}$ est inversible si et seulement si $\pi_1^{\hat{A}}(a)$ l'est c'est-à-dire si et seulement si puisque $\hat{A}/\hat{\mathfrak{J}} = A/\mathfrak{J}$, est un corps, si et seulement si $\pi_1^{\hat{A}}(a) \neq 0$ c'est-à-dire si et seulement si $a \notin \hat{\mathfrak{J}}$. On en déduit que $\hat{A}^\times = \setminus \hat{\mathfrak{J}}$ ce qui prouve que $\hat{A}$ est local d'idéal maximal $\hat{\mathfrak{J}}$.

Le reste des vérifications est laissé en exercice.

q.e.d

Proposition III.2.1.9.
i) Si $v : Q \to P$ est un morphisme surjectif de A-modules alors le morphisme de $\hat{A}$-modules $\hat{v} : \hat{Q} \to \hat{P}$ est surjectif. Plus précisément, si $u : R \to Q$ est un noyau de v

$$\operatorname{Ker} \hat{v} = \varprojlim_{n\in\mathbb{N}} R'_n \mid R'_n = R/(R \cap \mathfrak{J}^n Q) .$$

ii) Si L est un A-module libre de type fini le morphisme naturel $\lambda^{L,*} : L \otimes_A \hat{A} \to \hat{L}$ est un isomorphisme.

iii) Si M est un A-module de type fini, le morphisme $\lambda^{M,*}$ est surjectif.

Preuve :
i) En notant

$$u : R \to Q := \operatorname{Ker} v,$$

on a une suite exacte de A-modules,

$$0 \to R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P \to 0 .$$

Pour tout $n \in \mathbb{N}$, on a un diagramme commutatif à lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & R \otimes_A \mathfrak{J}^n & \to & Q \otimes_A \mathfrak{J}^n & \to & P \otimes_A \mathfrak{J}^n & \to 0 \\
 & & \downarrow & & \downarrow{\scriptstyle u'} & & \downarrow & \\
0 \to & & R & \xrightarrow{u} & Q & \xrightarrow{v} & P & \to 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \pi_n^Q} & & \downarrow{\scriptstyle \pi_n^P} & \\
 & & R \otimes_A A/\mathfrak{J}^n & \xrightarrow{u_n} & Q \otimes_A A/\mathfrak{J}^n & \xrightarrow{v_n} & P \otimes_A A/\mathfrak{J}^n & \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & \\
 & & 0 & & 0 & & 0 &
\end{array}$$

La flèche

$$q := \pi_n^P \circ v = v_n \circ \pi_n^Q : Q \to P_n = P \otimes_A A/\mathfrak{J}^n$$

est surjective et identifie donc P_n à un quotient de Q dont le noyau est

$$\operatorname{Im} u + \operatorname{Im} u' \;\cong\; R + \mathfrak{I}^n Q\ .$$

On a alors un morphisme naturel de suites exactes

$$\begin{array}{ccccccccc} 0 \to & & \mathfrak{I}^n Q & \to & Q & \to & Q_n & \to 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}_Q} & & \downarrow{\scriptstyle v_n} & \\ 0 \to & R+\mathfrak{I}^n Q & \to & Q & \xrightarrow{q} & P_n & \to 0 & \end{array}\ .$$

Ce diagramme permet, graçe au lemme du serpent par exemple, d'identifier le noyau de v_n à

$$R'_n \;:=\; (R+\mathfrak{I}^n Q)/\mathfrak{I}^n Q \;\cong\; R/(R\cap \mathfrak{I}^n Q)\ .$$

On obtient donc, pour tout $r \leq s$ dans $\mathbb{N}$, un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccc} 0 \to & R'_s & \to & Q_s & \xrightarrow{v_s} & P_s & \to 0 \\ & \downarrow{\scriptstyle \rho'_{r,s}} & & \downarrow{\scriptstyle \rho^Q_{r,s}} & & \downarrow{\scriptstyle \rho^P_{r,s}} & \\ 0 \to & R'_r & \to & Q_r & \xrightarrow{v_r} & P_r & \to 0 \end{array}\ .$$

Or la flèche $\rho'_{r,s}$ est induite par l'inclusion naturelle $(R\cap\mathfrak{I}^s Q) \subset (R\cap\mathfrak{I}^r Q)$ et est donc surjective. On est donc dans les conditions du lemme III.2.0.3 ; si bien que la suite

$$0 \;\to\; \varprojlim_{n\in\mathbb{N}} R'_n \;\longrightarrow\; \hat{Q} \longrightarrow \xrightarrow{\hat{v}} \hat{P} \;\to\; 0$$

est exacte.

ii) En effet, soit L un A module libre de base $e_{i\ ,i\in I}$. On a alors

$$\hat{L} \;=\; \varprojlim_{n\in\mathbb{N}} L\otimes_A A/\mathfrak{I}^n$$

puisque L est une somme directe on a encore

$$\hat{L} \;=\; \varprojlim_{n\in\mathbb{N}} \bigoplus_{i\in I} L_i\otimes_A A/\mathfrak{I}^n\ .$$

Si I est fini une somme directe de modules sur I est aussi un produit et commute donc à la limite projective (cf. I.6.3.3.ii) d'où il résulte que

$$\hat{L} \;=\; \prod_{i\in I} \varprojlim_{n\in\mathbb{N}} L_i\otimes_A A/\mathfrak{I}^n \;\cong\; \prod_{i\in I} \hat{A}\ .$$

iii) Si M est de type fini, il existe un morphisme surjectif de A-modules $v\ :\ L\ \to\ M$ avec L libre de type fini. Or on a

$$\hat{v}\ \circ\ \lambda^{L,*}\ =\ \lambda^{M,*}\circ(v\otimes_A \mathrm{Id}_{\hat{A}})$$

par naturalité. Par ailleurs $\hat{v}$ est surjectif en vertu de III.2.1.9.i, et $\lambda^{L,*}$ est un isomorphisme d'après III.2.1.9.ii. Le morphisme composé $\hat{v} \circ \lambda^{L,*}$ est donc surjectif ce qui entraîne que $\lambda^{M,*}$ est surjectif.

q.e.d

Proposition III.2.1.10. *Soient A un anneau noethérien et $\mathfrak{I} \subset A$ un idéal.*
i) Pour toute suite exacte de A-modules

$$0 \ \to \ R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P \ \to \ 0$$

avec Q de type fini, la suite

$$0 \ \to \ \hat{R} \xrightarrow{\hat{u}} \hat{Q} \longrightarrow \xrightarrow{\hat{v}} \hat{P} \ \to \ 0$$

est exacte.

ii) Si M est un A-module de type fini, le morphisme $\lambda^{M,*} \ : \ M \otimes_A \hat{A} \ \to \ \hat{M}$ est un isomorphisme.

iii) Si

$$0 \ \to \ R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P \ \to \ 0$$

est une suite exacte avec Q de type fini, la suite

$$0 \ \to \ R \otimes_A \hat{A} \xrightarrow{u \otimes_A \mathrm{Id}_{\hat{A}}} Q \otimes_A \hat{A} \longrightarrow \xrightarrow{v \otimes_A \mathrm{Id}_{\hat{A}}} P \otimes_A \hat{A} \ \to \ 0$$

est exacte.

Preuve :
i) Puisque Q est de type fini, on peut appliquer le lemme III.2.0.5 à $R \subset Q$. Soit $k \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$,

$$R \cap \mathfrak{I}^{k+n} Q \ = \ \mathfrak{I}^n (R \cap \mathfrak{I}^k Q) \ .$$

On en déduit que pour tout $n \in \mathbb{N}$,

$$\mathfrak{I}^{k+n} R \ \subset \ R \cap \mathfrak{I}^{k+n} Q \ = \ \mathfrak{I}^n (R \cap \mathfrak{I}^k Q) \ \subset \ \mathfrak{I}^n R \ \subset \ R \cap \mathfrak{I}^n Q \ .$$

On utilise les notations de III.2.1.9.i. Cette suite d'inclusions donne une suite de morphismes surjectifs

$$R_{k+n} \xrightarrow{f_n} R'_{k+n} \longrightarrow \xrightarrow{g_n} R_n \xrightarrow{h_n} R'_n \mid g_n \circ f_n \ = \ \rho^R_{n,n+k} \ \forall n \in \mathbb{N} \ .$$

Il est immédiat de vérifier que les flèches

$$f_n, g_n \text{ et } h_n \ , n \in \mathbb{N}$$

sont compatibles aux morphismes de transition. Il en résulte qu'on a une suite de morphismes

$$\varprojlim_{n \in \mathbb{N}} R_{n+k} \xrightarrow{f} \varprojlim_{n \in \mathbb{N}} R'_{n+k} \longrightarrow \xrightarrow{g} \varprojlim_{n \in \mathbb{N}} R_n \xrightarrow{h} \varprojlim_{n \in \mathbb{N}} R'_n \ .$$

Il découle du lemme III.2.0.2 que $h \circ g$ et $g \circ f$ sont des isomorphismes ce qui entraîne que g est un isomorphismes et achève la preuve en appliquant III.2.1.9.i.

ii) Si M est de type fini, il existe une suite exacte

$$0 \ \to \ R \xrightarrow{u} L \longrightarrow \xrightarrow{v} M \ \to \ 0$$

avec L libre de type fini qui done lieu, en vertu du point précédent, à un diagramme comutatif à lignes exactes :

$$\begin{array}{ccccccc} 0 \to & K & \xrightarrow{k} & L \otimes_A \hat{A} & \xrightarrow{v \otimes_A \mathrm{Id}_{\hat{A}}} & M \otimes_A \hat{A} & \to 0 \\ & {\scriptstyle j}\downarrow & & {\scriptstyle \lambda^{L,*}}\downarrow & & \downarrow{\scriptstyle \lambda^{M,*}} & \\ 0 \to & \hat{R} & \xrightarrow{\hat{u}} & \hat{L} & \xrightarrow{\hat{v}} & \hat{M} & \to 0 \end{array} .$$

Puisque $\lambda^{L,*}$ est un isomorphisme (cf. III.2.1.9.ii,) $\lambda^{M,*}$ est surjectif (ce qu'on a dailleurs déjà montré en III.2.1.9.iii, sans hypothèses sur A.) De plus la flèche j est injective.

Par ailleurs, on a un morphisme naturel

$$f \ : \ R \otimes_A \hat{A} \ \to \ K \mid k \circ f \ = \ u \otimes_A \mathrm{Id}_{\hat{A}} \, .$$

On a alors :

$$\begin{aligned} \hat{u} \circ j \circ f \ &= \ \lambda^{L,*} \circ k \circ f \\ &= \ \lambda^{L,*} \circ (u \otimes_A \mathrm{Id}_{\hat{A}}) \\ &= \ \hat{u} \circ \lambda^{R,*} . \end{aligned}$$

Puisque $\hat{u}$ est injectif, on en déduit que

$$j \circ f \ = \ \lambda^{R,*} \, .$$

Or A est noethérien, L de type fini, donc R est de type fini et il résulte du point III.2.1.9.iii que $\lambda^{R,*}$ est surjectif. Ceci entraîne que j est surjectif, ce qui entraîne finalement que $\lambda^{M,*}$ est injectif donc un isomorphisme.

iii) Puisque A est noethérien et Q de type fini, R est aussi de type fini. Il résulte alors du point III.2.1.10.ii que la flèche naturelle $\lambda^{R,*} \ : \ R \otimes_A \hat{A} \ \to \ \hat{R}$ est un isomorphisme et la conclusion découle alors du point III.2.1.10.i.

q.e.d

Définition III.2.1.11. Soit R un anneau et $\mathfrak{J} \ \subset \ R$ un idéal de R. La *topologie $\mathfrak{J}$-adique sur R* est la topologie la moins fine telle que, pour tout $a \in R$ et tout $n \in \mathbb{N}$, $a + \mathfrak{J}^n$ est un ouvert (cf. 0.2.1.) Cela signifie encore qu'une partie $U \subset R$ est ouverte si et seulement si, pour tout $a \in U$, il existe $n \in \mathbb{N}$ tel que

$$a + c\mathfrak{J}^n \ \subset \ U \, .$$

La somme et le passage à l'opposé dans R étant des applications continues pour la topologie $\mathfrak{J}$-adique, on dira que $(R, +)$ est un *groupe topologique* pour la topologie $\mathfrak{J}$-adique.

Comme de plus, le produit et le passage à l'inverse (quand il est défini,) sont également des applications continues, on dira que $(R, +, *)$ est un *anneau topologique* pour la topologie $\mathfrak{J}$-adique.

Proposition III.2.1.12. Propriétés topologiques de $\hat{A}$ *Soit A un anneau et $\mathfrak{I} \subset A$ un idéal. On peut munir les anneaux $A, \mathcal{S}(A)$ et $\hat{A}$ des topologies $\mathfrak{I}$-adique, $\mathcal{S}(\mathfrak{I})$-adique et $\hat{\mathfrak{I}}$-adique respectivement.*

On peut aussi munir A_n pour tout $n \in \mathbb{N}$ de la topologie discrète c'est-à-dire la topologie $\mathcal{P}(A_n)$ pour laquelle toute partie est ouverte (et fermée par voie de conséquence.) L'anneau $\hat{A}$ se trouve alors muni de la topologie de la limite projective (cf. I.6.2.3) puisque l'ensemble sous-jacent à la limite projective des anneaux et à la limite projective des espaces topologiques est le même à savoir la limite projective au sens des ensembles.

i) L'anneau A muni de la topologie $\mathfrak{I}$-adique, est un espace topologique séparé si et seulement si λ^A est injectif, si et seulement si $A \cong \mathcal{S}(A)$, si et seulement si

$$\bigcap_{n\in\mathbb{N}} \mathfrak{I}^n = \{0\} .$$

ii) La topologie $\hat{\mathfrak{I}}$-adique et la topologie de la limite projective coïncident sur $\hat{A}$.

iii) Les morphismes d'anneaux λ^A, θ^A et π^A ainsi que les morphismes

$$\pi_n^A, \pi_n^{\hat{A}}, \pi_n^{\mathcal{S}(A)} ,_{n\in\mathbb{N}}$$

sont des applications continues.

iv) L'image de λ^A ou encore celle de θ^A est dense dans $\hat{A}$.

v) L'anneau $\hat{A}$ est séparé et complet pour la topologie $\hat{\mathfrak{I}}$-adique.

Preuve :

i) Il suffit de remarquer que, sur un anneau topologique, pour que la topologie soit séparée il faut et il suffit que l'intersection de tous les voisinages de 0 soient $\{0\}$.

ii) Pour tout $a \in \hat{A}$ et tout $n \in \mathbb{N}$, $\{\pi_n^{\hat{A}}(a)\} \subset A_n$ est un ouvert puisqu'en particulier, la topologie discrète est caractérisée par le fait que tous les singletons sont ouverts. Il en résulte que

$$\pi_n^{\hat{A}^{-1}}(\{\pi_n^{\hat{A}}(a)\}) = a + \hat{\mathfrak{I}}^n$$

(cf. III.2.1.7.ii,) est ouvert dans $\hat{A}$ pour la topologie de la limite projective ; plus précisément les ouverts de la forme $a + \hat{\mathfrak{I}}^n$, $a \in \hat{A}$, $n \in \mathbb{N}$ engendrent la topologie de la limite projective qui coïncide donc avec la topologie $\hat{\mathfrak{I}}$-adique.

iii) On a

$$\begin{aligned} \lambda^{A,-1}(\hat{\mathfrak{I}}^n) &= \lambda^{A,-1}[\operatorname{Ker} \pi_n^{\hat{A}}] \\ &= \operatorname{Ker} \pi_n^{\hat{A}} \circ \lambda^A \\ &= \operatorname{Ker} \pi_n^A \\ &= \mathfrak{I}^n \end{aligned}$$

ce qui assure la continuité de λ^A. Les autres vérifications sont du même ordre et laissées en exercice.

iv) Pour tout $n \in \mathbb{N}$, $\lambda^{A,-1}(\hat{\mathfrak{J}}^n) = \mathfrak{J}^n$ d'où il résulte que

$$\lambda^A(\mathfrak{J}^n) \subset \hat{\mathfrak{J}}^n$$

ce qui prouve que

$$\hat{\mathfrak{J}}^n \cap \operatorname{Im}\lambda^A \neq \emptyset\,.$$

Tout voisinage de 0 dans $\hat{A}$ rencontre donc l'image de λ^A ce qui suffit, pour un anneau topologique, à assurer que $\operatorname{Im}\lambda^A$ est dense dans $\hat{A}$. Comme

$$\operatorname{Im}\lambda^A = \operatorname{Im}\theta^A,$$

le résultat vaut aussi pour θ^A.

v)

- Pour tout $a \in \hat{A}$, si
$$a \in \bigcap \mathbb{N}n\hat{\mathfrak{J}}^n,$$
pour tout $n \in \mathbb{N}$, $\pi_n^{\hat{A}}(a) = 0$. Ceci implique, puisque
$$\hat{A} = \varprojlim_{n\in\mathbb{N}} \hat{A}/\hat{\mathfrak{J}}^n$$
(cf. III.2.1.7.iii,) que $a = 0$. Il en résulte que
$$\bigcap_{n\in\mathbb{N}} \hat{\mathfrak{J}}^n = \{0\},$$
ce qui a en particulier pour conséquence que l'intersection de tous les voisinages de 0 est $\{0\}$ c'est-à-dire que $\hat{A}$ est séparé.
- Étant donnée une suite de Cauchy $(u_n)_{n\in\mathbb{N}}$ à valeurs dans $\hat{A}$. Pour tout $k \in \mathbb{N}$ il existe donc $n(k) \in \mathbb{N}$, tel que pour tous $r \geq n(k)$ $u_r - u_{n(k)} \in \hat{\mathfrak{J}}^k$. Il en résulte que pour tout $l < k$, $\pi_l^{\hat{A}}(u_r) = \pi_l^{\hat{A}}(u_{n(k)}$. Posons donc, pour tout $l < k$, $\alpha_l := \pi_l^{\hat{A}}(u_{n(k)}) \in \hat{A}/\hat{\mathfrak{J}}^l$. On voit qu'on peut ainsi construire $\alpha_l\ \forall l \in \mathbb{N}$. On constate ensuite que les α_l définissent un élément de $\hat{A}$ qui est la limite de la suite $(u_n)_{n\in\mathbb{N}}$. On a donc montré que $\hat{A}$ est complet.

q.e.d

Définition III.2.1.13. Séparé complété On appelle l'anneau $\hat{A}$ le *séparé complété* de A pour la topologie $\mathfrak{J}$-adique.

Corollaire III.2.1.14. *Si A est un anneau et $\mathfrak{J}$ est un idéal de A et si de plus la topologie $\mathfrak{J}$-adique sur A est métrique, i.e.donnée par une distance δ, le séparé complété au sens de la définition ci-dessus coïncide avec le complété pour les espaces métriques au sens de la définition 0.2.2.8.*

Théorème III.2.1.15. *Soit (K, v) un corps muni d'une valuation discrète normalisée, $\mathcal{O}_K$ l'anneau de la valuation, $\mathfrak{m}_K$ son idéal maximal et π une uniformisante.*

On fixe un nombre réel $0 < \gamma < 1$ et, pour tout $x \in K$, on note

$$|x| \ := \ \gamma^{v(x)},$$

$|\cdot|$ est alors une valeur absolue ultramétrique. On note encore $\hat{K}$ le complété de l'espace métrique $(K, |\cdot|)$ au sens de la définition 0.2.2.8 et $\widehat{\mathcal{O}_K}$ l'adhérence de $\mathcal{O}_K$ dans $\hat{K}$.

i) Il existe un une unique valeurs absolue $\widehat{|\cdot|}$ sur $\hat{K}$ prolongeant $|\cdot|$. La valeur absolue $\widehat{|\cdot|}$ est ultramétrique et il existe une unique valuation $\hat{v}$ sur $\hat{K}$ telle que

$$\widehat{|x|} \ = \ \gamma^{\hat{v}(x)} \ \forall x \in \hat{K}$$

et prolongeant v. La valuation $\hat{v}$ est alors une valuation discrète sur $\hat{K}$.

ii) La topologie $\mathfrak{m}_K$-adique sur $\mathcal{O}_K$ coïncide avec sa topologie de sous-espace métrique de $(K, |\cdot|)$.

iii) L'anneau $\widehat{\mathcal{O}_K}$ a les propriétés suivantes :

a)

$$\widehat{\mathcal{O}_K} \ = \ \varprojlim_{n\in\mathbb{N}} \mathcal{O}_K/\mathfrak{m}_K^n \ = \ \varprojlim_{n\in\mathbb{N}} \mathcal{O}_K/(\pi^n\mathcal{O}_K)$$

ce qui justifie la notation.

b) L'anneau $\widehat{\mathcal{O}_K}$ est la boule unité fermée dans $\hat{K}$.

c) L'anneau $\mathcal{O}_K$ est l'anneau de la valuation $\hat{v}$ c'est donc un anneau de valuation discrète. L'uniformisante π de $\mathcal{O}_K$ est encore une uniformisante de $\widehat{\mathcal{O}_K}$.

d) L'idéal maximal $\pi\widehat{\mathcal{O}_K}$ s'identifie à $\widehat{\mathfrak{m}_K}$ et l'on a

$$\mathcal{O}_K/\mathfrak{m}_K \ \cong \ \widehat{\mathcal{O}_K}/\widehat{\mathfrak{m}_K} \ \cong \ \widehat{\mathcal{O}_K}/\pi\widehat{\mathcal{O}_K} \ \cong \ \widehat{\mathcal{O}_K}/\mathfrak{m}_{\hat{K}} \ .$$

e) Le corps des fractions de $\widehat{\mathcal{O}_K}$ s'identifie à

$$\hat{K} \ \cong \ \widehat{\mathcal{O}_K}[\frac{1}{\pi}] \ .$$

f) On a des isomorphismes canoniques

$$\hat{K} \ \cong \ \widehat{\mathcal{O}_K}[\frac{1}{\pi}] \ \cong \ \mathcal{O}_K[\frac{1}{\pi}] \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}_K} \ \cong \ K \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}_K} \ .$$

Preuve :

i) On laisse le soin au lecteur de montrer que $\widehat{|\cdot|}$ existe, est unique et est ultramétrique. L'existence d'un unique $\hat{v}$ vérifiant $\widehat{|\cdot|} \ = \ \gamma^{\hat{v}(\cdot)}$ découle alors de la proposition II.1.2.10.i.

Enfin, pour tout $x \in \hat{K}$, x non nul, $\hat{v}(x) = \log_\gamma(\widehat{|x|})$. Il en résulte qu'au voisinage d'un point différent de 0, $\hat{v}(x)$ est continue. Il existe une suite $suitexn\mathbb{N}$ d'éléments de K dont la limite est x. Il s'ensuit que

$$\lim_{n\to+\infty} \hat{v}(x_n) = \hat{v}(x) .$$

Or $\hat{v}(x_n) = v(x_n) \in \mathbb{Z}$ ce qui entraîne que $\hat{v}(x) \in \mathbb{Z}$.

ii) L'ensemble

$$\mathcal{V} := \{\pi^n \mathcal{O}_k\}_{n\in\mathbb{N}}$$

est une base de voisinages de 0 pour la topologie $\mathfrak{m}_K$-adique. On a encore

$$\mathcal{V} = \big\{\{x \in K \mid v(x) \geq n\}\big\}_{n\in\mathbb{N}}$$

c'est-à-dire encore

$$\mathcal{V} = \big\{\{x \in K \mid |x| \leq \gamma^n\}\big\}_{n\in\mathbb{N}}$$

qui est une base de voisinages de 0 dans l'espace métrique $(K, |\cdot|)$.

iii)

a) Puisque $\widehat{\mathcal{O}_K}$ est fermé dans $\hat{K}$ qui est complet, il est complet et $\mathcal{O}_K$ est dense dans $\widehat{\mathcal{O}_K}$ par définition. C'est donc le complété de $\mathcal{O}_K$ au sens de la définition 0.2.2.8 qui coïncide avec le séparé complété au sens de la définition III.2.1.13 en vertu du corollaire III.2.1.14 puisque la topologie $\mathfrak{m}_K$-adique sur $\mathcal{O}_K$ est métrique grâce à III.2.1.15.ii.

b)

c) On sait d'ores et déjà que

$$\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x| \leq 1\} .$$

En particulier $\mathcal{O}_K$ est inclus dans la boule unité fermée de $\hat{K}$. Cette dernière étant fermée, elle contient encore l'adhérence de $\mathcal{O}_K$ c'est-à-dire que

$$\widehat{\mathcal{O}_K} \subset B := \{x \in \hat{K} \mid \widehat{|x|} \leq 1\} .$$

Soit $x \in B$, $x \neq 0$. Il existe une suite $suitexn\mathbb{N}$ à valeurs dans K qui converge vers x. Or $\hat{v}$ est continue au voisinage de x. Comme $\hat{v}$ est à valeurs dans $\mathbb{Z}$ il en découle que pour n assez grand, $\hat{v}(x_n) \geq 0$, c'est-à-dire que pour n assez grand, $x_n \in \mathcal{O}_K$ ce qui prouve que

$$B \subset \overline{\mathcal{O}_K} = \widehat{\mathcal{O}_K}$$

et finalement que

$$\widehat{\mathcal{O}_K} = \{x \in \hat{K} \mid \widehat{|x|} \leq 1\} .$$

d) Il découle immédiatement du point précédent que $\widehat{\mathcal{O}_K}$ est l'anneau de la valuation $\hat{v}$ qui est discrète c'est donc un anneau de valuation discrète. De plus,

$$\hat{v}(\pi) = v(\pi) = 1$$

ce qui prouve que π est une uniformisante de $\widehat{\mathcal{O}_K}$.

e) Est une conséquence de III.2.1.8.ii.

f) Est une conséquence de II.1.2.7.

q.e.d

Corollaire III.2.1.16. *Soit p un nombre premier. On munit le corps $\mathbb{Q}$ des nombres rationnels de la valuation p-adique normalisée v_p (cf. II.1.4.2.) L'anneau de la valuation v_p est alors $\mathbb{Z}_{(p)}$ (cf. II.1.4.3.) On notera $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la valeur absolue p-adique. L'anneau de la valuation de $\mathbb{Q}_p$ est alors*

$$\mathbb{Z}_p \ := \ \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_{(p)}/(p^n\mathbb{Z}_{(p)}) \ \cong \ \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \ .$$

Définition III.2.1.17. Un nombre premier p étant fixé, l'anneau

$$\mathbb{Z}_p \ := \ \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

est appelé *anneau des entiers p-adiques*

Corollaire III.2.1.18. *Pour tout nombre premier p, l'anneau $\mathbb{Z}_p$ est un anneau de valuation discrète complet d'uniformisante p si bien qu'on a :*

$$\mathbb{Z}/p^n\mathbb{Z} \ \cong \ \mathbb{Z}_p/(p^n\mathbb{Z}_p) \ .$$

C'est le complété p-adique de $\mathbb{Z}$ ou de $\mathbb{Z}_{(p)}$ qui se réalisent chacun comme un sous-anneau dense de $\mathbb{Z}_p$.

Le corps des fractions de $\mathbb{Z}_p$ est

$$\mathbb{Q}_p \ \cong \ \mathbb{Z}_p[\frac{1}{p}] \ .$$

Preuve : Ces résultats se déduisent facilement de ceux établis dans le reste du paragraphe III.2.1. *q.e.d*

Exemple III.2.1.19.

i) Si K est un corps, on peut voir l'anneau des séries formelles comme

$$K[[X]] \ = \ \varprojlim_{n\in\mathbb{N}} K[X]/X^n \ .$$

ii) Pour tout entier naturel d on notera

$$\mathbb{Z}_d \ := \ \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/d^n\mathbb{Z} \ .$$

Notons alors $d = \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i sont des nombres premiers deux à deux distincts et les α_i des entiers ≥ 1. On a alors, grâce au théorème chinois des restes

$$\mathbb{Z}_d = \varprojlim_{n\in\mathbb{N}} \big(\prod_{i=1}^{r} \mathbb{Z}/p_i^{n\alpha_i}\mathbb{Z} \big)$$

qui est encore égal, en vertu de la remarque I.6.3.3.ii, à

$$\prod_{i=1}^{r} \big(\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p_i^{n\alpha_i}\mathbb{Z} \big) \ .$$

On peut donc se ramener à l'étude de

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^{n\alpha}\mathbb{Z}$$

où p est un nombre premier et $\alpha \geq 1$ un entier. Or en vertu du corollaire III.2.0.2,

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^{n\alpha}\mathbb{Z} \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^{n}\mathbb{Z} = \mathbb{Z}_p \ .$$

III.2.2 . −Invariants du complété d'une extension d'anneaux de Dedekind

Lemme III.2.2.0. *Les hypothèses et notations sont celles du théorème II.3.1.2 .*

L'anneau $\mathcal{O}_L$ a les propriétés suivantes :

a) C'est l'anneau de valuation v_L ou de la valuation w ce qui revient au même et c'est donc la boule unité fermée de l'espace métrique L.

b) C'est un anneau de valuation discrète complet en particulier

$$\mathcal{O}_L \cong \widehat{\mathcal{O}_L} \cong \varprojlim_{n\in\mathbb{N}} \mathcal{O}_L/\mathfrak{m}_L^n \ .$$

Preuve :

a) Puisque $\mathcal{O}_L$ est un anneau de valuation discrète (cf. II.3.1.2.iii,) dont L est le corps des fractions, $\mathcal{O}_L$ est l'anneau de la valuation (cf. II.1.3.3.ii.) Il est clair qu'alors, $\mathcal{O}_L$ est la boule unité fermée de L.

b) Puisque L est complet (cf. II.3.1.2.ii,) et que $\mathcal{O}_L$ est la boule unité fermée dans L, il découle de III.2.1.15.b que $\mathcal{O}_L$ est le séparé complété de $\mathcal{O}_L$ *i.e.*est séparé et complet.

q.e.d

Dans la suite de cette section (III.2.2,) A est un anneau de Dedekind (cf. I.5.2.2,) K son corps des fractions,

$$K \subset L = K[X]/P$$

(où $P \in K[X]$ est un polynôme unitaire irréductible,) une extension séparable de degré d de K et B la clôture intégrale de A dans L.

Proposition III.2.2.1. *Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, et tout idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$ au-dessus de $\mathfrak{p}$:*
i) on a un carré commutatif de A-algèbres

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{q}} \end{array}$$

à flèches injectives ;
ii) le morphisme $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ est local c'est-à-dire que

$$B_{\mathfrak{q}}\mathfrak{q} \cap A_{\mathfrak{p}} = A_{\mathfrak{p}}\mathfrak{p} ;$$

iii) on a les relations

$$B_{\mathfrak{q}}\mathfrak{p} = (B_{\mathfrak{q}}\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} \qquad \textit{III.2.2.1.1}$$

(où $e_{\mathfrak{q}/\mathfrak{p}}$ est l'indice de ramification de $\mathfrak{q}$ par rapport à $\mathfrak{p}$ dans l'extension $A \subset B$ (cf. III.1.2.5.i)) et

$$\left[(B_{\mathfrak{q}}/B_{\mathfrak{q}}\mathfrak{q}) : (A_{\mathfrak{p}}/A_{\mathfrak{p}}\mathfrak{p})\right] = f_{\mathfrak{q}/\mathfrak{p}} \qquad \textit{III.2.2.1.2}$$

(où $f_{\mathfrak{q}/\mathfrak{p}}$ est le degré résiduel de $\mathfrak{q}$ par rraport à $\mathfrak{p}$ (cf. III.1.2.5.ii ;))
iv) Si on note

$$\widehat{A_{\mathfrak{p}}} := \varprojlim_{n\in\mathbb{N}} A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}} \ (\textit{resp.}\ \widehat{B_{\mathfrak{q}}} = \varprojlim_{n\in\mathbb{N}} B_{\mathfrak{q}}/\mathfrak{q}^n B_{\mathfrak{q}})$$

le séparé complété de $A_{\mathfrak{p}}$ (resp. $B_{\mathfrak{q}}$) pour la topologie $\mathfrak{p}$-adique (resp. $\mathfrak{q}$-adique) (cf. III.2.1.13,) le morphisme injectif

$$A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{q}}$$

se prolonge de manière à ce qu'on ait un diagramme commutatif à flèches injectives :

$$\begin{array}{ccccc} A & \hookrightarrow & A_{\mathfrak{p}} & \hookrightarrow & \widehat{A_{\mathfrak{p}}} \\ \downarrow & & \downarrow & & \downarrow \\ B & \hookrightarrow & B_{\mathfrak{q}} & \hookrightarrow & \widehat{B_{\mathfrak{q}}} ; \end{array} \qquad \textit{III.2.2.1.3}$$

de plus, on a encore

$$\widehat{B_{\mathfrak{q}}}\mathfrak{p} = (\widehat{B_{\mathfrak{q}}}\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} \text{ et } \left[(\widehat{B_{\mathfrak{q}}}/\widehat{B_{\mathfrak{q}}}\mathfrak{q}) : (\widehat{A_{\mathfrak{p}}}/\widehat{A_{\mathfrak{p}}}\mathfrak{p})\right] = f_{\mathfrak{q}/\mathfrak{p}} . \qquad \textit{III.2.2.1.4}$$

Preuve :

i) Pour tout $x \in A \setminus \mathfrak{p}$, $x \in B \setminus \mathfrak{q}$ (puisque $\mathfrak{q} \cap A = \mathfrak{p}$,) son image dans $B_\mathfrak{q}$ est donc inversible, si bien que le morphisme naturel

$$A \longrightarrow B \longrightarrow B_\mathfrak{q}$$

se factorise à travers $A_\mathfrak{p}$.

Les anneaux A et B étant intègres, les morphismes naturels

$$A \to A_\mathfrak{p} \text{ et } B \to B_\mathfrak{q}$$

sont injectifs. Il est facile de vérifier que $A_\mathfrak{p} \to B_\mathfrak{q}$ est injectif, et on le laisse en exercice.

ii) Vérification laissée en exercice.

iii) Notons

$$B_\mathfrak{p} := B \otimes_A A_\mathfrak{p} = (A \setminus \mathfrak{p})^{-1} B .$$

D'après la proposition III.1.2.4,

$$B\mathfrak{p} = \prod_{i=1}^{\text{gp}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$$

où les $\mathfrak{q}_i$,$1 \leq i \leq g_\mathfrak{p}$ sont les idéaux maximaux de B au-dessus de $\mathfrak{p}$. On peut donc supposer que $\mathfrak{q} = \mathfrak{q}_1$.

Dans $B_\mathfrak{p}$, on a encore

$$B_\mathfrak{p}\mathfrak{p} = (B_\mathfrak{p}\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} \prod_{i=2}^{g_\mathfrak{p}} (B_\mathfrak{p}\mathfrak{q}_i)^{e_{\mathfrak{q}_i/\mathfrak{p}}}$$

en vertu de III.1.2.9.iii. Appliquant ensuite la proposition I.3.2.5 à l'anneau $B_\mathfrak{p}$ et à la partie multiplicative $S := Bp \setminus B_\mathfrak{p}\mathfrak{q}$ on obtient

$$\begin{aligned} B_\mathfrak{q}\mathfrak{p} &= S^{-1} B_\mathfrak{p}\mathfrak{p} \\ &= (S^{-1} B_\mathfrak{p}\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} \prod_{i=2}^{g_\mathfrak{p}} S^{-1} (B_\mathfrak{p}\mathfrak{q}_i)^{e_{\mathfrak{q}_i/\mathfrak{p}}} \\ &= S^{-1} B_\mathfrak{p}\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}} \\ &= (B_\mathfrak{q}\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} \end{aligned}$$

puisque pour tout $2 \leq i \leq \text{gp}$, $idq_i \cap (B \setminus \mathfrak{q}) \neq \emptyset$.

Par ailleurs,

$$A/\mathfrak{p} \cong A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p} \text{ et } B/\mathfrak{q} \cong B_\mathfrak{q}/B_\mathfrak{q}\mathfrak{q}$$

ce qui établit l'égalité III.2.2.1.2.

iv) D'après le point III.2.2.1.ii, $B_\mathfrak{q}\mathfrak{q} \cap A_\mathfrak{p} = A_\mathfrak{p}\mathfrak{p}$. Il s'ensuit que, pour tout $n \in \mathbb{N}$,

$$(A_\mathfrak{p}\mathfrak{p})^n \subset (B_\mathfrak{q}\mathfrak{q})^n \cap A_\mathfrak{p}$$

d'où l'on déduit un morphisme

$$f_n : A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p}^n \to B_\mathfrak{q}/B_\mathfrak{q}\mathfrak{q}^n .$$

Les f_n ,$n\in\mathbb{N}$ forment évidemment un morphisme de systèmes projectifs, si bien que les f_n se factorisent en un morphisme

$$\hat{f} \ : \ \widehat{A_{\mathfrak{p}}} \ \rightarrow \ \widehat{B_{\mathfrak{p}}} \ .$$

De plus, il résulte du point III.2.2.1.1, qu'il existe une uniformisante u de $B_{\mathfrak{q}}$ telle que $t \ := \ u^{e_{\mathfrak{q}/\mathfrak{p}}}$ est une uniformisante de $A_{\mathfrak{p}}$. Pour tout $n \in \mathbb{N}$ on a encore

$$t \ \equiv \ u^{e_{\mathfrak{q}/\mathfrak{p}}} \ [\mathfrak{q}^n]$$

si bien que l'identité $t \ = \ u^{e_{\mathfrak{q}/\mathfrak{p}}}$ reste vraie dans $\widehat{B_{\mathfrak{p}}}$. Comme t (resp. u) reste une uniformisante de $\widehat{A_{\mathfrak{p}}}$ (resp. $\widehat{B_{\mathfrak{p}}}$) (cf. III.2.1.15.d,) ceci prouve la première égalité de III.2.2.1.4. Ceci prouve également l'injectivité du morphisme $\hat{f}$ ce qui achève de prouver III.2.2.1.3. Enfin l'égalité sur les degrés résiduels de III.2.2.1.4 vient simplement du fait qu'on a

$$A/\mathfrak{p} \ = \ A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \ = \ \widehat{A_{\mathfrak{p}}}/\mathfrak{p}\widehat{A_{\mathfrak{p}}} \ \text{et} \ B/\mathfrak{q} \ = \ B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}} \ = \ \widehat{B_{\mathfrak{q}}}/\mathfrak{q}\widehat{B_{\mathfrak{q}}}$$

obtenus en combinant III.2.1.15.d.

q.e.d

Lemme III.2.2.2. *Pour $\mathfrak{p} \in \mathrm{Spm}(A)$ un idéal maximal de A, on note toujours $\widehat{A_{\mathfrak{p}}}$ le séparé complété de A (ou de $A_{\mathfrak{p}}$ (cf. III.2.1.8.ii,)) pour la topologie $\mathfrak{p}$-adique,*

$$B_{\mathfrak{p}} \ := \ B \otimes_A A_{\mathfrak{p}} \ , \ \widehat{B_{\mathfrak{p}}} \ := \ B \otimes_A \widehat{A_{\mathfrak{p}}},$$

$$\mathfrak{q}_i \ ,1\leq i\leq g_{\mathfrak{p}} \ \in \ \mathrm{Spm}(B)$$

les idéaux maximaux de B au-dessus de $\mathfrak{p}$ (cf. III.1.2.4) et pour tout $1 \leq i \leq g_{\mathfrak{p}}$,

$$\widehat{B_{\mathfrak{q}_i}} \ = \ \varprojlim_{n\in\mathbb{N}} / \mathfrak{q}_i^n$$

le séparé complété de B pour la topologie $\mathfrak{q}_i$-adique (cf. III.2.1.13.)

On a alors des isomorphismes naturels de $\widehat{A_{\mathfrak{p}}}$-algèbres :

$$\widehat{B_{\mathfrak{p}}} \ \cong \ \varprojlim_{n\in\mathbb{N}} B/B\mathfrak{p}^n \ \cong \ \varprojlim_{n\in\mathbb{N}} B_{\mathfrak{p}}/B_{\mathfrak{p}}\mathfrak{p}^n \ \cong \ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{B_{\mathfrak{q}_i}} \ .$$

Preuve :
i) Puisque A est noethérien (cf. I.5.2.2) et B est un A-module de type fini (cf. I.4.4.2,) en vertu du point III.2.1.10.ii, le morphisme naturel

$$\lambda^{B,*} \ : \ B \otimes_A \widehat{A_{\mathfrak{p}}} \ \rightarrow \varprojlim_{n\in\mathbb{N}} B/\mathfrak{p}^n B$$

est un isomorphisme ; ce qui donne le premier isomorphisme.

ii) En suite on a

$$B \otimes_A \widehat{A_{\mathfrak{p}}} \;=\; (B \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} \;=\; B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}}$$

(cf. I.2.2.5.) Or $B_{\mathfrak{p}}$ est encore un $A_{\mathfrak{p}}$-module de type fini (c'est la fermeture intégrale de $A_{\mathfrak{p}}$ dans L (cf. I.4.2.3,)) sur $A_{\mathfrak{p}}$ qui est encore noethérien si bien que le raisonement ci-dessus s'applique encore mutatis mutandis et qu'on en déduit le deuxième isomorphisme.

iii) Enfin, on a en vertu de la proposition III.1.2.4,

$$B\mathfrak{p} \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}} \;.$$

Il en résulte, grâce au théorème chinois des restes, que, pour tout $n \in \mathbb{N}$,

$$B/\mathfrak{p}^n B \;\cong\; \prod_{i=1}^{g_{\mathfrak{p}}} B/\mathfrak{q}_i^{ne_{\mathfrak{q}_i/\mathfrak{p}}} \;.$$

Il en résulte, graçe à I.6.3.3.ii, que

$$\widehat{B_{\mathfrak{p}}} \;=\; \varprojlim_{n\in\mathbb{N}} B/\mathfrak{p}^n B \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} \big(\varprojlim_{n\in\mathbb{N}} B/\mathfrak{q}_i^{ne_{\mathfrak{q}_i/\mathfrak{p}}}\big) \;.$$

Le deuxième membre de l'égalité est encore égal, graçe au corollaire III.2.0.2, à

$$\prod_{i=1}^{g_{\mathfrak{p}}} \big(\varprojlim_{n\in\mathbb{N}} B/\mathfrak{q}_i^{n}\big)$$

ce qui achève la preuve.

q.e.d

Proposition III.2.2.3. *Pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, on note $K_{\mathfrak{p}}$ le complété de K pour la valuation $\mathfrak{p}$-adique, c'est-à-dire pour l'unique valuation discrète normalisée $v_{\mathfrak{p}}$ sur K dont $A_{\mathfrak{p}}$ est l'anneau de la valuation (cf. II.3.1.1.i,) $\widehat{A_{\mathfrak{p}}}$ le séparé complété de A pour la topologie $\mathfrak{p}$-adique et $L_{\mathfrak{p}} := L \otimes_K K_{\mathfrak{p}}$.*

On note encore

$$\mathfrak{q}_i \,,1\leq i\leq g_{\mathfrak{p}} \;\in\; \mathrm{Spm}(B)$$

les idéaux maximaux de B au-dessus de $\mathfrak{p}$, $\widehat{B_{\mathfrak{q}_i}}$ (resp. $\widehat{L_{\mathfrak{q}_i}}$) le séparé complété de B (resp. L) pour la topologie $\mathfrak{q}_i$-adique.

i) On a des isomorphismes canoniques de $K_{\mathfrak{p}}$-algèbres :

$$L_{\mathfrak{p}} \;\cong\; L \otimes_A \widehat{A_{\mathfrak{p}}} \;\cong\; L \otimes_B \widehat{B_{\mathfrak{p}}} \;. \qquad \textit{III.2.2.3.1}$$

ii) On déduit alors des isomorphisme du lemme III.2.2.2 un diagramme commutatif de $\widehat{A_\mathfrak{p}}$-algèbres :

$$\begin{array}{ccccc} \widehat{A_\mathfrak{p}} & \hookrightarrow & \widehat{B_\mathfrak{p}} & \cong & \prod_{i=1}^{g_\mathfrak{p}} \widehat{B_{\mathfrak{q}_i}} \\ \downarrow & & \downarrow & & \downarrow \\ K_\mathfrak{p} & \hookrightarrow & L_\mathfrak{p} & \cong & \prod_{i=1}^{g_\mathfrak{p}} \widehat{L_{\mathfrak{q}_i}} \end{array} \qquad \textit{III.2.2.3.2}$$

où les flèches verticales sont injectives, et la flèche verticale de droite est donée par le produit des inclusions naturelles (cf. III.2.1.15.)

iii) Pour tout $1 \leq i \leq g_\mathfrak{p}$, on a encore un carré commutatif de $\widehat{A_\mathfrak{p}}$-algèbres à flèches injectives :

$$\begin{array}{ccc} \widehat{A_\mathfrak{p}} & \hookrightarrow & \widehat{B_{\mathfrak{q}_i}} \\ \downarrow & & \downarrow \\ K_\mathfrak{p} & \hookrightarrow & \widehat{L_{\mathfrak{q}_i}} \end{array} \qquad \textit{III.2.2.3.3}$$

et $\widehat{B_{\mathfrak{q}_i}}$ s'identifie canoniquement à l'anneau des entiers de $\widehat{L_{\mathfrak{q}_i}}$.

Preuve :

i)

a) On dégage d'abord le sorite suivant qui nous sera utile tout au long de cette preuve : Si R est un anneau, S une partie multiplicative de R, M un $S^{-1}R$-module et R' une $S^{-1}R$-algèbre, on a un isomorphisme canonique

$$M \otimes_R R' \;\cong\; M \otimes_{S^{-1}R} R' \,. \qquad \text{III.2.2.3.4}$$

On a d'abord

$$M \otimes_{S^{-1}R} R' \;=\; (M \otimes_R S^{-1}R) \otimes_{S^{-1}R} R'$$

en vertu de I.3.1.7, le deuxième membre étant égal à

$$M \otimes_R R'$$

graçe à I.2.2.5.

b) $L_\mathfrak{p} \;\cong\; L \otimes_A \widehat{A_\mathfrak{p}}$ On a alors

$$L_\mathfrak{p} \;=\; L \otimes_K K_\mathfrak{p} \;=\; L \otimes_{A_\mathfrak{p}} K_\mathfrak{p}$$

grâce à III.2.2.3.4 ; puis

$$L_\mathfrak{p} \;=\; L \otimes_{A_\mathfrak{p}} (K \otimes_{A_\mathfrak{p}} \widehat{A_\mathfrak{p}})$$

grâce à III.2.1.15.f ; puis

$$L_\mathfrak{p} \;=\; (L \otimes_{A_\mathfrak{p}} K) \otimes_{A_\mathfrak{p}} \widehat{A_\mathfrak{p}}$$

grâce à I.2.1.8.ii ; puis

$$L_\mathfrak{p} \;=\; L \otimes_{A_\mathfrak{p}} \widehat{A_\mathfrak{p}}$$

grâce à I.3.1.7 ; puis

$$L_\mathfrak{p} \;=\; L \otimes_A \widehat{A_\mathfrak{p}}$$

grâce à III.2.2.3.4. Ceci donne le premier isomorphisme de III.2.2.3.1.
c) $L_{\mathfrak{p}} \cong L \otimes_B \widehat{B_{\mathfrak{p}}}$ D'après I.2.2.5, on a

$$\widehat{A_{\mathfrak{p}}} \otimes_A L = (\widehat{A_{\mathfrak{p}}} \otimes_A B) \otimes_B L = \widehat{B_{\mathfrak{p}}} \otimes_B L$$

ce qui définit le deuxième isomorphisme dans III.2.2.3.1.

ii)
a) $\widehat{A_{\mathfrak{p}}} \subset K_{\mathfrak{p}}$ L'inclusion $\widehat{A_{\mathfrak{p}}} \subset K_{\mathfrak{p}}$ résulte du fait que $K_{\mathfrak{p}}$ est le corps des fractions de $\widehat{A_{\mathfrak{p}}}$ (cf. III.2.1.15.e.)
b) $\widehat{A_{\mathfrak{p}}} \subset \widehat{B_{\mathfrak{p}}}$ Puisque A est noethérien et B est un A-module de type fini, l'inclusion naturelle $A \hookrightarrow B$ donne, par extension des scalaires, envertu du point III.2.1.10.i, un morphisme injectif

$$\widehat{A_{\mathfrak{p}}} = A \otimes_A \widehat{A_{\mathfrak{p}}} \hookrightarrow \widehat{B_{\mathfrak{p}}} = B \otimes_A \widehat{A_{\mathfrak{p}}} .$$

c) $K_{\mathfrak{p}} \subset L_{\mathfrak{p}}$ Puisque $K_{\mathfrak{p}}$ est un K-espace vectoriel il est plat sur K si bien que l'inclusion naturelle $K \subset L$ donne par extension des scalaires un morphisme injectif

$$K_{\mathfrak{p}} = K \otimes_K K_{\mathfrak{p}} \hookrightarrow L_{\mathfrak{p}} = L \otimes_K K_{\mathfrak{p}} .$$

d) **Le carré de gauche** Les isomorphismes III.2.2.3.1 donnent un diagramme commutatif

$$\begin{array}{ccccc} A & \hookrightarrow & B & \hookrightarrow & L \\ \downarrow & & \downarrow & & \downarrow \\ \widehat{A_{\mathfrak{p}}} & \hookrightarrow & \widehat{B_{\mathfrak{p}}} & \to & L_{\mathfrak{p}} = L \otimes_A \widehat{A_{\mathfrak{p}}} = L \otimes_B \widehat{B_{\mathfrak{p}}} . \end{array}$$

La seule chose qui reste donc à montrer est que le morphisme $\widehat{B_{\mathfrak{p}}} \to L_{\mathfrak{p}}$ est injectif.
D'après le sorite III.2.2.3.4,

$$L_{\mathfrak{p}} = L \otimes_K K_{\mathfrak{p}} = L \otimes_A K_{\mathfrak{p}} .$$

Or K est plat sur A (cf. I.3.1.11,) tandis que $K_{\mathfrak{p}}$ étant un K-espace vectoriel, il est plat sur K donc plat sur A. L'inclusion $B \subset L$ donne donc par tensorisation un morphisme injectif

$$B \otimes_A K_{\mathfrak{p}} \hookrightarrow L \otimes_A K_{\mathfrak{p}} = L \otimes_K K_{\mathfrak{p}} = L_{\mathfrak{p}} . \qquad \text{III.2.2.4}$$

D'après la proposition I.2.2.5,

$$\widehat{B_{\mathfrak{p}}} = (B \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} .$$

Or $B \otimes_A A_{\mathfrak{p}} = B_{\mathfrak{p}}$ est la fermeture intégrale de $A_{\mathfrak{p}}$ dans L (cf. I.4.2.3.) Comme $A_{\mathfrak{p}}$ est un anneau de valuation discrète (cf. I.5.2.1,) donc en particulier principal, $B_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$-module libre de rang d (cf. I.4.4.3.) Il en résulte que

$$\widehat{B_{\mathfrak{p}}} = {A_{\mathfrak{p}}}^d \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} = \widehat{A_{\mathfrak{p}}}^d . \qquad \text{III.2.2.5}$$

De même, on a

$$B \otimes_A K_{\mathfrak{p}} \;=\; (B \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} K_{\mathfrak{p}} \;=\; B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K_{\mathfrak{p}} \;=\; {A_{\mathfrak{p}}}^d \otimes_{A_{\mathfrak{p}}} K_{\mathfrak{p}}\,.$$

Le $A_{\mathfrak{p}}$-module libre ${A_{\mathfrak{p}}}^d$ est en particulier plat d'où il résulte que l'inclusion naturelle $\widehat{A_{\mathfrak{p}}} \hookrightarrow K_{\mathfrak{p}}$ donne un morphisme injectif

$$B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} \;\hookrightarrow\; B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K_{\mathfrak{p}}$$

ce qui grâce à l'inclusion III.2.2.4 donne finalement le morphisme injectif de $\widehat{A_{\mathfrak{p}}}$-modules :

$$\widehat{B_{\mathfrak{p}}} \;\hookrightarrow\; L_{\mathfrak{p}}\,.$$

a) $\widehat{B_{\mathfrak{p}}} \;\cong\; \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{B_{\mathfrak{q}_i}}$ Cet isomorphisme à été défini dans le lemme III.2.2.2.

b) **Le carré de droite** On a, d'après III.2.2.3.1

$$L_{\mathfrak{p}} \;=\; L \otimes_B \widehat{B_{\mathfrak{p}}}$$

c'est-à-dire, grâce au lemme III.2.2.2,

$$L_{\mathfrak{p}} \;=\; L \otimes_B \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{B_{\mathfrak{q}_i}}$$

c'est-à-dire, grâce au fait qu'un produit fini de $\widehat{A_{\mathfrak{p}}}$-algèbres est aussi une somme et à la proposition I.2.1.8.iv,

$$L_{\mathfrak{p}} \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} (L \otimes_B \widehat{B_{\mathfrak{q}_i}})$$

c'est-à-dire finalement grâce à III.2.1.15.f, donne

$$L_{\mathfrak{p}} \;=\; \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{L_{\mathfrak{q}_i}}$$

et achève la preuve.

q.e.d

Lemme III.2.2.6. *On note $L_{\mathfrak{p}} := L \otimes_K K_{\mathfrak{p}}$.*
i) Il existe un unique entier $g'_{\mathfrak{p}}$ tel que l'anneau $L_{\mathfrak{p}} := L \otimes_K K_{\mathfrak{p}}$ est isomorphe à

$$\prod_{i=1}^{g'_{\mathfrak{p}}} K_{\mathfrak{p}}[X]/P_i$$

où les

$$P_{i\,,1\leq i\leq g'_{\mathfrak{p}}} \in K_{\mathfrak{p}}[X]$$

sont les facteurs irréductibles de P dans $K_{\mathfrak{p}}[X]$. Pour tout $1 \leq i \leq g'_{\mathfrak{p}}$, l'extension $K_{\mathfrak{p}} \subset K_{\mathfrak{p}}[X]/P_i$ est donc finie séparable.

ii) Pour tout $1 \leq i \leq g'_{\mathfrak{p}}$, la valeur absolue $|\cdot|_{\mathfrak{p}}$ sur $K_{\mathfrak{p}}$ s'étend de manière unique en une valeur absolue ultramétrique $|\cdot|_i$ sur $K_{\mathfrak{p}}[X]/P_i$.

iii) Posons

$$||(x_1,\ldots,x_{g'_{\mathfrak{p}}})|| := \max_{1\leq i\leq g'_{\mathfrak{p}}}(|x_i|_i)\ \forall (x_1,\ldots,x_{g'_{\mathfrak{p}}} \in L_{\mathfrak{p}} = \prod_{i=1}^{g'_{\mathfrak{p}}} K_{\mathfrak{p}}[X]/P_i\ .$$

Alors $||\cdot||$ est une norme sur le $K_{\mathfrak{p}}$-espace vectoriel $L_{\mathfrak{p}}$ relativement à la valeur absolue $|\cdot|_{\mathfrak{p}}$ sur $K_{\mathfrak{p}}$. Toute norme sur $L_{\mathfrak{p}}$ relativement à $|\cdot|_{\mathfrak{p}}$, lui est équivalente.

iv) L'application naturelle

$$htlL\ :\ L\ \rightarrow\ L_{\mathfrak{p}}\ ,\ x \mapsto x\otimes 1$$

est injective et permet de restreindre la norme $||\cdot||$ en une norme sur L encore notée $||\cdot||$ qui restreinte à K est la valeur absolue $|\ldots|_{\mathfrak{p}}$.

De plus L est dense dans $L_{\mathfrak{p}}$, donc $L_{\mathfrak{p}}$ est en fait le séparé complété de L pour la norme $||\cdot||$.

v) La boule unité dans $L_{\mathfrak{p}}$

$$\mathcal{B}_{\mathfrak{p}} := \{x \in L_{\mathfrak{p}}\ |\ ||x|| \leq 1\}$$

s'identifie au produit

$$\prod_{i=1}^{g'_{\mathfrak{p}}} \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$$

où $\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$ est l'anneau des entiers de $K_{\mathfrak{p}}[X]/P_i$ c'est-à-dire le la fermeture intégrale de l'anneau de la valuation du corps valué $(K_{\mathfrak{p}}, v_{\mathfrak{p}})$.

Preuve :

i) Puisque L/K est une extension séparable, il existe un polynôme irréductible unitaire $P \in K[X]$ tel que L s'identifie à $K[X]/P$. Il se peut très bien cependant que P ne soit pas irréductible dans $K_{\mathfrak{p}}$. Notons donc $P_{i\,,1\leq i\leq g'_{\mathfrak{p}}}$ ses $g'_{\mathfrak{p}}$ facteurs irréductibles dans $K_{\mathfrak{p}}[X]$. Puisque P est séparable, les P_i le sont et deux à deux premiers entre eux.

On a alors $L\otimes_K K_{\mathfrak{p}} = K[X]/P\otimes_K K_{\mathfrak{p}}$ qui vaut encore, grâce à la proposition I.2.2.5

$$K[X]/P\otimes_{K[X]}(K[X]\otimes_K K_{\mathfrak{p}})$$

qui est encore égal à

$$K[X]/P\otimes_{K[X]} K_{\mathfrak{p}}[X]$$

(cf. I.2.2.3.ii,) encore égal à $K_{\mathfrak{p}}[X]/P$ finalement égal à

$$\prod_{i=1}^{g'_{\mathfrak{p}}} K_{\mathfrak{p}}[X]/P_i$$

grâce au théorème chinois des restes.

ii) C'est une conséquence des théorème III.2.1.15.i, II.3.1.2 et de la proposition II.1.2.10.i.

iii) La vérification que $||\cdot||$ est une norme est facile. Par ailleurs, $L_{\mathfrak{p}}$ étant un $K_{\mathfrak{p}}$-espace vectoriel de dimension finie, et $(K_{\mathfrak{p}}, |\cdot|_{\mathfrak{p}})$ étant complet toutes les normes relatives à $|\cdot|_{\mathfrak{p}}$ sont équivalentes.

iv) L'inclusion naturelle $K \subset K_{\mathfrak{p}}$ donne un morphisme injectif

$$L \ = \ K \otimes_K L \ \hookrightarrow \ L_{\mathfrak{p}} \ = \ K_{\mathfrak{p}} \otimes_K L$$

puisque L est plat en tant que K-espace vectoriel. Le fait que la norme $||\cdot||$ se restreigne en une norme sur L relativement à $|\cdot|_{\mathfrak{p}}$ est presque immédiat.

Le corps L est un K-espace vectoriel de dimension d dont on peut noter $(\epsilon_1, \ldots, \epsilon_d)$ une K-base. Alors

$$(\epsilon_1 \otimes 1_{K_{\mathfrak{p}}}, \ldots \epsilon_D \otimes 1_{K_{\mathfrak{p}}})$$

est une $K_{\mathfrak{p}}$-base de $L_{\mathfrak{p}}$. On peut donc écrire de manière unique tout élément de $L_{\mathfrak{p}}$

$$\xi \ = \ \sum_{i=1}^{d} \xi_i(\epsilon_i \otimes 1) \ \xi_i \, , 1 \leq \in \leq d \ \in \ K_{\mathfrak{p}} \, .$$

Puisque K est dense dans $K_{\mathfrak{p}}$, il existe une famille de suites $(\xi_{i,n})_{1 \leq i \leq d \ n \in \mathbb{N}}$ telle que

$$\lim_{n \to +\infty} \xi_{i,n} \ = \ \xi_i \, \forall 1 \leq i \leq d \, .$$

Il n'est pas difficile en suite de vérifier que

$$\lim_{n \to +\infty} \big(\sum_{i=1}^{d} \xi_i i, n\epsilon_i \big) \ = \ \xi \, .$$

v) Soit

$$x \ := \ (x_1, \ldots, x_{g'_{\mathfrak{p}}}) \in L_{\mathfrak{p}} \, .$$

$$\begin{array}{rrcl} & ||x|| & \leq & 1 \\ \Leftrightarrow & \max_{1 \leq i \leq g'_{\mathfrak{p}}} |x_i|_i & \leq & 1 \\ \Leftrightarrow & |x_i|_i & \leq & 1 \ \forall 1 \leq i \leq g'_{\mathfrak{p}} \end{array}$$

c'est à dire que x_i est dans l'anneau de la valuation de $K_{\mathfrak{p}}[X]/P_i$ pour tout $1 \leq i \leq d$. Le lemme III.2.2.0 a pour conséquence que cet anneau est $\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$.

q.e.d

Théorème III.2.2.7. *Soit A un anneau de Dedekind, K son corps des fractions, $L := K[X]/P$ une extension finie séparable de degré d et B la fermeture intégrale de A dans L.*

Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ on note $\widehat{A_{\mathfrak{p}}}$ (resp. $K_{\mathfrak{p}}$) le complété de A (resp. K) pour la topologie $\mathfrak{p}$-adique,

$$L_{\mathfrak{p}} \ := \ L \otimes_K K_{\mathfrak{p}} \text{ et } \widehat{B_{\mathfrak{p}}} \ := \ B \otimes_A \widehat{A_{\mathfrak{p}}} \, .$$

On note encore

$$\mathfrak{q}_{i\ ,1\leq i\leq g_{\mathfrak{p}}}\ \in\ \mathrm{Spm}(B)$$

les idéaux maximaux de B au-dessus de $\mathfrak{p}$,

$$e_{\mathfrak{q}_i/\mathfrak{p}}\ \in\ \mathbb{N}^*\ (\textit{resp. } f_{\mathfrak{q}_i/\mathfrak{p}}$$

leur indice de ramification (resp. degré résiduel.)

On note encore, pour tout $1 \leq i \leq g_{\mathfrak{p}}$, $\widehat{B_{\mathfrak{q}_i}}$ (resp. $\widehat{L_{\mathfrak{q}_i}}$) le complété de B (resp. L) pour la topologie $\mathfrak{q}_i$-adique.

On note enfin

$$P_{i\ ,1\leq i\leq g'_{\mathfrak{p}}}\ \in K_{\mathfrak{p}}[X]$$

les facteurs irréductibles du polynôme P dans $K_{\mathfrak{p}}[X]$.

i) On a une bijection naturelle

$$\{\mathfrak{q}_i\}_{1\leq i\leq g_{\mathfrak{p}}}\ \cong\ \{P_i\}_{1\leq i\leq g'_{\mathfrak{p}}} \qquad \textit{III.2.2.7.1}$$

si bien que $g_{\mathfrak{p}}\ =\ g'_{\mathfrak{p}}$ et que quitte à renuméroter on a des isomorphismes naturels de $K_{\mathfrak{p}}$-algèbres :

$$\widehat{L_{\mathfrak{q}_i}}\ \cong\ K_{\mathfrak{p}}[X]/P_i\ \forall 1 \leq i \leq g_{\mathfrak{p}}\ . \qquad \textit{III.2.2.7.2}$$

On en déduit finalement des isomorphismes de $K_{\mathfrak{p}}$-algèbres :

$$L_{\mathfrak{p}}\ \cong\ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{L_{\mathfrak{q}_i}}\ \cong\ \prod_{i=1}^{g_{\mathfrak{p}}} K_{\mathfrak{p}}[X]/P_i\ . \qquad \textit{III.2.2.7.3}$$

ii) Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, $\widehat{L_{\mathfrak{q}_i}}$ est une extension finie séparable de $K_{\mathfrak{p}}$ dont l'anneau des entiers est $\widehat{B_{\mathfrak{q}_i}}$. De plus,

$$\widehat{B_{\mathfrak{p}}}\ =\ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{B_{\mathfrak{q}_i}}$$

s'identifie à l' »anneau des entiers de $L_{\mathfrak{p}}$ » c'est-à-dire les éléments de $L_{\mathfrak{p}}$ annulés par un polynôme unitaire à coefficients dans $\widehat{A_{\mathfrak{p}}}$.

iii) Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, notons $\mathfrak{m}_i$ l'idéal maximal de l'anneau des entiers $\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$ de $K_{\mathfrak{p}}[X]/P_i$. Alors la correspondance III.2.2.7.1 est donnée par

$$P_i\ \mapsto\ \mathrm{Ker}\, B\ \to\ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_i\ . \qquad \textit{III.2.2.7.4}$$

iv) Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, notons

$$e_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} \text{ et } f_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}}$$

l'indice de ramification et le degré résiduel de l'extension de corps locaux

$$K_{\mathfrak{p}} \subset \widehat{L_{\mathfrak{q}_i}}$$

au sens de la définition II.3.1.4, alors

$$e_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} = e_{\mathfrak{q}_i/\mathfrak{p}} \text{ et } f_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} = f_{\mathfrak{q}_i/\mathfrak{p}} . \qquad \textit{III.2.2.7.5}$$

Preuve :
i) Remarquons d'abord que si E est un corps et

$$F := \prod_{i=1}^{g} F_i$$

est une F algèbre telle que pour tout $1 \leq i \leq g$, $E \subset F_i$ est une extension de E, les idéaux maximaux de F sont de la forme

$$\mathfrak{m}_i = \prod_{1 \leq j \leq g,\ j \neq i} F_j .$$

Ils sont donc au nombre de g. De plus, pour tout $1 \leq i \leq g$, $F/\mathfrak{m}_i$ s'identifie canoniquement à F_i.

Ainsi en utilisant la description de

$$L_{\mathfrak{p}} = \prod_{i=1}^{g'_{\mathfrak{p}}} K_{\mathfrak{p}}[X]/P_i$$

donnée en III.2.2.6.i, et celle

$$L_{\mathfrak{p}} = \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{L_{\mathfrak{q}_i}}$$

donnée en III.2.2.3.2, on peut égaler $g_{\mathfrak{p}}$ et $g'_{\mathfrak{p}}$.

En utilisant la description des idéaux maximaux de $L_{\mathfrak{p}}$ donnée ci-dessus, on peut, quitte à renuméroter les $\mathfrak{q}_i$ (resp. les P_i,) écrire

$$\mathfrak{m}_i = \prod_{1 \leq j \leq g_{\mathfrak{p}},\ j \neq i} K_{\mathfrak{p}}[X]/P_j = \prod_{1 \leq j \leq g_{\mathfrak{p}},\ j \neq i} \widehat{L_{\mathfrak{q}_j}} .$$

Ainsi, les $\mathfrak{m}_i$ sont à la fois en bijection avec les $\mathfrak{q}_i$ et les P_i ce qui définit la bijection III.2.2.7.1.

De plus, pour tout $1 \leq i \leq g_{\mathfrak{p}}$, $L_{\mathfrak{p}}/\mathfrak{m}_i$ s'identifie canoniquement à la fois à $\widehat{L_{\mathfrak{q}_i}}$ et $K_{\mathfrak{p}}[X]/P_i$ ce qui montre III.2.2.7.2.

ii) Comme, pour tout $1 \leq i \leq g_{\mathfrak{p}}$, l'extension $K_{\mathfrak{p}} \subset K_{\mathfrak{p}}[X]/P_i$ est finie séparable (cf. III.2.2.6.i,) les isomorphismes III.2.2.7.2 montrent que l'extension $K_{\mathfrak{p}} \subset \widehat{L_{\mathfrak{q}_i}}$ est finie séparable.

La valuation $\mathfrak{q}_i$-adique $v_{\mathfrak{q}_i}$ est la valuation discrète sur $\widehat{L_{\mathfrak{q}_i}}$ qui prolonge la valuation $\mathfrak{p}$-adique $v_{\mathfrak{p}}$ sur $K_{\mathfrak{p}}$ (cf. II.3.1.2e)t $\widehat{B_{\mathfrak{q}_i}}$ est bien entendu l'anneau de la valuation (cf. III.2.1.15.b,) ce qui entraîne, grâce au lemme III.2.2.0, que $\widehat{B_{\mathfrak{q}_i}}$ est l'anneau des entiers de $\widehat{L_{\mathfrak{q}_i}}$.

Comme

$$\widehat{B_{\mathfrak{p}}} \ = \ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{B_{\mathfrak{q}_i}}$$

(cf. III.2.2.2,) il suffit de constater qu'un élément de $L_{\mathfrak{p}}$ est entiers sur $\widehat{A_{\mathfrak{p}}}$ si et seulement s'il l'est après toute projection.

iii) Pour tout $1 \leq i \leq g'_{\mathfrak{p}}$, notons $\mathfrak{m}_i$ l'idéal maximal de $\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$,

$$\mathrm{pr}_i \ : \ \widehat{B_{\mathfrak{p}}} \ \rightarrow \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i} \text{ et } \{\pi_n^{\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}} \ : \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i} \ \rightarrow \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_i^n\}_{n\in\mathbb{N}}$$

les projection canoniques. Notons encore

$$\phi_i \ := \ \pi_1^{\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}} \circ \mathrm{pr}_i \circ \lambda^L{}_{|B} \ : \ B \ \rightarrow \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_{i\ ,1\leq i\leq g'_{\mathfrak{p}}} \ .$$

Le noyau $\mathrm{Ker}\,\phi_i$ de ϕ_i est un idéal de B et ϕ_i se factorise en un morphisme injectif

$$B/\mathrm{Ker}\,\phi_i \ \hookrightarrow \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_i$$

dont le but est un corps. Il en résulte que $\mathrm{Ker}\,\phi_i$ est un idéal premier de B. Qui plus est puisque $\mathfrak{m}_i$ est au-dessus de $\mathfrak{p}\widehat{A_{\mathfrak{p}}}$, $\mathrm{Ker}\,\phi_i$ est au-dessus de $\mathfrak{p}$ c'est donc un idéal maximal et par conséquent l'un des $\mathfrak{q}_{j\ ,1\leq j\leq g_{\mathfrak{p}}}$.

Il résulte de ce qui précède que, pour tout $n \in \mathbb{N}$,

$$\phi_i(\mathfrak{q}_j^n) \ \subset \ \mathfrak{m}_i^n,$$

ce qui définit une famille de morphismes

$$\{\phi_{i,n} \ : \ B/\mathfrak{q}_j^n \ \rightarrow \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_i^n\}_{n\in\mathbb{N}}$$

qui forme un morphisme de systèmes projectifs. On en déduit un morphisme

$$\hat{\phi}_i \ : \ \widehat{B_{\mathfrak{q}_j}} \ = \ \varprojlim_{n\in\mathbb{N}} B/\mathfrak{q}_j^n \ \rightarrow \ \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}/\mathfrak{m}_i^n \ = \ \mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$$

la dernière égalité provenant du fait que $\mathcal{O}_{K_{\mathfrak{p}}[X]/P_i}$ est $\mathfrak{m}_i$-adiquement complet.

Pour tout $x \in \widehat{B_{\mathfrak{q}_j}}$, $\hat{\phi}_i(x) \ = \ 0$, entraîne que x n'est pas inversible donc que x appartient à l'idéal maximal de $\widehat{B_{\mathfrak{q}_j}}$. Si l'on note t_j une uniformisante de l'anneau de valuation discrète $\widehat{B_{\mathfrak{q}_{j(i)}}}$, s'il existe $x \neq 0$ tel que $\hat{\phi}_i(x) \ = \ 0$, il existe $k \in \mathbb{N}^*$ tel que

$$\hat{\phi}_i(t_j)^k \ = \ \hat{\phi}_i(t_j^k) \ = \ 0$$

ce qui implique, puisque $\mathcal{O}_{K_\mathfrak{p}[X]/P_i}$ est un anneau intègre, que $\hat{\phi}_(t_j) = 0$ ce qui entraîne encore que l'image de l'idéal maximal de $\widehat{B_{\mathfrak{q}_j}}$ par $\hat{\phi}_i$ est nul. Or on a un carré commutatif à flèches horizontales injectives

$$\begin{array}{ccc} \widehat{A_\mathfrak{p}} & \hookrightarrow & \widehat{B_{\mathfrak{q}_{j(i)}}} \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \hat{\phi}_i} \\ \widehat{A_\mathfrak{p}} & \hookrightarrow & \mathcal{O}_{K_\mathfrak{p}[X]/P_i}\ . \end{array}$$

Ceci entraîne que l'image de l'idéal maximal de $\widehat{B_{\mathfrak{q}_j}}$ dans $\mathcal{O}_{K_\mathfrak{p}[X]/P_i}$ contient l'idéal maximal de $\widehat{A_\mathfrak{p}}$ qui est non nul. On en déduit que $\hat{\phi}_i$ est injectif.

Puisque $\widehat{L_{\mathfrak{q}_j}}$ (resp. $K_\mathfrak{p}[X]/P_i$) est le corps des fractions de $\widehat{B_{\mathfrak{q}_j}}$ (resp. $\mathcal{O}_{K_\mathfrak{p}[X]/P_i}$) le morphisme injectif $\hat{\phi}_i$ s'étend en un morphisme

$$\widehat{L_{\mathfrak{q}_j}} \ \to\ K_\mathfrak{p}[X]/P_i$$

qui est nécessairement injectif.

iv) Ce point est une conséquence maintenant presqu'immédiate des points précédents et de la proposition III.2.2.1.iv.

q.e.d

III.2.3 . −Complément dans le cas des extensions galoisiennes

Dans la suite de cette section (III.2.3,) A **est un anneau de Dedekind (cf. I.5.2.2,)** K **son corps des fractions,**

$$K \ \subset\ L \ =\ K[X]/P$$

(où $P \in K[X]$ **est un polynôme unitaire irréductible,) une extension galoisienne de degré** d **de** K **et** B **la clôture intégrale de** A **dans** L**. On note**

$$G \ :=\ \mathrm{Gal}_{L/K}$$

le groupe de Galois de l'extension $K \subset L$.

Lemme III.2.3.1.
i) Pour tout $\sigma \in G$, *et* $b \in B$, $\sigma(b) \in B$ *c'est-à-dire que le groupe de Galois* G *opère sur* B.

ii) Pour tout idéal maximal $\mathfrak{q} \subset B$, $\sigma(\mathfrak{q})$ *est encore un idéal maximal de* B *c'est-à-dire que* G *opère sur l'ensemble* $\mathrm{Spm}(B)$ *des idéaux maximaux de* B.

Proposition III.2.3.2. *Pour tout idéal maximal* $\mathfrak{p} \in \mathrm{Spm}(A)$, *et tout couple d'idéaux maximaux* $\mathfrak{q}$ *et* $\mathfrak{r}$ *de* B *au-dessus de* $\mathfrak{p}$ *(cf. I.4.3.1,) il existe* $\sigma \in G$ *tel que* $\sigma(\mathfrak{q}) = \mathfrak{r}$.

Preuve : Supposons que pour tout $\sigma \in G$, $\sigma(\mathfrak{q}) \neq \mathfrak{r}$.

En appliquant le lemme d'approximation (cf. III.1.1.12,) ou le théorème chinois des restes, il existe $b \in B$ tel que $b \in \mathfrak{r}$, et $b \equiv 1\ [[\sigma(\mathfrak{q})]]$ pour tout σ dans G. Or

$$\mathrm{N}_{L/K}(b) \ = \ \prod_{\sigma \in G} \sigma(b) \ \in \ K \cap B \ = \ A$$

et

$$\mathrm{N}_{L/K}(b) \ = \ b \prod_{\sigma \in G \setminus \{\mathrm{Id}\}} \sigma(b) \ \in \ \mathfrak{r}\,.$$

D'où $\mathrm{N}_{L/K}(b) \in A \cap \mathfrak{r} = \mathfrak{p}$. Or $\mathfrak{p} = \mathfrak{q} \cap A$ donc $\mathrm{N}_{L/K}(b) \in \mathfrak{q}$ c'est-à-dire, comme $\mathfrak{q}$ est premier, qu'il existe $\sigma \in G$ tel que $\sigma(b) \in \mathfrak{q}$ c'est-à-dire que $b \in \sigma^{-1}(\mathfrak{q})$ ou encore $b \equiv 0\ [[\sigma^{-1}(\mathfrak{q})]]$ ce qui est contradictoire. *q.e.d*

Définition III.2.3.3. Étant donné un idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$, on appelle *groupe de décomposition en* $\mathfrak{q}$ le sous-groupe

$$G_{\mathfrak{q}} \ := \ \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\} \ \subset \ G$$

de G.

Lemme III.2.3.4. *Soit $\mathfrak{p} \in \mathrm{Spm}(A)$ un idéal maximal.*
i) Pour tout idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$ au-dessus de $\mathfrak{p}$, l'indice de $G_{\mathfrak{q}}$ dans G est $g_{\mathfrak{p}}$ le nombre d'idéaux maximaux au-dessus de $\mathfrak{p}$ (cf. III.1.2.4.)

ii) Les groupes de décomposition au-dessus de $\mathfrak{p}$ sont tous conjugués et inversement tout conjugué de $G_{\mathfrak{q}_i}$ est un groupe de décomposition pour un $\mathfrak{q}_j$ convenable.

Proposition III.2.3.5. *Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, on note $K_{\mathfrak{p}}$ le complété de K pour la topologie $\mathfrak{p}$-adique et $L_{\mathfrak{p}} := L \otimes_K K_{\mathfrak{p}}$.*
i) Alors, pour tout $\sigma \in G$, il existe un unique automorphisme d'anneau encore noté

$$\sigma \ : \ L_{\mathfrak{p}} \ \to \ L_{\mathfrak{p}}$$

tel que

– $$\sigma_{|K_{\mathfrak{p}}} \ = \ \mathrm{Id}_{K_{\mathfrak{p}}}\ ;$$

– $$\sigma(a \otimes 1) \ = \ \sigma(a) \otimes 1 \ \forall a \in L\ ;$$

– *Le carré*

$$\begin{array}{ccc} L & \xrightarrow{\ \sigma\ } & L \\ {\scriptstyle \lambda^L}\downarrow & & \downarrow{\scriptstyle \lambda^L} \\ L_{\mathfrak{p}} & \xrightarrow{\ \sigma\ } & L_{\mathfrak{p}} \end{array}$$

(où λ^L est l'inclusion naturelle (cf. III.2.2.6.iv,)) est commutatif.

On définit ainsi un morphisme de groupes de G dans le groupe des $K_{\mathfrak{p}}$-automorphisme d'anneaux de $L_{\mathfrak{p}}$.

ii) On note

$$L_{\mathfrak{p}} \ = \ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{L_{\mathfrak{q}_i}}$$

comme en III.2.2.7.3 (ou les

$$\mathfrak{q}_{i\ ,1\leq i\leq g_{\mathfrak{p}}} \ \in \ \mathrm{Spm}(B)$$

sont les idéaux maximaux de B au-dessus de $\mathfrak{p}$.) Alors pour tout $\sigma \in G$ et tout $1 \leq i \leq g_{\mathfrak{p}}$, il existe un unique $1 \leq j \leq g_{\mathfrak{p}}$ tel que $\sigma(\widehat{L_{\mathfrak{q}_i}}) \ = \ \widehat{L_{\mathfrak{q}_j}}$ déterminé par $\sigma(\mathfrak{q}_i) \ = \ \mathfrak{q}_j$.

Preuve :

i) Ce point est laissé en exercice.

ii) Pour $\mathfrak{q} \in \mathrm{Spm}(B)$, on rappelle qu'on note

$$\widehat{B_{\mathfrak{q}}} \ := \ \varprojlim_{n\in\mathbb{N}} B/\mathfrak{q}^n$$

le séparé complété de B pour la topologie $\mathfrak{q}$-adique.

Il est facile de montrer que $\sigma(\mathfrak{q}_i) \ = \ \mathfrak{q}_j$ entraîne

$$\sigma(\widehat{B_{\mathfrak{q}_i}}) \ = \ \widehat{B_{\mathfrak{q}_j}}$$

ce qui entraîne finalement, puisque

$$\widehat{L_{\mathfrak{q}.}} \ = \ \mathrm{Frac}(\widehat{B_{\mathfrak{q}.}})$$

(cf. III.2.1.15.e,) que

$$\sigma(\widehat{L_{\mathfrak{q}_i}}) \ = \ \widehat{L_{\mathfrak{q}_j}} \ .$$

q.e.d

Théorème III.2.3.6. *Soit A un anneau de Dedekind, K son corps des fractions, $L \ := \ K[X]/P$ une extension galoisienne de degré d et B la fermeture intégrale de A dans L.*

Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, on note $K_{\mathfrak{p}}$ le complété de K pour la topologie $\mathfrak{p}$-adique et $L_{\mathfrak{p}} \ := \ L \otimes_K K_{\mathfrak{p}}$. On note

$$\mathfrak{q}_{i\ ,1\leq i\leq g_{\mathfrak{p}}} \ \in \ \mathrm{Spm}(B)$$

les idéaux maximaux de B au-dessus de $\mathfrak{p}$ et

$$L_{\mathfrak{p}} \ = \ \prod_{i=1}^{g_{\mathfrak{p}}} \widehat{L_{\mathfrak{q}_i}}$$

(cf. III.2.2.7.3.)

i) Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, *l'extension* $\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}$ *est galoisienne.*

ii) Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, *le groupe de Galois* $\mathrm{Gal}_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}}$ *s'identifie au groupe de décomposition* $G_{\mathfrak{q}_i}$.

iii) Pour tout $1 \leq i \leq j \leq g_{\mathfrak{p}}$,

$$e_{\mathfrak{q}_i/\mathfrak{p}} \;=\; e_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} \;=\; e_{\widehat{L_{\mathfrak{q}_j}}/K_{\mathfrak{p}}} \;=\; e_{\mathfrak{q}_j/\mathfrak{p}}$$

et

$$f_{\mathfrak{q}_i/\mathfrak{p}} \;=\; f_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} \;=\; f_{\widehat{L_{\mathfrak{q}_j}}/K_{\mathfrak{p}}} \;=\; f_{\mathfrak{q}_j/\mathfrak{p}}\ .$$

Si l'on note $e_{\mathfrak{p}}$ *(resp.* $f_{\mathfrak{p}}$*) l'indice de ramification (resp. le degré résiduel) commun des extensions* $L_i/K_{\mathfrak{p}}$, *on a*

$$d \;=\; e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}\ .$$

Remarque III.2.3.7. Les groupes d'inertie $I_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}}$ sont tous conjugués et si $I_{\widehat{L_{\mathfrak{q}_i}}/K_{\mathfrak{p}}} \;=\; 1$, on dit que $\mathfrak{p}$ est *non-ramifié*. L'ensemble des $\mathfrak{p} \in \mathrm{Spm}(A)$ ramifiés est fini. Si $\mathfrak{p}$ est non-ramifié $G_{\mathfrak{q}_i}$ s'identifie au groupe de Galois de l'extension résiduelle.

Exemple III.2.3.8. Si K est un corps de nombres, A l'anneau des entiers est la fermeture intégrale de $\mathbb{Z}$ dans K. Si on suppose que $K/\mathbb{Q}$ est galoisienne de groupe G, et que $p \in \mathbb{Z}$ est non ramifié, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, au-dessus de p, $G_{\mathfrak{p}}$ s'identifie au groupe de Galois $\mathrm{Gal}_{A/\mathfrak{p}/\mathbb{F}_p}$ qui est engendré par le Frobenius ϕ.

Comme élément de G, ϕ est caractérisé par $\phi(\mathfrak{p}) = \mathfrak{p}$ et

$$\phi(b) \;\equiv\; b^q\ [[\mathfrak{p}]]\ .$$

Pour tout p non ramifié on note C_p la classe de conjugaison du Frobenius en p.

Théorème III.2.3.9. Théorème de Densité de Tchebotarev sous une forme faible *Pour toute classe de conjugaison* $C \subset G$, *il existe une infinité de* p *non ramifiés tels que* $C_p = C$.

III.3 . −Construction de la fermeture intégrale d'un anneau de Dedekind dans une extension finie séparable

III.3.0 . −Compléments d'algèbre commutative

Dans tout ce paragraphe (III.3.0,) A **est un anneau.**

Définition III.3.0.1. On appelle *support d'un* A*-module* M, l'ensemble

$$\mathrm{Supp}_A(M) \;:=\; \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_{\mathfrak{p}} \;\neq 0\} \;\subset\; \mathrm{Spec}(A)$$

des idéaux premiers $\mathfrak{p}$ de A tels que $M_{\mathfrak{p}}$ (cf. I.3.3.7) ne soit pas le module nul.

Lemme III.3.0.2. *Si M est un A-module de type fini, le support $\mathrm{Supp}_A(M)$ s'identifie à l'ensemble des idéaux premiers de A qui contiennent l'idéal anulateur $\mathrm{Ann}_A(M)$ de M (cf. I.1.2.2,) ou encore à l'ensemble des idéaux premiers du quotient $A/\mathrm{Ann}_A(M)$ usuellement noté $\mathrm{Spec}(A/\mathrm{Ann}_A(M))$.*

Preuve : Pour tout $a \in \mathrm{Ann}_A(M)$, tout $\mathfrak{p} \in \mathrm{Spec}(A)$ tout $x \in M$, $a.x = 0$. Ceci implique en particulier, que pour tout $\xi \in M_{\mathfrak{p}}$, $a\xi = 0$ en particulier pour $\xi \neq 0$. Ceci implique en particulier, que $(a, 1) \in A_{\mathfrak{p}}$ n'est pas inversible, donc est dans l'idéal maximal c'est-à-dire finalement que $a \in \mathfrak{p}$.

Réciproquement pour $\mathfrak{p} \in \mathrm{Spec}(A)$ contenant $\mathrm{Ann}_A(M)$, aucun des éléments du complémentaire de $\mathfrak{p}$ n'est dans $\mathrm{Ann}_A(M)$. Si $M_{\mathfrak{p}}$ était nul, pour tout $\xi := (x, s) \in M_{\mathfrak{p}}$ on aurait $1_{A_{\mathfrak{p}}}(x, s) = 0$ c'est-à-dire qu'il existerait $t \notin \mathfrak{p}$ tel que $tx = 0$. Si M est de type fini engendré par x_i ,$1 \leq i \leq d$, les images des x_i dans $M_{\mathfrak{p}}$ engendrent encore $M_{\mathfrak{p}}$. Or, d'après ce qui précède, pour tout $1 \leq i \leq d$, il existe $t_i \notin \mathfrak{p}$ tel que $t_i x_i = 0$. Dès lors $\prod_{i=1}^{d} t_i \notin \mathfrak{p}$ et annule M ce qui est contradictoire. *q.e.d*

Lemme III.3.0.3. *Étant donné un A-module M, les applications naturelles*

$$M \longrightarrow \prod_{\mathfrak{m} \in \mathrm{Spm}(A)} M_{\mathfrak{m}} \longrightarrow \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} M_{\mathfrak{p}}$$

sont injectives.

Preuve : Soit $x \in M$. Si pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, l'image $x_{\mathfrak{m}}$ de x dans $M_{\mathfrak{m}}$ est nulle, il existe $s_{\mathfrak{m}} \in A \setminus \mathfrak{m}$ tel que $s_{\mathfrak{m}} x = 0$. Ceci implique en particulier, que l'idéal annulateur $\mathrm{Ann}_A(x)$ de x n'est contenu dans aucun idéal maximal de A. On a donc $\mathrm{Ann}_A(x) = A$ ce qui entraîne que $x = 0$. On a donc ainsi montré l'injectivité de la première application.

L'injectivité de la seconde application résulte simplement du fait que

$$\mathrm{Spm}(A) \subset \mathrm{Spec}(A) .$$

q.e.d

Corollaire III.3.0.4. *Pour un A-module M, les conditions suivantes sont équivalentes :*

a) M est le module nul.

b) Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$ de A, $M_{\mathfrak{p}} = 0$.

c) Pour tout idéal maximal $\mathfrak{m} \in \mathrm{Spm}(A)$ de A, $M_{\mathfrak{m}} = 0$.

d) Le support de m est l'ensemble vide.

Lemme III.3.0.5. *Soient*

$$\mathbf{C} \text{ et } \mathbf{C}_{i\ ,i \in I}$$

des catégories de modules et

$$F_i : \mathbf{C} \to \mathbf{C}_i$$

des foncteurs tels que :
a) Pour toute suite exacte

$$0 \ \to \ R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P \ \to \ 0$$

dans $\mathbf{C}$ *et tout* $i \in I$, *la suite*

$$0 \ \to \ F_i(R) \xrightarrow{F_i(u)} F_i(Q) \longrightarrow \xrightarrow{F_i(v)} F_i(P) \ \to \ 0$$

est exacte.
b) Pour tout objet P *de* $\mathbf{C}$, $P \ = \ 0$ *si et seulement si*

$$F_i(P) \ = \ 0 \, \forall i \in I \ .$$

Alors :
i) Pour tout morphisme $f \ : \ Q \ \to \ P$ *de* $\mathbf{C}$, *et tout* $i \in I$,

$$\operatorname{Ker} F_i(f) \ = \ F_i(\operatorname{Ker} f) \ , \ \operatorname{Coker} F_i(f) \ = \ F_i(\operatorname{Coker} f) \ , \ \operatorname{Im} F_i(f) \ = \ F_i(\operatorname{im}(f)) \ .$$

ii) Un morphisme $f \ : \ X \ \to \ Y$ *de* $\mathbf{C}$ *est injectif (resp. surjectif) (resp. nul,) si et seulement si pour tout* $i \in I$, $F_i(f)$ *l'est.*
iii) Étant donnée une suite de morphismes

$$R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P$$

dans $\mathbf{C}$, *la suite*

$$0 \ \to \ R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P \ \to \ 0$$

est exacte si et seulement si pour tout $i \in I$, *la suite*

$$0 \ \to \ F_i(R) \xrightarrow{F_i(u)} F_i(Q) \longrightarrow \xrightarrow{F_i(v)} F_i(P) \ \to \ 0$$

est exacte.

Preuve :
i) Pour tout morphisme $f \ : \ X \ \to \ Y$ de $\mathbf{C}$ on a un diagramme comme en I.1.1.18. En utilisant (a), pour tout $i \in I$, on obtient un diagramme analogue après application de F_i ce qui donne le résultat en vertu de la proposition I.1.1.18.
ii) Le sens direct est une conséquence immédiate de (a).
Réciproquement, on peut toujours écrire une suite exacte

$$0 \ \to \ \operatorname{Ker} f \ \longrightarrow \ X \xrightarrow{f} Y \longrightarrow \operatorname{Coker} f \ \to \ 0 \ .$$

Elle reste exacte après application du foncteur F_i pour tout $i \in I$ en vertu de (a). Si donc $F_i(f)$ est injectif (resp. surjectif) (resp. nul,) pour tout $i \in I$

$$\operatorname{Ker} F_i(f) \ = \ 0 \text{ (resp. } \operatorname{Coker} F_i(f) \ = \ 0) \text{ (resp. } \operatorname{Im} F_i(f) \ = \ 0 \text{ .)}$$

Il en résulte grâce au point III.3.0.5.i, que

$$\forall \in\in I\ ,\ F_i(\mathrm{Ker}\, f)\ =\ 0 \text{ (resp. } F_i(\mathrm{Coker}\, f)\ =\ 0) \text{ (resp. } F_i(\mathrm{Im}\, f)\ =\ 0\ .)$$

Ceci prouve finalement, en appliquant (b) que f est injectif (resp. surjectif) (ressp. nul.)

iii) Le sens direct est simplement (a).

Réciproquement, si pour tout $i \in I$, la suite

$$(*)_i\ :\ 0\ \to\ F_i(R) \xrightarrow{F_i(u)} F_i(Q) \longrightarrow \xrightarrow{F_i(v)} F_i(P)\ \to\ 0$$

est exacte, il découle du point III.3.0.5.ii que u est injectif, v est surjectif et $v \circ u\ =\ 0$. On a donc

$$\mathrm{Im}\, u\ \subset\ \mathrm{Ker}\, v\ .$$

La suite exacte

$$0\ \to\ \mathrm{Im}\, u\ \longrightarrow\ \mathrm{Ker}\, v \longrightarrow \mathrm{Ker}\, v/\mathrm{Im}\, u\ \to\ 0$$

reste exacte après application du foncteur F_i pour tout $i \in I$. Mais l'exactitude de $(*)_i$ entraîne que $F_i(\mathrm{Ker}\, v/\mathrm{Im}\, u)\ =\ 0$, ce qui implique finalement grâce à (b) que $\mathrm{Ker}\, v/\mathrm{Im}\, u\ =\ 0$ et achève la preuve.

q.e.d

Proposition III.3.0.6. *Pour une suite de morphismes*

$$R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P$$

de A-modules, les conditions suivantes sont équivalentes :

a) La suite de morphismes de A-modules

$$0\ \to\ R \xrightarrow{u} Q \longrightarrow \xrightarrow{v} P\ \to\ 0$$

est exacte.

b) Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$ de A, la suite de morphismes de $A_\mathfrak{p}$-modules

$$0\ \to\ R_\mathfrak{p} \xrightarrow{u_\mathfrak{p}} Q_\mathfrak{p} \longrightarrow \xrightarrow{v_\mathfrak{p}} P_\mathfrak{p}\ \to\ 0$$

est exacte.

c) Pour tout idéal maximal $\mathfrak{m} \in \mathrm{Spm}(A)$ de A, la suite de morphismes de $A_\mathfrak{m}$-modules

$$0\ \to\ R_\mathfrak{m} \xrightarrow{u_\mathfrak{m}} Q_\mathfrak{m} \longrightarrow \xrightarrow{v_\mathfrak{m}} P_\mathfrak{m}\ \to\ 0$$

est exacte.

Preuve :

i) (a) implique (b) résulte du fait que $A_\mathfrak{p}$ est A-plat (cf. I.3.1.11) et (b) implique (c) résulte simplement de ce que $\mathrm{Spm}(A)\ \subset\ \mathrm{Spec}(A)$.

ii) Pour montrer que (c) implique (a), on considère les foncteurs

$$M \ \mapsto \ M_{\mathfrak{m}\ ,\mathfrak{m}\in \mathrm{Spm}(A)}$$

de la catégorie des A-modules dans la catégorie des $A_{\mathfrak{m}}$-modules. Pour leur appliquer le point III.3.0.5.iii, il faut vérifier qu'il satisfont à l'hypothèse (a) de III.3.0.5, ce qui résulte du fait que $A_{\mathfrak{m}}$ est A-plat pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ et qu'il satisfont également à (b) ce qui résulte du corollaire III.3.0.4.

q.e.d

Lemme III.3.0.7. *Soit A un anneau local noethérien d'idéal maximal $\mathfrak{m}$. Pour tout A-module M, de type fini, on note*

$$\hat{M} \ := \varprojlim_{n\in\mathbb{N}} M/\mathfrak{m}^n M$$

(cf. III.2.1.2.) Alors le morphisme naturel

$$\lambda^M \ : \ M \ \to \ \hat{M}$$

est injectif.

Preuve : Le noyau de λ^M est

$$K \ = \ \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n M \ \subset \ M \ .$$

Comme A est noethérien et M de type fini, K est un A-module de type fini. De plus, il vérifie clairement

$$\mathfrak{m}K \ = \ K$$

ce qui entraîne, graçe au lemme de Nakayama (cf. I.3.3.8.i,) $K \ = \ 0$. *q.e.d*

Proposition III.3.0.8. *Soit A un anneau noethérien. Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$ de A, on note $A_{\mathfrak{p}}$ le localisé de A en $\mathfrak{p}$ (cf. I.3.3.7) et*

$$\widehat{A_{\mathfrak{p}}} \ := \varprojlim_{n\in\mathbb{N}} A/\mathfrak{p}^n \ = \ \varprojlim_{n\in\mathbb{N}} A_{\mathfrak{p}}/A_{\mathfrak{p}}\mathfrak{p}^n$$

le séparé complété de A (ou de $A_{\mathfrak{p}}$) pour la topologie $\mathfrak{p}$-adique.

Pour une suite de morphisme de A-modules,

$$R \xrightarrow{\ u\ } Q \longrightarrow \xrightarrow{\ v\ } P$$

avec Q de type fini, les conditions III.3.0.6.a à III.3.0.6.c sont encore équivalentes à

a) Pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$, la suite

$$0 \ \to \ R \otimes_A \widehat{A_{\mathfrak{p}}} \xrightarrow{u\otimes_A \widehat{A_{\mathfrak{p}}}} Q \otimes_A \widehat{A_{\mathfrak{p}}} \longrightarrow \xrightarrow{v\otimes_A \widehat{A_{\mathfrak{p}}}} P \otimes_A \widehat{A_{\mathfrak{p}}} \ \to \ 0$$

est exacte.

b) Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, *la suite*

$$0 \ \to \ R \otimes_A \widehat{A_\mathfrak{p}} \xrightarrow{u\otimes_A \widehat{A_\mathfrak{p}}} Q \otimes_A \widehat{A_\mathfrak{p}} \longrightarrow \xrightarrow{v\otimes_A \widehat{A_\mathfrak{p}}} P \otimes_A \widehat{A_\mathfrak{p}} \ \to \ 0$$

est exacte.

Preuve :
i) Le fait que III.3.0.6.a entraîne III.3.0.8.a est une conséquence de la proposition III.2.1.10.
ii) Le fait que III.3.0.8.a entraîne III.3.0.8.b résulte simplement du fait que $\mathrm{Spm}(A) \ \subset \ \mathrm{Spec}(A)$.
iii) On rappelle que si A est un anneau noethérien, il en est de même pour $S^{-1}A$ pour toute partie multiplicative S de A (cf. I.3.2.3.ii.) Ainsi donc, pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_\mathfrak{p}$ est un anneau local noethérien.

Enfin le fait que III.3.0.8.b entraîne III.3.0.6.a résulte du fait qu'en vertu de III.2.1.10 et du lemme III.3.0.7, les foncteurs

$$M \ \mapsto \ M \otimes_A \widehat{A_\mathfrak{p}} \, , \mathfrak{p}\in \mathrm{Spm}(A)}$$

satisfont aux conditions (a) et (b) du lemme III.3.0.5.

q.e.d

III.3.1 . –Étude des extensions rédisuelles

Soit A un anneau de Dedekind, K son corps des fractions, L une extension finie séparable de degré d de K et B la fermeture intégrale de A dans L. Étant doné un idéal maximal $\mathfrak{p} \in \mathrm{Spec}(A)$, on note $A_\mathfrak{p}$ le localisé de A en $\mathfrak{p}$ (cf. I.3.3.7.) Pour tout A-module X, on note

$$X_\mathfrak{p} \ := \ X \otimes_A A_\mathfrak{p} \ = \ (A \setminus \mathfrak{p})^{-1} X \ .$$

On note encore

$$\widehat{A_\mathfrak{p}} \ = \ \varprojlim_{n\in\mathbb{N}} A/\mathfrak{p}^n \ = \ \varprojlim_{n\in\mathbb{N}} A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p}^n$$

le séparé complété de A (ou de $A_\mathfrak{p}$) pour la topologie $\mathfrak{p}$-adique. Pour tout A-module X, on note

$$\widehat{X_\mathfrak{p}} \ := \ X \otimes_A \widehat{A_\mathfrak{p}} \ .$$

Lemme III.3.1.1. *Si C est une A-algèbre telle qu'on ait*

$$A \ \subset \ C \ \subset \ B$$

(on parlera de tour d'anneaux,) alors C est un anneau de dimension 1 (cf. I.1.3.2,) c'est-à-dire que C n'est pas un corps et que tout idéal premier non nul de C est maximal.

Preuve : L'extension $A \subset B$ étant entière, il en est de même des extensions $A \subset C$ et $C \subset B$ (cf. I.4.1.7.) Si donc $\mathfrak{r}$ est un idéal premier de C, il existe un idéal premier $\mathfrak{q}$ de B au-dessus de $\mathfrak{r}$ (cf. I.4.3.2.)

Puisque B est un anneau de Dedekind, $\mathfrak{q}$ est sioit nul soit maximal. Si $\mathfrak{q}$ est nul, $\mathfrak{r}$ l'est aussi. Sinon, il existe un idéal maximal $\mathfrak{r}' \subset C$ contenant $\mathfrak{r}$. Il existe alors un idéal $\mathfrak{q}' \subset B$ relvant $\mathfrak{r}'$ et contenant donc $\mathfrak{q}$. Ce dernier étant maximal, $\mathfrak{q} = \mathfrak{q}'$ d'où il résulte que $\mathfrak{r} = \mathfrak{r}'$. Autrement dit, un idéal premier de C est soit nul soit maximal. On a ainsi établi que la dimension de C est au plus égale à 1.

Or A lui-même n'est pas un corps et possède donc au moins un idéal maximal non nul $\mathfrak{p}$. Il y a alors au moins un idéal maximal non nul $\mathfrak{q}$ de B au-dessus de $\mathfrak{p}$ et

$$\mathfrak{r} = C \cap \mathfrak{q}$$

est un idéal maximal de C non nul puisqu'il contient au moins $\mathfrak{p}$. On a ainsi établi que C est vraiement de dimension 1. *q.e.d*

Définition III.3.1.2. Étant donné un anneau C tel que

$$A \subset C \subset B,$$

pour $\mathfrak{p} \in \mathrm{Spm}(A)$, on dit que C est $\mathfrak{p}$-*clos* si le morphisme naturel $C_{\mathfrak{p}} \to B_{\mathfrak{p}}$ déduit de $C \subset B$ par extension des scalaires est un isomorphisme.

Lemme III.3.1.3. *$C = B$ si et seulement si pour tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$, C est $\mathfrak{p}$-clos si et seulement si pour tout ideal maximal $\mathfrak{m} \in \mathrm{Spm}(A)$, C est $\mathfrak{m}$-clos.*

Preuve : Découle de la proposition III.3.0.6 et du lemme III.3.0.3. *q.e.d*

Proposition III.3.1.4. *Soit une tour d'anneaux*

$$A \subset C \subset B\,.$$

Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, les conditions suivantes sont équivalentes :
a) L'anneau C est $\mathfrak{p}$-clos.
b) Le morphisme naturel $\widehat{C_{\mathfrak{p}}} \to \widehat{B_{\mathfrak{p}}}$ déduit de $C \subset B$ par extension des scalaires est un isomorphisme.

Si de plus on suppose que le corps des fractions $\mathrm{Frac}([C)$ de C est égal à L, les conditions précédentes sont encore équivalentes à :
i) Il existe un entier g tel

$$\widehat{C_{\mathfrak{p}}} = \prod_{i=1}^{g} \mathcal{O}_i$$

où, pour tout $1 \leq i \leq g$, $\mathcal{O}_i$ est l'anneau de la valuation d'un corps complet pour une valuation discrète.
a) L'anneau $C_{\mathfrak{p}}$ est intégralement clos dans L.

Preuve :

i) **(a) éqivaut à (b)** Le sens direct est immédiat.

Réciproquement, si $\widehat{C_\mathfrak{p}} = \widehat{B_\mathfrak{p}}$, $\widehat{B_\mathfrak{p}}/\widehat{C_\mathfrak{p}} = 0$. Or il découle de la proposition III.3.0.8 que

$$\widehat{B_\mathfrak{p}}/\widehat{C_\mathfrak{p}} \cong (B/C) \otimes_A \widehat{A_\mathfrak{p}}$$

puisque b est un A-module de type fini et que A est noethérien. Or

$$(B/C) \otimes_A \widehat{A_\mathfrak{p}} = (B/C)_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A_\mathfrak{p}} .$$

Il résulte du lemme III.3.0.7 puisque $(B/C)_\mathfrak{p}$ est un $A_\mathfrak{p}$-module de type fini et que $A_\mathfrak{p}$ est local noethérien que $(B/C)_\mathfrak{p} = 0$. Enfin par A-platitude de $A_\mathfrak{p}$ on a un isomorphisme naturel de $A_\mathfrak{p}$-modules

$$B_\mathfrak{p}/C_\mathfrak{p} \cong (B/C)_\mathfrak{p}$$

ce qui prouve finalement que $B_\mathfrak{p}/C_\mathfrak{p} = 0$.

ii) **(a) équivaut à (d)** La tour d'anneaux

$$A \subset C \subset B$$

donne encore , puisque $A_\mathfrak{p}$ est A-plat, une tour

$$A_\mathfrak{p} \subset C_\mathfrak{p} \subset B_\mathfrak{p} .$$

Or $B_\mathfrak{p}$ est la fermeture intégrale de $A_\mathfrak{p}$ dans L ce qui établit le résultat.

iii) **(b) équivaut à (c)** Le sens direct n'est rien d'autre que III.2.2.7.ii.

Réciproquement, notons

$$L_i := \mathrm{Frac}(\mathcal{O}_i)\,,_{1\leq i\leq g}$$

le corps des fractions de $\mathcal{O}_i$, $\mathfrak{m}_i$ son idéal maximal et ℓ_i son corps résidueL.

Rappelons que A est noethérien (cf. I.5.2.2,) d'où il résulte que B est un A-module de type fini (cf. I.4.4.2,) et C qui est un sous-A-module de B, également.

Il s'ensuit que $\widehat{C_\mathfrak{p}} = C \otimes_A \widehat{A_\mathfrak{p}}$ est un $\widehat{A_\mathfrak{p}}$-module de type fini et donc que, pour tout $1 \leq i \leq g$, $\mathcal{O}_i$ est aussi un $\widehat{A_\mathfrak{p}}$-module de type fini comme quotient de $\widehat{C_\mathfrak{p}}$. En particulier, si $t_i\,,_{1\leq i\leq g}$ est une uniformisante de $\mathcal{O}_i$, il existe un polynôme unitaire $\chi_i \in \widehat{A_\mathfrak{p}}[X]$ tel que $\chi_i(t_i) = 0$. Si $\chi_{i,0}$ est le coefficient constant de χ_i, il en résulte que $\chi_{i,0} \in \mathfrak{m}_i$ et donc que l'image réciproque de $\mathfrak{m}_i$ dans $\widehat{A_\mathfrak{p}}$ contient au moins $\chi_{i,0} \neq 0$, et n'est donc pas réduite à $\{0\}$.

Or l'image réciproque de $\mathfrak{m}_i$ est un idéal premier, nécessairement non nul, de $\widehat{A_\mathfrak{p}}$. Ce dernier étant un anneau de valuation discrète, c'est nécessairement l'idéal maximal $\mathfrak{p}\widehat{A_\mathfrak{p}}$ de $\widehat{A_\mathfrak{p}}$. On en déduit que le morphisme naturel $\widehat{A_\mathfrak{p}} \to \mathcal{O}_i$ est injectif.

Pour tout $1 \leq i \leq g$, on a donc un diagramme commutatif

$$\begin{array}{ccccccc} A & \hookrightarrow & A_\mathfrak{p} & \hookrightarrow & \widehat{A_\mathfrak{p}} & & \\ \downarrow & & \downarrow & & \downarrow & \searrow & \\ C & \hookrightarrow & C_\mathfrak{p} & \hookrightarrow & \widehat{C_\mathfrak{p}} & \to & \mathcal{O}_i\,. \end{array} \qquad \text{III.3.1.4.1}$$

où l'injectivité des flèches horizontales résulte d'une part de la proposition I.3.2.i (pour le carré de gauche) et d'autre part de III.3.0.7 pour le carré central.

On rappelle qu'on a

$$L_{\mathfrak{p}} \;=\; L \otimes_A \widehat{A_{\mathfrak{p}}}$$

(cf. III.2.2.3.i.) Il en résulte que

$$L_{\mathfrak{p}} \;=\; (\widehat{A_{\mathfrak{p}}} \otimes_A C) \otimes_C l$$

d'après I.2.2.5 c'est-à-dire

$$\begin{array}{rcl} L_{\mathfrak{p}} & = & L \otimes_C \widehat{C_{\mathfrak{p}}} \\ & = & L \otimes_C \prod_{i=1}^{g} \mathcal{O}_i \\ & = & \prod_{i=1}^{g} (L \otimes_C \mathcal{O}_i) \\ & = & \prod_{i=1}^{g} (C \setminus \{0\})^{-1} \mathcal{O}_i \; . \end{array} \qquad \text{III.3.1.4.2}$$

puisque L est par hypothèse le corps des fractions de C.

Il est clair que

$$(C \setminus \{0\})^{-1} \mathcal{O}_i \;\subset\; L_i \; .$$

Notons $\mathfrak{r}_i$ l'image réciproque de $\mathfrak{m}_i$ par le morphisme naturel

$$C \;\longrightarrow\; \widehat{C_{\mathfrak{p}}} \longrightarrow \mathcal{O}_i$$

qui est un idéal premier de C. Il contient $\mathfrak{p}$ en vertu de III.3.1.4.1. Il existe donc un élément non nul $x \in \mathfrak{r}_i$ dont l'image x' est dans $\mathfrak{m}_i \setminus \{0\}$ et est donc inversible dans $(C \setminus \{0\})^{-1}\mathcal{O}_i$. Or $x' \neq 0$ sécrit ut_i^k, où $u \in \mathcal{O}_i^{\times}$ t_i est une uniformisante de $\mathcal{O}_i$ et $k \in \mathbb{N}^*$. Il en résulte que t_i est inversible dans $(C \setminus \{0\})^{-1}\mathcal{O}_i$ et donc que $(C \setminus \{0\})^{-1}\mathcal{O}_i$ contient $\mathcal{O}_i[\frac{1}{t_i}] \;=\; L_i$ (cf. III.2.1.15.)

Il en résulte donc finalement que, pour tout $1 \leq i \leq g$,

$$L \otimes_C \mathcal{O}_i \;=\; L_i \; .$$

Il s'ensuit donc, en vertu de III.3.1.4.2, que

$$L_{\mathfrak{p}} \;=\; \prod_{i=1}^{g} L_i \; .$$

Des arguments exactements analogues à ceux employés dans la preuve du théorème III.2.2.7 [10] permettent alors de montrer que g est exactement le nombre $g_{\mathfrak{p}}$ d'idéaux maximaux $\mathfrak{q}_i$ de B au-dessus de $\mathfrak{p}$ que pour tout $1 \leq j \leq$ gp il existe un unique $1 \leq i \leq g_{\mathfrak{p}}$ tel que

$$L_j \;=\; \widehat{L_{\mathfrak{q}_i}} \; .$$

[10] D'ailleurs il serait bon de dégager un énoncé qui permettrait d'obtenir la preuve du théorème III.2.2.7 et du présent point de manière plus économique et plus claire.

On en déduit alors que

$$\mathcal{O}_i \;=\; \widehat{B_{\mathfrak{q}_i}}$$

et finalement que

$$\widehat{C_{\mathfrak{p}}} \;=\; \widehat{B_{\mathfrak{p}}}\,.$$

q.e.d

Proposition III.3.1.5.
i) Il existe $\alpha \in B$ tel que $L \;=\; K[\alpha]$. On note donc P le polynôme minimal de α si bien que

$$L \;=\; K[X]/P\,,\; P \in A[X] \text{ et } A[\alpha] \;=\; A[X]/P\,.$$

ii) Avec les notations du point précédent, pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, on note

$$k_{\mathfrak{p}} \;:=\; A/\mathfrak{p} \;=\; A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$$

le corps résiduel de A en $\mathfrak{p}$ et $\tilde{P}_{\mathfrak{p}}$ l'image de P dans $k_{\mathfrak{p}}[X]$. Il existe alors un entier $h \in \mathbb{N}^*$, des entiers $\eta_i \in \mathbb{N}^*$ et des polynômes

$$\tilde{P}_{\mathfrak{p},i}\,,1\leq i\leq h \;\in k_{\mathfrak{p}}[X]$$

irréductibles et deux à deux premiers entre eux, tels que

$$\tilde{P}_{\mathfrak{p}} \;=\; \prod_{i=1}^{h} \tilde{P}_{\mathfrak{p},i}^{\eta_i}\,.$$

L'application naturelle

$$\tilde{P}_{\mathfrak{p},i} \;\mapsto\; \mathrm{Ker}\, A[\alpha] \;\to\; k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p},i}$$

induit une bijection de l'ensemble des idéaux maximaux de $A[\alpha]$ au-dessus de $\mathfrak{p}$ dans l'ensemble des $\tilde{P}_{\mathfrak{p},i}\,,1\leq i\leq h}$.
iii) Étant donné un idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, $A[\alpha]$ est $\mathfrak{p}$-clos, si et seulement si l'application

$$\mathfrak{r} \;\mapsto\; \mathfrak{r}B$$

de l'ensemble des idéaux de $A[\alpha]$ dans l'ensemble des idéaux de B induit une bijection de l'ensemble des idéaux maximaux de $A[\alpha]$ au-dessus de $\mathfrak{p}$ dans l'ensemble des idéaux maximaux de B au-dessus de $\mathfrak{p}$ si bien que $h \;=\; g_{\mathfrak{p}}$. De plus, si, pour tout $1 \leq i \leq g_{\mathfrak{p}}$, $e_{\mathfrak{q}_i/\mathfrak{p}}$ est l'indice de ramification (cf. III.1.2.5.i) de l'idéal $\mathfrak{q}_i \in \mathrm{Spm}(B)$ on a

$$e_{\mathfrak{q}_i/\mathfrak{p}} \;=\; \eta_i \text{ et } B/\mathfrak{q}_i \;=\; A[\alpha]/(\mathfrak{q}_i \cap A[\alpha])\,.$$

Preuve :
i) Il existe bien entendu $\beta \in L$ tel que $L \;=\; K[\beta]$ puisque l'extension $K \subset L$ est séparable. En vertu de la proposition I.4.1.10, il existe $a \in A$ tel que $a\beta \;\in B$. Posons donc $\alpha \;:=\; a\beta$.

Il est clair que $L \;=\; K[\alpha]$ et que si $P \in K[X]$ est le polynôme minimal de α, $L \;=\; K[X]/P$.

Par ailleurs, $\alpha \in B$ c'est-à-dire que α est entier sur A ou encore qu'il existe un polynôme unitaire $\chi_\alpha \in A[X]$ tel que $\chi_\alpha(\alpha) = 0$. Il s'ensuit que $P|\chi_\alpha$ dans $K[X]$. Il existe donc $Q \in K[X]$, nécessairement unitaire tel que $\chi_\alpha = PQ$.

Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$, la valuation $\mathfrak{p}$-adique $v_\mathfrak{p}$ sur K induit encore une valuation $v_\mathfrak{p}$ sur $K[X]$ (cf. II.2.1.1.) Puisque P et Q sont unitaires,

$$v_\mathfrak{p}(P) \leq 0 \text{ et } v_\mathfrak{p}(Q) \leq 0 .$$

Puisque $\chi_\alpha \in A[X]$ est unitaire, $v_\mathfrak{p}(\chi_\alpha) = 0$. Enfin $\chi_\alpha = PQ$ entraîne

$$v_\mathfrak{p}(\chi_\alpha) = v_\mathfrak{p}(P) + v_\mathfrak{p}(Q)$$

ce qui entraîne donc que

$$v_\mathfrak{p}(P) = v_\mathfrak{p}(Q) = 0 \; \forall \mathfrak{p} \in \mathrm{Spm}(A)$$

c'est-à-dire que

$$P \in A[X] .$$

Il en résulte immédiatement que

$$A[\alpha] = A[X]/P .$$

ii) Il découle du lemme III.3.1.1, que tous les idéaux premiers de $A[\alpha]$ au-dessus de $\mathfrak{p}$ sont maximaux. Ce sont les idéaux $\mathfrak{q} \in \mathrm{Spm}(A[\alpha])$ tels que $\mathfrak{q} \cap A = \mathfrak{p}$. Ce sont donc encore les idéaux maximaux de $A[\alpha]$ tels que

$$\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset .$$

Ils correspondent donc bijectivement par l'application

$$\mathfrak{q} \mapsto \mathfrak{q}(A[\alpha] \otimes_A A_\mathfrak{p})$$

aux idéaux maximaux de $A[\alpha] \otimes_A A_\mathfrak{p}$ (cf. I.3.2.3.) Comme les idéaux maximaux de $A[\alpha]$ au-dessus de $\mathfrak{p}$ sont exactement ceux qui contiennent $\mathfrak{p}A[\alpha]$, les idéaux maximaux de $A[\alpha] \otimes_A A_\mathfrak{p}$ contiennent tous $\mathfrak{p}(A[\alpha] \otimes_A A_\mathfrak{p})$ si bien qu'ils correspondent bijectivement aux idéaux du quotient

$$\begin{aligned}
(A[\alpha] \otimes_A A_\mathfrak{p})/\mathfrak{p}(A[\alpha] \otimes_A A_\mathfrak{p}) &= (A[\alpha] \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} k_\mathfrak{p} \\
&= A[\alpha] \otimes_A k_\mathfrak{p} \\
&= A[X]/P \otimes_A k_\mathfrak{p} \\
&= k_\mathfrak{p}[X]/\tilde{P}_\mathfrak{p} \\
&= k_\mathfrak{p}[X]/\prod_{i=1}^{h} \tilde{P}_{\mathfrak{p},i}^{\eta_i} \\
&= \prod_{i=1}^{h} k_\mathfrak{p}[X]/\tilde{P}_{\mathfrak{p},i}^{\eta_i} .
\end{aligned}$$

On laisse le soin au lecteur de vérifier que les idéaux maximaux de ce dernier produit sont les noyaux des applications naturelles

$$\prod_{i=1}^{h} k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p},i}^{\eta_i} \longrightarrow k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p},j}^{\eta_j} \longrightarrow k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p},j} \ , \ \forall 1 \leq j \leq h \ .$$

iii)
a) **Dans le sens direct :** Soit $\mathfrak{r} \in \mathrm{Spm}(A[\alpha])$ un idéal maximal au-dessus de $\mathfrak{p}$. L'idéal $B\mathfrak{r} \subset B$ se décompose de manière unique en

$$B\mathfrak{r} = \prod_{i=1}^{\gamma} \mathfrak{q}_i^{\epsilon_i}$$

où les $\mathfrak{q}_i$ sont des idéaux maximaux de B qui sont nécessairement au-dessus de $\mathfrak{p}$. Cette décomposition se conserve par localisation c'est-à-dire que

$$B_{\mathfrak{p}}\mathfrak{r} = \prod_{i=1}^{\gamma} B_{\mathfrak{p}}\mathfrak{q}_i^{\epsilon_i} \ .$$

Or si l'on suppose que $A[\alpha]$ est $\mathfrak{p}$-clos, par définition,

$$A[\alpha] \otimes_A A_{\mathfrak{p}} = B_{\mathfrak{p}}$$

d'où il résulte que

$$\prod_{i=1}^{\gamma} B_{\mathfrak{p}}\mathfrak{q}_i^{\epsilon_i} = B_{\mathfrak{p}}\mathfrak{r} = (A[\alpha] \otimes_A A_{\mathfrak{p}})\mathfrak{r}$$

ce dernier étant maximal (par localisation,) $\gamma = 1$, $\mathfrak{q}_1 = \mathfrak{r}$ et $\epsilon_1 = 1$ ce qui prouve que $B\mathfrak{r}$ est bien un idéal maximal de B au-dessus de $\mathfrak{p}$. On a donc bien construit une application de l'ensemble des idéaux maximaux de $A[\alpha]$ au-dessus de $\mathfrak{p}$ dans l'ensemble des idéaux maximaux de B au-dessus de $\mathfrak{p}$ dont il n'est pas difficile de montrer que l'application

$$\mathfrak{q} \mapsto \mathfrak{q} \cap A[\alpha]$$

est l'inverse. On en déduit donc immédiatement que $h = g_{\mathfrak{p}}$.

Notons

$$k_i := B/\mathfrak{q}_i = B_{\mathfrak{p}}/B_{\mathfrak{p}}\mathfrak{q}_i = A[\alpha]/(\mathfrak{q}_i \cap A[\alpha] = k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p},i} \qquad \text{III.3.1.5.1}$$

la dernière égalité résultant du point précédent.

Pour tout $1 \leq i \leq g_{\mathfrak{p}}$, le noyau $\mathfrak{r}_i$ de la flèche naturelle surjective $A[\alpha] \to ki_i$ est un des idéaux maximaux de $A[\alpha]$ au-dessus de $\mathfrak{p}$. Notons $\mathfrak{q}_i := B\mathfrak{r}_i$ de sorte qu'on a $\mathfrak{q}_i \cap A[\alpha] = \mathfrak{r}_i$. Si l'on suppose que $A[\alpha]$ est $\mathfrak{p}$-clos,

$$\begin{aligned} k_{\mathfrak{p}}[X]/\tilde{P}_{\mathfrak{p}}^{\eta_i} &= A[\alpha]_{\mathfrak{r}_i}/\mathfrak{p} \\ &= A[\alpha]_{\mathfrak{p}_{\mathfrak{r}_i}}/\mathfrak{p} \\ &= B_{\mathfrak{p}_{\mathfrak{q}_i}}/\mathfrak{p} \\ &= k_i^{e_{\mathfrak{q}_i/\mathfrak{p}}} \end{aligned}$$

ce qui permet, grâce à III.3.1.5.1 d'établir que

$$\eta_i \ = \ e_{\mathfrak{q}_i/\mathfrak{p}} \ .$$

b) **Réciproquement :** Pour tout

$$1 \leq i \leq g_{\mathfrak{p}} \text{ et } \forall n \in \mathbb{N},$$

si on note $\mathfrak{q}_i$ l'idéal maximal de B au-dessus de l'idéal maximal $\mathfrak{r}_i$ de $A[\alpha]$, on a un carré commutatif de $A_{\mathfrak{p}}$-algèbres

$$\begin{array}{ccc} A[\alpha]/\mathfrak{p}^n & \rightarrow & B/\mathfrak{p}^n \\ \downarrow & & \downarrow \\ A[\alpha]/\mathfrak{r}_i^n & \xrightarrow{\phi_{n,i}} & B/\mathfrak{q}_i^n \end{array}$$

qui donne par passage à la limite projective un carré commutatif

$$\begin{array}{ccc} A[\alpha] \otimes_A \widehat{A_{\mathfrak{p}}} & \rightarrow & \widehat{B_{\mathfrak{p}}} \\ \downarrow & & \downarrow \\ \widehat{A[\alpha]_{\mathfrak{r}_i}} := \varprojlim_{n\in\mathbb{N}} A[\alpha]/\mathfrak{r}_i^n & & \\ fld\hat{\phi}_i & \widehat{B_{\mathfrak{q}_i}} \ . & \end{array}$$

Si on suppose que $\mathfrak{q}_i \ = \ B\mathfrak{r}_i$, pour tout $n \in \mathbb{N}$, $\mathfrak{q}_i^n \ = \ B\mathfrak{r}_i^n$ d'où il résulte que

$$B/\mathfrak{q}_i^n \ = \ B/\mathfrak{r}_i^n B \ = \ B \otimes_{A[\alpha]} A[\alpha]/\mathfrak{r}_i^n \ .$$

En tant que A-module de type fini, $A[\alpha]$ est un anneau noethérien et B est un $A[\alpha]$-module de type fini si bien que

$$\widehat{B_{\mathfrak{q}_i}} \ = \ B \otimes_{A[\alpha]} \widehat{A[\alpha]_{\mathfrak{r}_i}} \ .$$

Il s'ensuit également que la flèche $\hat{\phi}_i$ est injective.

Le quotient $\widehat{B_{\mathfrak{q}_i}}/\widehat{A[\alpha]_{\mathfrak{r}_i}}$ est un $\widehat{A_{\mathfrak{p}}}$ module de type fini. Or l'égalité $\eta_i \ = \ e_{\mathfrak{q}_i/\mathfrak{p}}$ entraîne que

$$(\widehat{B_{\mathfrak{q}_i}}/\widehat{A[\alpha]_{\mathfrak{r}_i}}) \otimes_{\widehat{A_{\mathfrak{p}}}} k_{\mathfrak{p}} \ = \ 0$$

ce qui entraîne, en vertu du lemme de Nakayama que

$$\widehat{B_{\mathfrak{q}_i}} \ = \ \widehat{A[\alpha]_{\mathfrak{r}_i}} \ \forall 1 \leq i \leq g_{\mathfrak{p}}$$

et achève la preuve.

q.e.d

Exemple III.3.1.6. Soit L l'extension de $\mathbb{Q}$ par une racine α du polynôme $P \ := \ X^2 + 3$. Posons B la fermeture intégrale de $\mathbb{Z}$ dans L et $C \ := \ \mathbb{Z}[\alpha]$. Au-dessus du nombre premier 2,

$\tilde{P} = X^2+1 = (X+1)^2$. L'anneau C n'a donc qu'un idéal maximal $\mathfrak{r}$ au-dessus de 2 et $C/\mathfrak{r} \cong \mathbb{F}_2[X]/(X+1) = \mathbb{F}_2$ et $\eta = 2$. Si v est la valuation 2-adique, comme $v(3)=0$, pour toute racine α de P, $v(\alpha)=0$, d'où $v(1-\alpha)>0$, donc $\beta := \frac{1-\alpha}{2}$ est entier. Reste à montrer que l'anneau des entiers est bien $\mathbb{Z}_2[\beta]$. Autrement dit, C n'est pas 2-clos. On constate qu'alors, β est racine de $Q := X^2+X+1$. Ce polynôme est irréductible dans $\mathbb{F}_2[X]$, par conséquent, le degré résiduel est 2 et l'indice de ramification est 1.

Proposition III.3.1.7. [11]

Soit K un corps local (cf. II.3.2.1,) $\mathcal{O}_K$ l'anneau des entiers, $\mathfrak{m}_K$ l'idéal maximal et k le corps résiduel.

Soit $P \in \mathcal{O}_K[X]$ un polynôme unitaire. Notons $\tilde{P} \in k[X]$ son image dans $k[X]$. S'il existe des polynômes a et b de $k[X]$ premiers entre eux et tels que

$$\tilde{P} = ab,$$

alors il existe des polynômes A et B dans $\mathcal{O}_K[X]$ unitaires, premiers entre eux, relevant respectivement a et b et tels que

$$P = AB\ .$$

On en déduit en particulier que

$$\deg(A) = \deg(a) \text{ et } \deg(B) = \deg(b)\ .$$

Preuve :

i) On notera π une uniformisante de K (cf. II.1.3.4,) pour tout polynôme $T \in \mathcal{O}_K[X]$ on notera $\tilde{T} \in k[X]$ son image dans $k[X]$.

ii) On rappelle qu'étant donnés des polynômes α, β, γ dans $k[X]$, l'ensemble

$$\{(\xi,\eta) \in k[X]\times k[X] \mid \alpha\xi + \beta\eta = \gamma\}$$

est soit vide soit contient un élément $(\xi_i 0, \eta_0)$, et est alors l'ensemble

$$\mathcal{S}_{\alpha,\beta,\gamma} := \{(\xi_0+\beta\zeta, \eta_0-\alpha\zeta)\ ,\ \zeta \in k[X]\}\ . \qquad \text{III.3.1.7.1}$$

Il existe alors au moins un élément

$$(\xi,\eta) \in \mathcal{S}_{\alpha,\beta,\gamma} \mid \deg(\xi) < \deg(\beta) \text{etdeg}(\eta) \leq \max\{\deg(\gamma); \deg(\alpha)+\deg(\beta)-1\} - \deg(\beta)\ . \qquad \text{III.3.1.7.2}$$

iii) Les polynômes a et b étant premiers entre eux, il existe au moins un couple $(u,v) \in k[X] \times k[X]$, tel que $au+bv = 1$. En vertu de III.3.1.7.2, on fixe dans la suite

$$(u,v) \in k[X]\times k[X] \mid au + bv = 1\ ,\ \deg(u) < \deg(b) \text{ et } \deg(v) < \deg(a)\ . \qquad \text{III.3.1.7.3}$$

[11] Cette proposition est une version un peu plus précise de la proposition II.2.2.3 et qui la remplacerait avantageusement puisqu'elle n'utilise aucun résultat ultérieur.

Il résulte immédiatement de l'identité $au + bv \ = \ 1$

$$\deg(a) \ + \ \deg(u) \ = \ \deg(b) \ + \ \deg(v) \ . \qquad \text{III.3.1.7.4}$$

iv) On cherche à construire des suites

$$(A_n)_{n\in\mathbb{N}^*} \ , \ (B_n)_{n\in\mathbb{N}^*} \ , \ (U_n)_{n\in\mathbb{N}^*} \text{ et } (V_n)_{n\in\mathbb{N}^*}$$

vérifiant pour tout $n \in \mathbb{N}^*$ les conditions

C_1 Les polynômes A_n et B_n sont unitaires,

$$A_n \ \equiv \ a \ [\mathfrak{m}_K] \ , \ \deg(A_n) \ = \ \deg(a) \ , \ B_n \ \equiv \ b \ [\mathfrak{m}_K] \text{ et } \deg(B_n) \ = \ \deg(b) \ .$$

C_2

$$P - A_nB_n \ \equiv \ 0 \ [\mathfrak{m}_K^n] \ .$$

C_3

$$U_n \ \equiv \ u \ [\mathfrak{m}_K] \ , \ \deg(U_n) \ < \ \deg(b) \ , \ V_n \ \equiv \ v \ [\mathfrak{m}_K] \text{ et } \deg(V_n) \ < \ \deg(a) \ .$$

C_4

$$A_nU_n + B_nV_n \ \equiv \ 1 \ [\mathfrak{m}_K^n] \ .$$

Pour tout $n \geq 2$,

C_5

$$\begin{aligned} A_n &\equiv A_{n-1} \ [\mathfrak{m}_K^{n-1}] \\ B_n &\equiv B_{n-1} \ [\mathfrak{m}_K^{n-1}] \\ U_n &\equiv U_{n-1} \ [\mathfrak{m}_K^{n-1}] \\ V_n &\equiv V_{n-1} \ [\mathfrak{m}_K^{n-1}] \ . \end{aligned}$$

v) Notons A_1 (resp. B_1) un relèvement unitaire de a (resp. b) de même degré et U_1 (resp. V_1) un relèvement de u (resp. v) de même degré. Il est clair dès lors que le quadruplet (A_1, B_1, U_1, V_1) satisfait aux conditions III.3.1.7(C_1) à III.3.1.7(C_4).

vi) Pour $s \in \mathbb{N}^*$ supposons donnés pour tout $1 \leq n \leq s$ des quadruplets $(A_n, B_n, U_n, V_n) \in \mathcal{O}_K[X]^4$, vérifiant les conditions III.3.1.7(C_1) à III.3.1.7(C_4) et pour tout $2 \leq n \leq s$, la condition III.3.1.7(C_5).

vii) Il existe un polynôme $S_s \in \mathcal{O}_K[X]$ tel que

$$P - A_sB_s \ = \ \pi^s S_s \ .$$

Puisque A_s et B_s sont unitaires, $\deg(S_s) < \deg(a) + \deg(b)$. Il existe donc $(u', v') \in k[X]^2$ tel que

$$au' + bv' \ = \ \tilde{S}_s \ , \ \deg(u') \ < \ \deg(b) \text{ et } \deg(v') \ < \ \deg(a)$$

(cf. III.3.1.7.2.) Notons alors U' (resp. V') un relèvement de u' (resp. v') de même degré et posons

$$A_{s+1} \ := \ A_s + \pi^s V' \text{ et } B_{s+1} \ := \ B_s + \pi^s U' \ .$$

Il vient alors

$$\deg(A_{s+1}) \ = \ \deg(A_s) \ = \ \deg(a) \text{ et } \deg(B_{s+1}) \ = \ \deg(B_s) \ = \ \deg(b) \ . \qquad \text{III.3.1.7.5}$$

En outre

$$\begin{array}{rcl} P - A_{s+1}B_{s+1} & = & P - A_sB_s - \pi^s(A_sU' + B_sV') - \pi^{2s}U'V' \\ & = & \pi^s(S_s - A_sU' - Bs'_V) - \pi^{2s}U'V' \\ & \equiv & 0 \ [\mathfrak{m}_K^{s+1}] \ . \end{array} \qquad \text{III.3.1.7.6}$$

viii) Il existe un polynôme $T_s \in \mathcal{O}_K[X]$ tel que

$$1 - A_{s+1}U_s - B_{s+1}V_s \ = \ \pi^s T_s \ .$$

En effet, par construction même de A_{s+1} et B_{s+1},

$$1 - A_{s+1}U_s - B_{s+1}V_s \ \equiv \ 1 - A_sU_s - B_sV_s \ [\mathfrak{m}_K^s] \ .$$

De plus, $\deg(T_s) \ < \ \deg(a) + \deg(b)$. Il existe donc $(u'', v'') \in k[X]^2$ tel que

$$au'' + bv'' \ = \ \tilde{T_s} \ , \ \deg(u'') \ < \ \deg(b) \text{ et } \deg(v'') \ < \ \deg(a)$$

(cf. III.3.1.7.2.) Notons U'' (resp. V'') un relèvement de u'' (resp. v'') de même degré dans $\mathcal{O}_K[X]$ et posons

$$U_{s+1} \ := \ U_s + \pi^s U'' \text{ et } V_{s+1} \ := \ V_s + \pi^s V'' \ .$$

Il vient alors

$$\deg(U_{s+1}) \ < \ \deg(b) \text{ et } \deg(V_{s+1}) \ < \ \deg(a) \ . \qquad \text{III.3.1.7.7}$$

En outre

$$\begin{array}{rcl} 1 - A_{s+1}U_{s+1} - B_{s+1}V_{s+1} & = & 1 - A_{s+1}U_s - B_{s+1}V_s - \pi^s(A_{s+1}U'' + B_{s+1}V'') \\ & = & \pi^s(T_s - A_{s+1}U'' - B_{s+1}V'') \\ & \equiv & 0 \ [\mathfrak{m}_K^{s+1}] \ . \end{array} \qquad \text{III.3.1.7.8}$$

ix) On a donc construit par récurrence les suites

$$(A_n)_{n\in\mathbb{N}^*} \ , \ (B_n)_{n\in\mathbb{N}^*} \ , \ (U_n)_{n\in\mathbb{N}^*} \text{ et } (V_n)_{n\in\mathbb{N}^*}$$

satisfaisant les conditions III.3.1.7(C_1) à III.3.1.7(C_5)
(cf. III.3.1.7.5, III.3.1.7.6, III.3.1.7.7, III.3.1.7.8.)

La condition III.3.1.7(C_5) entraîne que ces quatre suites sont de Cauchy. Puisque par ailleurs ce sont des suites de polynômes dont le degré est borné indépendamment de $n \in \mathbb{N}^*$, et que $\mathcal{O}_K$ est $\mathfrak{m}_K$-adiquement complet, elles convergent vers des limites respectives A, B, U et V qui sont des éléments de $\mathcal{O}_K[X]$. La condition III.3.1.7(C_2) entraîne que

$$P - AB \ = \ 0$$

et la condition III.3.1.7(C_4) que

$$AU \ + \ BV \ = \ 1$$

ce qui achève la preuve.

q.e.d

Théorème III.3.1.8. *Soit $\alpha \in B$ tel que $L \ = \ K[\alpha]$ et $P \in A[X]$ le polynôme minimal de α. Étant donné un idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, $k_\mathfrak{p} \ := \ A/\mathfrak{p}$ le corps résiduel de A en $\mathfrak{p}$, si l'image $\tilde{P}_\mathfrak{p}$ de P dans $k_\mathfrak{p}[X]$ est séparable, alors l'anneau $A[\alpha]$ est $\mathfrak{p}$-clos et pour tout idéal $\mathfrak{q}$ de B au-dessus de $\mathfrak{p}$,*

$$e_{\mathfrak{q}/\mathfrak{p}} \ = \ 1$$

c'est-à-dire que $\mathfrak{q}$ est non ramifié.

Preuve :

i) Notons $P_\mathfrak{p}$ l'image de P dans $\widehat{A_\mathfrak{p}}[X]$. Le polynôme $\tilde{P}_\mathfrak{p}$ peut être vue aussibien comme la réduction modulo $\mathfrak{p}$ de P que comme la réduction modulo $\mathfrak{p}\widehat{A_\mathfrak{p}}$ de $P_\mathfrak{p}$.

ii) Si $\tilde{P}_\mathfrak{p}$ est séparable, il existe des polynômes

$$\tilde{P}_{\mathfrak{p},i}\ ,1\leq i\leq h \ \in \ k_\mathfrak{p}[X]$$

irréductibles, deux à deux premiers entre eux et tels que

$$\tilde{P}_\mathfrak{p} \ = \ \prod_{i=1}^{h} \tilde{P}_{\mathfrak{p},i} \ .$$

En vertu de la proposition III.3.1.7, il existe donc des polynômes

$$P_{\mathfrak{p},i}\ ,1\leq i\leq h \ \in \ \widehat{A_\mathfrak{p}}[X]$$

unitaires, deux à deux premiers entre eux, tels que pour tout $1 \leq i \leq h$, $P_{\mathfrak{p},i}$ relève $\tilde{P}_{\mathfrak{p},i}$, ce qui entraîne en particulier que $P_{\mathfrak{p},i}$ est irréductible, et

$$P_\mathfrak{p} \ = \ \prod_{i=1}^{h} P_{\mathfrak{p},i} \ .$$

iii) Pour tout $1 \leq i \leq h$, notons alors

$$L_i \ := \ K_\mathfrak{p}[X]/P_{\mathfrak{p},i}$$

(où $K_\mathfrak{p}$ est le complété $\mathfrak{p}$-adique de K.) Alors pour tout $1 \leq i \leq h$, L_i est un corps local (cf. II.3.1.2) dont on note $\mathcal{O}_i$ l'anneau des entiers *i.e.*la fermeture intégrale de $\widehat{A_\mathfrak{p}}$ dans L_i. L'inclusion naturelle $\widehat{A_\mathfrak{p}} \hookrightarrow K_\mathfrak{p}$ donne une inclusion naturelle

$$\widehat{A_\mathfrak{p}}[X]/P_{\mathfrak{p},i} \hookrightarrow L_i \ , \ \forall 1 \leq i \leq h \ .$$

Elle se factorise en fait en une inclusion

$$\widehat{A_\mathfrak{p}}[X]/P_{\mathfrak{p},i} \hookrightarrow \mathcal{O}_i \ \forall 1 \leq i \leq j \ .$$

Comme on a affaire à une inclusion de $\widehat{A_\mathfrak{p}}$-modules libres, on en déduit une inclusion

$$k_\mathfrak{p}[X]/\tilde{P}_{\mathfrak{p},i} = \widehat{A_\mathfrak{p}}[X].P_{\mathfrak{p},i} \otimes_{\widehat{A_\mathfrak{p}}} k_\mathfrak{p} \hookrightarrow \mathcal{O}_i/\mathfrak{p}\mathcal{O}_i = \mathcal{O}_i \otimes_{\widehat{A_\mathfrak{p}}} k_\mathfrak{p} \ \forall 1 \leq i \leq h \ .$$

Or $\mathfrak{p}\mathcal{O}_i \subset \mathfrak{m}_{\mathcal{O}_i}$ d'où il résulte un morphisme surjectif de $k_\mathfrak{p}$-espaces vectoriels

$$\mathcal{O}_i/\mathfrak{m}_{\mathcal{O}_i} \to \mathcal{O}_i/\mathfrak{p}\mathcal{O}_i \ .$$

On en déduit alors

$$\begin{aligned} f_{L_i/K_\mathfrak{p}} &= \dim_{k_\mathfrak{p}} \mathcal{O}_i/\mathfrak{m}_{\mathcal{O}_i} \\ &\geq \dim_{k_\mathfrak{p}} \mathcal{O}_i/\mathfrak{p}\mathcal{O}_i \\ &\geq \dim_{k_\mathfrak{p}} k_\mathfrak{p}[X]/\tilde{P}_{\mathfrak{p},i} \\ &= \deg(\tilde{P}_{\mathfrak{p},i}) \\ &= \deg(P_{\mathfrak{p},i}) \\ &= [L_i : K_\mathfrak{p}] \ . \end{aligned}$$

Comme par ailleurs on a $f_{L_i/K_\mathfrak{p}} \leq [L_i : K_\mathfrak{p}]$, les inégalités ci-dessus sont toutes des égalités et il en résulte que

$$[L_i : K_\mathfrak{p}] = f_{L_i/K_\mathfrak{p}} \ \forall 1 \leq i \leq h$$

c'est-à-dire que les extensions $K_\mathfrak{p} \subset L_i$ sont non ramifiées. Il résulte alors de la proposition II.3.3.1, [12] que

$$\mathcal{O}_i = \widehat{A_\mathfrak{p}}[X]/P_{\mathfrak{p},i} \ \forall 1 \leq i \leq h \ .$$

iv) On a enfin

$$\begin{aligned} A[\alpha] \otimes_A \widehat{A_\mathfrak{p}} &= A[X]/P \otimes_A \widehat{A_\mathfrak{p}} \\ &= \widehat{A_\mathfrak{p}}[X]/P_\mathfrak{p} \\ &= \prod_{i=1}^{h} \widehat{A_\mathfrak{p}}[X]/P_{\mathfrak{p},i} \\ &= \prod_{i=1}^{h} \mathcal{O}_i \end{aligned}$$

[12] Ou malheureusement plutôt de la preuve de cette proposition ; l'énoncé de la proposition n'étant pas optimal et la preuve donnant plus que ce qui est annoncé. On pourrait en effet donner un résultat plus fort : Pour tout générateur a de l etc ...

ce qui permet de conclure, en vertu de l'équivalence entre III.3.1.4.a et III.3.1.4.i que $A[\alpha]$ est $\mathfrak{p}$-clos.

il suffit finalement d'utiliser le théorème III.2.2.7.iv pour déduire du fait que $K_{\mathfrak{p}} \subset L_i$ est non ramifiée que les idéaux au-dessus de $\mathfrak{p}$ sont non ramifiés.

q.e.d

Corollaire III.3.1.9. *Avec les notations du théorème III.3.1.8, l'anneau $A[\alpha]$ est $\mathfrak{p}$-clos sauf en un nombre fini d'idéaux maximaux de A. En particulier il n'y a qu'un nombre fini d'idéaux maximaux de A qui sont ramifiés.*

Preuve : Le polynôme P étant séparable, il existe des éléments U_0 et V_0 de $K[X]$ tels que $U_0P + V_0P' = 1$. Il existe donc $s \in A$ tel que $U := sU_0$ et $V := sV_0$ sont dans $A[X]$ et l'on a $UP + VP' = s$.

Pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$ tel que $v_{\mathfrak{p}}(s) = 0$, $\tilde{P}$ est séparable et, d'après le théorème III.3.1.8, $A[\alpha]$ est $\mathfrak{p}$-clos et les idéaux au-dessus de $\mathfrak{p}$ sont tous non-ramifiés.

Or les $\mathfrak{p} \in \mathrm{Spm}(A)$ tels que $v_{\mathfrak{p}}(s) > 0$ sont en nombre fini ; c'est-à-dire les idéaux $\mathfrak{p}$ ramifiés sont en nombre fini. *q.e.d*

III.3.2 . −Discriminants, différente

Lemme III.3.2.1. *Soit*

$$E \subset F \subset \Omega$$

une tour d'extensions où $E \subset F$ est finie séparable de degré d et $E \subset \Omega$ est galoisienne. On note

$$\sigma_i : F \to \Omega\,, 1 \leq i \leq d$$

d plongements distincts.

i) L'application

$$\mathrm{Tr}_{F/E}\, x \mapsto \sum_{i=1}^{d} \sigma_i(x)\ \forall x \in F$$

est une application E-linéaire à valeurs dans E et indépendante de l'extension galoisienne $E \subset \Omega$ contenant F. Pour tout $x \in E$, $\mathrm{Tr}_{F/E}(x) = d \cdot x$.

ii) L'application

$$\mathrm{N}_{F/E})\, x \mapsto \prod_{i=1}^{d} \sigma_i(x)\ \forall x \in F$$

est à valeurs dans E et indépendante de l'extension galoisienne $E \subset \Omega$ contenant F. Pour tout $x \in E$, $\mathrm{N}_{F/E}(x) = x^d$. Si

$$E \subset F \subset G$$

est une tour d'extensions séparables,

$$\mathrm{N}_{G/E}) = \mathrm{N}_{F/E}) \circ \mathrm{N}_{G/F})\,.$$

iii) L'application

$$(x,y) \ \mapsto \ \mathrm{Tr}_{F/E}(xy) \, \forall \, (x,y) \ \in \ F \times F \qquad \textit{III.3.2.1.1}$$

est une forme bilinéaire symétrique non dégénérée sur F à valeurs dans E.

iv) Étant donnée une famille

$$m_{ij} \, , 1 \leq i \leq d \, , \, 1 \leq j \leq d \ \in \ F$$

d'éléments de F, on notera abusivement $\det(m_{ij})$ le déterminant de la matrice carré à d lignes et d colonnes de terme général m_{ij}.

Pour tous d-uplets

$$u_i \, , 1 \leq i \leq d \ \in \ F \text{ et } v_i \, , 1 \leq i \leq d \ \in \ F$$

d'éléments de F et tout $x \in F$, on a

$$\det(\mathrm{Tr}_{F/E}(xu_iv_j)) \ = \ \mathrm{N}_{F/E}(x)\det(\sigma_i(u_j))\det(\sigma_i(v_j)) \ = \ \mathrm{N}_{F/E}(x)\det(\mathrm{Tr}_{F/E}(u_iv_j)) \qquad \textit{III.3.2.1.2}$$

et

$$\forall \, g \ \in \ \mathrm{Gal}_{\Omega/E} \, , \ g\det(\sigma_j(u_i)) \ = \ \det(\sigma_i(g(u_j))) \ = \ \pm\det(\sigma_i(u_j)) \, . \qquad \textit{III.3.2.1.3}$$

v) L'application $\delta_{F/E}$ qui à tout d-uplet

$$u_i \, , 1 \leq i \leq d \ \in \ F$$

d'éléments de F associe

$$\delta_{F/E}(u_1, \ldots, u_d) \ := \ \det(\sigma_i(u_j))^2 \ = \ \det(\mathrm{Tr}_{F/E}(u_iu_j))$$

définie sur F^d est à valeurs dans E et est définie indépendamment de l'extension galoisienne $E \subset \Omega$ contenant F.

De plus on a

$$\forall \alpha \in F \ , \ \delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1}) \ = \ \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \ = \ (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} \sigma_i(\alpha) - \sigma_j(\alpha) \, . \qquad \textit{III.3.2.1.4}$$

Si $F \ = \ E[\alpha]$ et si P est le polynôme minimal de α,

$$\delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1}) \ = \ (-1)^{\frac{d(d-1)}{2}} \mathrm{N}_{L/K}(P'(\alpha)) \, . \qquad \textit{III.3.2.1.5}$$

En particulier, comme P est séparable, $\delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1}) \ \neq \ 0$.

Enfin, pour tout autre racine β de P,

$$\delta_{F/E}(1, \beta, \ldots, \beta^{d-1}) \ = \ \delta_{1, \alpha, \ldots, \alpha^{d-1}/}() \, .$$

vi) Étant donnés des d-uplets

$$(f_1, \ldots, f_d) \text{ et } (f'_1, \ldots, f'_d)$$

de F et des éléments

$$p_{ij}\ ,1\leq i\leq d\ ,\ 1\leq j\leq d\ \in\ E,$$

tels que pour tout $1 \leq i \leq d$, $f'_i \ = \ \sum_{j=1}^{d} p_{ij} f_j$ *alors*

$$\delta_{F/E}(f'_1, \ldots, f'_d) \ = \ \det(p_{ij})^2 \delta_{F/E}(f_1, \ldots, f_d)\ .$$

Pour tout d-uplet $(f_1, \ldots, f_d)$ d'éléments de F, $\delta_{F/E}(f_1, \ldots, f_d) \ \neq \ 0$ si et seulement si $(f_1, \ldots, f_d)$ est une E-base de F.

vii) Étant donnée une E-base $(f_1, \ldots, f_d)$ de F, la classe de $\delta_{F/E}(f_1, \ldots, f_d)$ dans le quotient $E^\times/(E^\times, 2)$ est indépendante de la base choisie.

On suppose que la caractéristique de E est différente de 2, on choisit α tel que $F \ = \ E(\alpha)$, on note P le polynôme minimal de α et Ω un corps de décomposition de P contenant F. L'extension $E \subset \Omega$ est galoisienne et l'on note $\rho \ : \ \mathrm{Gal}_{\Omega/E} \ \to \ \mathcal{S}_d$ l'homomorphisme naturel injectif donné par l'action du groupe des permutations sur les racines de P. Par composition avec la signature on définit un morphisme $\epsilon \ : \ \mathrm{Gal}_{\Omega/E} \ \to \ \{-1; 1\}$

- *Soit $\delta_{F/E}(\alpha)$ est un carré dans $E^\times$ et $\rho(\mathrm{Gal}_{\Omega/E}) \ \subset \ \mathcal{A}_d$;*
- *soit ϵ à valeurs dans $\{-1; 1\}$ est surjective de noyau H qui est un sous-groupe invariant d'indice 2 de $\mathrm{Gal}_{\Omega/E}$. Le corps F_H fixe par H est une extension de degré 2 de E de groupe de Galois $\mathrm{Gal}_{E/K}/H$. On a en fait $F_H \ = \ K[\beta]$ où $\beta^2 = \delta_{F/E}(\alpha)$.*

Preuve :

i) C'est un résultat de théorie de Galois bien connu.

ii) Idem.

iii) C'est une conséquence du lemme d'indépendance des caractères (cf. I.4.4.6.)

iv)

$$\begin{aligned}
\det(\mathrm{Tr}_{F/E}(xu_iv_j)) &= \det(\sum_{k=1}^{d} \sigma_k(xu_iv_j)) \\
&= \det(\sum_{k=1}^{d} \sigma_k(xu_i)\sigma_k(v_j)) \\
&= \det(\sigma_i(xu_j))\det(\sigma_i(v_j)) \\
&= \mathrm{N}_{F/E}(x)\det(\sigma_i(u_j))\det(\sigma_i(v_j)) \\
&= \mathrm{N}_{F/E}(x)\det(\mathrm{Tr}_{F/E}(u_iv_j))\ .
\end{aligned}$$

v)

- Le fait que $\delta_{F/E}$ soit bien définie et à valeurs dans E est une conséquence immédiate du point III.3.2.1.iv.
- La formule III.3.2.1.4 est un résultat bien connu sur les déterminants.

– Dans Ω P s'écrit

$$P \ = \ \prod_{i=1}^{d} X - \sigma_i(\alpha) \ .$$

D'où

$$P' \ = \ \sum_{i=1}^{d} \prod_{\tau \neq \sigma_i} X - \tau(\alpha) \ .$$

On peut supposer que $\sigma_1(\alpha) = \alpha$ d'où

$$P'(\alpha) \ = \ \prod_{j=2}^{d} (\alpha - \sigma_j(\alpha)) \ .$$

Comme $P'(\alpha) \in F$, on peut calculer

$$\begin{aligned}
\mathrm{N}_{L/K}(P'(\alpha)) &= \prod_{i=1}^{d} \prod_{j=2}^{d} \sigma_i(\alpha - \sigma_j(\alpha)) \\
&= \prod_{i=1}^{d} \prod_{j=2}^{d} \sigma_i(\alpha) - \sigma_i\sigma_j(\alpha) \\
&= \prod_{i=1}^{d} \prod_{j \neq i} \sigma_i(\alpha) - \sigma_j(\alpha) \\
&= \prod_{i=1}^{d} \prod_{j<i} \sigma_i(\alpha) - \sigma_j(\alpha) \prod_{j>i} \sigma_i(\alpha) - \sigma_j(\alpha) \\
&= (-1)^{\frac{d(d-1)}{2}} \delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1}) \ .
\end{aligned}$$

vi) Il suffit de remarquer pour cela, que, les p_{ij} étant des éléments de E, on a encore, pour tout E-plongement σ $f_i' \ = \ \sum_{j=1}^{d} p_{ij}\sigma(f_j)$.

vii) Notons $\beta \ := \ \det(\sigma_i(\alpha^{j-1}))$ et

$$a \ := \ \beta^2 \ = \ \delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1}) \ .$$

Alors pour tout $\gamma \in \mathrm{Gal}_{\Omega/E}$,

$$\gamma(\beta) \ = \ \epsilon(\gamma)\beta \ .$$

Si E n'est pas de caractéristique 2, on peut avoir, a priori, $\epsilon(\gamma) \neq 1 \in \Omega$.

Si $\mathrm{Im}\,\rho \subset \mathcal{A}_d$ pour tout $\gamma \in \mathrm{Gal}_{\Omega/E}$, $\gamma(\beta) = \beta$ et par conséquent, $\beta \in E$. Sinon, il existe γ tel que $\gamma(\beta) = -\beta$ et dans ce cas, $\beta \notin E$.

q.e.d

Définition III.3.2.2.
i) L'application

$$\mathrm{Tr}_{F/E} \ : \ F \ \to \ E$$

sera appelée *trace*.

ii) La forme bilinéaire III.3.2.1.1 sera appelée *forme trace*.

iii) L'application

$$\mathrm{N}_{F/E}) \ : \ F \ \to \ E$$

sera appelée *norme*.

iv) Pour tout d-uplet $(u_1, \ldots, u_d) \in F^d$ d'éléments de F, on appellera *discriminant du système* $(u_1, \ldots, u_d)$ l'élément $\delta_{F/E}(u_1 \ldots, u_d) \in E$ de E.

Pour tout $\alpha \in F$, on notera parfois simplement

$$\delta_{F/E}(\alpha) \ := \ \delta_{F/E}(1, \alpha, \ldots, \alpha^{d-1})$$

qu'on appellera *discriminant de* α.

Enfin si $F \ = \ E[X]/P$ où P est un polynôme irréductible séparable de degré d, il résulte de III.3.2.1.v, que

$$\delta_{F/E}(\alpha) \ = \ \mathrm{N}_{F/E}(P'(\alpha))$$

est indépendant de la racine α de P choisie si bien que c'est un invariant associé au polynôme P qu'on notera $\delta_{F/E}(P)$ et qu'on appellera *discriminant du polynôme* P.

Définition III.3.2.3. Résultant Soient A un anneau commutatif, m et n deux entiers positifs. Pour tout couple

$$\begin{pmatrix} P & := & \sum_{i=0}^{m} a_i X^i, \\ Q & := & \sum_{i=0}^{n} b_i X^i \end{pmatrix}$$

d'éléments de $A[X]$, on note $\mathrm{Res}_{m,n}(P, Q)$ le déterminant de la matrice à $m+n$ lignes et $m+n$ colonnes

$$\begin{pmatrix} a_m & a_{m-1} & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & a_m & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 & 0 \\ & & & & \ldots & & & & & \\ 0 & 0 & \ldots & a_m & a_{m-1} & \ldots & & \ldots & a_1 & a_0 \\ b_n & b_{n-1} & \ldots & b_1 & b_0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & b_n & \ldots & b_2 & b_1 & b_0 & 0 & \ldots & 0 & 0 \\ & & & & \ldots & & & & & \\ 0 & 0 & \ldots & b_n & b_{n-1} & \ldots & & \ldots & b_1 & b_0 \end{pmatrix}$$

Si $a_m = 0$ ou $b_n = 0$, $\mathrm{Res}_{m,n}(P, Q) = 0$. Si $a_m \neq 0$ et $b_n \neq 0$ on note

$$\mathrm{Res}(P, Q) \ := \ \mathrm{Res}_{m,n}(P, Q)$$

qu'on appelle *résultant des polynômes* P et Q.

Lemme III.3.2.4. *Soient A un anneau, m et n des entiers positifs, P et Q des éléments de $A[x]$ tels que $\deg(P) \leq m$ et $\deg(Q) \leq n$.*
i) Si $\mathfrak{J}$ est l'idéal de $A[X]$ engendré par P et Q,

$$\mathrm{Res}_{m,n}(P,Q) \ \in \ A \cap \mathfrak{J} \ .$$

Si A est un corps et si P est de degré m et Q de degré n, $\mathrm{Res}(P,Q)$ est non nul si et seulement si P et Q sont premiers entre eux.

ii) S'il existe des éléments

$$\alpha_{i\ ,1\leq i\leq m} \ \in \ A$$

de A tels que

$$P \ = \ a_m \prod_{i=1}^{m} (X-\alpha_i),$$

alors

$$\mathrm{Res}_{m,n}(P,Q) \ = \ a_m^n \prod_{i=1}^{m} Q(\alpha_i) \ .$$

iii) S'il existe des éléments

$$\beta_{i\ ,1\leq i\leq n} \in A$$

de A tels que

$$Q \ = \ b_n \prod_{i=1}^{n} (X-\beta_i),$$

alors

$$\mathrm{Res}_{m,n}(P,Q) \ = \ (-1)^{mn} b_n^m \prod_{i=1}^{n} P(\beta_j) \ .$$

iv) Si les hypothèses de III.3.2.4.ii et III.3.2.4.iii sont simultanément satisfaites, alors

$$\mathrm{Res}_{m,n}(P,Q) \ = \ a_m^n . b_n^m . \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) \ .$$

Proposition III.3.2.5. *Soient A un anneau intègre et*

$$P \ := \ a_m X^m + a_{m-1} X^{m-1} + \cdots + a_i X^i + \cdots + a_1 X + a_0 \ \in \ A[X]$$

un polynôme de degré $m \geq 2$.
i) Il existe un unique $\delta \in A$ tel que

$$\mathrm{Res}_{m,m-1}(P,P') \ = \ (-1)^{m(m-1)/2} . a_m . \delta \ .$$

ii) Si E est un corps contenant A dans lequel P peut s'écrire

$$P \ = \ a_m(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_m),$$

on a

$$\delta \ = \ (-1)^{m(m-1)/2}.a_m^{2m-2}.\prod_{i\neq j}(\alpha_i-\alpha_j)\ .$$

En particulier, $\delta \neq 0$ si et seulement si P est séparable.

iii) Si P est unitaire,

$$\mathrm{Res}_{m,m-1}(P,P') \ = \ \delta_/(P)\ .$$

iv) Soient K un corps, m,n deux entiers ≥ 1, $P,Q \in K[X]$ des polynômes de degrés m et n respectivement. Alors

$$\delta_/(PQ) \ = \ (\mathrm{Res}(P,Q))^2.\delta_/(P).\delta_/(Q)\ .$$

Dans la suite de cette section (III.3.2,) A est un anneau de Dedekind, K son corps des fractions, $K \subset L$ une extension finie séparable de degré d de K et B la fermeture intégrale de A dans L.

On note $\mathcal{I}(A)$ (resp. $\mathcal{I}(B)$) le groupe des idéaux fractionnaires de A (resp. B) (cf. III.1.1.11.)

Par ailleurs on fixe une extension galoisienne $K \subset \Omega$ contenant L et

$$\sigma_i \ : \ L \ \to \ \Omega\ ,1\leq i\leq d$$

des K-plongements deux à deux distincts.

Lemme III.3.2.6.

i) L'application

$$\nu_{\ /:(\ )}\mathcal{I}(A) \ \to \ \mathcal{I}(B)\ ,\ \mathfrak{I} \mapsto B\mathfrak{I}$$

est un morphisme de groupes injectif.

ii) Il existe un unique homomorphisme de groupes

$$\mathcal{I}(B) \ \to \ \mathcal{I}(A)\ ,\ \mathfrak{q} \ \mapsto \ (\mathfrak{q}\cap A)^{f_{\mathfrak{q}/(\mathfrak{q}\cap A)}}\ \forall \mathfrak{q} \in \mathrm{Spm}(B)$$

où $f_{\mathfrak{q}/(\mathfrak{q}\cap A)}$ est le degré résiduel défini en III.1.2.5.

Preuve :

i) Le fait que $\nu_{L/K}$ soit un morphisme est immédiat et le fait qu'il est injectif est laissé en exercice.

ii) Il suffit de se rappeler ici que $\mathcal{I}(B)$ est un $\mathbb{Z}$-module libre de base $\mathrm{Spm}(B)$ (cf. III.1.1.11.)

q.e.d

Définition III.3.2.7. Norme On appelle *norme* l'application définie ci-dessus qu'on note

$$\mathrm{N}_{L/K)}\ :\ \mathcal{I}(B) \ \to \ \mathcal{I}(A)\ .$$

Proposition III.3.2.8. Propriétés de la norme
i) Pour tout $\mathfrak{I} \in \mathcal{I}(A)$, idéal fractionnaire de A,

$$\mathrm{N}_{L/K}(\nu_{L/K}(\mathfrak{I})) \;=\; \mathfrak{I}^{[L:K]} \;=\; \mathfrak{I}^d \,. \qquad \textit{III.3.2.8.1}$$

ii) Si S est une partie multiplicative de A ne contenant pas 0, les applications $\nu_{L/K}$ et $\mathrm{N}_{L/K}$) commutent à la localisation c'est-à-dire que les applications

$$\nu_{/:}(\,)\mathcal{I}(S^{-1}A) \;\to\; \mathcal{I}(S^{-1}B) \text{ et } \mathrm{N}_{L/K}) \;:\; \mathcal{I}(S^{-1}B) \;\to\; \mathcal{I}(S^{-1}A)$$

sont bien définies et que

$$\nu_{L/K}(S^{-1}\mathfrak{J}) \;=\; S^{-1}\nu_{L/K}(\mathfrak{J}) \,\forall\, \mathfrak{J} \;\in\; \mathcal{I}(B) \qquad \textit{III.3.2.8.2}$$

et

$$\mathrm{N}_{L/K}(S^{-1}\mathfrak{J}) \;=\; S^{-1}\mathrm{N}_{L/K}(\mathfrak{J}) \,\forall\, \mathfrak{J} \;\in\; \mathcal{I}(A) \,. \qquad \textit{III.3.2.8.3}$$

iii) Soit M une extension finie séparable de L, C la fermeture intégrale de A ou B dans M. Pour tout idéal fractionnaire $\mathfrak{K} \in \mathcal{I}(C)$ de C,

$$\mathrm{N}_{M/K}(\mathfrak{K}) \;=\; \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathfrak{K})) \,. \qquad \textit{III.3.2.8.4}$$

iv) Si L/K est une extension galoisienne, pour tout idéal fractionnaire $\mathfrak{J} \in \mathcal{I}(B)$ de B,

$$\prod_{\sigma \in \mathrm{Gal}_{L/K}} \sigma(\mathfrak{J}) \;=\; \nu_{L/K}(\mathrm{N}_{L/K}(\mathfrak{J})) \,. \qquad \textit{III.3.2.8.5}$$

v) On ne suppose plus que L/K soit galoisienne,mais simplement finie séparable. Pour tout $b \in L$ non nul,

$$\mathrm{N}_{L/K}(Bb) \;=\; A\mathrm{N}_{L/K}(b) \,. \qquad \textit{III.3.2.8.6}$$

Preuve :
i) Puisque $\nu_{L/K}$ et $\mathrm{N}_{L/K}$) sont des morphismes de groupes, il suffit d'établir la formule III.3.2.8.1 pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ en vertu du théorème III.1.1.11. Notons alors

$$\nu_{L/K}(\mathfrak{p}) \;=\; B\mathfrak{p} \;=\; \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$$

la décomposition de $B\mathfrak{p}$ donnée par la proposition III.1.2.4. Comme les $\mathfrak{q}_i$,$1\leq i\leq g_\mathfrak{p}$ sont par définition au-dessus de $\mathfrak{p}$ il vient

$$\begin{aligned}
\mathrm{N}_{L/K}(\nu_{L/K}(\mathfrak{p})) &= \mathrm{N}_{L/K}(B\mathfrak{p}) \\
&= \mathrm{N}_{L/K}(\prod_{i=1}^{g_\mathfrak{p}} \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}) \\
&= \prod_{i=1}^{g_\mathfrak{p}} \mathrm{N}_{L/K}(\mathfrak{q}_i)^{e_{\mathfrak{q}_i/\mathfrak{p}}} \\
&= \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}}} \\
&= \mathfrak{p}^{\sum_{i=1}^{g_\mathfrak{p}} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}}} \\
&= \mathfrak{p}^d
\end{aligned}$$

la dernière égalité résultant de la proposition III.1.2.10.

ii) Remarquons d'abord que $S^{-1}A$ est encore un anneau de Dedekind dont le corps des fractions est K (cf. I.5.2.5 [13],) quant à $S^{-1}B$ c'est encore la fermeture intégrale de $S^{-1}A$ dans L (cf. I.4.2.3.) Les applications

$$\nu_{/:}(\,)\mathcal{I}(S^{-1}A) \;\to\; \mathcal{I}(S^{-1}B) \text{ et } \mathrm{N}_{L/K}) \;:\; \mathcal{I}(S^{-1}B) \;\to\; \mathcal{I}(S^{-1}A)$$

sont donc bien définies.

Notons ensuite que les applications

$$\mathcal{I}(A) \;\to\; \mathcal{I}(S^{-1}A)\,,\; \mathfrak{I} \;\mapsto\; S^{-1}\mathfrak{I} \text{ et } \mathcal{I}(B) \;\to\; \mathcal{I}(S^{-1}B)\,,\; \mathfrak{J} \;\mapsto\; S^{-1}\mathfrak{J}$$

sont des morphismes de groupes en vertu de la proposition I.3.2.5.

Les formules III.3.2.8.2 et III.3.2.8.3 équivalent donc au fait que les carrés de morphismes de groupes

$$\begin{array}{ccc} \mathcal{I}(A) & \to & \mathcal{I}(S^{-1}A) \\ {\scriptstyle \nu_{L/K}}\downarrow & & \downarrow{\scriptstyle \nu_{L/K}} \\ \mathcal{I}(B) & \to & \mathcal{I}(S^{-1}B) \end{array} \qquad \text{et} \qquad \begin{array}{ccc} \mathcal{I}(B) & \to & \mathcal{I}(S^{-1}B) \\ {\scriptstyle \mathrm{N}_{L/K})}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K})} \\ \mathcal{I}(A) & \to & \mathcal{I}(S^{-1}A) \end{array}$$

sont commutatifs. Il suffit donc de vérifier III.3.2.8.2 (resp. III.3.2.8.3) pour $\mathfrak{p} \in \mathrm{Spm}(A)$, (resp. $\mathfrak{q} \in \mathrm{Spm}(B)$.)

Cette réduction n'est même pas nécessaire pour établir III.3.2.8.2 qui résulte simplement du fait que

$$S^{-1}B\mathfrak{I} \;\cong\; S^{-1}BS^{-1}\mathfrak{I}\;\forall\,\mathfrak{I} \;\in \mathcal{I}(A)$$

[13] Le cas où $S^{-1}A$ est un corps est sans intérêt et d'ailleurs dans ce cas les groupes d'idéaux fractionnaires sont triviaux et le résultat immédiat.

qui n'est lui-même rien d'autre que le lemme I.3.2.4.

Finalement, pour tout $\mathfrak{q} \in \mathrm{Spm}(B)$, notons

$$\mathfrak{p} \ := \ \mathfrak{q} \cap A \ \in \ \mathrm{Spm}(A) \ .$$

On peut supposer que $\mathfrak{p} \cap S \ = \ \emptyset$ et on laisse au lecteur le soin de traiter le cas $\mathfrak{p} \cap S \ \neq \ \emptyset$ qui est essentiellement trivial. En vertu de III.1.2.9.ii,

$$S^{-1}\mathfrak{q} \cap S^{-1}A \ = \ S^{-1}\mathfrak{p}$$

d'où il vient

$$\mathrm{N}_{L/K}(S^{-1}\mathfrak{q}) \ = \ S^{-1}\mathfrak{p}^{f_{s^{-1}\mathfrak{q}/^{-1}\mathfrak{p}S}}$$

qui vaut encore, grâce à III.1.2.9.iii,

$$\begin{aligned} S^{-1}\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}} &= S^{-1}\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}} \\ &= S^{-1}\mathrm{N}_{L/K}(\mathfrak{q}) \ . \end{aligned}$$

iii) Une fois encore, il suffit de vérifier la formule III.3.2.8.4 pour $\mathfrak{r} \in \mathrm{Spm}(C)$. Notons alors

$$\mathfrak{q} \ := \ \mathfrak{r} \cap B \ \mathrm{et} \ \mathfrak{p} \ := \ \mathfrak{q} \cap A \ = \ \mathfrak{r} \cap A \ .$$

On a alors

$$\begin{aligned} \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathfrak{r})) &= \mathrm{N}_{L/K}(\mathfrak{q}^{f_{\mathfrak{r}/\mathfrak{q}}}) \\ &= \mathrm{N}_{L/K}(\mathfrak{q})^{f_{\mathfrak{r}/\mathfrak{q}}} \\ &= (\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}})^{f_{\mathfrak{r}/\mathfrak{q}}} \\ &= \mathfrak{p}^{f_{\mathfrak{r}/\mathfrak{q}}f_{\mathfrak{q}/\mathfrak{p}}} \\ &= \mathfrak{p}^{f_{\mathfrak{r}/\mathfrak{p}}} \\ &= \mathrm{N}_{M/K}(\mathfrak{r}) \end{aligned}$$

en utilisant le lemme III.1.2.7.

iv) Il suffit de le vérifier pour un idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$. Posons alors $\mathfrak{p} \ := \ \mathfrak{q} \cap A$. on a alors

$$B\mathfrak{p} \ = \ (\prod_{i=1}^{g_{\mathfrak{p}}} \mathfrak{q}_i)^{e_{\mathfrak{p}}}$$

(cf. III.2.3.6.iii.)

On suppose que $\mathfrak{q}_1 = \mathfrak{q}$. Le groupe de Galois opère transitivement sur les idéaux premiers au-dessus de $\mathfrak{p}$ (cf. III.2.3.2.) Choisissons $\tau_i \in G$ tels que $\tau_i(\mathfrak{q}) = \mathfrak{q}_i$. G est l'union disjointe des $\tau_i G_{\mathfrak{q}}$ d'où

$$\prod_{\sigma \in G} \sigma(\mathfrak{q}) \ = \ \prod_{\sigma \in G_{\mathfrak{q}}} \prod_{i=1}^{g_{\mathfrak{p}}} \tau_i(\sigma(\mathfrak{q})) \ = \ \prod_{i=1}^{g_{\mathfrak{p}}} (\tau_i(\mathfrak{q}))^{|G_{\mathfrak{q}}|} \ .$$

Or $G_{\mathfrak{q}}$ est d'indice $g_{\mathfrak{p}}$ (cf. III.2.3.4,) donc $|G_{\mathfrak{q}}| \ = \ e_{\mathfrak{p}} f_{\mathfrak{p}}$. donc le produit ci-dessus vaut

$$\prod i = 1 g_{\mathfrak{p}} \mathfrak{q}_i^{e_{\mathfrak{p}} f_{\mathfrak{p}}} \ = \ B(\mathfrak{p}^{f_{\mathfrak{p}}}) \ = \ \nu_{L/K}(\mathrm{N}_{L/K}(\mathfrak{q})) \ .$$

v) Si $K \subset L$ est galoisienne, d'après le point précédent :

$$\begin{aligned} \nu_{L/K}(A\mathrm{N}_{L/K}(b)) &= BA\mathrm{N}_{L/K}(b) \\ &= B\mathrm{N}_{L/K}(b) \\ &= B \prod_{\sigma i \in \mathrm{Gal}_{L/K}} \sigma(b) \\ &= \prod_{\sigma \in \mathrm{Gal}_{L/K}} \sigma(Bb) \\ &= \nu_{L/K}(\mathrm{N}_{L/K}(Bb)) \end{aligned}$$

ce qui prouve le résultat puisque $\nu_{L/k}$ est injectif (cf. III.3.2.6.i.)

Si l'extension L/K n'est pas galoisienne, soit M une extension finie galoisienne de K contenant L. On note $r \ := \ [M : L]$ et on introduit C la fermeture de A ou B dans M. Enfin on note $\nu_{\prime/} \ (:) \ \mathcal{I}(B) \ \to \ \mathcal{I}(C)$ le morphisme défini comme en III.3.2.6.i.

Pour tout $b \in L, \ b \ \neq \ 0$, le résultat déjà montré ci-dessus pour les extensions galoisiennes entraîne que

$$\begin{aligned} A\mathrm{N}_{M/K}(b) &= \mathrm{N}_{M/K}(Cb) \\ &= \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(Cb)) \\ &= \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\nu_{\prime/(}(B)b))) \\ &= \mathrm{N}_{L/K}((Bf)^r) \\ &= (\mathrm{N}_{L/K}(Bb))^r \ . \end{aligned}$$

Par ailleurs,

$$\mathrm{N}_{M/L}(b) \ = \ \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(b)) \ = \ \mathrm{N}_{L/K}(b^r) \ = \ (\mathrm{N}_{L/K}(b))^r$$

puisque b est dans L.

Il en résulte que l'on a l'égalité

$$(A\mathrm{N}_{L/K}(b))^r \ = \ (\mathrm{N}_{L/K}(Bb))^r$$

dans $\mathcal{I}(A)$ qui est un groupe abélien libre (cf. III.1.1.11,) donc sans r-torsion si bien que

$$A\mathrm{N}_{L/K}(b) \ = \ \mathrm{N}_{L/K}(Bb) \ .$$

q.e.d

Remarque III.3.2.9. Le calcul de la norme pour les idéaux principaux effectué en III.3.2.8.v, justifie la définition III.3.2.7 qui « recouvre » alors la définition III.3.2.2.iii.

Lemme III.3.2.10. *Pour tout idéal fractionnaire $\mathfrak{I} \in \mathcal{I}(B)$ de B, on note*

$$\mathfrak{I}^* \ := \ \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in A \ \forall y \in \mathfrak{I}\} \ . \qquad \textit{III.3.2.10.1}$$

i) L'objet $\mathfrak{I}^*$ défini ci-dessus est encore un idéal fractionnaire de B.

De plus, si $\mathfrak{I}$ est un A-module libre et si $e_1, \ldots, e_d$ est une base de $\mathfrak{I}$ sur A alors $\mathfrak{I}^*$ est un A-module libre de base la base duale.

Ce qui s'applique en particulier lorsque A est un anneau principal.

ii) Soit $(\mathfrak{I}, \mathfrak{J}) \in \mathcal{I}(B)^2$ un couple d'idéaux fractionnaires de B :

$$\mathfrak{I} \ \subset \ \mathfrak{J} \ \Rightarrow \ \mathfrak{J}^* \ \subset \ \mathfrak{I}^* \, ; \qquad \textit{III.3.2.10.2}$$

$$\mathfrak{J} \ \subset \ \mathfrak{I}^* \ \Leftrightarrow \ \mathrm{Tr}_{L/K}(\mathfrak{J}\mathfrak{I}) \ \subset \ A \, ; \qquad \textit{III.3.2.10.3}$$

iii) Pour tout idéal fractionnaire $\mathfrak{I}$ de B, $\mathrm{Tr}_{L/K}(\mathfrak{I}^*\mathfrak{I}) \ = \ A$.

iv) Pour tout idéal fractionnaire $\mathfrak{I}$ de B, $\mathfrak{I}^* \ = \ B^*\mathfrak{I}^{-1}$.

Preuve :

i)

- $\mathfrak{I}^*$ est un sous B-module de L, puisque

$$\mathrm{Tr}_{L/K}(\lambda xy) \ = \ \mathrm{Tr}_{L/K}(x\lambda y) \ \forall \lambda \in L \ .$$

- Il existe $x \in B$, non nul tel que $x\mathfrak{I} \subset B$ (cf. I.1.5.3.) En fait $x \in \mathfrak{I}^*$. En effet, pour tout $y \in \mathfrak{I}$, $xy \in B$, et bien sûr $\mathrm{Tr}_{L/K}(B) \subset A$. Donc $\mathfrak{I}^*$ est non nul.
- On va noter e_i ,$1 \leq i \leq d$ une K-base de L. On peut la choisir formée d'éléments de $\mathfrak{I}$ On note e_i^* la base duale qui est encore une K-base de L. Pour tout $x \in L$ on peut donc écrire

$$x \ = \ \sum_{i=1}^{d} \lambda_i e_i^* \ \lambda_i \in K \ .$$

  De plus pour tout $1 \leq j \leq d$, $\mathrm{Tr}_{L/K}(xe_j) \ = \ \lambda_j$. Si $x \in \mathfrak{I}^*$, $\lambda_i \in A$, c'est-à-dire que $\mathfrak{I}^*$ est inclus dans le A-module engendré par les e_i^* qui est encore plus de type fini comme B-module.

ii) Ces formules sont pour ainsi dire tautologiques.

iii) Laissé en exercice.

iv) Pour tout $x \in B^*$, $u \in \mathfrak{I}^{-1}$ et $y \in \mathfrak{I}$, $\mathrm{Tr}_{L/K}(xuy) \ \in A$ puisque $uy \in B$ donc $xu \in \mathfrak{I}^*$ donc $B^*\mathfrak{I}^{-1} \subset \mathfrak{I}^*$.

Si $a \in \mathfrak{I}^*$, $s \in \mathfrak{I}$ et $b \in B$, $\mathrm{Tr}_{L/K}(asb) \in A$ puisque $sb \in \mathfrak{I}$ donc $as \in B^*$, donc $\mathfrak{I}^*\mathfrak{I} \subset B^*$ donc $\mathfrak{I}^* \subset B^*\mathfrak{I}^{-1}$.

q.e.d

Définition III.3.2.11. Différente $\mathrm{Tr}_{L/K}(B) \subset A$, donc $B \subset B^*$ d'où ${B^*}^{-1} \subset B$ est un vrai idéal de B qu'on appelle la *différente* de B par rapport à A et qu'on note $\mathcal{D}_{B/A}$. On appelle aussi usuellement

$$\mathcal{D}_{B/A}{}^{-1} \;=\; B^*$$

la *codifférente*.

Proposition III.3.2.12. Propriétés de la différente
i) Si S est une partie multiplicative de A ne contenant pas 0,

$$\mathcal{D}_{S^{-1}B/S^{-1}A} \;=\; S^{-1}\mathcal{D}_{B/A}\,.$$

ii) Étant donnée une tour $K \subset L \subset M$ d'extensions finies séparables B et C les anneaux d'entiers :

$$\mathcal{D}_{C/A} \;=\; \mathcal{D}_{C/B}\,\nu_{M/L}(\mathcal{D}_{B/A})\,.$$

Preuve :
i) Laissé en exercice.
ii) Il revient au même de démontrer que

$$\mathcal{D}_{C/B}{}^{-1} \;=\; \mathcal{D}_{B/A}\mathcal{D}_{C/A}{}^{-1}\,.$$

Introduisons les notations :

$$\begin{aligned} t &:= \mathrm{Tr}_{M/K}(\cdot)\\ t' &:= \mathrm{Tr}_{L/K}(\cdot)\\ t'' &:= \mathrm{Tr}_{M/L}(\cdot)\end{aligned}$$

d'où $t \;=\; t't''$. Soit $\mathfrak{J}$ un idéal fractionnaire de C, $\mathfrak{J} \subset \mathcal{D}_{C/B}{}^{-1}$ si et seulement si $t''(\mathfrak{J}) \subset B$ si et seulement si $\mathcal{D}_{B/A}{}^{-1}t''(\mathfrak{J}) \subset \mathcal{D}_{B/A}{}^{-1}$ si et seulement si $t'(\mathcal{D}_{B/A}{}^{-1}t''(\mathfrak{J})) \subset A$.

Soit $x \in \mathcal{D}_{B/A}{}^{-1}$ et $y \in \mathfrak{J}$. $t'(xt''(y)) = t(xy)$ donc $t(\mathcal{D}_{B/A}{}^{-1}\mathfrak{J}) \subset A$, c'est-à-dire que $\mathcal{D}_{B/A}{}^{-1}\mathfrak{J} \subset \mathcal{D}_{C/A}{}^{-1}$ ce qui équivaut encore à $\mathfrak{J} \subset \mathcal{D}_{B/A}\mathcal{D}_{C/A}{}^{-1}$.

q.e.d

Définition III.3.2.13. Discriminant d'un A-module Pour tout sous-A-module M de type fini de L, on appelle *discriminant par rapport à l'extension L/K de M*, et on note $\mathfrak{d}^A_{L/K}(M)$ le sous-A-module de K engendré par les $\delta_{L/K}(f_1,\ldots,f_d)$ (cf. III.3.2.1.v,) pour $(f_1,\ldots,f_d)$ des d-uplets d'éléments de M.

Lemme III.3.2.14.
i) Pour tout couple (M,N) de sous-A-modules de type fini de L $N \subset M$, entraîne

$$\mathfrak{d}^A_{L/K}(N) \;\subset\; \mathfrak{d}^A_{L/K}(M)\,.$$

ii) Si M est un sous-A-module libre de L de base $(m_1,\ldots,m_d)$, $\mathfrak{d}^A_{L/K}(M)$ est un A-module libre de rang 1 engendré par $\delta_{L/K}(m_1,\ldots,m_d)$.

iii) Pour tout sous-A-module de type fini M de L, $\mathfrak{d}^A_{L/K}(M) \neq 0$ si et seulement si M contient une K-base de L ; dans ce cas c'est un idéal fractionnaire de A.

iv) Pour $M = B$, $\mathfrak{d}^A_{L/K}(B)$ est un idéal de A.

Définition III.3.2.15.

i) On note

$$\mathfrak{d}_{B/A} := \mathfrak{d}^A_{L/K}(B)$$

qu'on appelle parfois *idéal discriminant de B* par rapport à A.

ii) Si K est un corps complet pour une valuation discrète, A l'anneau des entiers, L une extension finie séparable, alors $B := \mathcal{O}_L$ est l'anneau des entiers de L et on note

$$\mathfrak{d}_{L/K} := \mathfrak{d}_{B/A}$$

qu'on appelle *discriminant de l'extension*.

iii) Si L est un corps de nombres, le discriminant $\mathfrak{d}_{\mathcal{O}_L/\mathbb{Z}}$ est un idéal de $\mathbb{Z}$ engendré par un unique entier positif qu'on appelle *discriminant du corps*.

Proposition III.3.2.16. Propriétés des discriminants

i) Pour S une partie multiplicative de A, ne contenant pas 0, et M un sous-A-module de type fini de L alors

$$\mathfrak{d}^{S^{-1}A}_{L/K}(S^{-1}M) = S^{-1}\mathfrak{d}^A_{L/K}(M)\,.$$

ii) Si M est un sous-A-module de B contenant une K-base de L, il existe un idéal non nul $\mathfrak{I}$ de A tel que

$$\mathfrak{d}^A_{L/K}(M) = \mathfrak{I}^2\mathfrak{d}_{B/A}\,.$$

iii) Si $\mathfrak{J}$ est un idéal fractionnaire de B,

$$\mathfrak{d}^{\mathfrak{J}}_{L/K}(\,) = \mathrm{N}_{L/K}(\mathfrak{J})^2\mathfrak{d}_{B/A}\,.$$

Preuve :

i) Laissé en exercice.

ii) Supposons d'abord A principal. Alors B est un A-module libre de type fini dont on choisit une A-base $(f_1, \ldots, f_d)$. L'idéal discriminant $\mathfrak{d}_{B/A}$ est alors l'idéal principal engendré par $\delta_{L/K}(f_1, \ldots, f_d)$ (cf. III.3.2.14.ii.) Puisque A est principal, M est un A-module libre de type fini dont on note $u_1, \ldots, u_d$ une A-base. Il s'ensuit que $\mathfrak{d}^M_{L/K}()$ est le A-module libre engendré par $\delta_{L/K}(u_1, \ldots, u_d)$. Pour tout $1 \leq i \leq d$, on peut écrire $u_i = \sum_{j=1}^{d} p_{ij} f_j$. Il suffit alors de prendre $\mathfrak{I} := \det(p_{ij})A$.

Il faut ensuite montrer qu'on peut déduire le cas global du cas local.

iii) On suppose que A et B sont principaux. Il existe alors $\lambda \in L$ tel que $\mathfrak{J} = B\lambda$. Si $(f_1, \ldots, f_d)$ est une A-base de B, λf_i est une A-base de $\mathfrak{J}$. Le résultat est alors une conséquence du point III.3.2.1.vi et du point III.3.2.8.v.

Il faut encore déduire le cas global du cas local.

q.e.d

Lemme III.3.2.17. *On suppose que A est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}$, d'uniformisante π et de corps résiduel $k = A/\mathfrak{p}$.*
i) Pour tout idéal $\mathfrak{I} \subset B$ de B, $B/\mathfrak{I}$ est un k-espace vectoriel de dimension finie et

$$\mathrm{N}_{L/K}(\mathfrak{I}) = A\pi^{\dim_k B/\mathfrak{I}} .$$

ii) Pour tout idéal $\mathfrak{I} \subset B$ de B, $B \subset \mathfrak{I}^{-1}$, $\mathfrak{I}^{-1}/B$ est un k-espace vectoriel de dimension finie et

$$\mathrm{N}_{L/K}(\mathfrak{I}) = A\pi^{\dim_k \mathfrak{I}^{-1}/B} .$$

Preuve :
i) On a

$$\mathfrak{I} = \prod_{\mathfrak{q}\in \mathrm{Spm}(B)} \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{I})}$$

avec

$$v_{\mathfrak{q}}(\mathfrak{I}) \geq 0 \, \forall \, \mathfrak{q} \in \mathrm{Spm}(B) .$$

Rappelons que dans cette situation,

$$\mathfrak{q} \cap A = \mathfrak{p} \, \forall \, \mathfrak{q} \in \mathrm{Spm}(B) .$$

Il en résulte que

$$\mathrm{N}_{L/K}(\mathfrak{I}) = \prod_{\mathfrak{q}\in \mathrm{Spm}(B)} \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}} v_{\mathfrak{q}}(\mathfrak{I})} = A\pi^{\sum_{\mathfrak{q}\in \mathrm{Spm}(B)} f_{\mathfrak{q}/\mathfrak{p}} v_{\mathfrak{q}}(\mathfrak{I})} .$$

D'autre part,

$$\begin{aligned} B/\mathfrak{I} &= B/\prod_{\mathfrak{q}\in \mathrm{Spm}(B)} \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{I})} \\ &= \prod_{\mathfrak{q}\in \mathrm{Spm}(B)} B/\mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{I})} \end{aligned}$$

en vertu du théorème chinois des restes. Or pour tout $\mathfrak{q} \in \mathrm{Spm}(B)$, $B/\mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{I})}$ est un $B/\mathfrak{q}$-espace vectoriel de dimension $v_{\mathfrak{q}}(\mathfrak{I})$ (cf. II.3.1.3.) Comme $B/\mathfrak{q}$ est lui-même un k-espace vectoriel de dimension $f_{\mathfrak{q}/\mathfrak{p}}$, On a

$$\dim_k B/\mathfrak{I} = \sum_{\mathfrak{q}\in \mathrm{Spm}(B)} f_{\mathfrak{q}/\mathfrak{p}} v_{\mathfrak{q}}(\mathfrak{I})$$

ce qui achève la preuve.

ii) Les idéaux maximaux de B sont tous au-dessus de $\mathfrak{p}$. Par conséquent, B est un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux maximau, c'est donc un anneau principal en vertu du corollaire III.1.1.13. Pour tout idéal $\mathfrak{I} \subset B$, il existe donc $b \in B$ tel que $\mathfrak{I} = Bb$. Il s'ensuit que

$$\mathfrak{I}^- = B\frac{1}{b} \subset L\,.$$

Si l'on note encore $b : L \to L$ la multiplication par b dans L, on a alors un diagramme commutatif

$$\begin{array}{ccccccccc} 0 \to & B & \to & \mathfrak{I}^{-1} & \to & \mathfrak{I}^{-1}/B & \to 0 \\ & {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} & & \downarrow & \\ 0 \to & \mathfrak{I} & \to & B & \to & B/\mathfrak{I} & \to 0 \end{array}$$

dans lequel les flèches verticales de gauches et du centre sont des isomorphismes si bien que la flèche vertical de droite est encore un isomorphisme (ce qui peut par exemple résulter du lemme du serpent voir TD II, exercice A.) Il suffit alors d'appliquer le point III.3.2.17.i pour conclure.

q.e.d

Théorème III.3.2.18. *Soit A un anneau de Dedekind, K son corps des fractions, $K \subset L$ une extension finie séparable de degré d et B la fermeture intégrale de A dans L.*
i) Si A est un anneau de valuation discrète on a :

$$\mathfrak{d}_{B/A} = \mathrm{N}_{L/K}(\mathcal{D}_{B/A})\,. \qquad \textit{III.3.2.18.1}$$

ii) Dans le cas général on a encore

$$\mathfrak{d}_{B/A} = \mathrm{N}_{L/K}(\mathcal{D}_{B/A})\,. \qquad \textit{III.3.2.18.2}$$

iii) Étant donné un sous-A-module C de B, pour tout $\mathfrak{p} \in \mathrm{Spm}(A)$, C est $\mathfrak{p}$-clos (cf. III.3.1.2,) si et seulement si

$$v_{\mathfrak{p}}(\mathfrak{d}_{B/A}) = v_{\mathfrak{p}}(\mathfrak{d}^A_{L/K}(C))\,. \qquad \textit{III.3.2.18.3}$$

iv) Étant donnés un anneau de Dedekind A, K son corps des fractions, une tour d'extensions finies séparables

$$K \subset L \subset M,$$

B (resp. C) la fermeture intégrale de A dans L (resp. M,) on a

$$\mathfrak{d}_{C/A} = \mathrm{N}_{L/K}(\mathfrak{d}_{C/B}) \cdot \mathfrak{d}_{B/A}{}^{[M:L]}\,. \qquad \textit{III.3.2.18.4}$$

Preuve :

i) Si A est un anneau de valuation discrète il est en particulier principal. L'anneau B est alors, en vertu du corollaire I.4.4.3, un A-module libre de rang d. Notons $\mathrm{GL}_d(K)$ (resp. $\mathrm{GL}_d(A)$) le groupe des matrices carrés $d \times d$ inversibles à coefficients dans K (resp. A.)

Puisque A est un anneau principal, que $B \hookrightarrow B^*$ est une inclusion de A-modules, que B et B^* sont des A-modules libres de rang d, (cf. III.3.2.10.i,) il existe, en vertu du théorème de la base adaptée, une A-base $\beta_{i\ ,1\leq i\leq d}$ de B^* et des éléments $\alpha_{i\ ,1\leq i\leq d} \in A$ de A, tels que

$$b_i \ := \ \alpha_i \beta_{i\ ,1\leq i\leq d} \qquad \text{III.3.2.18.5}$$

est une A-base de B. Notons donc $M \in \mathrm{GL}_d(K)$ la matrice diagonale de terme diagonal $\alpha_{i\ ,1\leq i\leq d}$.

Notons encore $b_i^{*\ ,1\leq i\leq d}$ la base duale de $b_{i\ ,1\leq i\leq d}$ pour la forme trace. Il existe une matrice $N \in \mathrm{GL}_d(K)$ de terme général n_{ij} telle que

$$b_i^* \ = \ \sum_{j=1}^{d} n_{ij} b_j \ . \qquad \text{III.3.2.18.6}$$

Pour tout

$$1 \leq i \leq d \text{ et } 1 \leq j \leq d,$$

si δ_{ij} désigne le symbole de Kronecker,

$$\begin{aligned} \delta_{ij} &= \mathrm{Tr}_{L/K}(b_i b_j^*) \\ &= \mathrm{Tr}_{L/K}(\sum_{k=1}^{d} b_i n_{jk} b_k) \\ &= \sum_{k=1}^{d} n_{jk} \mathrm{Tr}_{L/K}(b_k b_i) \ . \end{aligned}$$

Ce qui s'écrit encore, si l'on note $T \in \mathrm{GL}_d(K)$ la matrice de terme général $\mathrm{Tr}_{L/K}(b_i b_j)$,

$$N \ \cdot \ T \ = \ \mathrm{Id}_{K^d} \ . \qquad \text{III.3.2.18.7}$$

Enfin,

$$\beta_{i\ ,1\leq i\leq d} \text{ et } b_i^{*\ ,1\leq i\leq d}$$

étant deux A-bases de B^*, il existe une matrice

$$P \ \in \ \mathrm{GL}_d(A) \ \subset \ \mathrm{GL}_d(K),$$

de terme général p_{ij} telle que

$$\beta_i \ = \ \sum_{j=1}^{d} p_{ij} b_j^* \ \forall 1 \leq i \leq d \ . \qquad \text{III.3.2.18.8}$$

Les égalités III.3.2.18.5, III.3.2.18.6 et III.3.2.18.8 entraînent alors que

$$P \cdot N \cdot M = \mathrm{Id}_{K^d}$$

ce qui entraîne encore grâce à III.3.2.18.7 que

$$P \cdot T^{-1} \cdot M = \mathrm{Id}_{K^d}$$

dans $\mathrm{GL}_d(K)$. Il s'ensuit que

$$\det(T) = \det(P)\det(M) .$$

Comme $P \in \mathrm{GL}_d(A), \det(P) \in A^\times$ si bien que

$$A\det(T) = A\det(M) .$$

Or par définition, $A\det(T) = \mathfrak{d}_{B/A}$ si bien qu'on obtient l'égalité

$$\mathfrak{d}_{B/A} = A\prod_{i=1}^{d} \alpha_i$$

qui s'écrit encore, si l'on note π une uniformisante de A,

$$\mathfrak{d}_{B/A} = A\pi^{\sum_{i=1}^{d} v_\mathfrak{p}(\alpha_i)} . \qquad \text{III.3.2.18.9}$$

En outre

$$B^*/B = \prod_{i=1}^{d} A/A\alpha_i = \prod_{i=1}^{d} A/A\pi^{v_\mathfrak{p}(\alpha_i)} .$$

Or si l'on note $k := A/\mathfrak{p}$ le corps résiduel de A, il résulte du lemme II.3.1.3 que

$$\dim_k A/A\pi^{v_\mathfrak{p}(\alpha_i)} = v_\mathfrak{p}(\alpha_i) \; \forall 1 \leq i \leq d$$

si bien que

$$\dim_k {\mathcal{D}_{B/A}}^{-1}/B = \dim_k B^*/B = \sum_{i=1}^{d} v_\mathfrak{p}(\alpha_i) .$$

Cette dernière identité combinée avec légalité III.3.2.18.9 et le point III.3.2.17.ii permet de conclure.

ii) Les deux membres de l'égalité sont des idéaux de A. On a donc, en vertu du théorème III.1.1.11, une unique décomposition

$$\begin{aligned} \mathfrak{d}_{B/A} &= \prod_{\mathfrak{p}\in \mathrm{Spm}(A)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d}_{B/A})} \\ \mathrm{N}_{L/K}(\mathcal{D}_{B/A}) &= \prod_{\mathfrak{p}\in \mathrm{Spm}(A)} \mathfrak{p}^{v_\mathfrak{p}(\mathrm{N}_{L/K}(\mathcal{D}_{B/A}))} \end{aligned}$$

où les $v_{\mathfrak{p}}(\cdot)$ sont nuls sauf pour un nombre fini d'idéaux maximaux. L'égalité III.3.2.18.2 équivaut donc à

$$v_{\mathfrak{p}}(\mathfrak{d}_{B/A}) \;=\; v_{\mathfrak{p}}(\mathrm{N}_{L/K}(\mathcal{D}_{B/A}))\;\forall\,\mathfrak{p} \;\in\; \mathrm{Spm}(A)\;. \qquad \text{III.3.2.18.10}$$

Ceci équivaut encore à

$$\mathfrak{d}_{B/A_{\mathfrak{p}}} \;=\; \mathfrak{d}_{B/A}\otimes_A A_{\mathfrak{p}} \;\cong\; \mathrm{N}_{L/K}(\mathcal{D}_{B/A})_{\mathfrak{p}} \;=\; \mathrm{N}_{L/K}(\mathcal{D}_{B/A})\otimes_A A_{\mathfrak{p}}\;\forall\,\mathfrak{p} \;\in\; \mathrm{Spm}(A)\;. \qquad \text{III.3.2.18.11}$$

Notons $B_{\mathfrak{p}} \;:=\; B\otimes_A A_{\mathfrak{p}}$. On a alors, en vertu du point III.3.2.16.i,

$$\mathfrak{d}_{B/A_{\mathfrak{p}}} \;=\; \mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}\;.$$

Par ailleurs, grâce à III.3.2.8.ii,

$$\mathrm{N}_{L/K}(\mathcal{D}_{B/A})_{\mathfrak{p}} \;=\; \mathrm{N}_{L/K}(\mathcal{D}_{B/A_{\mathfrak{p}}})$$

qui vaut encore, grâce à III.3.2.12.i, $\mathrm{N}_{L/K}(\mathcal{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}})$. Il en résulte que III.3.2.18.11 équivaut encore à

$$\mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} \;=\; \mathrm{N}_{L/K}(\mathcal{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}})\;\forall\,\mathfrak{p} \;\in\; \mathrm{Spm}(A)\;. \qquad \text{III.3.2.18.12}$$

Le résultat découle alors du point III.3.2.18.i appliqué aux anneau $A_{\mathfrak{p}}\;,\mathfrak{p}\in\mathrm{Spm}(A)}$.

iii) Pour tout $\mathfrak{p}\in\mathrm{Spm}(A)$, l'égalité III.3.2.18.3 équivaut à

$$\mathfrak{d}_{B/A_{\mathfrak{p}}} \;\cong\; \mathfrak{d}^{A}_{L/K}(C)_{\mathfrak{p}}$$

ce qui équivaut encore, en vertu du point III.3.2.16.i,

$$\mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} \;\cong\; \mathfrak{d}^{A_{\mathfrak{p}}}_{L/K}(C_{\mathfrak{p}})\;. \qquad \text{III.3.2.18.13}$$

Or $A_{\mathfrak{p}}$ étant un anneau principal, $B_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$ module libre de rang d. Il s'ensuit que $C_{\mathfrak{p}}$ est également un $A_{\mathfrak{p}}$-module libre. L'égalité III.3.2.18.13 ci-dessus implique en particulier que $\mathfrak{d}^{A_{\mathfrak{p}}}_{L/K}(C_{\mathfrak{p}}) \;\neq\; 0$ ce qui entraîne, grâce à III.3.2.14.iii, que $C_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$-module libre de rang d.

Il existe alors, grâce au théorème de la base adaptée, puisque $A_{\mathfrak{p}}$ est principal, une base $(b_1,\ldots,b_d)$ de $B_{\mathfrak{p}}$ et des éléments $\alpha_{i}\;,1\leq i\leq d} \;\in\; A_{\mathfrak{p}}$ de $A_{\mathfrak{p}}$ tous non nuls tels que

$$\alpha_i b_{i}\;,1\leq i\leq d}$$

est une $A_{\mathfrak{p}}$-base de $C_{\mathfrak{p}}$. L'égalité III.3.2.18.13 équivaut alors, en vertu de III.3.2.14.ii, à

$$\begin{aligned}
A\mathrm{det}(\sigma_j(b_i)) &= \mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}\\
&= \mathfrak{d}^{A_{\mathfrak{p}}}_{L/K}(C_{\mathfrak{p}})\\
&= A\mathrm{det}(\sigma_j(\alpha_i b_j))\\
&= A\mathrm{det}(\alpha_i\sigma_j(b_i))\\
&= A\prod_{i=1}^{d}\alpha_i\mathrm{det}(\sigma_j(b_i))
\end{aligned}$$

ce qui entraîne que $\prod_{i=1}^{d} \alpha_i$ est inversible donc que $C_{\mathfrak{p}} = B_{\mathfrak{p}}$ autrement dit que C est $\mathfrak{p}$-clos dans B. La réciproque est bien entendu immédiate.

iv) On a

$$\mathfrak{d}_{C/A} = \mathrm{N}_{M/K}(\mathcal{D}_{C/A})$$

grâce au point III.3.2.18.ii, qui vaut encore, en vertu de III.3.2.12.ii,

$$\begin{aligned}\mathrm{N}_{M/K}(\mathcal{D}_{C/B}\nu_{M/L}(\mathcal{D}_{B/A})) &= \mathrm{N}_{M/K}(\mathcal{D}_{C/B}) \cdot \mathrm{N}_{M/K}(\nu_{M/L}(\mathcal{D}_{B/A})) \\ &= \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathcal{D}_{C/B})) \cdot \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\nu_{M/L}(\mathcal{D}_{B/A}))) \\ &= \mathrm{N}_{L/K}(\mathfrak{d}_{C/B})\mathrm{N}_{L/K}({\mathcal{D}_{B/A}}^{[M:L]})\end{aligned}$$

cette dernière égalité provenant de III.3.2.8.1.

On obtient donc

$$\begin{aligned}\mathfrak{d}_{C/A} &= \mathrm{N}_{L/K}(\mathfrak{d}_{C/B}) \cdot \mathrm{N}_{L/K}({\mathcal{D}_{B/A}}^{[M:L]}) \\ &= \mathrm{N}_{L/K}(\mathfrak{d}_{C/B}) \cdot \mathrm{N}_{L/K}(\mathcal{D}_{B/A})^{[M:L]} \\ &= \mathrm{N}_{L/K}(\mathfrak{d}_{C/B}) \cdot {\mathfrak{d}_{B/A}}^{[M:L]} .\end{aligned}$$

q.e.d

Dans la suite de cette section (III.3.2,) on suppose que K est un corps local (cf. II.3.2.1,) $K \subset L$ une extension séparable de degré d, $\mathcal{O}_K, \mathfrak{m}_K$ (resp. $\mathcal{O}_L, \mathfrak{m}_L$) le anneau d'entiers et l'idéal maximal de K (resp. L) v_K (resp. v_L) la valuation discrète normalisée sur K (resp. L.)

Définition III.3.2.19. L'extension $K \subset L$ est *modérément ramifiée* si l'indice de ramification $e_{L/K}$ (cf. II.3.1.4) est premier à la caractéristique résiduelle.

Lemme III.3.2.20.

i) Si $\alpha \in L$ est tel que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ et si P est le polynôme minimal de α sur K, on a

$$v_K(\mathfrak{d}_{L/K}) = f_{L/K}.v_L(P'(\alpha)) .$$

ii) Si l'extension $K \subset L$ est non ramifiée,

$$\mathfrak{d}_{L/K} = \mathcal{O}_K .$$

iii) Si l'extension $K \subset L$ est totalement ramifiée,

$$v_K(\mathfrak{d}_{L/K}) \geq [L : K] - 1$$

avec égalité si et seulement si l'extension $K \subset L$ est modérément ramifiée.

iv) Dans le cas général, on a

$$v_K(\mathfrak{d}_{L/K}) \geq f_{L/K}(e_{L/K}-1)$$

avec l'égalité si et seulement si l'extension L/K est modérément ramifiée.

v) Si $\mathfrak{d}_{L/K} = \mathcal{O}_K$ l'extension L/K est non ramifiée.

Preuve :

i) Par définition, (cf. III.3.2.15,) on a

$$\mathfrak{d}_{L/K} = \mathfrak{d}_{\mathcal{O}_L/\mathcal{O}_K} = \mathfrak{d}_{L/K}^{\mathcal{O}_K}(\mathcal{O}_L)\,.$$

Or si $\mathcal{O}_L = \mathcal{O}_k[\alpha]$, $\alpha^i\,, 0 \leq i \leq d-1$ est une $\mathcal{O}_K$-base de $\mathcal{O}_L$. Il résulte alors de III.3.2.14.ii, que

$$\mathfrak{d}_{L/K}^{\mathcal{O}_K}(\mathcal{O}_L) = \mathcal{O}_K\delta_{L/K}(1,\alpha,\ldots,\alpha^{d-1})$$

qui est encore égal, si l'on note P le polynôme minimal de α, à

$$\mathcal{O}_K\mathrm{N}_{L/K}(P'(\alpha))$$

grâce à III.3.2.1.5.

Il en résulte que

$$\begin{aligned} v_K(\mathfrak{d}_{L/K}) &= v_K(\mathrm{N}_{L/K}(P'(\alpha))) \\ &= \frac{1}{e}v_L(\mathrm{N}_{L/K}(P'(\alpha)) \\ &= \frac{1}{e}dv_L(P'(\alpha)) \\ &= f_{L/K}v_L(P'(\alpha))\,. \end{aligned}$$

ii) Notons k (resp. ℓ) le corps résiduel de K (resp.L L.) Puisque k est parfait, l'extension $k \subset \ell$ est séparable et il existe donc (théorème de l'élément primitif,) un élément $a \in \ell$ tel que $\ell = k[a]$. Si $P_a \in k[x]$ est le polynôme minimal de a, il existe un polynôme $P \in \mathcal{O}_K[X]$ relevant P_a, $\alpha \in \mathcal{O}_K$ relevant a tel que

$$P(\alpha) = 0 \text{ et } 0 \text{ et } \mathcal{O}_L = \mathcal{O}_K[\alpha] \text{ (cf. II.3.3.1.)}$$

On a alors

$$P'(\alpha) \equiv P'_a(a)\ [\mathfrak{m}_L]\,.$$

comme P_a est séparable, $P'_a(a) \neq 0$ c'est-à-dire que $P'(\alpha) \notin \mathfrak{m}_L$ c'est-à-dire que $P'(\alpha) \in \mathcal{O}_L^\times$. Il s'ensuit que $\mathrm{N}_{L/K}(P'(\alpha)) \in \mathcal{O}_K^\times$ ce qui entraîne finalement que

$$\mathfrak{d}_{L/K} = \mathcal{O}_K\mathrm{N}_{L/K}(P'(\alpha)) = \mathcal{O}_K\,.$$

iii) Si l'extension $K \subset L$ est totalement ramifiée, d'après le théorème (cf. II.3.2.8,) si l'on choisit une uniformisante π de L et qu'on note

$$P \ := \ X^d \ + \ \sum_{i=0}^{d-1} a_i X^i \ \in \ K[X]$$

son polynôme minimal sur K, alors $L \ = \ K[\pi]$ et P est un polynôme d'Eisenstein.

On a

$$P'(\pi) \ = \ d\pi^{d-1} + \sum_{i=1}^{d-1} i a_i \pi^{i-1} \ .$$

Pour tout $1 \leq i \leq d$,

$$v_L(ia_i\pi^{i-1}) \ = \ v_L(ia_i) \ + \ i-1 \ = \ dv_K(ia_i) + i - 1 \ .$$

Comme $1 \leq i \leq d$, les valuations ci-dessus sont toutes distinctes modulo d donc toutes distinctes. Il en résulte que

$$v_L(P'(\pi =)) \ = \ \min_{i=1}^{d}(dv_K(ia_i) + i - 1) \ .$$

Comme P est d'Eisenstein, pour tout $1 \leq i \leq d-1$, $v_K(a_i) > 0$ qui entraîne que $v_K(ia_i) > 0$, entraîne encore $dv_K(ia_i) \geq d$, entraîne

$$v_L(ia_i\pi^{i-1}) \ \geq \ d + i - 1 \ \forall 1 \leq i \leq d-1 \text{ et } v_L(d\pi^{d-1}) \ = \ dv_K(d) + d - 1 \ .$$

- Si le corps résiduel k est de caractéristique 0 ou de caractéristique p telle que p ne divise pas d, on a $v_K(d) \ = \ 0$ ce qui entraîne que $v_L(P'(\pi)) \ = \ d-1$.
- Si le corps résiduel est de caractéristique p et $p|d$:
  - Si K est de caractéristique p $d = 0$ dans K donc $dv_K(d) \ = \ +\infty$ on a alors $v_L(P'(\pi)) \geq d-1$.
  - Si K est de caractéristique 0, on définit l'*indice de ramification absolu* $e_K \ := \ v_K(p)$ C'est l'indice de ramification de l'extension $K/\mathbb{Q}_p$. Si $p|d$, on a encore $v_L(P'(\pi)) \geq d-1$.

Il suffit alors pour conclure d'appliquer le point III.3.2.20.i en remarquant que, l'extension $K \subset L$ étant totalement ramifiée, $f_{L/K} \ = \ 1$.

iv) Notons $K \subset L_0 \subset L$ l'extension maximal non ramifiée (cf. II.3.3.3.) On a alors une tour d'extensions finies séparables si bien qu'il résulte de l'identité III.3.2.18.4 que

$$\mathfrak{d}_{L/K} \ = \ \mathrm{N}_{L_0/K}(\mathfrak{d}_{L/L_0}) \cdot \mathfrak{d}_{L_0/K}{}^{[L:L_0]} \ .$$

L'extension $K \subset L_0$ étant non ramifiée, il résulte du point III.3.2.20.ii que

$$\mathfrak{d}_{L_0/K} \ = \ \mathcal{O}_K$$

si bien que

$$\mathfrak{d}_{L/K} \ = \ \mathrm{N}_{L/K}(\mathfrak{d}_{L/L_0}) \ .$$

On en déduit que

$$\begin{aligned} v_K(\mathfrak{d}_{L/K}) &= v_K(\mathrm{N}_{L/K}(\mathfrak{d}_{L/L_0})) \\ &= \frac{1}{e_{L_0/K}} v_{L_0}(\mathrm{N}_{L/K}(\mathfrak{d}_{L/L_0})) \\ &= v_{L_0}(\mathrm{N}_{L/K}(\mathfrak{d}_{LL/L_0})) \\ &= f_{L_0/K} v_{L_0}(\mathfrak{d}_{L/L_0}) \\ &= f_{L/K} v_{L_0}(\mathfrak{d}_{L/L_0}) \\ &\geq f_{L/K}([L:L_0]-1) \end{aligned}$$

la dernière inégalité résultant du point III.3.2.20.iii. comme $[L : L_0] = e_{L/K}$, on a établi le résultat.

v) Si $\mathfrak{d}_{L/K} = \mathcal{O}_K, v_K(\mathfrak{d}_{L/K}) = 0$, ce qui entraîne, grâce au point précédent, que $e_{L/K} = 1$.
q.e.d

Théorème III.3.2.21. *Soient K un corps local et $K \subset L$ une extension finie séparable.*
i) L'extension $K \subset L$ est non ramifiée si et seulement si

$$\mathfrak{d}_{L/K} = \mathcal{O}_K .$$

ii) On a

$$v_K(\mathfrak{d}_{L/K} \geq f_{L/K}(e_{L/K}-1)$$

avec égalité si et seulement si l'extension est modérément ramifiée.

Preuve :
i) Découle immédiatement de III.3.2.20.ii et III.3.2.20.v.
ii) N'est autre que III.3.2.20.iv.
q.e.d

Remarque III.3.2.22. Dans le cas général la formule III.3.2.18.2 ne suffit pas à déterminer la différente par la seule donnée du déterminant. Néanmoins, si $K \subset L$ est une extension finie séparable de corps locaux, le seul idéal maximal de $\mathcal{O}_L$ au-dessus de $\mathfrak{m}_K$ étant $\mathfrak{m}_L$ discriminant et différente sont uniquement déterminés par leurs valuations respectives et la donée de l'un équivaut à la donnée de l'autre.

Lemme III.3.2.23. *Supposons que K est un corps local de corps résiduel k de caractéristique p et que l'extension $K \subset L$ est totalement ramifiée et galoisienne de groupe de Galois $G := \mathrm{Gal}_{L/K}$. On note v_L la valuation discrète normalisée sur L. Pour une uniformisante π de L, on note*

$$\begin{array}{rccl} i_{L/K} & G & \to & \mathbb{Z} \\ & \sigma & \mapsto & v_L(\sigma(\pi)-\pi)-1 . \end{array} \qquad \textit{III.3.2.23.1}$$

i) L'application $i_{L/K}$ est indépendante du choix de l'uniformisante.

ii) L'application $i_{L/K}$ est en fait à valeurs dans $\mathbb{N} \cup \{+\infty\}$ et pour tout $\sigma \in G$,

$$i_{L/K}(\sigma) \ = \ +\infty \ \Leftrightarrow \ \sigma \ = \ \mathrm{Id} \ .$$

iii) Pour tout $j \in \mathbb{N}$ le sous-ensemble

$$G_j \ := \ \{\sigma \in G \mid i_{L/K}(\sigma) \geq j\} \ \subset \ G$$

de G est un sous-groupe normal (distingué/invariant) de G et $G_0 \ = \ G$.

iv) Le quotient G/G_1 est un groupe cyclique d'ordre premier à p.

v) Pour tout $i \geq 1$, le quotient G_i/G_{i+1} est un groupe abélien d'ordre une puissance de p.

vi) Le groupe G_1 est d'ordre une fini une puissance de p.

Preuve : Voir TD IV, exercice A. *q.e.d*

Corollaire III.3.2.24. *les hypothèses étant celle du lemme III.3.2.23, sans supposer toutefois que $K \subset L$ est totalement ramifiée, on peut faire la même construction en remplaçant le groupe de Galois $\mathrm{Gal}_{L/K}$ par le groupe d'inertie*

$$I_{L/K} \ = \ \mathrm{Gal}_{L/L_0}$$

(cf. II.3.3.iv,) où $K \subset L_0$ est l'extension maximale non-ramifiée.

Définition III.3.2.25. Groupes de ramification supérieure Étant donée une extension finie galoisienne de corps locaux $K \subset L$, les groupes G_i définis dans le lemme III.3.2.23 s'appellent *groupes de ramification supérieure*. Le groupe G/G_1 s'appelle le *groupe d'inertie modérée* et le groupe G_1 le *groupe d'inertie sauvage*.

Théorème III.3.2.26. *Soit K un corps local, $K \subset L$ une extension finie galoisienne si on note G_1 le groupe d'inertie sauvage, alors*

$$v_K(\mathfrak{d}_{L/K}) \ = \ f_{L/K}(e_{L/K} - 1 + \sum_{\sigma \in G_1 \ , \ \sigma \neq \mathrm{Id}} i_{L/K}(\sigma)) \ .$$

Preuve : Notons $K \subset L_0 \subset L$ l'extension maximale non-ramifiée et π une uniformisante de L. Le polynôme minimal P de π sur L_0 s'écrit alors :

$$P \ = \ \prod_{\sigma \in I_{L/K}} X - \sigma(\pi)$$

et

$$\begin{aligned} P'(\pi) \ &= \ \sum_{\sigma \in I_{L/K}} \prod_{\tau \in I_{L/K} \ , \ \tau \neq \sigma} \pi - \tau(\pi) \\ &= \ \prod_{\tau \in I_{L/K} \ , \ \tau \neq \mathrm{Id}} \pi - \tau(\pi) \ . \end{aligned}$$

On en déduit que

$$\begin{aligned} v_L(P'(\pi)) &= \sum_{\tau\in I_{L/K}\ ,\ \tau\neq \mathrm{Id}} v_L(\pi-\tau(\pi)) \\ &= \sum_{\tau\in I_{L/K}\ ,\ \tau\neq \mathrm{Id}} 1+i_{L/}(K)\tau \\ &= e_{L/K}-1+\sum_{\tau\in I_{L/K}\ ,\ \tau\neq \mathrm{Id}} i_{L/K}(\tau)\ . \end{aligned}$$

Or, pour tout $\sigma\in I_{L/K}\setminus G_1, i_{L/K}(\sigma)\ =\ 0$ si bient que

$$v_L(P'(\pi))\ =\ e_{L/K}-1+\sum_{\tau\in G_1\ ,\ \tau\neq \mathrm{Id}} i_{L/K}(\tau)\ .$$

Il suffit ensuite d'appliquer le lemme III.3.2.20 pour conclure. *q.e.d*

Lemme III.3.2.27. *Soit r un anneau de dedekind. Pour tout idéal maximal $\mathfrak{m}\in \mathrm{Spm}(R)$ de R, on note $\widehat{R_{\mathfrak{m}}}$ le séparé complété de R en $\mathfrak{m}$ (cf. III.2.1.13[14].) On note encore (un peu abusivement,) $\mathfrak{m}$ l'idéal maximal de $R_{\mathfrak{m}}$ et de $\widehat{R_{\mathfrak{M}}}$.*
i) Pour tout idéal maximal $\mathfrak{m}\in \mathrm{Spm}(R)$ de R, les applications

$$\begin{aligned} \mathcal{I}(R)\ &\to\ \mathcal{I}(R_{\mathfrak{m}}) \quad ,\quad \mathfrak{I}\mapsto \mathfrak{I}\otimes_R R_{\mathfrak{m}} \\ \mathcal{I}(R_{\mathfrak{m}})\ &\to\ \mathcal{I}(\widehat{R_{\mathfrak{m}}}) \quad ,\quad \mathfrak{I}\mapsto \mathfrak{I}\otimes_{R_{\mathfrak{m}}} \widehat{R_{\mathfrak{m}}} \\ \mathcal{I}(R)\ &\to\ \mathcal{I}(\widehat{R_{\mathfrak{m}}}) \quad ,\quad \mathfrak{I}\mapsto \mathfrak{I}\otimes_R \widehat{R_{\mathfrak{m}}} \end{aligned}$$

forment un triangle commutatif de morphismes de groupes :

$$\begin{array}{ccc} \mathcal{I}(R) & \to & \mathcal{I}(R_{\mathfrak{m}}) \\ & \searrow & \\ & & \mathcal{I}(\widehat{R_{\mathfrak{m}}})\ . \end{array}$$

ii) De plus, pour tout idéal maximal $\mathfrak{m}\in \mathrm{Spm}(R)$ de R, et tout idéal fractionnaire $\mathfrak{I}\in\mathcal{I}(R)$ de R,

$$v_{\mathfrak{m}}(\mathfrak{I})\ =\ v_{\mathfrak{m}}(\mathfrak{I}\otimes_R R_{\mathfrak{m}})\ =\ v_{\mathfrak{m}}(\mathfrak{I}\otimes_R \widehat{R_{\mathfrak{m}}})\ .$$

Preuve : Laissée en exercice. *q.e.d*

Dans toute la fin de cette section (III.3.2,) A est un anneau de Dedekind et K son corps des fractions. On suppose que, pour tout $\mathfrak{p}\in\mathrm{Spm}(A)$, le corps résiduel en $A/\mathfrak{p}$ en $\mathfrak{p}$ est parfait et on note $\widehat{A_{\mathfrak{p}}}$ le séparé complété de A en $\mathfrak{p}$ (cf. III.2.1.13,) et $K_{\mathfrak{p}}$ son corps des fractions (qui se trouve être un corps local.) On note $v_{\mathfrak{p}}$ l'unique valuation discrète normalisée de K

[14] Idéalement ce lemme trouverait plutôt sa place au paragraphe III.2.1

dont $A_\mathfrak{p}$ est l'anneau de valuation et encore $v_\mathfrak{p}$ la valuation discrète normalisée sur $K_\mathfrak{p}$ qui la prolonge.

Soient $K \subset L$ une extension finie séparable de K et B la fermeture intégrale de A dans L. Étant donné un idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A, on note $\mathfrak{q}_i\ ,1\leq i\leq g_\mathfrak{p} \in \mathrm{Spm}(B)$ les idéaux maximaux de B au-dessus de $\mathfrak{p}$ (cf. III.1.2.4,)

$$\widehat{B_\mathfrak{p}} := B \otimes_A \widehat{A_\mathfrak{p}}\ ,\ L_\mathfrak{p} := L \otimes_K K_\mathfrak{p},$$

$\widehat{B_{\mathfrak{q}_i}}\ ,1\leq i\leq g_\mathfrak{p}$ le séparé complété de B en $\mathfrak{q}_i$ et $\widehat{L_{\mathfrak{q}_i}}\ ,1\leq i\leq g_\mathfrak{p}$ son corps des fractions.

Lemme III.3.2.28. *On définit une application*

$$\begin{array}{rccc} \mathrm{Tr}_{L_\mathfrak{p}/K_\mathfrak{p}} : & L_\mathfrak{p} & \to & K_\mathfrak{p} \\ & (\alpha_1,\ldots,\alpha_{g_\mathfrak{p}}) & \mapsto & \sum_{=i}^{1} g_\mathfrak{p} \mathrm{Tr}_{\widehat{L_{\mathfrak{q}_i}}/K_\mathfrak{p}}(\alpha_i)\ . \end{array}$$

On a alors un diagramme commutatif

$$\begin{array}{ccc} L & \lambda^L & L_\mathfrak{p} \\ {\scriptstyle \mathrm{Tr}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{L_\mathfrak{p}/K_\mathfrak{p}}} \\ K & \lambda^K & K_\mathfrak{p}\ . \end{array}$$

Définition III.3.2.29. Un idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$ au-dessus de $\mathfrak{p} \in \mathrm{Spm}(A)$ est *non-ramifié* si $e_{\mathfrak{q}/\mathfrak{p}} = 1$. Un idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ est *non-ramifié* si tous les idéaux maximaux de B au-dessus de $\mathfrak{p}$ sont non-ramifiés au sens précédent.

Théorème III.3.2.30. *Soit A un anneau de Dedekind, K son corps des fractions, $K \subset L$ une extension finie séparable et B la fermeture intégrale de A dans L.*

i) Pour tout idéal maximal $\mathfrak{q} \in \mathrm{Spm}(B)$ de B,

$$v_\mathfrak{q}(\mathcal{D}_{B/A}) = v_\mathfrak{q}(\mathcal{D}_{\widehat{B_\mathfrak{q}}/\widehat{A_\mathfrak{p}}})\ .$$

ii) Pour tout $\mathfrak{q} \in \mathrm{Spm}(B)$, $v_\mathfrak{q}(\mathcal{D}_{B/A}) = 0$ si et seulement si $\mathfrak{q}$ est non ramifié.
De plus,si $\mathfrak{p} = \mathfrak{q} \cap A$,

$$v_\mathfrak{q}(\mathcal{D}_{B/A}) \geq e_{\mathfrak{q}/\mathfrak{p}} - 1 \qquad \textit{III.3.2.30.1}$$

avec égalité si et seulement si la caractéristique du corps résiduel $A/\mathfrak{p}$ ne divise pas l'indice de ramification $e_{\mathfrak{q}/\mathfrak{p}}$.

iii) Pour tout idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ de A,

$$v_\mathfrak{p}\big(\mathfrak{d}_{B/A}\big) = \sum_{\mathfrak{q}\in\mathrm{Spm}(B)\ ,\ \mathfrak{q}|\mathfrak{p}} v_\mathfrak{p}\big(\mathfrak{d}_{\widehat{L_\mathfrak{q}}/K_\mathfrak{p}}\big)\ .$$

iv) Un idéal maximal $\mathfrak{p} \in \mathrm{Spm}(A)$ *de* A *est non-ramifié si et seulement si*

$$v_{\mathfrak{p}}\big(\mathfrak{d}_{B/A}\big) \;=\; 0\;.$$

Preuve :
i) Est une conséquence des lemmes III.3.2.27 et III.3.2.28.
ii) Notons $\mathfrak{p} \;:=\; \mathfrak{q} \cap A$ et $\widehat{L_{\mathfrak{q}}}$ le corps des fractions de $\widehat{B_{\mathfrak{q}}}$ si bien que $K_{\mathfrak{p}} \subset \widehat{L_{\mathfrak{q}}}$ est une extension de corps locaux. On a $v_{\mathfrak{q}}(\mathcal{D}_{B/A}) \;=\; 0$ si et seulement si $v_{\mathfrak{q}}(\mathcal{D}_{Bqh/\widehat{A_{\mathfrak{p}}}}) \;=\; 0$ en vertu de III.3.2.30.i. Ceci équivaut encore (puisque $\mathfrak{q}$ est le seul idéal maximal de $\widehat{B_{\mathfrak{q}}}$ au-dessus de l'idéal maximal $\mathfrak{p}$ de $\widehat{A_{\mathfrak{p}}}$,) à $v_{\mathfrak{p}}[\mathrm{N}_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}(\mathcal{D}_{\widehat{B_{\mathfrak{q}}}/\widehat{A_{\mathfrak{p}}}})] \;=\; 0$ ce qui équivaut encore, grâce à III.3.2.18.2, à

$$v_{\mathfrak{p}}(\mathfrak{d}_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}) \;=\; 0\;.$$

Cette dernière égalité équivaut au fait que l'extension $K_{\mathfrak{p}} \subset \widehat{L_{\mathfrak{q}}}$ est non ramifiée en vertu de III.3.2.21.i, c'est-à-dire que $e_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}} \;=\; 1$. Or d'après III.2.2.7.5, $e_{\mathfrak{q}/\mathfrak{p}} \;=\; e_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}$ ce qui prouve le résultat.

La majoration III.3.2.30.1 s'obtient par des arguments tout à fait analogues en utilisant III.3.2.21.ii.
iii) On a

$$v_{\mathfrak{p}}(\mathfrak{d}_{B/A}) \;=\; v_{\mathfrak{p}}(\mathrm{N}_{L/K}(\mathcal{D}_{B/A}))$$

grâce à III.3.2.18.2 c'est-à-dire

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}_{B/A}) \;&=\; v_{\mathfrak{p}}\big(\mathrm{N}_{L/K}\big(\prod_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{v_{\mathfrak{q}}(\mathcal{D}_{B/A})}\big)\big) \\ &=\; v_{\mathfrak{p}}\big(\prod_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}v_{\mathfrak{q}}(\mathcal{D}_{B/A})}\big) \\ &=\; \sum_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}v_{\mathfrak{q}}(\mathcal{D}_{B/A})\;. \end{aligned}$$

En appliquant III.3.2.30.i et III.2.2.7.5 on obtient

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}_{B/A \;&=\; \sum_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} f_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}v_{\mathfrak{q}}(\mathcal{D}_{\widehat{B_{\mathfrak{q}}}/\widehat{A_{\mathfrak{p}}}}) \\ &=\; \sum_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} v_{\mathfrak{p}}\big(\mathrm{N}_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}(\mathcal{D}_{\widehat{B_{\mathfrak{q}}}/\widehat{A_{\mathfrak{p}}}})\big) \\ &=\; \sum_{\mathfrak{q}\in\mathrm{Spm}(B)\;,\;\mathfrak{q}|\mathfrak{p}} v_{\mathfrak{p}}\big(\mathfrak{d}_{\widehat{L_{\mathfrak{q}}}/K_{\mathfrak{p}}}\big) \end{aligned}$$

la dernière égalité résultant une fois encore de III.3.2.18.2.
iv) Est une conséquence immédiate des points précédents.
q.e.d

III.3.3 . −Le groupe de Picard d'un corps de nombres

Dans cette section (III.3.3,) K **est un corps de nombres c'est-à-dire une extension finie de** $\mathbb{Q}$. **On note** $d := [K : \mathbb{Q}]$ **le degré de l'extension et** $\mathcal{O}_K$ **son anneau d'entiers. Pour tout idéal fractionnaire** $\mathfrak{I} \in \mathcal{I}(\mathcal{O}_K)$ **de** $\mathcal{O}_K$, $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{I})$ **(cf. III.3.2.7,) est un idéal fractionaire de** $\mathbb{Z}$ **qui est donc, puisque** $\mathbb{Z}$ **est un anneau principal, de la forme** $a\mathbb{Z}$ **avec** $a \in \mathbb{Q}$. **On notera**

$$N(\mathfrak{I}) := |\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{I})| := |a|$$

où $|\cdot|$ **est la valeur absolue archimédienne sur** $\mathbb{Q}$.

Lemme III.3.3.1. *Étant donnée* $(e_1, \ldots, e_d)$ *une* $\mathbb{Q}$*-base de* K, *il existe* $c > 0$ *tel que, pour tout* d*-uplet* $(a_1, \ldots, a_d)$ *d'éléments de* $\mathbb{Q}$,

$$|\mathrm{N}_{K/\mathbb{Q}}(\sum_{i=1}^{d} a_i e_i)| \leq c \sup\{|a_i|^d\}_{1 \leq i \leq d} .$$

Preuve : Notons σ_i ,$_{1 \leq i \leq d}$ des $\mathbb{Q}$-plongements de K dans une extension bien choisie. Pour tout d-uplet $(a_1, \ldots, a_d)$ d'éléments de $\mathbb{Q}$,

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(\sum_{i=1}^{d} a_i e_i) &= \prod_{j=1}^{d} \sum_{i=1}^{d} \sigma_j(a_i e_i) \\ &= \prod_{j=1}^{d} \sum_{i=1}^{d} a_i \sigma_j(e_i) . \end{aligned}$$

À partir de quoi, le résultat est élémentaire. *q.e.d*

Lemme III.3.3.2. *Il existe* $c > 0$ *(ne dépendant que de* K,$)$ *tel que pour tout idéal* $\mathfrak{I}$ *de* $\mathcal{O}_K$ *il existe* $\gamma \in \mathfrak{I}$ $\gamma \neq 0$, *tel que*

$$|\mathrm{N}_{K/\mathbb{Q}}(\gamma)| \leq cN(\mathfrak{I}) .$$

Preuve : Soient $(e_1, \ldots, e_d)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$ et

$$E := \{\sum_{i=1}^{d} a_i e_i \mid a_i \in \mathbb{Z} \text{ et } 0 \leq a_i \leq N(\mathfrak{I})^{\frac{1}{d}}\} .$$

i) Si δ est le plus grand entier inférieur à $N(\mathfrak{I})^{\frac{1}{d}}$, on a $\delta + 1 > N(\mathfrak{I})^{\frac{1}{d}}$, d'où $(\delta + 1)^d > N(\mathfrak{I})$, d'où

$$\#(E) > N(\mathfrak{I}) .$$

ii) La composée des applications

$$E \longrightarrow \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{I}$$

ne peut donc être injective puisque $\#(\mathcal{O}_K/\mathfrak{I}) = N(\mathfrak{I})$ (c'est une conséquence du théorème chinois des restes.)

iii) Il existe α et β différents dans E qui ont la même image modulo $\mathfrak{I}$ ce qui signifie que $\alpha - \beta \in \mathfrak{I}$. Posons

$$\gamma := \alpha - \beta = \sum_{i=1}^{d} (a_i - b_i)e_i$$

et $|a_i - b_i i| \leq N(I)^{\frac{1}{d}}$. En appliquant le lemme III.3.3.1 à γ, on obtient précisément que

$$|\mathrm{N}_{K/\mathbb{Q}}(\gamma)| \leq cN(\mathfrak{I}) .$$

q.e.d

Lemme III.3.3.3. *Pour tout idéal fractionnaire $\mathfrak{I} \in \mathcal{I}(\mathcal{O}_K)$ de $\mathcal{O}_K$, il existe $\alpha \in K^\times$, tel que $\alpha\mathfrak{I} = \mathfrak{J}^{-1}$ où $\mathfrak{J}$ est un idéal de $\mathcal{O}_K$ tel que $N(\mathfrak{J}) \leq c$.*

Preuve : Pour tout idéal fractionnaire $\mathfrak{I}$ de $\mathcal{O}_K$, il existe $\alpha_0 \in \mathcal{O}_K$ tel que $\alpha_0\mathfrak{I}$ est un idéal de $\mathcal{O}_K$ (cf. I.1.5.3.) Quitte donc à remplacer $\mathfrak{I}$ par $\alpha_0\mathfrak{I}$, on peut supposer que $\mathfrak{I}$ est un idéal.

Il existe donc, d'après le lemme III.3.3.2, $\gamma \in \mathfrak{I}$, $\gamma \neq 0$, tel que $|\mathrm{N}_{K/\mathbb{Q}}(\gamma)| \leq cN(\mathfrak{I})$.

Posons alors $\mathfrak{J}^{-1} := \gamma^{-1}\mathfrak{I}$. Comme $\gamma \in \mathfrak{I}$, $\mathfrak{J} = \gamma\mathfrak{I}^{-1}$ est bien un idéal de $\mathcal{O}_K$ et on a

$$\begin{aligned} N(\mathfrak{J}) &= |\frac{\mathrm{N}_{K/\mathbb{Q}}(\gamma)}{N(\mathfrak{I})}| \\ &\leq c . \end{aligned}$$

q.e.d

Théorème III.3.3.4. *Pour $K/\mathbb{Q}$ un corps de nombres, c'est-à-dire une extension finie de degré d de $\mathbb{Q}$, le groupe de Picard $\mathrm{Pic}(\mathcal{O}_K)$ (cf. III.1.1.14) est un groupe fini.*

Preuve :

Fixons $c > 0$ défini comme en III.3.3.2. Le lemme III.3.3.3 signifie alors que tout élément x de $\mathrm{Pic}(\mathcal{O}_K)$ c'est-à-dire toute classe d'idéaux fractionnaires de $\mathcal{O}_K$, contient un élément $\mathfrak{I} \in x$ tel que $\mathfrak{I}^{-1} \subset \mathcal{O}_K$ est un idéal $N(\mathfrak{I}^{-1}) \leq c$.

Si l'on note

$$\mathcal{I}(\mathcal{O}_K)^c := \{\mathfrak{I} \in \mathcal{I}(\mathcal{O}_K) \mid \mathfrak{I} \subset \mathcal{O}_K \ , \ N(\mathfrak{I}) \leq c\} \subset \mathcal{I}(\mathcal{O}_K),$$

on a construit une application injective

$$\mathrm{Pic}(\mathcal{O}_K) \hookrightarrow \mathcal{I}(\mathcal{O}_K)^c .$$

Pour tout $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$, il existe un unique nombre premier $p \in \mathbb{Z}$ tel que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Notons $f_{\mathfrak{p}/p}$ le degré résiduel de $\mathfrak{p}$. Tout idéal de $\mathcal{O}_K$ s'écrit

$$\mathfrak{I} = \prod_{\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{I})},$$

les $v_{\mathfrak{p}}(\mathfrak{I})$ étant presque tous nuls et positifs. Il en résulte que pour tout $\mathfrak{I} \in \mathcal{I}(\mathcal{O}_K)$,

$$\begin{aligned} N(\mathfrak{I}) &= |\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{I})| \\ &= |\mathrm{N}_{K/\mathbb{Q}}(\prod_{\mathfrak{p}\in \mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{I})})| \\ &= |\prod_{p\in \mathrm{Spm}(\mathbb{Z})\ ,\ \mathfrak{p}|p} p^{f_{\mathfrak{p}/p} v_{\mathfrak{p}}(\mathfrak{I})}| \ . \end{aligned}$$

Il est immédiat de voir que cette formule entraîne que $\mathcal{I}(\mathcal{O}_K)^c$ est fini. *q.e.d*

III.3.4 . −Le théorème de Minkowski (1896)

Dans cette section (III.3.4,) K est un corps de nombres c'est-à-dire une extension finie du corps $\mathbb{Q}$ des rationnels. On note $d := [K : \mathbb{Q}]$ le degré de K sur $\mathbb{Q}$.

On note $\mathbb{C}$ le corps des complexes et $\gamma : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe. On fixe d plongements

$$\sigma_i : K \to \mathbb{C}\ ,_{1\leq i\leq d}$$

deux à deux distincts.

Définition III.3.4.1. Pour tout $1 \leq i \leq d$, si $\gamma \circ \sigma_i = \sigma_i$, on dit que σ_i est un *plongement réel* sinon on dit que σ_i est un *plongement complexe*.

Lemme III.3.4.2. *Pour tout $1 \leq i \leq d$, si σ_i est un plongement complexe, $\gamma \circ \sigma_i$ est encore un plongement complexe distinct de σ_i si bien que le nombre de plongements complexes est pair.*

Définition III.3.4.3. Étant donné un $\mathbb{Q}$-espace vectoriel (resp. $\mathbb{R}$-espace vectoriel) V de dimension finie δ, on appellera *$\mathbb{Z}$-réseau* de V un sous-$\mathbb{Z}$-module libre de rang δ de V.

Lemme III.3.4.4. *Étant donné un $\mathbb{Z}$-réseau Λ d'un $\mathbb{Q}$-(resp. $\mathbb{R}$)-espace vectoriel V de dimension finie δ, et $\lambda_i\ ,_{1\leq i\leq \delta}$ une $\mathbb{Z}$-base de Λ, on note*

$$F(\Lambda, \lambda_1, \ldots, \lambda_\delta) := \{\sum_{i=1}^{\delta} a_j\lambda_j\}_{0\leq a_j<1\ ,\ \forall 1\leq j\leq d} \ .$$

i) L'ensemble $F(\Lambda, \lambda_1, \ldots, \lambda_\delta)$ est indépendant du choix de la base $\lambda_i\ ,_{1\leq i\leq \delta}$ de Λ.

ii)

$$V = \coprod_{\lambda\in\Lambda} F + \lambda \ .$$

Définition III.3.4.5. Soit Λ un $\mathbb{Z}$-réseau d'un $\mathbb{Q}$-(resp. $\mathbb{R}$)-espace vectoriel V de dimension finie δ.

i) L'ensemble $F(\Lambda, \cdot, \ldots, \cdot)$ défini dans le lemme III.3.4.4 sera simplement noté $F(\Lambda)$ et appelé *domaine fondamental* de Λ.

ii) Une base orthonormée $\mathcal{B}$ de V étant fixée, on note $\mu(V/\Lambda)$ ou encore $\mu(F(\Lambda))$ qu'on appelle *volume du réseau* ou *volume du domaine fondamental* le nombre

$$|\det(\lambda_1, \ldots, \lambda_\delta)_{\mathcal{B}}|$$

où $\lambda_{i\ ,1\leq i\leq \delta}$ est une $\mathbb{Z}$-basede Λ.

Définition III.3.4.6. Pour une partie $\Delta \subset V$ d'un $\mathbb{R}$-espace vectoriel normé de dimension finie V, on note $\mathrm{Vol}(V)$ son volume relativement à la métrique induite par la norme.

On dit que Δ est *convexe* si pour tout couple de points (x, y) dans Δ le segment $[x; y]$ est contenu dans Δ ; Δ est *symétrique* si pour tout $x \in \Delta$, $-x \in \Delta$.

Proposition III.3.4.7. *Soient V un $\mathbb{Q}$-(resp. $\mathbb{R}$)-espace vectoriel normé de dimension finie δ et Λ un $\mathbb{Z}$-réseau de V.*

Si Δ est une partie fermée bornée convexe symétrique de V telle que

$$\mathrm{Vol}(\Delta) \geq 2^\delta \mu(V/\Lambda)\ ,$$

alors il existe un point non nul dans $\Lambda \cap \Delta$.

Preuve :
i) Supposons que $\mathrm{Vol}(\Delta) > 2^\delta \mu(V/\Lambda)$. Posons

$$\frac{1}{2}\Delta\ :=\ \{\frac{x}{2}\ ,\ x \in \Delta\}\ ,$$

d'où il résulte que $\mathrm{Vol}(\frac{1}{2}\Delta)\ =\ \frac{1}{2}^\delta \mathrm{Vol}(\Delta)$. Or

$$\frac{1}{2}\Delta\ =\ \coprod_{\lambda\in\Lambda}(\lambda + F) \cap \frac{1}{2}\Delta\ .$$

en particulier,

$$\begin{aligned}\mathrm{Vol}(\frac{1}{2}\Delta)\ &=\ \sum_{\lambda\in\Lambda}\mathrm{Vol}((\lambda + F) \cap \frac{1}{2}\Delta)\\ &=\ \sum_{\lambda\in\Lambda}\mathrm{Vol}(F \cap (-\lambda + \frac{1}{2}\Delta))\ .\end{aligned}$$

Or

$$\mathrm{Vol}(\frac{1}{2}\Delta)\ >\ \mathrm{Vol}(F)\ =\ \mu(V/\Lambda)\ .$$

Il existe donc des éléments α et β de Λ distincts tels que $-\alpha + \frac{1}{2}\Delta\ \cap\ -\beta + \frac{1}{2}\Delta\ \neq\ \emptyset$ c'est-à-dire qu'il existe des éléments x et y de Δ tels que $-\alpha + \frac{x}{2}\ =\ -\beta + \frac{y}{2}$ c'est-à-dire que $\frac{1}{2}(x - y)\ =\ \alpha - \beta\ \in \Lambda$ et $\alpha - \beta\ \neq\ 0$. De plus, Δ étant convexe et symétrique, $\frac{1}{2}(x - y) \in \Delta$.
ii) Si $\mathrm{Vol}(\Delta) = 2^\delta \mu(V/\Lambda)$ on considère $(1 + \epsilon)\Delta$, pour $\epsilon > 0$. Il s'ensuit que

$$\mathrm{Vol}((1 + \epsilon)\Delta)\ >\ 2^\delta \mu(V/\Lambda)\ \forall \epsilon > 0\ .$$

Il s'ensuit que l'ensemble

$$E_\epsilon \ := \ (1+\epsilon)\Delta \ \cap \ (\Lambda \setminus \{0\}$$

est non vide et fini d'après le point précédent. Pour $\epsilon \ = \ \frac{1}{n}$,$_{n\in\mathbb{N}}$, à partir d'un certain rang le cardinal de $E_{\frac{1}{n}}$ est stationnaire. Il y a donc des points non nuls de Λ dans

$$\bigcap_{n\in\mathbb{N}}(1+\frac{1}{n})\Delta \ = \ \Delta$$

puisque Δ est fermé.

q.e.d

Lemme III.3.4.8.
i) Si on note r_1 (resP. $2r_2$) le nombre de plongements réels (resp. complexes) de K dans $\mathbb{C}$ on a un isomorphisme naturel

$$K \ \otimes_{\mathbb{Q}} \ \mathbb{R} \ \cong \ \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ .$$

ii) Si Λ est un $\mathbb{Z}$-réseau de K (vu comme $\mathbb{Q}$-espace vectoriel,) le plongement naturel

$$K \ \hookrightarrow \ K \otimes_{\mathbb{Q}} \mathbb{R}$$

fait de Λ un $\mathbb{Z}$-réseau de $K \otimes_{\mathbb{Q}} \mathbb{R}$.

Proposition III.3.4.9. *Pour tout $\mathbb{Z}$-réseau Λ de K,*

$$\mu((K \otimes_{\mathbb{Q}} \mathbb{R})/\Lambda) \ = \ 2^{-r_2}\sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|}$$

(où $2r_2$ est le nombre de plongements complexes de K.)

Preuve : Soit λ_i ,$_{1\leq i\leq d}$ une $\mathbb{Z}$-base de Λ. On note σ_j ,$_{1\leq j\leq r_1}$ les r_1 plongements réels, τ_j ,$_{1\leq j\leq r_2}$ les r_2 plongements complexes dans chacun des facteurs de $\mathbb{C}^{r_2}$ et $\overline{\tau}_j$,$_{1\leq j\leq r_2}$ les composés des précédents avec la conjugaison complexe. Il en résulte que si on note $\tau_j(\lambda_k)$,$_{1\leq j\leq r_2 \ , \ 1\leq k\leq d} \ = \ x_{jk} + iy_{jk}$ on a

$$\begin{aligned}
\sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|} &= |\det(\sigma_j(\lambda_k), x_{jk}+iy_{jk}, x_{jk}-iy_{jk})| \\
&= |\det(\sigma_j(\lambda_k), 2x_{jk}, x_{jk}-iy_{jk})| \\
&= 2^{r_2}|\det(\sigma_j(\lambda_k), x_{jk}, x_{jk}-iy_{jk})| \\
&= 2^{r_2}|\det(\sigma_j(\lambda_k), x_{jk}, -iy_{jk})| \\
&= 2^{r_2}\det(\sigma_j(\lambda_k), x_{jk}, y_{jk}) \ .
\end{aligned}$$

En prenant pour base de $K \otimes_{\mathbb{Q}} \mathbb{R}$, la base e_j ,$_{1\leq j\leq d}$ formée de tous les d-uplets dont toutes les composantes sont nulles exceptée

- la $j^{\text{ième}}$ qui vaut 1 pour $1 \leq j \leq r_1 + r_2$;
- la $j - r_2{}^{\text{ième}}$ qui vaut i pour $r_1 + r_2 < j \leq d$

on montre que le déterminant ci-dessus est exactement $\mu((K \otimes_{\mathbb{Q}} \mathbb{R})/\Lambda)$. *q.e.d*

Théorème III.3.4.10. *Étant donné un corps de nombre K de degré d, on note r_1 le nombre de plongements réels et $2r_2$ le nombres de plongements complexes de sorte que $d = r_1 + 2r_2$. On note*

$$C_k := (\frac{4}{\pi})^{r_2} \frac{d!}{d^\delta}$$

qu'on appelle la constante de Minkowski.

Alors pour tout $\mathbb{Z}$-réseau Λ de K, il existe $\lambda \in \Lambda$ tel que

$$|\mathrm{N}_{K/\mathbb{Q}}(\lambda)| \leq C_K \sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|}$$

(où $\mathfrak{d}^{\mathbb{Z}}_{K/Q}(\Lambda)$ est le discriminant défini en III.3.2.13.)

Preuve : D'après les propositions III.3.4.7 et III.3.4.9, si Δ est une partie convexe symétrique de $K \otimes_{\mathbb{Q}} \mathbb{R}$, telle que

$$\mathrm{Vol}(\Delta) \geq 2^{d-r_2} \sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|},$$

il existe $\lambda \neq 0$ tel que $\lambda \in \Delta \cap \Lambda$.

Pour $a > 0$ réel on pose

$$\Delta_a := \{x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mid \sum_{j=1}^{r_1} |x_j| + 2 \sum_{j=1}^{r_2} |z_j| \leq a\} .$$

On a naturellement $\mathrm{Vol}(\Delta_a) = a^d \mathrm{Vol}(\Delta_1)$ et $\mathrm{Vol}(\Delta_1) = \frac{2^{r_1-r_2}}{d!}\pi^{r_2}$. $\mathrm{Vol}(\Delta_a) = 2^d \mu(V/\Lambda)$ équivaut à

$$a^d \frac{2^{r_1-r_2}}{d!}\pi^{r_2} = 2^{d-r_2} \sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|}$$

ce qui équivaut à

$$a^d = (\frac{4}{\pi})^{r_2} d! \sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|} .$$

Il existe alors $\lambda \in \Lambda$ non nul, tel que $\lambda \in \Delta_a$.

Or our tout $x \in \Delta_a$,

$$\begin{aligned} |\mathrm{Tr}_{L/\mathbb{Q}}(x)| &= |\sum_{j=1}^{r_1} x_j + \sum_{j=1}^{r_2} z_j + \sum_{j=1}^{r_2} \overline{z_j}| \\ &\leq \sum_{j=1}^{r_1} |x_j| + 2\sum_{j=1}^{r_2} |z_j| \\ &\leq a . \end{aligned}$$

Sur le modèle de la remarque ci-dessus, on peut majorer la norme d'un élément de Δ_a en vertu du fait que la moyenne géométrique de d nombres positifs, est toujours inférieure à leur moyenne arithmétique. Il en résulte que pour $x \in \Delta_a$,

$$|\mathrm{N}_{L/\mathbb{Q}}(x)| \leq \frac{a^d}{d^d} = (\frac{4}{\pi})^{r_2} \frac{d!}{d^d} \sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\Lambda)|} .$$

q.e.d

Corollaire III.3.4.11. *Pour tout idéal fractionnaire $\mathfrak{J} \in \mathcal{I}(\mathcal{O}_K)$ de K, il existe $\lambda \in K^*$ tel que $\lambda\mathfrak{J} \subset \mathcal{O}_K$ est un « vrai » idéal, et*

$$|\mathrm{N}_{K/\mathbb{Q}}(\lambda\mathfrak{J})| \leq C_K\sqrt{|\mathfrak{d}_{K/\mathbb{Q}}|}\,.$$

Preuve : Quitte à remplacer $\mathfrak{J}$ par $b\mathfrak{J}$ on peut supposer que $\mathfrak{J}^{-1}$ est un vrai idéal. D'après minkowski il existe $\lambda \in \mathfrak{J}^{-1}$ $\lambda \neq 0$ tel que

$$\mathrm{N}_{K/\mathbb{Q}}(\lambda) \;\leq\; C_K\sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\mathfrak{J}^{-1})|}\,.$$

On peut écrire $\lambda = \mathfrak{J}^{-1}\mathfrak{J}'$. Comme $\lambda \in \mathfrak{J}^{-1}$, $\mathfrak{J}'$ est un idéal de $\mathcal{O}_K$. Il en résulte que

$$N(\mathfrak{J}^{-1})N(\mathfrak{J}') \;=\; |\mathrm{N}_{K/\mathbb{Q}}(\lambda)| \;\leq\; C_K\sqrt{|\mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\mathfrak{J}^{-1})|} \;=\; C_K N(\mathfrak{J}^{-1})\sqrt{|\delta_{K/\mathbb{Q}}(\mathcal{O}_K)|}$$

la dernière égalité résultant de III.3.2.18.2.

Il en résulte que $N(\mathfrak{J}') \leq C_K\sqrt{|\mathfrak{d}_{K/\mathbb{Q}}|}$ et $\mathfrak{J}' = \lambda\mathfrak{J}$ par définition. *q.e.d*

Remarque III.3.4.12. Ce résultat entraîne en particulier la finitude du nombre de classe (cf. III.3.3.4,) et la borne obtenue ici est bien meilleure en général que celle obtenue dans le lemme III.3.3.3.

Corollaire III.3.4.13. *Si $K \neq \mathbb{Q}$, $\mathfrak{d}_{K/\mathbb{Q}} > 1$, ce qui revient à dire qu'il existe au moins un nombre premier ramifié en vertu de III.3.2.30.ii.*

Table des matières

Index