Extensions Galoisiennes

Florent Mayencourt

Professeur : Bayer Fluckiger Eva

Sous la direction de Pickett Erik Jarl

EPFL, Semestre d'hivers 2009

La mathématique est une science dangereuse :
elle dévoile les supercheries et les erreurs de calcul.
Galile

Résumé

Le titre de ce travail résume assez mal un projet hétéroclite. Nous commencerons par rappeler quelques éléments sur les polynômes. Puis nous présenterons la notion de domaine de Dedekind. Nous verrons ensuite comment une métrique sur ces domaines, puis comment les compléter. Nous exhiberons un exemple par le corps des p-adiques. Nous finirons ce travail en traitant des extensions, notamment galoisiennes, d'un corps complet.

Table des matières

CHAPITRE 1

Rappels

1.1 Anneaux des polynômes

Nous ferons ici quelques rappels utiles pour la suite du travail, et nous en profiterons pour fixer nos notations. Nous suivrons principalement le livre de théorie algébrique des nombres de A. Fröhlich et M.J. Taylor [1].
F décrit un corps, $F[X]$ l'anneau des polynômes à une variable à coefficient dans F. Pour éviter des lourdeurs dans le texte, les anneaux intègres seront appelé *domaines*, en accord avec le terme anglais.

Définition 1.1.1
$f \in F[X]$ est dit séparable *si dans une extension assez grande, toutes ses racines sont distinctes.*
Soit f un polynôme unitaire, f' sa dérivée formelle et $\{a_j\}_{j=1}^n$ ses racines. On définit le discriminant *de f par*

$$\operatorname{Disc} f = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} f'(a_j).$$

Théorème 1.1.2
f est séparable si et seulement si $\operatorname{Disc}(f) \neq 0$.

Définition 1.1.3
F est dit parfait *si tout polynôme irréductible est séparable.*

Théorème 1.1.4
Tout corps de caractéristique nul est parfait.
Tout corps fini est parfait.

Théorème 1.1.5 (Théorème de l'élément primitif)
Soit $E = F(\alpha, \beta)$, α, β algébriques sur F et α séparable sur F (i.e. le polynôme minimal de α, noté $m_{F,\alpha}$, est séparable).
Alors il existe $\gamma \in F$ tel que $E = F(\gamma)$.

Théorème 1.1.6
Soient E/F une extension de corps de degré n, L un corps algébriquement clos et σ un homomorphisme de corps de F dans L. Alors il existe n homomorphismes distincts σ_j de E dans L dont la restriction à F est σ.

Définition 1.1.7
Pour un élément $\alpha \in E/F$, on définit la trace

$$t_{E/F} = \sum_i \alpha^{\sigma_i},$$

la norme

$$N_{E/F} = \prod_i \alpha^{\sigma_i}$$

et le polynôme caractéristique

$$c_{E/F,\alpha}(X) = \prod_i (X - \alpha^{\sigma_i}).$$

Pour $\{u_i\}$ une F base de E, on définit le discriminant *par*

$$d(v_1, \ldots, v_n) = \det(t_{E/F}(u_i u_j)).$$

1.2 F-Algèbres

Remarquons qu'une F-algèbre finie commutative est un anneau commutatif A contenant F comme sous-anneau avec la même identité multiplicative.

Définition 1.2.1
Un élément $e \in A$ est idempotent *si $e^2 = e$.*
Deux élément e et e' dans A sont orthogonaux si $ee' = 0$.

Remarque 1.2.2
Si A est isomorphe à un produit d'anneaux, i.e. $A \simeq \prod_{i=1}^{r} A_i$ avec multiplication par élément, on peut construire un système par

$$e_i = (0, \ldots, 0, 1_{A_i}, 0, \ldots, 0).$$

On remarque que $e_i^2 = e_i$, i.e. que e_i est idempotent et que pour $i \neq j$ $e_i e_j = 0$. Un tel système est appelé *système orthogonal idempotent.*

Définition 1.2.3
Un élément e idempotent est primitif *si il est non nul et que pour toute décomposition idempotente $e = e' + e''$ telle que $e'e'' = 0$ on a e' ou e'' est nul.*
Un élément $a \in A$ est nilpotent *s'il existe un naturel n tel que $a^n = 0$.*
Le radical *de A est l'ensemble de tous les éléments nilpotents, noté* $\mathrm{Rad}\,(A)$.
On peut montrer que c'est un idéal de A.

Théorème 1.2.4
Pour $\bar{A} = A/\mathrm{Rad}\,A$, on a :

(*i*) $\mathrm{Rad}\,(\bar{A}) = (0)$,
(*ii*) *A indécomposable si et seulement si $\bar{A}$ indécomposable.*

Théorème 1.2.5
Pour A une F-algèbre de degré fini, alors les assertions suivantes sont équivalentes :

(*i*) $\mathrm{Rad}\,(A) = (0)$,
(*ii*) *$A \simeq \prod(A_i)$ A_i un corps.*

Si de plus F est parfait

(*iii*) *$d(v_1, \ldots, v_n) \neq 0$ pour une certaine F-base de A,*
(*iv*) *$d(v_1, \ldots, v_n) \neq 0$ pour toutes F-base de A.*

Théorème 1.2.6
Pour K un corps contenant F et $f \in F[X]$ non constant, on a

$$A \otimes_F K \simeq K[X]/fK[X].$$

Théorème 1.2.7
Si A est une extension finie séparable de F, alors $A \otimes_F K$ est un produit d'extensions finies séparables de K.

1.3 Modules Noetheriens

Définition 1.3.1
Soit $\mathfrak{o}$ *un module et* $\mathfrak{D}$ *une extension. Remarquons que pour* $\{a_1, \ldots, a_n\} \subset \mathfrak{D}$, *alors* $(a_1, \ldots, a_n)\mathfrak{o}$ *est un* $\mathfrak{o}$*-sous module de* $\mathfrak{D}$ *engendré par les* a_i *et* $\mathfrak{o}$.
On dit qu'un élément $a \in \mathfrak{D}$ *est* entier de $\mathfrak{D}$ dans $\mathfrak{o}$ *s'il existe* $f \in \mathfrak{o}[X]$ *un polynôme unitaire tel que* $f(a) = 0$.
La clôture intégrale *d'un domaine* $\mathfrak{o}$ *est l'ensemble de tous les éléments de* $\mathfrak{D}$ *qui sont des entiers de* $\mathfrak{o}$.
Un domaine entiers $\mathfrak{o}$ *de corps de fractions* K *est dit* intégralement clos *s'il coïncide avec la clôture intégrale de* K.

Théorème 1.3.2
La clôture intégrale d'un domaine $\mathfrak{o}$ *est intégralement close.*

Définition 1.3.3
Un $\mathfrak{o}$*-module dont tous les* $\mathfrak{o}$*-sous modules sont de génération finie sur* $\mathfrak{o}$ *s'appelle un* $\mathfrak{o}$-module Noetherien.
De la même manière équivalente, un anneau Noetherien $\mathfrak{o}$ *est un* $\mathfrak{o}$*-module Noetherien, i.e. dont tous les idéaux sont de génération finie sur* $\mathfrak{o}$.

Théorème 1.3.4
Les assertions suivantes sont équivalentes :

(*i*) M *est un* $\mathfrak{o}$*-module Noetherien ;*

(*ii*) *chaque chaîne ascendante de* $\mathfrak{o}$*-sous modules de* M *se stabilise ;*

(*iii*) *chaque famille de* $\mathfrak{o}$*-sous modules de* M *contient un élément maximal (pour l'ordre partiel d'inclusion).*

Théorème 1.3.5
Soit

$$0 \longrightarrow M \xrightarrow{\rho} N \xrightarrow{\pi} P \longrightarrow 0$$

une suite exacte de $\mathfrak{o}$*-modules. Alors* N *est un* $\mathfrak{o}$*-module Noetherien si et seulement si* M *et* P *sont tous deux des* $\mathfrak{o}$*-modules Noetheriens.*
Soit $\mathfrak{o}$ *un anneau Noetherien et* M *un* $\mathfrak{o}$*-module de génération finie. Alors* M *est un* $\mathfrak{o}$*-module Noetherien.*
Soit $\phi : \mathfrak{o} \longrightarrow \mathfrak{R}$ *un homomorphisme surjectif d'anneau. Si* $\mathfrak{o}$ *est un anneau Noetherien, alors* $\mathfrak{R}$ *ausi et seulement si.*
Si $\mathfrak{o}$ *est un anneau Noetherien, alors l'anneau des polynômes à un nombre fini de variables sur* $\mathfrak{o}$ *est ausi et seulement si un anneau Noetherien.*
Si $\mathfrak{o}$ *est un anneau Noetherien et* $\mathfrak{o}$ *une extension de génération finie alors c'est un anneau Noetherien.*

1.4 Domaines de Dedekind

Définition 1.4.1
Un domaine intégrale $\mathfrak{o}$ *est un* domaine de Dedekind *si*

(*i*) $\mathfrak{o}$ *est un anneau Noetherien ;*

(*ii*) $\mathfrak{o}$ *est intégralement clos dans son corps des fractions* K *;*

(*iii*) *tous les idéaux non nuls premier de* $\mathfrak{o}$ *sont maximaux.*

Théorème 1.4.2
Un anneau principal est un domaine de Dedekind.

Définition 1.4.3
Soit $\mathfrak{o}$ *un domaine intégrale et* K *son corps de fractions. Un* idéal fractionnaire *est un* $\mathfrak{o}$*-sous module* $\mathfrak{b}$ *de* K *de la forme*

$$\mathfrak{b} = c\mathfrak{a} = \{x \in K \,|\, x = ca \text{ pour } a \in \mathfrak{a}\},$$

où $c \in K^\star$ *et* $\mathfrak{a}$ *un idéal non nul de* $\mathfrak{o}$.
On définit le produits de deux idéaux fractionnaires $\mathfrak{b}_1$ *et* $\mathfrak{b}_2$ *par le groupe additif contenant toutes les sommes finies* $\sum x_i y_i$ *telles que* $x_i \in \mathfrak{b}_1$ *et* $y_j \in (b)_2$.

Théorème 1.4.4
Tout idéal fractionnaire non nul $\mathfrak{a}$ *d'un domaine de Dedekind peut s'écrire comme produit d'idéaux premier, i.e.*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n.$$

De plus, cette décomposition est unique à l'ordre des facteurs près.

Lemme 1.4.5
Si $\mathfrak{o}$ *est un anneau Noetherien intégralement clos, alors*

$$R_\mathfrak{a} := \{x \in K \,|\, x\mathfrak{a} \subset \mathfrak{a}\} = \mathfrak{o}.$$

Démonstration. Soit $a_1, \dots, a_n$ les générateurs de $\mathfrak{a}$ sur $\mathfrak{o}$, et $b \in R_\mathfrak{a}$. Alors

$$ba_i = \sum_j c_{ij} a_j \text{ avec } c_{ij} \in \mathfrak{o}.$$

Ainsi $\det(b\dot{1}_n - (c_{ij}))(a_j) = 0$ pour tout j. b est donc racine du polynôme unitaire $\det(X\dot{1}_n - (c_{ij}))$ dont tous les coefficients sont dans $\mathfrak{o}$. Ainsi $b \in \mathfrak{o}$ par clôture intégrale.

q.e.d

Lemme 1.4.6
Si tous les idéaux premier d'un domaine intégral sont maximaux, alors si

$$\mathfrak{p} \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$$

où $\mathfrak{p}$ et $\mathfrak{p}_\mathfrak{j}$ sont des idéaux premiers non nuls, on a que $\mathfrak{p} = \mathfrak{p}_j$ pour un certain j.

Démonstration. Par récurrence sur r. Si $r = 1$, alors $\mathfrak{p} \supset \mathfrak{p}_1$ et donc par maximalité $\mathfrak{p} = \mathfrak{p}_1$.
Supposons maintenant vrai pour $r - 1 > 1$. Alors si $\mathfrak{p} \neq \mathfrak{p}_\mathfrak{r}$, alors il existe $c \in \mathfrak{p}_r$ tel que $c \notin \mathfrak{p}$. Soit $b \in \mathfrak{p}_1 \dots \mathfrak{p}_{r-1}$. Alors $bc \in \mathfrak{p}$ et comme $c \notin \mathfrak{p}$, puisque $\mathfrak{p}$ est premier, $b \in \mathfrak{p}$. Comme b est quelconque, $\mathfrak{p} \supset \mathfrak{p}_1 \dots \mathfrak{p}_{r-1}$.

q.e.d

Pour la suite, nous aurons besoin d'une notion supplémentaire : Un idéal non nul $\mathfrak{a}$ est *faiblement inversible* s'il existe $c \in \mathfrak{a}^{-1}$ tel que $c \notin \mathfrak{o}$. On notera $\mathcal{S}$ l'ensemble des idéaux faiblement inversibles. De plus, si $\mathfrak{o}$ n'est pas un corps, alors $\mathcal{S}$ n'est pas vide ; en effet, soit $a \in \mathfrak{o}\backslash\mathfrak{o}^\star$ non nul, alors (a) est faiblement inversible. On peut ausi et seulement si noter que (a) est inversible et que si $\mathfrak{o}$ est un anneau Noetherien, alors il possède des éléments maximaux.

Lemme 1.4.7
Soit $\mathfrak{o}$ un domaine de Dedekind qui n'est pas un corps et M un idéal non nul maximal dans $\mathcal{S}$. Alors M est un idéal premier inversible de $\mathfrak{o}$.

Démonstration. Voyons tout d'abord que M est un idéal premier. Soit $a \in \mathfrak{o}\backslash M$ et supposons que $b \in \mathfrak{o}$ tel que $ab \in M$. Par hypothèse, il existe $c \in M^{-1}\backslash d$ De plus, puisque M est maximal, alors $(M+a)c \not\subset \mathfrak{o}$, et donc puisque $Mc \subset M$, alors $ac \notin \mathfrak{o}$. Puisque $ab \in M$, alors $b(ac) = a(bc) = (ab)c \in \mathfrak{o}$. Ainsi $ac \in (b)^{-1}$ et, puisque $a \in \mathfrak{o}$, alors $ac \in M^{-1}$. Ainsi $M + b\mathfrak{o}$ est faiblement inversible, et par maximalité de M, $b \in M$.
Le lemme 1.4.5 nous dit que $M^{-1} \not\subset R_M$, et donc $MM^{-1} \not\subset M$. De plus $M \subset MM^{-1} \subset \mathfrak{o}$. Ainsi $MM^{-1} = \mathfrak{o}$ par maximalité de M.

q.e.d

Lemme 1.4.8
Soit $\mathfrak{o}$ un domaine de Dedekind. Un idéal non nul $\mathfrak{a}$ est inversible si et seulement si

$$\mathfrak{a} = \mathfrak{m}_1 \dots \mathfrak{m}_r$$

où les $\mathfrak{m}_j$ sont des idéaux premier inversibles de $\mathfrak{o}$.

Démonstration. Si $\mathfrak{a}$ est un produit d'idéaux premiers inversibles, alors $\mathfrak{a}^{-1} = \mathfrak{m}_1^{-1} \dots \mathfrak{m}_r^{-1}$.
Supposons maintenant que $\mathfrak{a}$ est un idéal propre inversible, alors $\mathfrak{a}^{-1} \supsetneq \mathfrak{a}$ et donc $\mathfrak{a}$ est faiblement inversible et donc il est contenu dans un idéal maximal $\mathfrak{m}_1$. Ainsi par le lemme 1.4.7, $\mathfrak{o} \supset \mathfrak{a}\mathfrak{m}^{-1} \supset \mathfrak{a}$ et par le lemme 1.4.5, $\mathfrak{a}\mathfrak{m}^{-1} \neq \mathfrak{a}$ et donc $\mathfrak{a}\mathfrak{m}^{-1}$ est inversible. Si $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{o}$, alors $\mathfrak{a} = \mathfrak{m}^{-1}$. Sinon, puisque $\mathfrak{o}$ est Noetherien, alors on peut itérer le processus un nombre fini de fois et on obtient l'égalité $\mathfrak{o} = \mathfrak{a}\mathfrak{m}_1^{-1} \dots \mathfrak{m}_r^{-1}$, et donc $\mathfrak{a} = \mathfrak{m}_1 \dots \mathfrak{m}_r$.

q.e.d

Démonstration du théorème 1.4.4. Tout d'abord, montrons que tout idéal premier $\mathfrak{p}$ est inversible : soit $a \in \mathfrak{p} \backslash 0$, alors en appliquant le lemme 1.4.8 à l'idéal inversible (a), on peut écrire

$$\mathfrak{p} \supset (a) = \mathfrak{m}_1 \dots \mathfrak{m}_r$$

où les $\mathfrak{m}_j$ sont des idéaux premiers inversibles. Par le lemme 1.4.6, on a $\mathfrak{p} = \mathfrak{m}_j$ pour un certain j.
Soit maintenant un idéal propre non nul $\mathfrak{a}$ de $\mathfrak{o}$. Alors $\mathfrak{a} \subset \mathfrak{p}$ pour un certain idéal premier $\mathfrak{p}$. On vient de montrer que $\mathfrak{p}$ est inversible et donc $\mathfrak{o} \supset \mathfrak{p}^{-1}\mathfrak{a} \supset \mathfrak{a}$, avec $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$ par le lemme 1.4.5. La suite est obtenue par induction finie du procédé.
Soient maintenant $\mathfrak{p}_1 \dots \mathfrak{p}_s = \mathfrak{q}_1 \dots \mathfrak{q}_r$ des produits d'idéaux premier. Alors par le lemme 1.4.6, $\mathfrak{p}_s \supset \mathfrak{q}_1 \dots \mathfrak{r}_r$ implique que $\mathfrak{p}_r = \mathfrak{q}_j$ pour un certain j que nous supposerons, quitte à renuméroter, être r. Ainsi $\mathfrak{p}_s^{-1} = \mathfrak{q}_r^{-1}$ et donc l'égalité devient

$$\mathfrak{p}_1 \dots \mathfrak{p}_{s-1} = \mathfrak{q}_1 \dots \mathfrak{q}_{r-1}.$$

Par itération, on obtient l'unicité de la décomposition.

q.e.d

Définition 1.4.9
Un $\mathfrak{o}$-idéal fractionnaire $\mathfrak{a}$ est inversible *s'il existe un $\mathfrak{o}$-idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$.*

Théorème 1.4.10
Tout idéal fractionnaire d'un domaine de Dedekind est inversible.

Remarque 1.4.11
Par ce théorème, on remarque que, pour un domaine de Dedekind $\mathfrak{o}$, l'ensemble des idéaux fractionnaires forme un groupe multiplicatif, que nous noterons $I_\mathfrak{o}$. L'inverse de $\mathfrak{a}$, noté $\mathfrak{a}^{-1}$, est l'idéal fractionnaire tel que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$. Ainsi,

en regroupant les idéaux premiers dans la décomposition, tout idéal fractionnaire $\mathfrak{a}$ d'un anneau de Dedekind peut s'écrire comme

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}, \quad v_p(\mathfrak{a}) \in \mathbb{Z}.$$

Puisque la décomposition est unique, une fois les facteurs regroupés, la fonction $\mathfrak{a} \mapsto \bigoplus v_{\mathfrak{p}}(\mathfrak{a})$ induit un isomorphisme de groupe

$$I_{\mathfrak{o}} \simeq \bigoplus_{\mathfrak{p}} \mathbb{Z}.$$

Il s'ensuit que, étant donné un groupe abélien A, et un ensemble d'éléments $a(\mathfrak{p}) \in A$, alors il existe un unique homomorphisme $f : I_{\mathfrak{o}} \longrightarrow A$ tel que $f(\mathfrak{p}) = a(\mathfrak{p})$ pour tout idéal premier $\mathfrak{p}$.
On peut voir ausi et seulement si cette fonction $v_{\mathfrak{p}}$ définie sur $K^\star$ par $v_{\mathfrak{p}}(a) := v_{\mathfrak{p}}(a\mathfrak{o})$.

Propriété 1.4.12
En définissant $\mathfrak{b}|\mathfrak{c}$ s'il existe un idéal $\mathfrak{a}$ tel que $\mathfrak{c} = \mathfrak{b}\mathfrak{a}$, on a

(*i*) $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$;
(*ii*) $v_{\mathfrak{p}}(\mathfrak{a}^{-1}) = -v_{\mathfrak{p}}(\mathfrak{a})$;
(*iii*) $\mathfrak{b}|\mathfrak{c} \Leftrightarrow v_{\mathfrak{p}}(\mathfrak{b}) \leq v_{\mathfrak{p}}(\mathfrak{c})$ *pour tout* $\mathfrak{p} \Leftrightarrow \mathfrak{b} \subset \mathfrak{c}$;
(*iv*) $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$;
(*v*) $v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \inf(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$;
(*vi*) $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) + v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b})$.

Proposition 1.4.13
Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux non nuls de $\mathfrak{o}$; alors les assertions suivantes sont équivalentes :

(*i*) $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$,
(*ii*) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$,
(*iii*) $v_{\mathfrak{p}}(\mathfrak{a})v_{\mathfrak{p}}(\mathfrak{b}) = 0$ *pour tout* $\mathfrak{p}$.

On dit alors que $\mathfrak{a}$ et $\mathfrak{b}$ sont copremiers.

Théorème 1.4.14
Soient $\mathfrak{p}_j$, $j = 1, \ldots, n$ des idéaux premiers distincts de $\mathfrak{o}$, et r_j des exposants positifs, alors la fonction donnée par le produit des fonctions quotients

$$f : \mathfrak{o} \longrightarrow \prod_{j=1}^{n} [\mathfrak{o}/\mathfrak{p} : j^{r_j}]$$

induit un isomorphisme d'anneau $\mathfrak{o}/\prod \mathfrak{p}_j^{r_j} \simeq \prod(\mathfrak{o}/\mathfrak{p}_j^{r_j})$.

Corollaire 1.4.15
Un domaine de Dedekind ayant un nombre fini d'idéaux premier et un domaine principal.

Corollaire 1.4.16
Chaque idéal fractionnaire peut être généré sur $\mathfrak{o}$ *par deux ou moins d'éléments.*

Définition 1.4.17
Rappelons tout d'abord que l'ensemble des idéaux fractionnaires principaux forme un sous groupe $P_{\mathfrak{o}}$ *de* $I_{\mathfrak{o}}$*. Ainsi, on définit le* groupe de classe d'idéaux *de* $\mathfrak{o}$*, noté* $\mathrm{Cl}(\mathfrak{o})$*, est le quotient de* $I_{\mathfrak{o}}$ *par* $P_{\mathfrak{o}}$*. Ce groupe va mesurer le 'défaut de principalité' d'un domaine de Dedekind.*

Définition 1.4.18
Le groupe des unités *est le groupe des éléments inversibles de* $\mathfrak{o}$*, noté abusivement* $\mathfrak{o}^\star$ *ou* U_K*. Remarquons que la fonction donnée par* $a \in K^\star \mapsto (a) \in I_{\mathfrak{o}}$ *nous donne la suite exacte :*

$$a \longrightarrow \mathfrak{o} \longrightarrow K^\star \longrightarrow I_{\mathfrak{o}} \longrightarrow \mathrm{Cl}(\mathfrak{o}) \longrightarrow 1.$$

Théorème 1.4.19
Soit $\mathfrak{o}$ *un domaine de Dedekind de corps de fraction* K*,* L/K *une extension finie séparable de corps,* $\mathfrak{o}$ *la clôture intégrale de* $\mathfrak{o}$*. Alors*

(*i*) $\mathfrak{o}$ *est un* $\mathfrak{o}$*-module de génération finie qui étend* L *sur* K *;*

(*ii*) $\mathfrak{o}$ *est un domaine de Dedekind ;*

(*iii*) *tout idéal premier* $\mathfrak{B}$ *de* $\mathfrak{o}$ *étend un idéal premier* $\mathfrak{p}$ *de* $\mathfrak{o}$*; de manière réciproque, pour tout idéal premier* $\mathfrak{p}$ *de* $\mathfrak{o}$ *s'étend à un moins un, au plus un nombre fini, d'idéaux premiers* $\mathfrak{B}$ *de* $\mathfrak{o}$*.*

Corollaire 1.4.20
L'anneau des entiers algébriques d'un corps de nombre algébrique est un domaine de Dedekind.

Appliquons ce théorème au cas $\mathfrak{o} = \mathbb{Z}$, $K = \mathbb{Q}$. De plus on sait que que l'anneau des entiers algébriques $\mathfrak{o}$ d'un corps de nombre L est un $\mathbb{Z}$-module sans torsion de génération finie ; puisque $\mathfrak{o}$ possède une $\mathbb{Z}$-base libre $\omega_1, \ldots, \omega_n$ et que $\mathfrak{o}$ étend L sur $\mathbb{Q}$, alors $\omega_1, \ldots, \omega_2$ est base de L sur $\mathbb{Q}$, et donc $n = [L : \mathbb{Q}]$. On appellera une telle base $\omega_1, \ldots, \omega_n$ une *base intégrale de* L.
Pour une autre base intégrale $\mu_1, \ldots, \mu_n$ de L, on a les deux systèmes d'équations

$$\begin{aligned} \mu_j &= \sum a_{jk}\omega_k \quad a_{j,k} \in \mathbb{Z}, \\ \omega_j &= \sum b_{jk}\mu_k \quad b_{j,k} \in \mathbb{Z}. \end{aligned}$$

Puisque (a_{ij}) et $(b_{i,j})$ sont des matrices inversibles dans $\mathbb{Z}$, leur déterminant est un inversible de $\mathbb{Z}$, i.e. $\{-1, 1\}$. Ainsi on a

$$\det(t_{L/\mathbb{Q}}(\mu_i\mu_j)) = \det(t_{L/\mathbb{Q}}(\omega_i\omega_j)) = d_L$$

qui ne dépend pas de la base choisie. d_L est appelé *discriminant absolu de* L.

Théorème 1.4.21 (Stickelberger, Schur)
Si L est un corps de nombre algébrique, alors soit $d_L \equiv 0(4)$, soit $d_L \equiv 1(4)$.

Proposition 1.4.22
Soit a un élément de K, alors si a est entier sur $\mathfrak{o}$, le polynôme minimal de a sur K est dans $\mathfrak{o}[X]$.

Proposition 1.4.23
Pour deux polynômes non nuls f_1 et f_2 dans $K[X]$

$$v_\mathfrak{p}(f_1 f_2) = v_\mathfrak{p}(f_1) + v_\mathfrak{p}(f_2).$$

En particulier, on dit que f est primitif *si $v_\mathfrak{p} = 0$ pour tout $\mathfrak{p}$.*

Proposition 1.4.24
Un élément $\alpha \in K = \mathbb{Q}[\sqrt{m}]$ est un entier algébrique si et seulement si l'on peut l'écrire comme

$$\begin{cases} \alpha &= \frac{1}{2}(u + v\sqrt{m}) \quad u, v \in \mathbb{Z} \\ u^2 - mv^2 &\equiv 0(4). \end{cases}$$

Théorème 1.4.25
Si m est congru à 2 ou 3 modulo 4, alors $\{1, \sqrt{m}\}$ est une base intégrale de K et $d_K = 4m$.
Si m est congru à 1 modulo 4, alors $\{1, \frac{1+\sqrt{m}}{2}\}$ est une base intégrale de K et $d_K = m$.

CHAPITRE 2

Valeurs absolues et complétions

2.1 Valeurs absolues

Définition 2.1.1
Pour K un corps, la fonction $|.|$ de K dans $\mathbb{R}_+$ est appelée valeur absolue *si pour tout tout x, y les conditions suivantes ont lieu :*

(*i*) $|x| = 0$ *si et seulement si* $x = 0$,

(*ii*) $|xy| = |x|\,|y|$,

(*iii*) $|x + y| \leq |x| + |y|$.

La fonction qui associe à tout x dans $K^\star$ la valeur 1 et à 0 la valeur 0 est clairement une valeur absolue, appelée valeur absolue triviale *et notée $|.|_0$.*
Une valeur absolue qui satisfait de plus la condition $|x + y| \leq \sup(|x|, |y|)$ est appelée une ultramétrique.
Si l'image d'une valeur absolue des inversibles d'un corps est un sous-ensemble discret des réels strictement positifs, alors elle est appelée valeur absolue discrète. *$\mathbb{Q}$ n'est pas un sous-ensemble discret de $\mathbb{R}$!*

Définition 2.1.2
Soit K un corps. Un fonction surjective $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ est une valuation de K *si et seulement si pour tout $x, y \in K$*

(*i*) $v(x) = \infty$ *si et seulement si* $x = 0$,

(*ii*) $v(xy) = v(x)v(y)$,

(*iii*) $v(x + y) \geq \inf(v(x), v(y))$.

Proposition 2.1.3
Si $|.|$ est une valeur absolue discrète non-triviale, alors $|K^\star| = \lambda^{\mathbb{Z}}$ pour $0 < \lambda < 1$ (où $\lambda^{\mathbb{Z}}$ est le sous-groupe cyclique de $\mathbb{R}^\star$ engendré par λ).

Démonstration. Par hypothèse, $|K^\star| \cap (0,1)$ est non-vide. Puisque $|K^\star|$ est discret, on peut trouver un élément maximal $\lambda \in |K^\star| \cap (0,1)$, et donc on peut choisir $x \in K^\star$ tel que $|x| = \lambda$. Pour $y \in K^\star$, alors on veut montrer que $|y| = \lambda^{\mathbb{Z}}$. Si $|y| = 1$, alors c'est clair. D'autre part, quitte à remplacer y par y^{-1}, on peut supposer $|y| < 1$. Ainsi $\lambda^{n+1} \leq |y| < \lambda^n$ pour un certain n, donc $\lambda < |yx^{-n}| < 1$. Ainsi puisque λ est maximal, alors $|yx^{-n}| = \lambda$ et donc $|y| = \lambda n + 1$.

q.e.d

Définition 2.1.4
Pour K un corps et $|.|$ une valeur absolue sur K, alors la paire $(K, |.|)$ est appelée corps évalué.
Un homomorphisme de corps $\sigma : (K, |.|_1) \longrightarrow (L, |.|_2)$ est une homomorphisme de corps évalués *si et seulement si pour tout élément x de K, on a $|\sigma(x)|_2 = |x|_1$.*

Exemple 2.1.5
1. Soit $\sigma : K \hookrightarrow \mathbb{R}$ un plongement de corps. Alors la fonction $|x|_\sigma := |x^\sigma|_{\mathbb{R}}$, où $|y|_{\mathbb{R}}$ est la valeur absolue usuelle sur $\mathbb{R}$.
2. Soit $\sigma : K \hookrightarrow \mathbb{C}$ un plongement de corps, alors $|x|_\sigma := |x^\sigma|$ est une valeur absolue de K, où $|y|_{\mathbb{C}}$ est le module du nombre complexe y. Si ρ est un automorphisme de K, avec $x^{\rho\circ\sigma}$ est le conjugué complexe de x^σ pour tout x dans K, alors ρ induit un automorphisme de corps évalué sur $(K, |.|_\sigma)$. Cela est surtout intéressant quand l'image de σ est complexe, i.e. $\rho \circ \sigma \neq \sigma$.

Définition 2.1.6
Deux normes $|.|_1$ et $|.|_2$ sont équivalentes *s'il existe un nombre réel positif α tel que pour tout $x \in K$ on a $|x|_1 = |x|_2^\alpha$.*
La valeur absolue sur un corps de nombre algébrique équivalente à une valeur absolue du type des exemples est appelée valeur absolue archimédienne.

Proposition 2.1.7
Soient $|.|_1$ et $|.|_2$ deux valeurs absolues sur K. Alors ces deux normes sont équivalentes si et seulement si

$$\{x \in K \mid |x|_1 > 1\} \subset \{x \in K \mid |x|_2 > 1\}.$$

Démonstration. Le sens 'aller' est clair. Supposons maintenant l'inclusion du complémentaire des deux ensembles, par l'automorphisme $x \mapsto x^{-1}$. Soit

$x, y \in K$ de première valeur absolue positive. Alors on peut trouver un unique nombre réel positif α tel que $|y|_1 = |x|_1^\alpha$. Alors il existe m et n des naturels tel que $\frac{m}{n} > \alpha$. Ainsi $|y|_1 = |x|_1^\alpha \leq |x|_1^{\frac{m}{n}}$ et donc $|y^n x^- m|_1 < 1$. Ainsi par hypothèse, $|y^n x^- m|_2 < 1$ et donc $|y|_2 < |x|_2^{\frac{m}{n}}$.

De la même manière on peut borner inférieurement $|x|_2^{\frac{m'}{n'}} < |y|$ et par le théorème des deux gendarmes on a donc en cas limite $|y|_2 = |x|_2^\alpha$. Pour conclure, soit l'unique réel β tel que $|x|_1 = |x|_2^\beta$ et on a

$$|y|_1 = |x|_1^\alpha = |x|_2^{\alpha\beta} = |y|_2^\beta .$$

q.e.d

Proposition 2.1.8
Soit K un corps possédant deux valeurs absolues $|.|_1$ et $|.|_2$. Alors les deux topologies induites coïncident si et seulement si les deux valeurs absolues sont équivalentes.

Démonstration. Nous allons utiliser le fait que deux topologies coïncident si et seulement si pour une suite (a_i) d'éléments de K, alors $|x_i|_1 \longrightarrow 0$ si et seulement si $|x_i|_2 \longrightarrow 0$. Ainsi si les deux valeurs absolues sont équivalentes alors immédiatement les topologies coïncident. Supposons maintenant que les deux valeurs absolues ne sont pas équivalentes. Alors par la proposition précédente on peut trouver un $x \in K$ tel que $|x|_1 < 1$ et $|x|_2 \geq 1$. La suite des (x^i) est telle que $|x^i|_1 \longrightarrow 0$ mais pas $|x^i|_2$.

q.e.d

Théorème 2.1.9 (Théorème d'approximation faible)
Soient $|.|_1, \ldots, |.|_n$ des valeurs absolues équivalentes sur K. Pour $\varepsilon > 0$ et $x_1, \ldots, x_n \in K$, on peut trouver $y \in K$ tel que pour tout $i = 1, \ldots, n$

$$|y - x_i|_i < \varepsilon.$$

Lemme 2.1.10
Pour n valeurs absolues non-équivalentes, on peut trouver $a \in K$ tel que

$$|a|_1 > 1 \quad |a|_i < 1 \quad \textit{pour } i = 1, \ldots, n.$$

Démonstration. Par récurrence sur n : pour $n = 1$, la proposition 2.1.7 on peut trouver un tel a. Supposons maintenant le lemme vrai pour $(n-1) \geq 2$, ainsi on peut trouver $b \in K$ tel que

$$|b|_1 > 1 \quad |b|_i < 1 \quad \text{pour } i = 1, \ldots, n-1.$$

Si deux normes ($i > 1$) sont équivalentes, alors on a fini. Supposons que toutes les normes sont deux à deux non-équivalentes ; en particulier $|.|_1$ et $|.|_n$. On peut donc trouver $c \in K$ tel que $|c|_1 > 1$ et $|c|_n < 1$. Pour r suffisamment grand, on peut définir le a du lemme par

$$a = \begin{cases} b & \text{si } |b|_n < 1, \\ cb^r & \text{si } |b|_n = 1, \\ \frac{cb^r}{1+b^r} & \text{si } |b|_n > 1. \end{cases}$$

q.e.d

Démonstration du théorème d'approximation faible. Par le lemme 2.1.10, on peut trouver des $a_j \in K$ tel que $|a_j|_j > 1$, avec $|a_j|_i < 1$ si $i \neq j$. Ainsi pour un r suffisamment grand, le y du théorème est définit par

$$\sum_{j=1}^{n} \left(\frac{a_j^r}{1 + a_j^r} \right) x_j.$$

q.e.d

Définition 2.1.11
Pour p un nombre premier, on définit la valeur absolue p-adique *de $\mathbb{Q}$ dans $\mathbb{R}$ par, pour $x \in \mathbb{Q}$, $x = p^r \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ et $(ab, p) = 1$, on a $|x|_p = p^{-r}$. On pose que $0 = p^\infty 0$ et donc $|0| = 0$.*

Théorème 2.1.12 (Ostrowski)
Soit $|.|$ une valeur absolue non-triviale de $\mathbb{Q}$. Alors elle est équivalente soit à la valeur absolue héritée de la norme euclidienne, soit à une norme p-adique pour un certain premier p.

Démonstration. Rappelons (ou donnons) le fait suivant : l'ensemble des valeurs absolues de $\mathbb{Q}$ est relié par la *formule du produit* :

$$|x|_{\mathbb{R}} \prod_p |x|_p = 1$$

pour tout $x \in \mathbb{Q}^\star$. La preuve de cette formule suit de la décomposition de x en facteurs premier.
Supposons, pour commencer, que la valeur absolue donnée est telle que $|n| \leq 1$ pour tout $n \in \mathbb{Z}$. On peut donc trouver des nombres premier distincts p et q, des naturels a, b et des relatifs λ et μ tels que $p^a < \frac{1}{2}$, $q^b < \frac{1}{2}$ et $\lambda p^a + \mu q^b = 1$ (formule de Bézout). Il s'ensuit

$$1 = |1| = \left| \lambda p^a + \mu q^b \right| < \frac{|\lambda| + |\mu|}{2} \leq 1,$$

ce qui est absurde. Ainsi $|p| = |p|_p^\alpha$ et donc $|x| = |x|_p^\alpha$ pour tous les rationnels x.
Maintenant supposons qu'il y ait un naturel n tel que $|n| > 1$ et $|n| = n^\alpha$. De plus par définition (inégalité du triangle), on doit avoir pour toute norme $|m| < m$ quelque soit le naturel m, ainsi $0 \leq m \leq 1$. Pour un entier m on peut l'écrire $m = \sum_{i=1}^{k} m_i n^i$ avec $0 \leq m_i < n$, $m_k \neq 0$ et $m_i \in \mathbb{N}$. On en déduit que

$$\begin{aligned} |m| &\leq \sum_{i=0}^{k} |m_i|\, n^{\alpha i} \\ &\leq \sum_{i=0}^{k} m_i n^{\alpha i} \\ &\leq \frac{(n-1)n^{\alpha(k+1)}}{(n^\alpha - 1)}. \end{aligned}$$

Ainsi il existe une certaine constante c, indépendante de $m \in \mathbb{N}$ telle que $|m| \leq cm^\alpha$. De plus, en remplaçant m par m^r, avec r suffisamment grand, on remarque que $|m| \leq c^{(1/r)} |m|_{\mathbb{R}}^\alpha$. Ainsi donc nous avons

$$|m| \leq |m|_{\mathbb{R}}^\alpha$$

pour tout $m \in \mathbb{Z}$.
Avec la même notation, on a $m = n^{k+1} - b$ avec $0 \leq b \leq n^{k+1} - n^k$. Il s'ensuit donc

$$|b| \leq b^\alpha \leq (n^{k+1} - n^k)^\alpha.$$

Par l'inégalité su triangle :

$$\begin{aligned} |m| &\geq \left|n^{k+1}\right| - |b| \\ &\geq n^{(k+1)\alpha} - (n^{k+1} - n^k)^\alpha \\ &\geq n^{(k+1)\alpha}\left[1 - (1 - \frac{1}{n})^\alpha\right] \\ &\geq c' n^{(k+1)\alpha} \\ &\geq c' m^\alpha \end{aligned}$$

pour une certaine constante c' indépendante de m. De la même manière que précédemment, en remplaçant m par m^r avec r assez grand, on a que $|m| \geq |m|_{\mathbb{R}}^\alpha$ pour tout $m \in \mathbb{Z}$. Ainsi on voit que $|.| = |.|_{\mathbb{R}}^\alpha$.

q.e.d

Proposition 2.1.13
Si $|.|$ est borné sur $\overline{\mathbb{Z}}$ (l'image de $\mathbb{Z}$ dans K), alors $|.|$ est ultramétrique.

Démonstration. Soit C la borne de $\overline{\mathbb{Z}}$. Alors pour tout $x, y \in K$, par le binôme de Newton

$$\begin{aligned} |x+y| &\leq \sum_{i=0}^{m} |x|^i \, |y|^{m-1} \left| \begin{pmatrix} m \\ i \end{pmatrix} \right| \\ &\leq C \sum_{i=0}^{m} |x|^i \, |y|^{m-1} \\ &\leq C(m+1) \sup(|x|^m, |y|^m). \end{aligned}$$

Donc pour tout $m > 0$

$$|x+y| \leq (C(m+1))^{(1/m)} \sup(|x|, |y|).$$

En passant à la limite, on a la formule voulue.

q.e.d

Corollaire 2.1.14
Si $|.|$ est une valeur absolue discrète ou si K est de caractéristique positive, alors $|.|$ est une ultramétrique.

2.2 Complétions

Nous allons nous intéresser maintenant à la forme d'un corps K muni d'une valeur absolue $|.|$. Par exemple, dans le corps $\mathbb{Q}$, les suites de Cauchy n'y convergent pas forcément, mais on peut le compléter ($\mathbb{R}$) pour que cela arrive.

Définition 2.2.1
Le corps évalué $(K, |.|)$ est dit complet *si toute suite de Cauchy possède une limite dans le corps.*

Théorème 2.2.2
Soit un corps évalué $(K, |.|)$, alors il existe une paire $j, (\overline{K}, \|.\|)$, où $(\overline{K}, \|.\|)$ est un corps évalué complet et $j : (K, |.|) \longrightarrow (\overline{K}, \|.\|)$ est un homomorphisme de corps évalué, qui a les propriétés suivantes :

- *(i) $j(K)$ est dense dans $\overline{K}$, i.e pour tout ε-voisinage $N_\varepsilon = \{x \in \overline{K} \mid \|x - b\| < \varepsilon\}$ de $b \in \overline{K}$ contient un élément a de $j(K)$.*
- *(ii) Si $(L, |.|')$ est un corps évalué complet et si $k : (K, |.|) \longrightarrow (L, |.|')$ est un homomorphisme de corps évalué, alors il existe un unique homomorphisme de corps évalués $k' : (\overline{K}, \|.\|) \longrightarrow (L, |.|')$ avec $k = k' \circ j$.*

De plus, ces deux propriétés caractérisent la paire $j, (\overline{K}, \|.\|)$ de manière unique à isomorphisme près.

Corollaire 2.2.3
Si $(K, |.|)$ est complet, alors $j : (K, |.|) \longrightarrow (\overline{K}, \|.\|)$ est un isomorphisme de corps évalués.

Nous démontrerons le théorème et son corollaire par une suite de petits lemmes, dont certains donnés sans preuve.

Lemme 2.2.4
La somme et le produit deux deux suites convergentes $\{a_n\}$ et $\{b_n\}$ sont des suites convergentes et

$$\lim_{n\longrightarrow\infty}(a_n + b_n) = \lim_{n\longrightarrow\infty} a_n + \lim_{n\longrightarrow\infty} b_n$$
$$\lim_{n\longrightarrow\infty}(a_n \cdot b_n) = \lim_{n\longrightarrow\infty} a_n \cdot \lim_{n\longrightarrow\infty} b_n.$$

Lemme 2.2.5
La somme et le produit de deux suites de Cauchy $\{a_n\}$ et $\{b_n\}$ sont des suites de Cauchy ; $\{1_n\}$ est une suite de Cauchy ; si $\{b_n\}$ est une suite convergente vers 0, alors $\{a_n\} \cdot \{b_n\}$ converge ausi et seulement si vers 0.

Lemme 2.2.6
Soit $\{a_n\}$ une suite de Cauchy, alors il existe un réel positif k tel que $|a_n| < k$ pour tout n.

Démonstration. Puisque $\{a_n\}$ est une suite de Cauchy, il existe un entier N tel que $|a_n, a_m| < 1$ pour tout $m, n \geq N$, et on choisi

$$k > \max_{1\leq i\leq N}(1 + |a_i|).$$

Ainsi, si $n < N$, alors par définition $|x_n| < k$ et d'autre côté, pour $n > N$ on a

$$|a_n| \leq |a_n - a_N| + |a_N| < k.$$

q.e.d

Démonstration du lemme 2.2.5. Soient $\{a_n\}$ et $\{b_n\}$ deux suites de Cauchy. Par le lemme précédent, on peut trouver k tel que $|a_i| < k$ et $|b_i| < k$. Ainsi

$$\begin{aligned} |a_n b_n - a_m b_m| &\leq |a_n|\,|b_n - b_n| + |b_m|\,|a_n - a_m| \\ &\leq k(|a_n - a_m| + |b_n - b_m|). \end{aligned}$$

Pour $\varepsilon > 0$, on peut trouver $M \in \mathbb{N}$ tel que pour tout $m, n \geq M$ on a

$$|b_n - b_m|\,,\ |a_n - a_m| < \frac{\varepsilon}{2k}.$$

Ainsi $\{a_n\} \cdot \{b_n\}$ est bien une suite de Cauchy.
Soit maintenant une suite $\{b_n\}$ convergent vers 0, alors on peut choisir M tel que $|b_n| < \varepsilon/k$ lorsque $n \geq M$. Ainsi $|a_n b_n| < \varepsilon$ pour $n \geq M$, et donc $\{a_n\} \ldots \{b_n\}$ est une suite convergente vers 0. q.e.d

Lemme 2.2.7
Soit $\{a_n\}$ une suite de Cauchy qui ne converge pas vers 0. Alors il existe un nombre réel strictement positif k' et $M \in \mathbb{N}$ tel que $|a_n| > k'$ pour tout $n \geq M$.

Démonstration. Procédons par l'absurde : soit $\varepsilon > 0$ et $M \in \mathbb{N}$, alors il existe $l \geq \mathbb{N}$ tel que $|a_l| < \varepsilon/2$. Quitte à augmenter la valeur de M, on peut supposer ausi et seulement si que $|a_n - a_m| < \varepsilon/2$ pour tout $m, n \geq M$. Ainsi pour tout $n \geq M$, $|a_n| \leq |a_n - a_l| + |a_l| < \varepsilon$, et donc $\{a_n\}$ est une suite tendant vers 0. q.e.d

Lemme 2.2.8
Soient $\{a_n\}$, k' et M comme dans le lemme précédent, alors la suite $\{b_n\}$ définie par $b_n = a_n$ pour $n \geq M$ et $b_n = 1$ sinon est ausi et seulement si une suite de Cauchy.

Démonstration. Soit $\varepsilon > 0$, on choisi $n_1 > M$ tel que $|a_n - a_m| < \varepsilon k'^2$ pour tout $m, n \geq n_1$. Alors pour de tes n, m on a

$$|b_n - a_n| = \frac{|a_n - a_m|}{|a_n a_m|} < \varepsilon.$$

q.e.d

Les lemmes que nous venons de montrer nous indique que les suites de Cauchy forment un sous-anneau R_0, avec identité $\{1_n\}$, de l'anneau R des suites. De plus, les suites convergentes vers 0 forment un idéal $\mathfrak{n}$ de R_0. On a de plus que pour toute suite $\{a_n\} \in R_0 \backslash \mathfrak{n}$ il existe une suite $\{b_n\} \in R_0$ telle que $\{a_n\}\{b_n\} \equiv \{1_n\}(\mathfrak{n})$. Ainsi $\mathfrak{n}$ est maximal et $R_0/\mathfrak{n} = \overline{K}$ est un corps.
Étendons maintenant la valeur absolue $|.|$ à $\overline{K}$. L'inégalité du triangle nous donne :

$$\begin{aligned} |a_n| - |a_m| &\leq |a_n - a_m| \\ |a_m| - |a_n| &\leq |a_n - a_m|\,. \end{aligned}$$

Ainsi, avec $|.|_{\mathbb{R}}$ la valeur absolue sur $\mathbb{R}$, on obtient

$$||a_n| - |a_m||_{\mathbb{R}} \leq |a_n - a_m| .$$

Ainsi, si $\{a_n\}$ est une suite de Cauchy pour $|.|$, alors $\{|a_n|\}$ est une suite de Cauchy pour $|.|_{\mathbb{R}}$ dans $\mathbb{R}$. Mais de plus $\mathbb{R}$ est complet pour $|.|_{\mathbb{R}}$, et donc $|a_n|$ possède sa limite dans $\mathbb{R}$. On définit ainsi

$$\|\{a_n\}\| = \lim_{n \longrightarrow \infty} |a_n| .$$

Nous avons remarqué que si $|.|'$ est une valeur absolue équivalente à $|.|$ sur K, alors l'anneau R_0 et l'idéal $\mathfrak{n}$ restent inchangé sous $|.|'$. Ainsi $j : K \longrightarrow \overline{K}$ dépend uniquement de la classe d'équivalence de $|.|$. D'autre part, la valeur absolue $\|.\|$ dépend étroitement de la valeur absolue $|.|$; si $|.|' = |.|^{\alpha}$, alors

$$\|.\|' = \|.\|^{\alpha} .$$

Lemme 2.2.9
$\|a_n\| \geq 0$ et $\|a_n\| = 0$ si et seulement si $\{a_n\}$ est une suite tendant vers 0.

Observons que

$$\begin{aligned} \|\{a_n\} + \{b_n\}\| &= \|\{a_n + b_n\}\| \\ &= \lim_{n \longrightarrow \infty} |a_n + b_n| \\ &\leq \lim_{n \longrightarrow \infty} (|a_n| + |b_n|) \\ &= \lim_{n \longrightarrow \infty} |a_n| + \lim_{n \longrightarrow \infty} |b_n| \\ &= \|a_n\| + \|b_n\| . \end{aligned}$$

En particulier, si $\{b_n\}$ est une suite tendant vers 0, alors $\|\{a_n\} + \{b_n\}\| \leq \|\{a_n\}\|$ et $\|\{a_n\}\| = \|\{a_n + b_n\} - \{b_n\}\| \leq \|\{a_n + b_n\}\|$. Ainsi $\|\{a_n\}\| = \|\{a_n\} + \{b_n\}\|$. Du plus, clairement

$$\|\{a_n\}\{b_n\}\| = \|\{a_n\}\| \, \|\{b_n\}\| .$$

Lemme 2.2.10
La fonction $\{a_n\} + \mathfrak{n} \mapsto \|\{a_n\}\|$ est bien définie ; c'est de plus une valeur absolue sur $\overline{K}$ dont la classe d'équivalence ne dépend que de celle de $|.|$.

Lemme 2.2.11
Tout élément $\alpha \in \overline{K}$ est une limite $\alpha = \lim_{n \longrightarrow \infty, \|.\|} j(b_n)\, b_n \in K$, i.e. $j(K)$ est dense dans $\overline{K}$. En particulier, si α est représenté par une suite $\{b_n\}$ $(b_n \in K)$, alors $\alpha = \lim_{n \longrightarrow \infty, \|.\|} j(b_n)$.

Lemme 2.2.12
$\overline{K}$ est complet pour $\|.\|$.

Démonstration. Soit $\{x_n\}$ une suite de Cauchy dans $\overline{K}$ pour $\|.\|$. Par le lemme précédent, on sait que chaque $x_n = \lim_{n\longrightarrow\infty,\|.\|} j(b_{n,m})$ avec $b_{n,m} \in K$. Pour tout n, on fixe $m = m(n)$ tel que

$$\|x_n - j(b(n))\| < \frac{a}{2^n}.$$

Alors, par l'inégalité du triangle :

$$\begin{aligned} |b(r) - b(n)| &= \|j(b(r)) - j(b(n))\| \\ &< \frac{1}{2^r} + \frac{1}{2^n} + \|x_r - x_n\|. \end{aligned}$$

Ainsi $\{b_r\}$ est une suite de Cauchy pour $|.|$. On notera donc x la classe de $\{b_r\}$ dans $\overline{K}$. Alors $x = \lim_{n\longrightarrow\infty,\|.\|} j(b(n))$, et d'autre part $0 = \lim_{n\longrightarrow\infty,\|.\|}(x_n - j(b(n)))$ et donc $x = \lim_{n\longrightarrow\infty,\|.\|} x_n$.

q.e.d

Démonstration du théorème 2.2.2. Il ne nous reste plus qu'à montrer la seconde partie du théorème ainsi que les unicité. Soient donc $(L, |.|')$ et k. Une suite de Cauchy $\{a_n\}$ dans K pour $|.|$ détermine un élément $\alpha \in \overline{K}$. Puisque k est un homomorphisme de corps évalué, la suite définie par $k\{a_n\} = \{k(a_n)\}$ est une suite de Cauchy dans L pour $|.|'$. Montrons tout d'abord l'unicité d'un tel $k' : (\overline{K}, \|.\|) \longrightarrow (L, |.|')$ avec $k' \circ j = k$. De ce fait, puisque k' est un homomorphisme de corps évalué, $|k'(a) - k' \circ j(a_n)|' = \|\alpha - j(a_n)\|$, et donc

$$k'(\alpha) = \lim_{|.|'} k(a_n).$$

Montrons maintenant l'existence de k' : soient deux suites de Cauchy $\{a_n\}$ et $\{a'_n\}$ dans K définissant le même élément $\alpha \in \overline{K}$. Ainsi $\{a_n - a'_n\}$ est une suite tendant vers 0 dans K pour $|.|$. Ainsi $\{k(a_n) - k(a'_n)\}$ est une suite tendant vers 0 dans L pour $|.|'$. On conclue de la sorte que $k'(\alpha) = \lim_{|.|'} k(a_n)$ définit un unique élément de L qui dépend uniquement de α et pas du choix du représentant. On vérifie facilement que le k' ainsi définit est bien un homomorphisme.
Montrons maintenant que les propriétés caractérisent $(\overline{K}, \|.\|)$. Supposons donc $(K_1, |.|_1)$ complet et un homomorphisme $j : K \longrightarrow K_1$ tel que $j(K)$ est dense dans K_1. Ainsi il existe un homomorphisme $k : (\overline{K}, \|.\|) \longrightarrow (K_1, |.|_1)$ avec $k \circ j = l$. Remarquons que k est surjective. Soit $y \in K_1$, par densité $y = \lim_{|.|_1}(l(a_n))$ avec $\{a_n\}$ une suite de Cauchy dans K. Mais alors $y = k(x)$

où $x = \lim_{\|.\|} j(a_n)$.
Finalement, soit $(K_1, |.|_1)$ un corps évalué complet et soit $j_1 : (K, |.|) \longrightarrow (K_1, |.|_1)$ un homomorphisme de corps évalué ayant la seconde propriété. Alors par hypothèse, on a l'homomorphisme de corps évalué

$$\begin{aligned} l : (\overline{K}, \|.\|) &\longrightarrow (K_1, |.|_1) \\ l_1 : (K_1, |.|_1) &\longrightarrow (\overline{K}, \|.\|) \end{aligned}$$

avec $l_1 \circ j_1 = j$, $l \circ j = j_1$. Ainsi $l_1 \circ l \circ j = j$ et donc par unicité de l'homomorphisme $l_1 \circ l = \mathrm{id}_{\overline{K}}$, et de la même manière $l \circ l_1 = \mathrm{id}_{K_1}$. Ainsi l_1 et l sont des isomorphismes mutuellement inverses de corps évalués.

q.e.d

Théorème 2.2.13
Pour $\mathfrak{o}$ un domaine de Dedekind de corps de fractions K, $v = v_{\mathfrak{p}}$ la valuation sur K d'un idéal maximal $\mathfrak{p}$ et $|.| = |.|_v$ la valeur absolue discrète on a vu qu'il existe un réel $0 < \lambda < 1$ tel que $|a| = \lambda^{v(a)}$. De plus on a

(*i*) *Il existe une unique valuation $\hat{v}$ de $\overline{K}$ tel que $\|.\| = |.|_{\hat{v}}$, i.e. tel que $\|\alpha\| = \lambda^{\hat{v}(\alpha)}$ pour $\alpha \in \overline{K}$. Ainsi la restriction de $\hat{v}$ sous j est v ;*

(*ii*) *Soit $\hat{\mathfrak{o}}$ l'anneau de valuation de $\hat{v}$ et $\hat{\mathfrak{p}}$ l'idéal de valuation de $\hat{v}$. Pour $Y \subset \overline{K}$, $\overline{Y}$ désignant la clôture de Y dans $\overline{K}$ respectant la topologie induite par $\|.\|$, on a pour tout $r \in \mathbb{Z}$ $\overline{j(\mathfrak{p}^r)} = \hat{p}^r$, en particulier $\overline{j(\mathfrak{o})} = \hat{\overline{d}}$;*

(*iii*) *La fonction $j : \mathfrak{o} \longrightarrow \hat{\mathfrak{o}}$ induit un isomorphisme $\mathfrak{o}/\mathfrak{p}^r \simeq \hat{\mathfrak{o}}/\hat{\mathfrak{p}}^r$.*

Démonstration. L'ensemble des valeurs non nulles λ^m de $|.|$ est discret dans $\mathbb{R}_{>0}$. Ainsi, par définition de $\|.\|$. Ainsi c'est ausi et seulement si l'ensemble des valeurs non nulles de $\|.\|$. On peut donc écrire $\|\alpha\| = \lambda^{\hat{v}(\alpha)}$ et le fait que $\|.\|$ soit discret implique que $\hat{v}$ est une valuation. Cela termine le point (i).
Supposons que $\alpha \notin \mathfrak{p}^r$, ainsi $\|\alpha\| \geq \lambda^{r-1}$. Si $\|\alpha - j(a)\| < \lambda^{r-1} - \lambda^r$, alors on en déduit de la chaîne d'inégalité

$$\|j(a)\| \geq \|\alpha\| - \|\alpha - j(a)\| \geq \lambda^{r-1} - \|\alpha - j(a)\| > \lambda^r$$

qu'une suite de voisinage de α est disjoint de $j(\mathfrak{p}^r)$. Ainsi $\overline{j(\mathfrak{p}^r)} \subset \hat{\mathfrak{p}}^r$.
L'inclusion inverse est plus compliquée est nécesi et seulement site les assertions suivantes :
Assertion : Si $\alpha \in \hat{\mathfrak{o}}$, alors α est représenté par une suite de Cauchy $\{a_n\}$ de K, avec tous les $a_n \in \mathfrak{o}$.
Supposons pour l'instant l'assertion vraie. On note alors que si $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$, alors $\hat{v}(\pi^r) = v(\pi^r) = r$ et donc que $\hat{\mathfrak{p}}^r = j(\pi^r)\hat{\mathfrak{o}}$. Ainsi un élément de $\hat{\mathfrak{p}}^r$ peut être représenté par une suite de Cauchy de la forme $\{\pi^r a_n\}$ avec $a_n \in \mathfrak{o}$. Cela

montre que $\hat{\mathfrak{p}}^r \subset \overline{j(\mathfrak{p}^r)}$.
Pour démontrer l'assertion, remarquons que par discrétion, un élément $\alpha \in \hat{\mathfrak{o}}$ est représenté par une suite de Cauchy $\{a_n\}$ avec pour un n suffisamment grand $v(a_n) \geq 0$, et l'on peut, quitte à changer les n premiers termes de la suite, supposer que c'est le cas pour tout n. L'assertion est donc conséquence immédiate de faite que pour $N \in \mathbb{N}$ et $a \in K$ avec $v(a) \geq 0$, il existe $b \in \mathfrak{o}$ tel que $v(a-b) \geq N$. En effet, on peut écrire $a = a_1/a_2$ avec $a_1, a_2 \in \mathfrak{o}$ et $a_2 \notin \mathfrak{p}$. Ainsi la classe de a_2 modulo $\mathfrak{p}^N$ est une unité dans $\mathfrak{o}/\mathfrak{p}^N$ et l'on peut trouver $c \in \mathfrak{o}$ avec $ca_2 \equiv 1(\mathfrak{p}^N)$. Ainsi $aca_2 \in \mathfrak{o}$ et $v(a - aca_2) = v(a(1 - ca_2)) \geq N$.
La troisième partie est conséquence immédiate des deux points précédents.
q.e.d

Corollaire 2.2.14
$\mathfrak{p}\hat{\mathfrak{o}} = \hat{\mathfrak{p}}$ et si $\mathfrak{q}$ est un idéal premier de $\mathfrak{o}$ autre que $\hat{\mathfrak{p}}$, alors $\mathfrak{q}\hat{\mathfrak{o}} = \hat{\mathfrak{o}}$.

Démonstration. Par la deuxième partie du théorème, $\mathfrak{p}\hat{\mathfrak{o}} \subset \hat{\mathfrak{p}}$ et par la première partie $\mathfrak{p}$ contient un élément de la $v_{\hat{\mathfrak{p}}}$. Ainsi $\mathfrak{p}\hat{\mathfrak{o}} = \hat{\mathfrak{p}}$. La même partie du théorème nous donne $\mathfrak{p}\hat{\mathfrak{o}} \not\subset \hat{\mathfrak{p}}$, mais $\mathfrak{q}\hat{\mathfrak{q}} \subset \hat{\mathfrak{o}}$, ainsi $\mathfrak{q}\hat{\mathfrak{o}} = \hat{\mathfrak{o}}$. q.e.d

Pour étudier les complétions plus en profondeur, nous avons besoin d'un outil supplémentaire : la *limite inverse*. Pour un anneau R, on définit un *système inverse* par des R-modules A_n et des homomorphismes de R-modules $\alpha_m^n : A_n \longrightarrow A_m$ pour $n \geq M$ satisfaisant :

(i) $\alpha_n^n = \mathrm{id}_{A_n}$;

(ii) $\alpha_r^m \circ \alpha_m^n = \alpha_r^n$.

Pour un tel système, on définit la *limite inverse*, notée $\lim_{\leftarrow} A_n$, par le R-sous module du produit directe $\prod_n A_n$ consistant en les suites $a = (a(1), a(2), \dots)$ où $a(m) = \alpha_m^n(a(n))$ pour $n \geq m$. L'homomorphisme de R-modules associé

$$\alpha_m : \lim_{\leftarrow} A_n \longrightarrow A_m$$

est appelé la *fonction de la m-ème composante*, où $\alpha_m(a) = a(m)$. On a de plus la propriété évidente $\alpha_r = \alpha_r^m \circ \alpha_m$.
Supposons maintenant un autre système inverse, $\{B_n, \beta_m^n\}$ et des homomorphismes de R-modules $\theta_n : B_n \longrightarrow A_n$ tels que $\theta_m \circ \beta_m^n = \alpha_m^n \circ \theta_n$. On peut passer cet homomorphisme ausi et seulement si à la limite inverse, ce qui nous donne

$$\lim_{\leftarrow} \theta_n = \theta : \lim_{\leftarrow} B_n \longrightarrow \lim_{\leftarrow} A_n,$$

où $\theta(n)(n) = \theta_n(b(n))$. Naturellement, si chaque θ_n est un isomorphisme, alors θ l'est ausi et seulement si.

Illustrons maintenant cela par un exemple. Soit B un R-module et $\theta_n : B \longrightarrow A_n$. Ainsi pour $n \geq m$, le diagramme suivant commute :

$$\begin{array}{ccc} B & \xrightarrow{\theta_n} & A_n \\ & \searrow^{\theta_m} & \downarrow{\scriptstyle \alpha_m^n} \\ & & A_m. \end{array}$$

On obtient donc un unique homomorphisme $\theta : B \longrightarrow \lim_{\leftarrow} A_n$ faisant commuter le diagramme suivant :

$$\begin{array}{ccc} B & \xrightarrow{\theta} & \lim_{\leftarrow} A_n \\ & \searrow^{\theta_m} & \downarrow{\scriptstyle \alpha_m} \\ & & A_m. \end{array}$$

De fait, cette propriété détermine $\lim_{\leftarrow} A_n$ de manière unique à homomorphisme près.
Appliquons maintenant cette construction au système inverse $\{\mathfrak{o}/\mathfrak{p}^n, \pi_m^n\}$, où π_m^n est la classe de fonction quotient $\mathfrak{o}/\mathfrak{p}^n \longrightarrow \mathfrak{o}/\mathfrak{p}^m$ avec $n \geq m$. On peut écrire

$$\begin{aligned} \tilde{\mathfrak{o}} &= \lim_{\leftarrow} \mathfrak{o}/\mathfrak{p}^n \\ \tilde{\mathfrak{p}^r} &= \ker(\pi_r : \tilde{\mathfrak{o}} \longrightarrow \mathfrak{o}/\mathfrak{p}^r) \ \ (r \geq 0). \end{aligned}$$

Nous possédons maintenant trois symboles différents : $\overline{j(\mathfrak{o})}$, $\hat{\mathfrak{o}}$ et $\tilde{\mathfrak{o}}$. Nous verrons plus tard qu'il s'agit essentiellement du même objet, mais du fait des trois constructions différentes on obtient une caractérisation intéressante de $\overline{K}$ comme le corps des fractions de $\lim_{\leftarrow} \mathfrak{o}/\mathfrak{p}^n$. L'intérêt de cette représentation consiste en une méthode purement algébrique de complétion.
Avant de prouver un théorème important sur ces notions, notons le lemme suivant provenant directement de la construction de la limite inverse :

Lemme 2.2.15
Il existe un homomorphisme $l : \mathfrak{o} \longrightarrow \tilde{\mathfrak{o}}$ tel que le digramme suivant

$$\begin{array}{ccc} \mathfrak{o} & \xrightarrow{l} & \tilde{\mathfrak{o}} \\ & \searrow^{r^m} & \downarrow{\scriptstyle \pi_m} \\ & & \mathfrak{o}/\mathfrak{p}^m \end{array}$$

commute.

Théorème 2.2.16
Les propriétés suivantes ont lieu :

1. *Pour tout entier positif m, π_m induit un isomorphisme $\tilde{\mathfrak{o}}/\tilde{\mathfrak{p}^m} \simeq \mathfrak{o}/\mathfrak{p}^m$;*
2. *Il existe un unique homomorphisme $\hat{l} : \hat{\mathfrak{o}} \longrightarrow \tilde{\mathfrak{o}}$ tel que*
   (i) *$\tilde{l}(j(a)) = l(a)$ pour tout $a \in \mathfrak{o}$,*
   (ii) *$\alpha \in \hat{\mathfrak{p}}^r$ si et seulement si $\tilde{l}(\alpha) \in \tilde{\mathfrak{p}^r}$ pour tout r ;*
3. *$\hat{l}$ est un isomorphisme $\hat{\mathfrak{o}} \simeq \tilde{\mathfrak{o}}$ par l'isomorphisme $\hat{\mathfrak{p}^r} \simeq \tilde{\mathfrak{p}^r}$.*

Observons que ce théorème implique que la fonction $\mathfrak{o}/\mathfrak{p}^r \longrightarrow \hat{\mathfrak{o}}/\hat{\mathfrak{p}}^r$, induite par j, est un isomorphisme.

Démonstration. Puisque les fonctions r_m sont surjectives, par le lemme 2.2.15 il en est de même pour les π_m. Le premier point du théorème est donc un conséquence du théorème d'isomorphisme.
Construisons maintenant $\hat{l}$. Soit $\{a_n\}$ une suite de Cauchy dans K, où tous les a_n sont dans $\mathfrak{o}$. Ainsi, pour un $N \in \mathbb{N}$ donné, il existe un $n_0 \in \mathbb{N}$ tel que

$$a_n \equiv a_{n_0} (\mathfrak{p}^N) (\forall n).$$

Soit $\tilde{a}(N)$ la classe de a_{n_0} dans $\mathfrak{o}/\mathfrak{p}^N$, nous l'appellerons *dernière classe de* $\{a_n\}$ *mod* $\mathfrak{p}^N$. On peut clairement remplacer n_0 par un entier naturel plus grand ou égal. étant donnée une autre suite de Cauchy $\{b_n\}$ avec $b_n \in \mathfrak{o}$, on a $a \tilde{+} b(N) = \tilde{a}(N) + \tilde{b}(N)$ la dernière classe de $\{a_n + b_n\}$ mod $\mathfrak{p}^N$. Ainsi, pour $N \geq M$, $\tilde{a}(M) = \pi_M^N \tilde{a}(N)$ et on a donc une fonction $\{a_n\} \mapsto \tilde{a} \in \tilde{\mathfrak{o}}$ qui définit un homomorphisme de groupes additifs $R_0(\mathfrak{o}) \longrightarrow \hat{\mathfrak{o}}$, avec $R_0(\mathfrak{o})$ l'anneau des suites de Cauchy à valeur dans $\mathfrak{o}$. Ainsi $\tilde{a}(N) = 0$ pour tout N si et seulement si $\{a_n\}$ est une suite de Cauchy tendant vers zéro. On a donc un homomorphisme injectif

$$R_0(\mathfrak{o})/R_0(\mathfrak{o}) \cap \mathfrak{n} \longrightarrow \tilde{\mathfrak{o}}.$$

Or, par le théorème 2.2.13, on sait que $\hat{\mathfrak{o}} = \overline{j(\mathfrak{o})}$ est le sous-ensemble de $\overline{K}$ représenté par les suites de Cauchy à valeur dans $\mathfrak{o}$. Ainsi, la fonctions $\{a_n\} \mapsto \tilde{a}$ donne lieu à un homomorphisme injectif $\hat{l} : \hat{\mathfrak{o}} \longrightarrow \tilde{\mathfrak{o}}$.
Revenons maintenant à la construction de $\hat{l}$. Si $\{a_n\}$ est une suite constante dans $\mathfrak{o}$, $a_n = a$ pour tout n, alors $\tilde{a}(N)$ est simplement la classe quotient $r_N(a)$ de a mod $\mathfrak{p}^N$. Ainsi $\hat{l} \circ j = l$.
Pour montrer que $\hat{l}$ est un isomorphisme, nous n'avons plus qu'à montrer sa surjectivité. Soit $\tilde{a} \in \tilde{\mathfrak{o}}$, choisissons $b_n \in \mathfrak{o}$ tels que leurs classes mod $\mathfrak{p}^n$ soient $\tilde{a}(n)$. Ainsi $\{b_n\}$ est une suite de Cauchy représentant un élément $\beta \in \hat{\mathfrak{o}}$ avec $\hat{l}(\beta) = \tilde{a}$.

Vérifions maintenant que $\alpha \in \hat{\mathfrak{p}}^r$ si et seulement si $\tilde{l}(\alpha) \in \tilde{\mathfrak{p}}^{\mathfrak{r}}$; cela montrera ausi et seulement si que la restriction de $\hat{l}$ à $\hat{\mathfrak{p}}^r$ est isomorphe à $\tilde{\mathfrak{p}}^{\mathfrak{r}}$. Soit α représenté par une suite de Cauchy $\{a_n\}$ à valeur dans $\mathfrak{o}$. Alors $\alpha \in \hat{\mathfrak{p}}^r$ si et seulement si pour une n assez grand, $a_n \in \mathfrak{p}^r$, i.e. $\hat{a}(r) = 0$; de plus, c'est équivalent à dire que $\tilde{a} \in \tilde{\mathfrak{p}}^r$.
En sus, remarquons que les propriétés 2.(i) et 2.(ii) déterminent entièrement $\hat{l}$. Soit l' un homomorphisme de $\hat{\mathfrak{o}} \longrightarrow \tilde{\mathfrak{o}}$ ayant ces deux propriétés. Soit $\alpha \in \hat{\mathfrak{o}}$ représenté par une suite de Cauchy $\{a_n\}$ à valeur dans $\mathfrak{o}$. Comme nous l'avons vu précédemment, $\hat{l}(\alpha)(N)$ est la dernière classe de $\{a_n\}$ mod $\mathfrak{p}^N$. Choisissons $b \in \mathfrak{o}$ avec $r_N(b) = \hat{l}(\alpha)(N)$. Ainsi, par la la propriété (i), $l'(j(b))(N) = l(b)(N) = r_N(b) = \hat{l}(\alpha)(N)$; Ainsi, par la seconde propriété, $\alpha - j(b) \in \hat{\mathfrak{p}}^N$. Il s'ensuit que $l'(\alpha) - l'(j(b)) \in \hat{\mathfrak{p}}^N$, ainsi $l'(\alpha) - l'(j(b))(N) = 0$ et $l'(\alpha)(N) = \hat{l}(\alpha)(N)$. Cela étant vrai pour tout N, on a $l'(\alpha) = \hat{l}(\alpha)$.

q.e.d

Grâce à ce théorème, on peut simplifier les notations : nous avons vu que K est plongé dans $\overline{K}$, nous pouvons donc omettre le j et identifier $\overline{\mathfrak{o}}$, $\hat{\mathfrak{o}}$ et $\tilde{\mathfrak{o}}$, de même pour $\overline{\mathfrak{p}}$, $\hat{\mathfrak{p}}$ et $\tilde{\mathfrak{p}}$. On peut donc écrire $|.|_v$ pour $\|.\|$, omettre Dans le cas où K est complet (avec $|.|$ discret) et $\mathfrak{o}$ l'anneau de valuation $\{x \in K \mid |x| < 1\}$, le théorème nous dit que $\mathfrak{o} \simeq \lim_{\leftarrow} \mathfrak{o}/\mathfrak{p}^n$.
Munis de ces notations et sous les hypothèses du théorème précédent, nous avons :

Lemme 2.2.17
L'homomorphisme $\theta : \hat{\mathfrak{o}} \otimes_{\mathfrak{o}} K \longrightarrow \overline{K}$ définit par $a \otimes x \mapsto ax$ est un isomorphisme.

Démonstration. Soit $\pi \in \mathfrak{o}$ tel que $v(\pi) = 1$, alors $\overline{K} = \hat{\mathfrak{o}}[\pi^{-1}]$ et donc θ est surjectif. étant donné un élément $y = \sum_i a_i \otimes x_i$ de $\hat{\mathfrak{o}} \otimes K$, soit $n = \min_i(0, v(x_i))$; alors $y = (\sum a_i x_i \pi^{-n}) \otimes \pi^n$. Donc si $\sum a_i x_i = 0$ alors $y = 0$, i.e. θ est injective.

q.e.d

Soit R l'ensemble des représentants dans $\hat{\mathfrak{o}}$ pour les éléments de $k = \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$, où le zéro de $\hat{\mathfrak{o}}$ représente le zéro de k. Pour tout $n \in \mathbb{Z}$, soit π_n un élément de $\overline{K}$ tel que $\hat{v}(\pi_n) = n$. Soit une série $\sum_{n=N}^{\infty} r_n \pi_n$, $r_n \in R$, qui converge. Si

$$\alpha = \sum_{n=N}^{\infty} r_n \pi_n,$$

alors pour toute somme partielle avec M sufisemment grand

$$\hat{v}\left(\sum_{n=n}^{M} r_n \pi_n\right) = \inf(n \mid r_n \neq 0).$$

Le passage à la limite nous donne

$$\hat{v}(\alpha) = \inf(n \,|\, r_n \neq 0).$$

Cela a du sens pour $\alpha = 0$, puisque $\hat{v}(0) = \infty$.

Lemme 2.2.18
Tout élément α de $\overline{K}$ peut être représenté comme somme définie ci-dessus.

Démonstration. Comme nous l'avons fait remarqué, on peut supposer que $\alpha \neq 0$, i.e. $\hat{v}(\alpha) = N$. Ainsi $\alpha\pi_N^{-1} \in \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ puisque $\alpha\pi_n^{-1} \equiv r_N(\hat{\mathfrak{p}})$ pour un certain $r_n \in R$, $r_N \neq 0$. Ainsi $\alpha \equiv r_n\pi_N\,(\hat{\mathfrak{p}})^{N+1}$. Nous pouvons maintenant commencer la récurence. Si maintenant

$$\alpha \equiv \sum_{n=N}^{M} r_n\pi_n \;\; (\hat{\mathfrak{p}}^{M+1}),$$

alors $\left(\alpha - \sum_{n=N}^{M} r_n\pi_n\right)\pi_{M+1}^{-1} \in \hat{\mathfrak{o}}$, donc α est congrue à r_{M+1} mod $\hat{\mathfrak{p}}$ pour un certain $r_{M+1} \in R$. Ainsi

$$\alpha \equiv \sum_{n=N}^{M+1} r_n\pi_n \;\; (\hat{\mathfrak{p}}^{M+2}),$$

et donc $\lim_M \left|\alpha - \sum_{n=N}^{M+1} r_n\pi_n\right| = 0$.

q.e.d

Soit p un nombre premier. Considérons la complétion de $\mathbb{Q}$ pour la valeur absolue $|.|_p$. Rappelons que pour $ab^{-1}p^s$, avec $a, b \in \mathbb{Z}$, $p \nmid ab$, on a $|ab^{-1}p^s|_p = p^{-s}$. Le corps obtenu est noté $\mathbb{Q}_s$ et appelé *corps de nombre p-adique* ou *corps p-adique*. On note $\mathbb{Z}_p$ la clôture de $\mathbb{Z}$ dans $\mathbb{Q}_p$ et on l'appelle *anneau p-adique des entiers*. On sait que $p\mathbb{Z}_p$ est l'idéal de valuation de $\mathbb{Z}$ et que

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p.$$

Par le lemme précédent, on peut écrire chaque élément $\alpha \in \mathbb{Q}_p$ comme $\alpha = \sum_{i=N}^{\infty} r_i p^i$ où $r_i \in \{0, 1, \ldots, p-1\}$.

Théorème 2.2.19 (Lemme d'Hensel)
Soit $f \in \hat{\mathfrak{o}}[X]$ et α_n tel que $\hat{v}(f'(\alpha_n)) \geq c$ et $\hat{v}(f(\alpha_n)) \geq n+c$ où $n > c$. Alors il existe $\alpha_{n+1} \in \hat{\mathfrak{o}}$ avec $\hat{v}(\alpha_{n+1} - \alpha_n) \geq n$, $\hat{v}(f'(\alpha_{n+1})) = c$ et $\hat{v}(f(\alpha_{n+1})) \geq n + 1 + c$. De plus, $\alpha = \lim_n \alpha_n \in \hat{\mathfrak{o}}$ est tel que $f(\alpha) = 0$.

Démonstration. Soit π un générateur de $\hat{\mathfrak{p}}$ sur $\hat{\mathfrak{o}}$. On sait que pour $\lambda \in \hat{\mathfrak{o}}$, on a

$$f(\alpha_n + \lambda\pi^n) = f(\alpha_n) + \lambda\pi^n f'(\alpha_n) + (\lambda\pi^n)^2 h(\alpha_n, \lambda\pi^n)$$

où $h(X, Y)$ est un polynôme à deux variables dans $\hat{\mathfrak{o}}$. De plus

$$f(\alpha_n + \lambda\pi^n) = f(\alpha_n) + \lambda\pi^n f'(\alpha_n) \bmod \hat{\mathfrak{p}}^{2n}.$$

Ainsi, en posant $\lambda = -f(\alpha_n)\pi^{-n} f'(\alpha_n)^{-1} \in \hat{\mathfrak{o}}$ et $\alpha_{n+1} = \alpha_n + \lambda\pi^n$, alors $f(\alpha_{n+1}) \in \hat{\mathfrak{p}}^{2n} \subset \hat{\mathfrak{p}}^{n+1+c}$. D'un autre côté, on a

$$\hat{v}(f'(\alpha_{n+1})) = \hat{v}(f'(\alpha_n)) = c.$$

En itérant le processus, on obtient une suite de Cauchy $\{\alpha_n\}$. Elle converge donc vers une limite, disons α. Ainsi $f(\alpha_n)$ tend vers zéro et donc

$$0 = \lim_n f(\alpha_n) = f(\lim_n \alpha_n) = f(\alpha).$$

q.e.d

Corollaire 2.2.20
Soit $k = \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ et supposons que la classe du polynôme $\overline{f} \in k[X]$ possède une unique racine $\overline{\alpha}$ dans k. Alors f possède une racine simple $\alpha \in \hat{\mathfrak{o}}$ dont la classe dans k est $\overline{\alpha}$.

Démonstration. Pour démontrer ce théorème, nous débuterons la récurence avec $\hat{v}(f(\alpha_1)) \geq 1$, $\hat{v}(f'(\alpha_1)) = 0$. En appliquant le lemme, on obtient la racine α de f avec $\alpha = \alpha_1 \bmod \hat{\mathfrak{p}}$ et $f'(\alpha) \neq 0 \bmod \hat{\mathfrak{p}}$, i.e. $f'(\alpha) \neq 0$, donc α est une racine simple.

q.e.d

Appliquons le lemme d'Hensel au cas où $[\hat{\mathfrak{o}} : \hat{\mathfrak{p}}] = q$ est fini. Ainsi $\hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ est un corps de caractéristique premier p. Ecrivons $\mu'_{\overline{K}}$ l'ensemble des racines de l'unité dans $\overline{K}$ d'ordre premier à p. Clairement $\mu'_{\overline{K}} \in \hat{\mathfrak{o}}^\star$ et le passage au quotient nous donne un homomorphisme

$$\rho : \mu'_{\overline{K}} \longrightarrow (\hat{\mathfrak{o}}/\hat{\mathfrak{p}})^\star.$$

Proposition 2.2.21
ρ est un isomorphisme.

Démonstration. Supposons que $\mu'_{\overline{K}}$ contient le groupe μ_m des m-èmes racines de l'unité. Comme $X^m - 1$ est séparable sur $\hat{\mathfrak{o}}/\hat{\mathfrak{p}}$, $\rho|_{\mu_m}$ est injective. Puisque $\mu'_{\overline{K}}$ est fini, il en est de même pour ρ. Et puisque X^{q-1} est séparable, par le lemme d'Hensel ρ est surjective.

q.e.d

A partir de cette proposition, on sait que $\mathbb{Q}_p$ contient μ_{p-1}, le groupe des $p-1$ racines de l'unité, et que c'est l'ensemble entier des représentants des classes non nulles de $\mathbb{Z}_p/p\mathbb{Z}_p$. Ainsi tout élément α peut être écrit sous la forme

$$\alpha = \sum_{i=N}^{\infty} \zeta_i p^i$$

où $\zeta_i \in \mu_{p-1} \cup \{0\}$. On appelle cela la *représentation de Teichmüller de* α.
Finalement, appliquons le lemme d'Hensel aux résidus quadratiques dans $\mathbb{Q}_p$.

Lemme 2.2.22
Soit $\xi \in \mathbb{Z}_p^\star$; alors $\xi \in \mathbb{Q}_p^{\star 2}$ si et seulement si

$$\begin{cases} \left(\frac{\xi}{p}\right) = 1 & si \quad p \neq 2 \\ \xi \equiv 1(8\mathbb{Z}_2) & si \quad p = 2. \end{cases}$$

Démonstration. Si $y \in \mathbb{Q}_p$ avec $y^2 = \xi$, alors $2\hat{v}(y) = \hat{v}(\xi) = 0$ et donc $y \in \mathbb{Z}_p^\star$. En particulier, $y^2 = \xi \bmod p\mathbb{Z}_p$ et ainsi $\xi \bmod p\mathbb{Z}_p$ est un carré dans $\mathbb{F}_p^\star$. De plus, si $p = 2$, on peut écrire $y = 1 + 2\beta \bmod 8\mathbb{Z}_2$ avec $\beta \in \mathbb{Z}_2$. Alors $y^2 = 1 + 4(\beta^2 + \beta) \bmod 8\mathbb{Z}_2$. Il s'ensuit que $y \equiv 1(8\mathbb{Z}_2)$.
D'autre part, si $p \neq 2$ et si $y^2 = \xi \bmod p\mathbb{Z}_p$, alors $X^2 - \xi$ a une solution dans $\mathbb{Z}_p$ et le résultat s'ensuit. Enfin, si $p = 2$ et si $\xi \equiv 1(8\mathbb{Z}_2)$,alors on peut appliquer le corollaire du lemme d'Hensel au polynôme $X^2 - \xi$ (avec $n > c = 1$).

q.e.d

Pour terminer ce chapitre, nous allons nous intéresser aux topologies induites sur les limites inverses. Pour commencer, supposons que chaque A_n est muni de la topologie discrète (cela nous donnera une idée pour la suite). Une base de voisinage d'un point $a \in A$ consiste alors en tous les points $x \in A$ avec $\alpha_n(x) = \alpha_n(a)$ pour un certain $n \in \mathbb{N}$, où $\alpha_n : A \longrightarrow A_n$ est la fonction composante.
Soit maintenant $\overline{K}, |.|_{\hat{v}}$ un corps complet valué selon la valeur absolue venant de $\hat{v}$. Nous avons précédemment identifié algébriquement l'anneau de valuation $\hat{\mathfrak{o}}$ de $\overline{K}$ et la limite inverse $\tilde{\mathfrak{o}} = \lim_{\leftarrow} \hat{\mathfrak{o}}/\hat{\mathfrak{p}}^n$. Observons maintenant que les deux topologies en question coïncident, i.e. les sous-espaces de l'espace métrique $(\overline{K}, |.|_{\hat{v}})$ est le même que l'ensemble des ouverts obtenus par la limite des topologies.. En fait, c'est seulement une réinterprétation du théorème 2.2.16.
La topologie $(\overline{K}, |.|_{\hat{v}})$ est de Hausdorff, puisqu'elle est induite d'une métrique ; et c'est ausi et seulement si vrai pour un corps valué. Le fait que $|.|_{\hat{v}}$ est discret

produit en fait un résultat plus fort. On remarque cela depuis la définition de $\hat{\mathfrak{p}}^r$

$$\begin{aligned}\hat{\mathfrak{p}}^r &= \{x \in \overline{K} \,|\, \hat{v}(x) > r-1\} \\ &= \{x \in \overline{K} \,|\, \hat{v} \geq r\}\end{aligned}$$

et donc $\{\hat{\mathfrak{p}}^r \,|\, r \in \mathbb{N}\}$ est une base des voisinages ouverts de 0 ; de plus ce sont tous des ensembles fermée. Donc $\overline{K}$ est un espace topologique discret.

Lemme 2.2.23
Si $k = \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ est fini, alors chaque ensemble $\hat{\mathfrak{p}}^r$ est compact.

Démonstration. En utilisant les notations précédentes $\hat{\mathfrak{p}}^r = \pi^r \hat{\mathfrak{o}}$ il nous suffit de prouver le résultat pour $\hat{\mathfrak{o}}$. Suppsons par l'absurde que $\mathfrak{C}$ soit une couverture de $\hat{\mathfrak{o}}$ qui ne contient aucune sous-couverture finie de $\hat{\mathfrak{o}}$.
Par récurence, on assert que pour un j donné, on peut trouver une classe $y_j + \hat{\mathfrak{p}}^{j+1}$ qui n'a pas de sous-couverture finie par $\mathfrak{C}$ et tel que $y_j + \hat{\mathfrak{p}}^j = y_{j-1} + \hat{\mathfrak{p}}^j$. Supposons que $y_1, \ldots, y_{j-1}$ soient construits. Puisque $\hat{\mathfrak{p}}^j/\hat{\mathfrak{p}}^{j+1} \simeq k$ est fini, alors il n'existe qu'un nombre fini de classes $z + \hat{\mathfrak{p}}^{j+1}$ qui représentent $y_{j-1} + \hat{\mathfrak{p}}^j$ sous $\hat{\mathfrak{o}}/\hat{\mathfrak{p}}^{j+1} \longrightarrow \hat{\mathfrak{o}}/\hat{\mathfrak{p}}^j$. Puisque $y_{j-1} + \hat{\mathfrak{p}}^j$ n'a pas de sous-recouvrement sous $\mathfrak{C}$. Il s'ensuit qu'au moins l'une des classes $z + \hat{\mathfrak{p}}^{j+1}$ possède ausi et seulement si cette propriété. Choisissons-en donc une et écrivons-la $y_j + \hat{\mathfrak{p}}^{j+1}$. Ainsi on a établit l'étape de récurence.
Pour montrer le lemme, soit $y = \lim_{j \longrightarrow \infty} y_j$. Alors y se trouve dans un ensemble ouvert $U \in \mathfrak{C}$; ainsi $y_i + \hat{\mathfrak{p}}^{j+1}$ est contenu dans U pour des j assez grand, ce qui contredit le fait que $y_j + \hat{\mathfrak{p}}^{j+1}$ n'a pas de sous-recouvrement fini de $\mathfrak{C}$.

q.e.d

Corollaire 2.2.24
$\mathbb{Z}_p$ est compact.

Proposition 2.2.25
Si $\hat{\mathfrak{o}}$ est compact, alors k est fini.

Démonstration. k est nécessairement compact, car il est l'image de $\hat{\mathfrak{o}}$ sous la surjection continue $\hat{\mathfrak{o}} \longrightarrow \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$. Puisque $\hat{\mathfrak{p}}$ est un ouvert dans $\hat{\mathfrak{o}}$, $\hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ doit être descret. Le résultat vient du fait qu'un ensemble discret et compact est fini.

q.e.d

CHAPITRE 3

Extensions

3.1 Décomposition et ramification

Avant de débuter cette section, nous fixons quelques notations. Dorénavant nous utiliserons les lettres u et w pour désigner les valeurs absolues. Commençons donc par regarder ce qu'il se passe pour une extension d'un corps complet évalué (K, u) ayant la propriété suivante

Propriété 3.1.1
Pour une extension finie E/K, il y a une valeur absolue $w : E \longrightarrow \mathbb{R}$ telle que $w|_K = u$.

Théorème 3.1.2
Soit (K, u) un corps évalué complet ayant la propriété 3.1.1 et E une extension finie séparable de K. Alors l'extension w de u sur E est unique, et (E, w) est complet. De plus pour $a \in E$

$$w(a)^{(E:K)} = u(N_{E/K}(a))$$

et si u est une valeur absolue discrète, il en est de même pour w.

Définition 3.1.3
*Soit V un K-espace vectoriel et u une valeur absolue sur K. La fonction $\|.\| : V \longrightarrow \mathbb{R}_{\geq 0}$ est une u-*norme *si pour $x \in V$*

(i) $\|x\| = o$ *si et seulement si* $x = 0$,

(ii) $\|x\lambda\| = \|x\| \cdot u\lambda$ *pour* $\lambda \in L$,

(iii) Pour $y \in V$, $\|x+y\| \leq \|x\| + \|y\|$.

Deux norme $\|.\|$ *et* $\|.\|'$ *sont* équivalentes *si et seulement si il existe des réels positifs* c *et* d *tel que pour tout* $x \in V$

$$c\,\|x\| \leq \|x\|' \leq d\,\|x\|\,.$$

On remarque clairement que deux normes équivalentes induisent la même topologie sur V.
Soit $\mathfrak{o}$ un anneau de Dedekind de corps de fraction K. Soit $\mathfrak{p}$ un idéal premier de $\mathfrak{o}$. Supposons de plus que L/K est une extension finie séparable de K. $\mathfrak{o}_L$ est la clôture intégrale de $\mathfrak{o}$ dans L, et $\mathfrak{B}$ est un idéal premier de $\mathfrak{o}_L$ étendant $\mathfrak{p}$, i.e. $\mathfrak{o} \cap \mathfrak{B} = \mathfrak{p}$. $K_\mathfrak{p}$ est la complétion de K selon la valeur absolue discrète $|.|_\mathfrak{p}$ associée à $v_\mathfrak{p}$. $\mathfrak{o}_\mathfrak{p}$ désigne la clôture de $\mathfrak{o}$ dans $K_\mathfrak{p}$ et $\overline{\mathfrak{p}}$ celle de $\mathfrak{p}$ dans $K_\mathfrak{p}$.

Définition 3.1.4
*L'*indexe de ramification de $\mathfrak{B}$ dans L/K *est donné par la fonction*

$$e_\mathfrak{B}(L/K) = v_\mathfrak{B}(\mathfrak{p}\mathfrak{o}_L)$$

où $v_\mathfrak{B}$ *désigne la valuation associée à* $\mathfrak{B}$.

Remarquons que cette définition est équivalente à dire que

$$\mathfrak{p}\mathfrak{o}_l = \mathfrak{B}^e\mathfrak{a}$$

pour un certain $\mathfrak{o}_L$-idéal qui est copremier à $\mathfrak{B}$. Clairement $e \geq 1$. L'idéal premier $\mathfrak{B}$ est dit *ramifié dans* L/K si $e > 1$.
On remarque que l'inclusion $\mathfrak{o} \hookrightarrow \mathfrak{o}_L$ induit une inclusion sur les ensembles quotients $\mathfrak{o}/\mathfrak{p} \hookrightarrow \mathfrak{o}_L/\mathfrak{B}$, et du plus $\mathfrak{o}_L/\mathfrak{B}$ vu comme une extension de $\mathfrak{o}/\mathfrak{p}$ est de degré fini, puisque $\mathfrak{o}_L$ est de génération finie sur $\mathfrak{o}$.

Définition 3.1.5
On appelle le degré de la classe de résidu de $\mathfrak{B}$ dans L/K *la fonction définie par*

$$f_\mathfrak{B} = \dim_{\mathfrak{o}/\mathfrak{p}}(\mathfrak{o}_L/\mathfrak{B}) = [\mathfrak{o}_L/\mathfrak{B} : \mathfrak{o}/\mathfrak{p}].$$

Lemme 3.1.6
e et f sont invariants par complétion sous $|.|_\mathfrak{B}$.

Démonstration. Il s'agit en fait principalement d'un conséquence du théorème 2.2.13 et de son corollaire :
En écrivant la clôture dans la complétion et du fait que $\overline{\mathfrak{B}}$ est l'unique idéal premier de $\overline{\mathfrak{o}_L}$, on sait par le corollaire que $\overline{\mathfrak{p}} \cdot \overline{\mathfrak{o}_L} = \overline{\mathfrak{B}}^e$ et donc l'indice de

ramification reste inchangé. De plus on sait que l'on a un isomorphisme de $\mathfrak{o}$-module

$$\mathfrak{o}_L/\mathfrak{B} \simeq \overline{\mathfrak{o}_L}/\overline{\mathfrak{B}}.$$

Le lemme est ainsi prouvé.

q.e.d

Lemme 3.1.7
Soit $N \supset L \supset K$ une tour d'extensions finie séparables et $\mathfrak{q}$ un idéal premier de $\mathfrak{o}_N$ étendant $\mathfrak{B}$. Alors on a les formules suivantes :

$$\begin{aligned} e_{\mathfrak{q}}(N/K) &= e_{\mathfrak{q}}(N/L)e_{\mathfrak{B}}(L/K) \\ f_{\mathfrak{f}}(N/K) &= f_{\mathfrak{q}}(N/L)f_{\mathfrak{B}}(L/K). \end{aligned}$$

Démonstration. Le résultat pour les indices de ramification est conséquence immédiate de la représentation en produit. Celui des degré des classes de résidu est déduit de la formule en tours pour les extensions finies séparables.

q.e.d

Lemme 3.1.8
Si K est complet pour la valeur absolue $|.|_{\mathfrak{p}}$, alors $\mathfrak{p}$ (resp. $\mathfrak{B}$) est l'unique idéal premier de $\mathfrak{o}$ (resp. $\mathfrak{o}_L$). On peut donc écrire

(*i*) *$ef = [L : K]$;*

(*ii*) *le diagramme suivant commute*

$$\begin{array}{ccc} K^\star & \xrightarrow{v_{\mathfrak{p}}} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^\star & \xrightarrow{v_{\mathfrak{B}}} & \mathbb{Z}; \end{array}$$

(*iii*) *le diagramme suivant commute*

$$\begin{array}{ccc} L^\star & \xrightarrow{v_{\mathfrak{B}}} & \mathbb{Z} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow f \\ K^\star & \xrightarrow{v_{\mathfrak{p}}} & \mathbb{Z}. \end{array}$$

Démonstration. Puisque $\mathfrak{o}_L$ est $\mathfrak{o}$-libre de rang $[L : K]$, il s'ensuit que $\mathfrak{o}_L/\mathfrak{p}\mathfrak{o}_L$ est un $\mathfrak{o}/\mathfrak{p}$-espace vectoriel de dimension $[L : K]$. De plus on peut montrer facilement que les $\mathfrak{o}/\mathfrak{p}$-espace vectoriel $\mathfrak{B}^j/\mathfrak{B}^{j+1}$ ont tous la même dimension, f. Puisque de plus $\mathfrak{B}^e = \mathfrak{p}\mathfrak{o}_L$, il s'ensuit immédiatement que $ef = [L : K]$. De plus par la représentation en produit, on en déduit que si $x \in K^\star$, alors

$v_{\mathfrak{B}}(x) = ev_{\mathfrak{p}}$.
Il ne nous reste donc plus qu'à montrer la commutativité du second diagramme : on déduit du théorème 3.1.2 que $v_{\mathfrak{B}}(a) = 0$ si et seulement si $v_{\mathfrak{p}}(N_{L/K}(a)) = 0$ pour $a \in L^\star$. On peut montrer que pour un certain entier f', le diagramme suivant commute

$$\begin{array}{ccc} L^\star & \xrightarrow{v_{\mathfrak{B}}} & \mathbb{Z} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle f'} \\ K^\star & \xrightarrow{v_{\mathfrak{p}}} & \mathbb{Z}. \end{array}$$

. Pour déterminer exactement ce f', on choisi un $\mathfrak{o}$-générateur π de $\mathfrak{p}$. Alors $v_{\mathfrak{p}}(\pi) = 1$, puisque $N_{L/K}(\pi) = \pi^{[L:K]}$ et donc $v_{\mathfrak{p}}(N_{L/K}(\pi)) = [L : K]$. Mais puisque $v_{\mathfrak{B}}(\pi) = e$, on a $ef' = [L : K]$ et par le point (i), on en déduit que $f' = f$.

q.e.d

3.2 Extensions non-ramifiées et totalement ramifiées

Dans cette section, nous utiliserons la notation suivante : K sera un corps complet pour une valeur absolue u associée à une évaluation v. $\mathfrak{o}$ sera l'anneau d'évaluation de K et $\mathfrak{p}$ l'idéal d'évaluation. Nous supposerons de plus $k = \mathfrak{o}/\mathfrak{p}$ fini.

Définition 3.2.1
Un élément $\pi \in \mathfrak{p}$ est paramètre uniformisant de K *si $\pi\mathfrak{o} = \mathfrak{p}$.*
Considérons l'équation fournie par le lemme 3.1.8 : $[L : K] = e(L/K)f(L/K)$.
Une extension est dite totalement ramifiée *si $e(L/K) = [L : K]$. Dans ce cas $f = 1$ et le corps de la classe de résidu de $\mathfrak{o}_l$, noté k_L, est égal à k.*
Le polynôme unitaire

$$g(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in \mathfrak{o}[X]$$

est un polynôme d'Eisenstein *sur K si $a_j \in \mathfrak{p}$ pour tout j et $a_0 \notin \mathfrak{p}^2$, i.e. a_0 est un paramètre uniformisant de K.*

La dernière définition provient du critère d'irréductibilité d'Eisenstein pour les polynômes. En appliquant ce critère au domaine principal $\mathfrak{o}$, on voit que g est irréductible dans $\mathfrak{o}[X]$. Ainsi par le lemme de Gauss, il est irréductible dans $K[X]$. Nous allons montrer cela d'une autre façon.

Théorème 3.2.2
Soit L/K une extension finie séparable :

1. *Les assertions suivantes sont équivalentes*
   - *(i)* $L = K(\lambda)$ *pour* λ *une racine d'un certain polynôme d'Eisenstein* $g(X)$,
   - *(ii)* L/K *est totalement ramifiée,*
   - *(iii)* $\mathfrak{o}_L = \mathfrak{o}[\lambda]$ *pour un paramètre uniformisant* λ *;*
2. *Si la condition (i) est satisfaite, alors* λ *est un paramètre uniformisant et* $\deg(g) = [L : K]$ *et donc* g *est irréductible sur* K *;*
3. *Le polynôme minimal sur* K *d'un paramètre uniformisant d'une extension totalement ramifiée et séparable* L *de* K *est un polynôme d'Eisenstein dur* K.

Démonstration. Supposons que $L = K(\lambda)$ pour λ racine d'un certain polynôme d'Eisenstein, disons $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$. Puisque $g \in \mathfrak{o}[X]$, on en déduit que $\lambda \in \mathfrak{o}_L$. Ainsi

$$\lambda^n = -\sum_{j=0}^{n-1} b_j X^j \ \in \ \mathfrak{p}\mathfrak{o}_L,$$

de plus si v_L est la valuation sur L (associée à l'idéal premier $\mathfrak{B}$ de $\mathfrak{o}_L$ étendant $\mathfrak{p}$), alors $v_L(\lambda) \geq 1$. De plus comme

$$v_L(\lambda^n + b_0) = v_L\left(-\sum_{j=1}^{n-1} b_j \lambda^j\right) \geq 1 + e(L/K)$$

et $v_L(b_0) = e(L/K)$, on doit avoir $v(\lambda^n) = e(L/K)$. On a ainsi les inégalités

$$[L : K] \geq e(L/K) = nv_L(\lambda) \geq n \geq [L : K].$$

Ainsi puisque $e(L/K) = [E : K]$, L/K est totalement ramifié, puisque $n = [L : K]$, g est irréductible et puisque $nv_L(\lambda) = n$ λ est un paramètre uniforme.
Supposons maintenant que L/K est totalement ramifiée et montrons que $\mathfrak{o}_L = \mathfrak{o}[\lambda]$ pour un paramètre uniformisant $\lambda \in L$. Puisque $k_l = k$, on peut choisir l'ensemble des représentants R de k_l par $\mathfrak{o}$. Pour un paramètre uniformisant λ de L, et pour $h = i + ej$ (la division euclidienne forte par e de h), on pose $\lambda_h = \lambda^i \pi^j$ où π est un paramètre uniformisant de K. Il nous faut donc montrer que tout élément de $\mathfrak{o}_L$ peut s'écrire de la forme $\sum_{i=0}^{e-1} a_i \lambda^i \in \mathfrak{o}[\lambda]$ (par la représentation des éléments de $\mathfrak{o}_L$). Mais puisque $\lambda \in \mathfrak{o}_L$, il s'ensuit

évidemment que $\mathfrak{o}[\lambda] \subset \mathfrak{o}_L$.
Enfin, supposons que $\mathfrak{o}_L = \mathfrak{o}[\lambda]$ pour un paramètre uniformisant λ. Soit P l'idéal premier de $\mathfrak{o}_L$, alors on sait que $\mathfrak{o}_L/P = \mathfrak{o}/\mathfrak{p}$, puisque $f(L/K) = 1$ et donc $e = e(L/K) = [L : K]$. Ainsi L/K est totalement ramifiée et d'autre part $L = K(\lambda)$. Montrons que λ est la racine d'un polynôme d'Eisenstein.
Par hypothèse, on peut écrire $\lambda^e = \sum_{i=0}^{e-1} c_i\lambda^i$ avec $c_i \in \mathfrak{o}$. Il s'ensuit donc que $v_L(\lambda^e - c_0) \geq 1$, d'où $v_L(c_0) \geq 1$. Ce la implique que $v_K(c_0) \geq 1$; ainsi $v_L(c_0) \geq e$ et donc $v_L(\lambda^e - c_0) \geq e$. En procédant de la même manière, $v_L(\lambda^e - c_1\lambda - c_0) \geq 2$ et donc $v_K(c_1) \geq 1$. Par induction on en déduit que $v_K(c_j) \geq 1$ pour tout $j = 0, \ldots, e-1$. On en déduit que $v_L(\lambda^e - c_0) \geq e+1$ et donc $e = ev_L(\lambda) = v_L(\lambda^e) = v_L(c_0)$. Ainsi $v_K(c_0) = 1$ et $g(X) = X^e - \sum_{j=0}^{e-1} c_j X^j$ est un polynôme d'Eisenstein.

q.e.d

Corollaire 3.2.3
Soit F un corps de nombre algébrique, et $g \in \mathfrak{o}_F[X]$ tel que g est un polynôme d'Eisenstein dans $F_\mathfrak{p}[X]$ pour un certain idéal premier $\mathfrak{p}$ de $\mathfrak{o}_F$. Alors g est irréductible dans $F[X]$.

Considérons maintenant le cas opposé où l'extension L/K c'est pas ramifiée, i.e. $e(L/K) = 1$ et donc $f(L/K) = [L : K]$.
Pour un corps F et un entier positif m tel qu'il est copremier à la caractéristique de F. On écrira $F[m]$ le corps obtenu en ajoutant une m-ème racine de l'unité (donnée dans une clôture séparable de F) de F.

Théorème 3.2.4
Soit un entier positif f, alors il existe une extension $K\{f\}$ de K de degré f. De plus cette extension est unique à isomorphisme près dans une clôture algébrique de K. De fait, $K\{f\} = K[m]$ pour un certain m tel que $N(\mathfrak{p})$ est d'ordre f dans $(\mathbb{Z}/m\mathbb{Z})^\star$. En particulier, $K\{f\}$ est généré sur K par une $N(\mathfrak{p})^f - 1$-racine primitive de l'unité.
Si L/K est une extension finie séparable, alors $L \supset K\{f\} \supset K$ pour $f = f(L/K)$. De plus L/Kf est totalement ramifiée et $K\{f\}$ est l'unique extension maximale non-ramifiée de K dans L.

Démonstration. Assertion Soit M une extension finie séparable de K et k_M le corps de la classe de résidu de $\mathfrak{o}_M$. Soit m un entier positif tel que $(m, N\mathfrak{p}) = 1$. Alors les facteurs irréductibles de $\overline{g(X)}$ de $X^m - 1$ dans $k_M[X]$ sont exactement les réductions des facteurs irréductibles de $X^m - 1$ dans $M[X]$.
Par le lemme d'Hensel, $X^m - 1$ est séparable. Ainsi, soit $g(X)$ un diviseur irréductibles de $X^m - 1$ dans $M[X]$ et $h(X)$ un diviseur unitaire du polynôme

de la classe de résidu $\overline{g(X)}$ dans $k_M[X]$. On choisi $f(X)$ dans $M[X]$ tel que $\overline{f(X)} = h(X)$; ainsi $f(X)$ doit être irréductible.
étendons M à une racine α de $f(X)$; écrivons $N = M(\alpha)$. Dans k_N, le polynôme $h(X)$ possède ainsi $\overline{\alpha}$ comme racine et donc ausi et seulement si $\overline{g(X)}$. Par le lemme d'Hensel, $g(X)$ possède une racine dans N. Ainsi $\deg g(X) \geq \deg h(X) = [N : M] \geq \deg g(X)$. Ainsi $\overline{g(X)} = h(X)$, i.e. $g(X)$ est irréductible.
Par l'assertion, on a donc

$$[K[m] : K] = [k[m] : k],$$

et ainsi $k_{K[m]} \supset k[M]$. Comme précédemment $[K[m] : K] \geq [k_{K[m]} : k]$, on déduit que

$$k[m] = k_{K[m]}.$$

Ainsi $K[m]/K$ n'est pas ramifié.
Si maintenant L est une extension de K finie et séparable, il s'ensuit que $L \supset K[m]$ si et seulement si $k_L \supset k[m]$. Soit m_1 tel que $k_L = k[m_1]$. Supposons d'abord que L n'est pas ramifié, alors $[L : K] = [k[m_1]]$. Et nous venons que voir qu'alors $L = K[m_1]$.
Ainsi les corps $K[m]$ avec $(m, N\mathfrak{p}) = 1$ sont exactement les extensions non-ramifiées de K, $K[m]$ est contenu dans L si et seulement si $k[m] \subset k_L$.
Nous savons qu'un corps fini k possède une extension de degré donné f unique à isomorphisme près. Nous l'écrirons $k\{f\}$. Si $|k| = N\mathfrak{p}$, alors $k\{f\} = k[m]$ pour un certain m tel que f est l'ordre de $N\mathfrak{p}$ modulo m, par exemple $m = N\mathfrak{p}^f - 1$. Soit donc un tel m, $K[m]$ doit donc être de degré f sur K. Comme $m | N\mathfrak{p}^f - 1$, $K[m]$ doit être contenu dans $K[N\mathfrak{p}^f - 1]$. De plus, comme ils ont le même degré, ils doivent coïncider. Ainsi K possède une extension non-ramifiée $K\{f\}$, unique dans une clôture algébrique de K et unique à isomorphisme près sur K. De plus si $f_1 | f$, alors $N\mathfrak{p}^{f_1} - 1 | N\mathfrak{p}^f - 1$ et donc $K\{f_1\} \subset K\{f\}$.
Si maintenant L est une extension finie séparable de K, alors $k_L = k\{f(L/K)\}$. On a donc que $K\{f(L/K)\} = L_0$ est une extension non-ramifiée de K dans L. Ainsi $f(L/K) = f(L_0/K)$ et donc $f(L/L_0) = 1$, i.e. L/L_0 est totalement ramifiée.

q.e.d

3.3 Ramification dans les extensions galoisiennes

Avant de commencer cette section, nous fixerons quelques conventions. K désignera un corps complet selon une valeur absolue discrète u, associée

à l'évaluation v. La classe de résidu k de l'anneau $\mathfrak{o}$ est toujours finie de caractéristique p. L désignera une extension finie galoisienne de K, et $\Delta = \mathrm{Gal}\,(L/K)$, et v_L sera l'évaluation associée à l'unique idéal premier $\mathfrak{b}$ de $\mathfrak{o}_L$ étendant l'idéal premier $\mathfrak{p}$ de $\mathfrak{o}$.

Définition 3.3.1
Le groupe d'inertie de L/K, *noté* Δ_0, *est le groupe*

$$\Delta_0 = \{\delta \in \Delta \,|\, a^\delta \equiv a \bmod \mathfrak{b} \text{ pour tout } a \in \mathfrak{o}_L\}.$$

Théorème 3.3.2
Soit l'homomorphisme $\rho : \Delta \longrightarrow \mathrm{Gal}\,(k_L/k)$ *défini par* $\overline{a}^{\rho(\delta)} = \overline{a}^\delta$. *Alors* ρ *est surjective et de plus la suite suivante*

$$1 \longrightarrow \Delta_0 \longrightarrow \Delta \longrightarrow \mathrm{Gal}\,(k_L/k) \longrightarrow 1$$

est exacte. Ainsi l'extension maximale non-ramifiée L_0 *de* K *dans* L *est le corps fixé de* Δ_0.

Démonstration. Nous utiliserons beaucoup des résultats intermédiaires du théorème 3.2.4. Nous conseillons donc au lecteur de relire sa preuve pour les points qui peuvent paraître troubles. Le corps fixé k_L^Δ est de la forme $k[m]$, $(m, N\mathfrak{p}) = 1$. Comme $k[m] \subset k_L$, alors $K[m] \subset L$, et l'on sait que $k[m]$ est la classe de résidu de $K[m]$. Soit η une m-ème racine primitive de l'unité. Alors $\overline{\eta} \in k_L^\Delta$, i.e. $\overline{\eta}^\delta = \overline{\eta}$, pour tout $\delta \in \Delta$. Puisque $X^m - 1$ est séparable sur k, alors $\eta^\delta = \eta$ pour tout $\delta \in \Delta$, i.e. $K[m] \subset L^\Delta$, ainsi $K[m] = K$. Mais $[K[m] : K] = [k[m] : k]$. Ainsi $k_L^\Delta = k$, donc ρ est surjective.
Appliquons cela à L_0 à la place de L. Puisque L_0 est galoisienne sur K, il est de la forme $K[m]$. Mais étant donné que $[k_{L_0} : k] = [L_0 : K]$ et $k_{L_0} = k_L$, on a l'isomorphisme

$$\mathrm{Gal}\,(L_0/K) \simeq \mathrm{Gal}\,(k_L/k).$$

Ainsi $L_0 = L^{\Delta_0}$.

q.e.d

Corollaire 3.3.3
Les deux points suivants sont vérifiés :

(*i*) $|\Delta_0| = e(L/K)$;

(*ii*) L/K *est non-ramifiée si et seulement si* $|\Delta_0| = 1$.

Démonstration. Le premier point provient de l'égalité $[L : K] = e(L/K)f(L/K)$; $f(L/K) = |\mathrm{Im}\ (\rho)|$; $|\Delta_0|\,|\mathrm{Im}\ (\rho)| = [L : K]$. Le second point est déduit immédiatement du théorème.

q.e.d

La théorie de Galois nous dit que l'extension de corps k_L/k est toujours galoisienne et que l'automorphisme $x \mapsto x^{|k|}$ est un générateur particulier de $\mathrm{Gal}\,(k_L/k)$. Nous appellerons un tel automorphisme l'*automorphisme de Frobenius de* k_L/k. Par le théorème 3.3.2, il existe un $\delta \in \Delta$ tel que

$$a^\delta \equiv a^{|k|} \bmod \mathfrak{b}$$

pour tout $a \in \mathfrak{o}_L$. De plus si L/K n'est pas ramifiée, alors ce δ est unique dans Δ, puisque ρ est alors injective. Nous appellerons un tel δ un *élément de Frobenius de* L/K, noté $\phi(L/K)$.
Soit λ un paramètre uniformisant de L. On rappelle que d'après le théorème 3.2.2, on a

$$\mathfrak{o}_L = \mathfrak{o}_{L_0}[\lambda].$$

Si $\delta \in \Delta$, alors λ^δ est ausi et seulement si un paramètre uniformisant de L, et ainsi $\lambda^{1-\delta} \in \mathfrak{o}_L^\star$ où $\lambda^{1-\delta} = \lambda/\lambda^\delta$. On écrit $\theta(\delta)$ la classe de résidu de $\lambda^{1-\delta}$ modulo $\mathfrak{b}$.

Proposition 3.3.4
La restriction de θ à Δ_0 est un homomorphisme de groupe :

$$\theta : \Delta_0 \longrightarrow k_L^\star.$$

Démonstration. Remarquons tout d'abord que de par la définition même de Δ_0, on a $\theta(\sigma)^\delta = \theta(\sigma)$ pour $\sigma \in \Delta$ et $\delta \in \Delta_0$. La multiplicativité de θ provient des congruences suivantes modulo $\mathfrak{b}$:

$$\theta(\sigma\tau) \equiv \frac{\lambda}{\lambda^{\sigma\tau}} \equiv \left(\frac{\lambda}{\lambda^\tau}\right)\left(\frac{\lambda}{\lambda^\sigma}\right)^\tau \equiv \theta(\tau)\theta(\sigma)^\tau \equiv \theta(\tau)\theta(\sigma).$$

q.e.d

En faite, on peut remarquer que θ est indépendant du choix du paramètre uniformisant, puisque pour $b \in \mathfrak{o}_L^\star$, $\delta \in \Delta_0$, $b^{1-\delta} \equiv 1 \bmod \mathfrak{b}$, et ainsi

$$(\lambda b)^{1-\delta} \equiv \lambda^{1-\delta} b^{1-\delta} \equiv \lambda^{1-\delta}.$$

Définition 3.3.5
On appelle groupe d'inertie sauvage de L/K *le noyau de θ, noté Δ_1. On l'appelle ausi et seulement si le groupe de ramification ou premier groupe de ramification.*

Théorème 3.3.6
Les assertions suivantes ont lieux :

(*i*) *Pour $\sigma \in \Delta_0$, les assertions suivantes sont équivalentes*

(*a*) $\sigma \in \Delta_1$;

(*b*) $\lambda^\sigma \equiv \lambda$ *modulo* $\mathfrak{b}^2$ *pour un paramètre uniformisant de* L ;

(*c*) *Pour tout* $i \geq 0$ *et pour tout* $\lambda_i \in L$ *avec* $\lambda_i \mathfrak{o}_L = \mathfrak{b}^i$,

$$\lambda_i^\sigma \equiv \lambda_i \bmod \mathfrak{b}^{i+1};$$

(*d*) *Pour tout* $a \in \mathfrak{o}_L$, $a^\sigma \equiv a \bmod \mathfrak{b}^2$;

(*e*) *Pour tout* $b \in L^\star$, $b^\sigma/b \equiv 1 \bmod \mathfrak{b}$.

(*ii*) Δ_1 *est l'unique p-sous-groupe de Sylow (donc normal) de* Δ_0, *et* Δ_0/Δ_1 *est un groupe cyclique dont l'ordre divise* $N\mathfrak{b} - 1$; Δ_1 *est normal dans* Δ.

Par la suite, pour simplifier l'écriture, nous noterons L_1 pour L^{Δ_1}.

Corollaire 3.3.7
On peut déduire du théorème précédent les trois points suivants :

(*i*) *En écrivant* $e(L/K) = e'p^r$, *avec* $(e', p) = 1$, *on a*

$$[L_1 : L_0] = e(L_1/L_0) = e(L_1/L) = e'[L : L_1] = e(L/L_1) = p^r.$$

(*ii*) *En particulier,* L_1/K *est totalement ramifié,* L/L_1 *est totalement et simplement ramifié.*

(*iii*) L/K *est simplement ramifié si et seulement si* $\Delta_1 = \{1\}$.

Démonstration. Commençons par montrer que (1) $\Rightarrow$ (5). Soit $\sigma \in \Delta_1$. On peut écrire b de la forme $\eta\lambda^i$, pour λ un paramètre uniformisant de L, $i \in \mathbb{Z}$ et $\eta \in \mathfrak{o}_L^\star$. Ainsi $\eta^{\sigma-1} \equiv 1 \bmod \mathfrak{b}$ puisque $\sigma \in \Delta_0$. De plus $\sigma \in \ker\theta$ et donc $(\lambda_{\sigma-1})^i \equiv 1 \bmod \mathfrak{b}$.
Notons maintenant que (5) $\Rightarrow$ (3). Il suffit de remplacer b par λ_i et d'amplifier la congruence $\lambda_i^{\sigma-1} \equiv 1 \bmod \mathfrak{b}$ par λ_i.
Le point (2) est une conséquence particulière de (3). Maintenant si $\lambda^\sigma = \lambda + \beta$, $\beta \in \mathfrak{b}^2$, alors $\lambda^{\sigma-1} = 1 + \beta\lambda^{-1} \in 1 + \mathfrak{b}$. Ainsi $\sigma \in \Delta_1$.
Il ne nous reste plus qu'à montrer l'équivalence de (4) avec les autres points. Rappelons-nous que $\mathfrak{o}_L = \mathfrak{o}_{L_0}[\lambda]$ et donc en particulier un élément $a \in \mathfrak{o}_L$ peut être écrit de la forme $a = c + y$ où $y \in \mathfrak{b}$ et $c \in \mathfrak{o}_{L_0}$. Puisque $\sigma \in \Delta_0$, $c^\sigma - c = 0$. Par (3), $y^\sigma - y \in \mathfrak{b}^2$. Ainsi (4) est vérifié. Conversément, (4) implique trivialement (2).
Par la définition de θ et par le premier théorème d'isomorphisme, on a $\Delta_0/\Delta_1 \simeq \Im\theta \subset k_L^\star$, et ainsi $[\Delta_0 : \Delta_1] | N\mathfrak{b} - 1$. Puisque Δ_1 est normal dans Δ_0 par définition, il suffit de vérifier que Δ_1 est un p-groupe. Ab absurdo,

soit $\sigma \in \Delta_1$ d'ordre $r > 1$, $p \nmid r$. Par (2), $\lambda^\sigma = \lambda(1+\alpha)$ pour un certain $\alpha \in \mathfrak{b}$. Puisque $\alpha \neq 0$, on peut supposer que $\alpha \in \mathfrak{b}^t$, $\alpha \notin \mathfrak{b}^{t+1}$ avec $t \geq 1$. Ainsi $\lambda^{\sigma^2} = \lambda(1+\alpha)(1+\alpha^\sigma)$, et de la même manière

$$\lambda^{\sigma^p} = \lambda \prod_{i=0}^{p-1} (1+\alpha^{\sigma^i}).$$

Par (3), $\alpha^{\sigma^i} \equiv \alpha \bmod \mathfrak{b}^{t+1}$ pour tout i, et ainsi

$$\lambda^{\sigma^p} \equiv \lambda(1+\alpha) \equiv \lambda \bmod \mathfrak{b}^{t+1}.$$

Ainsi pour un entier s, $\lambda^{\sigma^{sp}} = \lambda(1+\beta_s)$ pour un certain $\beta_s \in \mathfrak{b}^{t+1}$. De par ailleurs, λ^{σ^r}, et ainsi $\lambda^{\sigma^{rR}} = \lambda$ pour un entier R. Par Bézout, on peut choisir R et s tels que $rR + sp = 1$. On en conclue que

$$\lambda(1+\alpha) = \lambda^\sigma = \lambda^{\sigma^{rR+sp}} = \lambda^{\sigma^{sp}} = \lambda(1+\beta_s).$$

Mais cela est absurde car $\alpha \notin \mathfrak{b}^{t+1}$ et $\beta_s \in \mathfrak{b}^{t+1}$.
Le fait que Δ_1 est normal dans Δ s'en suit trivialement.

q.e.d

Exemple 3.3.8
Soit $K = \mathbb{Q}_p$ et $L = \mathbb{Q}[rp^n]$ avec $p \nmid r$. Par le théorème 3.2.4, on sait que $\mathbb{Q}[r]$ n'est pas ramifié sur $\mathbb{Q}_p$. De plus nous avons vu que $\mathbb{Q}_p[p^n]/\mathbb{Q}_p$ est totalement ramifié de degré $p^{n-1}(p-1)$. Ainsi $\mathbb{Q}_p[p]/\mathbb{Q}_p$ est totalement ramifié de degré $p-1$. De plus, dans ce cas, nous avons $L_0 = \mathbb{Q}_p[r]$ et $L_1 = \mathbb{Q}_p[rp]$.

Proposition 3.3.9
Soit L/K une extension galoisienne telle que $L_0 = K$ et $L_1 = L$. Soit $e = e(L/K)$. Alors $K = K[e]$, i.e K contient les racines primitives e-ème de l'unité, et $L = K[\alpha^{1/e}]$ pour $\alpha \in K$ un paramètre uniformisant.

Démonstration. Puisque $\Delta_1 = 1$ et $\Delta_0 = \Delta$, l'homomorphisme θ est un isomorphisme de Δ avec le sous-groupe $\mu_{k,e}$ de $k^\star$ d'ordre e. Par un corollaire du lemme d'Hensel, $K^\star$ contient un groupe $\mu_{K,e}$ isomorphe à $\mu_{k,e}$ par la surjection canonique $x \mapsto \overline{x}$. En particulier il existe un isomorphisme

$$\psi : \Delta \simeq \mu_{k,e} \text{ avec } \overline{\psi} = \tau.$$

Par la théorie de Kummer, $L^\star$ contient un élément β tel que

$$\beta^{1-\delta} = \psi(\delta), \quad \forall\, \delta \in \Delta.$$

En considérant les «résidus de Lagrange », il est facile de constater que

$$\beta_i = \sum_{\delta \in \Delta} a_i^{\delta} \psi(\delta)^{-1}$$

où $\{a_i\}$ est une base de L/K. Puisque $\det(a_i^{\delta}) \neq 0$, un certain β_{i_0} est non nul, et ainsi doit satisfaire $\beta = \beta_{i_0}$. De plus, puisque $\beta^{\delta} = \beta$, il s'ensuit que $\delta = 1$ et donc

$$L = K(\beta).$$

Observons maintenant que $(\beta^e)^{1-\delta} = \psi(\delta)^e = 1$. Ainsi $\beta = \alpha^{1/e}$, $\alpha \in K^{\star}$. Sans limiter la généralité, on peut donc remplacer β par βc, $c \in K^{\star}$, i.e remplacer α par αc^e. En choisissant un bon c, on peut supposer que

$$0 \leq v < e, \;\; v = v_K(\alpha).$$

Ainsi $\beta = \alpha^{1/e} = \lambda^v \eta$, où λ est un paramètre uniformisant de L et $\eta \in \mathfrak{o}_l^{\star}$. Ainsi par définition de θ,

$$\beta^{1-\delta} \bmod \mathfrak{b} = \theta(\delta)^v,$$

c'est-à-dire

$$\beta^{1-\delta} = \psi(\delta)^v,$$

parce que

$$\beta^{1-\delta} = \psi(\delta).$$

Ainsi $v \equiv 1 \bmod (e)$, et donc par l'inégalité ci-dessus, $v = 1$. Ainsi β est un paramètre uniformisant de L.

q.e.d

Théorème 3.3.10
Soit Σ un sous-groupe de $\Delta = \mathrm{Gal}\,(L/K)$ et $N = L^{\Sigma}$ le sous-corps fixé. On identifie Σ à $\mathrm{Gal}\,(L/N)$. Le groupe d'inertie Σ_0, respectivement le groupe d'inertie sauvage Σ_1, de L/N est donné par

$$\Sigma_i = \Sigma \cap \Delta_i.$$

Si L/K est non-ramifié, alors $\phi(L/N) = \phi(L/K)^{f(N/K)}$.
Supposons que Σ est de plus normal dans Δ. Soit $\Omega = \Delta/\Sigma$. On identifie Ω au groupe de Galois $\mathrm{Gal}\,(N/K)$. Alors

$$\Omega_i = \Delta_i \Sigma / \Sigma.$$

De plus si L/K est non-ramifié, alors $\phi(L/K)$ a image $\phi(N/K)$ dans Ω.

Démonstration. Le premier point est une simple suite d'équivalence : $\sigma \in \Sigma_i$ si et seulement si $a^\sigma = a \bmod \mathfrak{b}^{i+1}$ pour tout $a \in \mathfrak{o}_L$ si et seulement si $\sigma \in \Delta_i \cap \Sigma$. Le résultat sur les éléments de Frobenius est une conséquence de $|k_N| = |k|^{f(N/K)}$.
Le second point demande plus de travail. Soit $\mathfrak{q} = \mathfrak{b} \cap N$, et soit $\delta \in \Delta_0$. Alors $a^\delta - a \in \mathfrak{b}$ pour tout $a \in \mathfrak{o}_L$. Ainsi si de plus $a \in \mathfrak{o}_N$ $a^\delta - a \in \mathfrak{b} \cap N = \mathfrak{q}$. Ainsi $\delta|_N \in \Delta_0$, et donc on a montré que $\Delta_0\Sigma/\sigma \subset \Omega_0$. De plus par le premier point, $\Delta_0 \cap \Sigma = \Sigma_0$. Ainsi en comparant les ordres, on a

$$[\Delta_0\Sigma : \Sigma] = [\Delta_0 : \Sigma_0] = e(L/K)e(L/N)^{-1} = e(N/K) = |\Omega_0| .$$

Ainsi donc $\Delta_0\Sigma/\Sigma = \Omega$.
Utilisons maintenant la caractérisation des groupes d'inertie sauvages comme p-sous-groupe de Sylow du groupe d'inertie. Clairement $\Delta_1\Sigma/\Sigma$ est un p-sous-groupe de $\Omega_0 = \Delta_0\Sigma/\Sigma$. Ainsi il est contenu dans Ω_1. Mais l'ordre de $\Delta_0\Sigma/\Delta_1\Sigma$ divise $[\Delta_0 : \Delta_1]$, i.e. premier à p. Ainsi $\Delta_1\Sigma/\Sigma = \Omega_1$.
Remarquons que les automorphismes de Frobenius de k_L/k sont une restriction des automorphismes de Frobenius de k_N/k.

q.e.d

3.4 Théorème de la base normale

Définition 3.4.1
Un polynôme f à n variables sur K est dit réduit *si* $\deg f < |K|$ *en chaque variable.*

Théorème 3.4.2
Soit K un corps et $f \in K[X]$ un polynôme de degré n. Alors f a au plus n racines dans K, et si $a \in K$ est une racine de f, alors $(X - a)$ divise f.

Démonstration. Soit $a \in K$ tel que $f(a) = 0$. Alors par division euclidienne, on peut trouver $q, r \in K[X]$ tels que

$$f(X) = q(X)(X - a) + r(X)$$

avec $\deg r < 1$. Comme de plus $f(a) = 0 = r(a)$, alors $r \equiv 0$ et donc $(X - a)$ divise f.
Soient maintenant $a_+, \ldots, a_m$ les racines de f dans K. Alors on vient juste de voir que $(X - a_1) \ldots (X - a_m)$ divise f. Ainsi $m \leq \deg f = n$.

q.e.d

Corollaire 3.4.3
Soit K un corps et $f \in K[X_1, \ldots, X_n]$. Soient $S_1, \ldots, S_n \subset K$ des sous-ensembles tels que $|S_i| > \deg f(X_i)$.
Si $f(a_1, \ldots, a_n) = 0$ pour tout $a_i \in S_i$, alors $f \equiv 0$.

Démonstration. Nous procéderons par récurrence sur le nombre de variables. Le théorème précédent nous donne le point d'ancrage pour une variable. En effet, si $f \neq 0$, alors f ne peut s'annuler sur aucun des sous-ensembles de K de cardinalité plus grande que le degré du polynôme.
Soit $n \geq 2$ et $S_1, \ldots, S_n \subset K$ tels que f s'annule sur ces ensembles. Alors $f(X_1, \ldots, X_n) = \sum_j f_j(X_1, \ldots, X_{n-1}) X_n^j$ où $f_j \in K[X_1, \ldots, X_{n-1}]$. Supposons qu'il existe $(b_1, \ldots, b_{n-1}) \in S_1 \times \cdots \times \S_{n-1}$ tels que $f_j(b_1, \ldots, b_{n-1}) \neq 0$ pour tout j. Alors $f(b_1, \ldots, b_{n-1}, X_n) \in K[X_n]$ est un polynôme de degré 1 qui a plus de racines que son degré. Ainsi $f_j \equiv 0$ et donc $f \equiv 0$.

q.e.d

Théorème 3.4.4 (Théorème de la base normale)
Soit L une extension galoisienne finie de K de degré n. Soit $\Delta = \operatorname{Gal} L/K = \{\sigma_1 \ldots, \sigma_n\}$. Alors il existe $w \in L$ tel que $\{\sigma_1 w, \ldots, \sigma_n w\}$ est une K-base de L, i.e. une base de L vu comme K-espace vectoriel.

Démonstration. Nous traiterons uniquement le cas où K est de cardinalité infinie. Le cas fini résulte d'un démonstration d'algèbre linéaire.
Pour $\sigma, \tau \in \Delta$, on définit X_σ une variable et $t_{\sigma,\tau} = X_{\sigma^{-1}\tau}$. Posons $X_i = X_{\sigma_i}$ et

$$f(X_1, \ldots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Remarquons que f n'est pas identiquement nul, en effet par exemple pour $X_{\mathrm{id}} = 1$ et $X_\sigma = 0$. De plus puisque K est de cardinalité infinie, f est réduit, et donc il existe $w \in L$ tel que

$$\det(\sigma_{i-1}\sigma_j w) \neq 0.$$

Montrons maintenant que $\{\sigma_1 w, \ldots, \sigma_n w\}$ est une K-base de L :
Soient $a_1, \ldots, a_n \in K$ tels que

$$f(w) = \sum_i a_i \sigma_i(w) = 0.$$

Posons $g_j(a_1, \ldots, a_n) = \sigma_j^{-1} f(w)$. Ainsi $\{g_j\}$ est un système de n équations à n inconnus et de plus $\det(\sigma_i \sigma_j^{-1}(w)) \neq 0$ et donc $a_i = 0$ pour tout i.

q.e.d

CHAPITRE 4

Exercices

Exercice 1
Montrer que pour ζ une p-ème racine de l'unité, $\mathbb{Z}[\zeta]$ est l'anneau des entiers de $\mathbb{Q}[\zeta]$.

On a clairement que $\mathbb{Z}[\zeta]$ est contenu dans l'anneau des entiers. Il nous faut donc montrer la réciproque ; ce que nous ferons à travers quelques assertions : *Assertion : Soient r et s deux entiers positifs premier entre eux, alors $\frac{\zeta^r-1}{\zeta^s-1}$ est une unité (i.e. inversible) de $\mathbb{Z}[\zeta]$*. En effet, on peut écrire $r \equiv st \mod p$ pour un certain t et donc nous avons

$$\frac{\zeta^r-1}{\zeta^s-1} = \frac{\zeta^{st}-1}{\zeta^s-1} = 1+\zeta^s+\cdots+\zeta^{s(t-1)} \in \mathbb{Z}[\zeta].$$

De la même manière $\frac{\zeta^s-1}{\zeta^r-1} \in \mathbb{Z}[\zeta]$.

Assertion : L'idéal engendré par $(1-\zeta)$ est un idéal premier de l'anneau des entiers et $(1-\zeta)^{p-1} = (p)$. Ainsi p est totalement ramifié dans $\mathbb{Q}[\zeta]$. Soit le polynô me cyclotomique de ζ : $X^{p-1}+\cdots+X+1 = \prod_{i=1}^{p-1}(X-\zeta^i)$. Alors pour $X=1$ on a $p = \prod(1-\zeta^i)$. Par l'assertion précédente, on a l'égalité des idéaux engendrés par $(1-\zeta)$ et $1-\zeta^i$. Ainsi $(p) = (1-\zeta)^{p-1}$. Puisque (p) peut avoir au plus $p-1 = \deg(\mathbb{Q}[\zeta]/\mathbb{Q})$ facteurs premiers dans $\mathbb{Q}[\zeta]$, il s'ensuit que $(1-\zeta)$ doit être un idéal premier de l'anneau des entiers. Une autre manière de le voir est de passer par les normes : si $1-\zeta = A \cdot B$, alors $p = N(1-\zeta) = N(A)\cdot N(B)$ et donc $N(A) = 1$ ou $N(B) = 1$, et donc l'idéal $(1-\zeta)$ est premier dans l'anneau des entiers.

Appliquons maintenant cela à $\mathbb{Z}[\zeta]$. Soit v l'évaluation correspondante à l'idéal $(1-\zeta)$. Ainsi $v(1-\zeta)=1$ et $v(p)=p-1$. Puisque $\mathbb{Q}[\zeta]=\mathbb{Q}[1-\zeta]$, alors la famille $\{1,(1-\zeta),(1-\zeta)^2,\ldots,(1-\zeta)^{p-2}\}$ est une base de $\mathbb{Q}[\zeta]$ vu comme $\mathbb{Q}$ espace vectoriel. Soit maintenant α dans l'anneau des entiers. Alors

$$\alpha = a_0 + a_1(1-\zeta) + \cdots + a_{p-2}(1-\zeta)^{p-2}$$

avec $a_i \in \mathbb{Q}$. Puisque pour $a \in \mathbb{Q}$, $v(a) \equiv 0 \bmod (p-1)$et que les nombres $v(a_i(1-\zeta)^i)$ sont distincts modulo $(p-1)$, alors ils sont distincts. Ainsi par ultramétrique $v(\alpha)=\min(v(a_i(1-\zeta)^i))$. Puisque $v(\alpha)\leq 0$ et que $v((1-\zeta)^i)<p-1$, on doit avoir $v(a_i)\leq 0$. Ainsi un certain a_i ne contient pas p au dénominateur. On réarrange l'expresi et seulement sion pour avoir

$$\alpha = b_0 + b_1\zeta + \cdots + \zeta^{p-2}$$

avec $b_i \in \mathbb{Q}$, mais aucun b_i n'a de p au dénominateur.
La preuve sera complétée en observant que le discriminant de la base $\{1,\zeta,\ldots,\zeta^{p-2}\}$ est une puissance de p. Plus explicitement on a

$$\alpha^\sigma = b_0 + b_1\zeta^\sigma + \cdots + b_{p-2}(\zeta^\sigma)^{p-2}$$

où σ parcourt $\mathrm{Gal}\,(\mathbb{Q}[\zeta]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\star$. Soit $\alpha_i=\alpha^\sigma$ où $\sigma(\zeta)=\zeta^i$. Alors on a

$$\begin{pmatrix} a_1 \\ \vdots \\ a_{p-1} \end{pmatrix} = \begin{pmatrix} 1 & \zeta & \zeta^2 & \cdots \\ 1 & \zeta^2 & \zeta^4 & \cdots \\ 1 & \zeta^3 & \zeta^6 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ b_{p-2} \end{pmatrix}.$$

Mais le déterminant de cette matrice est un déterminant de Vandermonde, ainsi il est égal à

$$\prod_{1\leq j\leq k\leq p-1} (\zeta^k - \zeta^j) = (\text{unité})(\text{puissance de } 1-\zeta).$$

Ainsi chaque b_i doit être le quotient d'un entier par une puissance de $(1-\zeta)$, mais puisque b_i n'a pas de p dans son dénominateur, $b_i \in \mathbb{Z}$.

Exercice 2
Montrer que $\mathbb{Q}_p$ est indénombrable.

Par une proposition, on sait que tout élément de $\mathbb{Q}_p$ peut s'écrire sous la forme $\sum a_i p^i$ avec $a_i \in \{0,1,\ldots,p-1\}$, et réciproquement. Nous monterons seulement que l'ensemble

$$I = \{\sum a_i p^i \,|\, a_i \in \{0,1\}\}$$

est indénombrable. Comme il s'agit une sous-partie de $\mathbb{Z}_p$, cette écriture est de plus unique. Supposons que I soit dénombrable. Alors on peut ordonner ses éléments selon l'ordre hérité de $\mathbb{N}$ par la bijection. Mais le nombre $\sum(1-a_{1_i})p^i$n'appairait nulle part dans la liste, ce qui contredit la bijection avec $\mathbb{N}$. Ainsi I n'est pas dénombrable et à forteriori $\mathbb{Q}_p$.

Exercice 3
Montrer que la série

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$$

converge sur $p\mathbb{Z}_p$ pour la valeur absolue $|.|_p$.
Montrer que la série

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converge sur $p\mathbb{Z}_p$ si $p > 2$, respectivement sur $4\mathbb{Z}_2$ si $p = 2$.
Finalement, montrer que $(1+p\mathbb{Z}_p)^\times \simeq (p\mathbb{Z}_p)^+$ si $p > 2$ et $(1+4\mathbb{Z}_2)^\times \simeq (4\mathbb{Z}_2)^+$ si $p = 2$.

Par ultramétrique, il suffit de montrer que l'évaluation v_p du dernier terme tend vers l'infini pour montrer qu'une série converge. Or

$$\begin{aligned} v_p(\frac{(-1)^{n+1}x^n}{n}) &= v_p(x^n) - v_p(n) \\ &= nv_p(x) - v_p(n) \\ &\geq n - [\frac{n}{p}], \end{aligned}$$

donc la série converge.
Etudions maintenant le cas de $v_p(n!)$. Par définition, on sait que $v_p(n!) = \sum_{i=0}^{n} v_p(i) = \sum_{p|i\leq n} v_p(i) \leq \sum_{i\geq 0} \frac{n}{p^i} \leq \frac{n}{p-1}n$ si $p > 2$ et $v_2(n!) \leq n$ si $p = 2$.
Ainsi pour $p > 2$

$$v_p(\frac{x^n}{n!}) = v_p(x^n) - v_p(n!) \geq nv_p(x) - \varepsilon n \geq n(1-\varepsilon),$$

et donc la série converge. Dans le cas où $p = 2$, comme $v_2(x) > 1$ pour $x \in 4Z_2$, la série converge ausi et seulement si.
Les fonctions log et exp étant inverses l'une de l'autre, l'isomorphisme est donné immédiatement par des deux homomorphismes de groupe.

Exercice 4
Montrer que pour ζ une p-ème racine de l'unité, l'anneau des entiers de $\mathbb{Q}_p[\zeta]$ est $\mathbb{Z}_p[\zeta]$.

On pose $\phi(X) := \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + 1$. Clairement ζ est une racine de ϕ. Malheureusement ce n'est pas un polynô me d'Eisenstein. On pose alors

$$g(X) = \Phi(X+1).$$

Dans $\mathbb{F}_p$, on a alors $\overline{g}(X) = \frac{(X^p+1)-1}{(X+1)-1} = X^{p-1}$ et donc p divise tous les coefficients des X^i. Comme de plus le dernier des coefficient est l'évaluation de g en 0, on a $g(0) = \phi(1) = p$ et donc p^2ne divise pas le dernier terme. Ainsi g est un polynô me d'Eisenstein dont une racine est $\zeta - 1$. Par le théorème 3.2.2, on a que l'anneau des entiers de $\mathbb{Q}_p[\zeta] = \mathbb{Q}_p[\zeta - 1]$ est égal à $\mathbb{Z}[\zeta - 1] = \mathbb{Z}[\zeta]$.

Exercice 5
Montrer que pour ζ une p^n-ème racine de l'unité, l'anneau des entiers de $\mathbb{Q}_p[\zeta]$ est $\mathbb{Z}_p[\zeta]$.

On pose $\phi(X) := \frac{X^{p^n}-1}{X^{p^{n-1}}-1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^{n-1}} + 1$. Clairement ζ est une racine de ϕ. Malheureusement ce n'est pas un polynô me d'Eisenstein. On pose alors

$$g(X) = \Phi(X+1).$$

Dans $\mathbb{F}_p$, on a alors $\overline{g}(X) = \frac{(X^{p^n}+1)-1}{(X^{p^{n-1}}+1)-1} = X^{p^{n-1}(p-1)}$ et donc p divise tous les coefficients des X^i. Comme de plus le dernier des coefficient est l'évaluation de g en 0, on a $g(0) = \phi(1) = p$ et donc p^2ne divise pas le dernier terme. Ainsi g est un polynô me d'Eisenstein dont une racine est $\zeta - 1$. Par le théorème 3.2.2, on a que l'anneau des entiers de $\mathbb{Q}_p[\zeta] = \mathbb{Q}_p[\zeta - 1]$ est égal à $\mathbb{Z}[\zeta - 1] = \mathbb{Z}[\zeta]$.

Exercice 6
Soit L une extension galoisienne de $K = \mathbb{Q}_p$ dont l'indice de ramification est e. Pour quelles valeurs de e les séries

$$\begin{array}{lccc} \exp: & \mathfrak{o}_K & \to & 1+\mathfrak{o}_K \\ \log: & 1+\mathfrak{o}_K & \to & \mathfrak{o}_K \end{array}$$

convergent-elles ?

Commençons par remarquer que par le lemme 3.1.8,

$$v_{\mathfrak{b}}(x) = \frac{v_{\mathfrak{p}}(N_{L/K}(x))}{f}.$$

pour $x \in L$, où $\mathfrak{p} = \mathbb{Z}_p$ et $\mathfrak{b}$ est l'anneau des entiers correspondant dans L. Comme dans l'exercice précédent, pour montrer la convergence d'une série, il suffit de s'intéresser à son dernier terme. On a donc, en se rappelant que $v_\mathfrak{b}$ est une évaluation, pour $x \in \mathfrak{o}_K$

$$\begin{aligned} v_\mathfrak{b}(x^n/n) &= v_\mathfrak{b}(x^n) - v_\mathfrak{b}(n) \\ &= nv_\mathfrak{b}(x) - \frac{v_\mathfrak{p}(N_{L/K}(n))}{f} \\ &= nv_\mathfrak{b}(x) - \frac{v_\mathfrak{p}(n^{ef})}{f} \\ &= nv_\mathfrak{b}(x) - \frac{efv_\mathfrak{p}(n)}{f} \\ &> n - e(n/p) \\ &= n(1 - e/p), \end{aligned}$$

car $N_{L/K}(n) = \prod_{\sigma \in \mathrm{Gal}\,(L/K)} n^\sigma = \prod_{\sigma \in \mathrm{Gal}\,(L/K)} n = n^{|\mathrm{Gal}\,(L/K)|}$. Ainsi pour que la série exp converge si $e \leq p$.
De la même manière, on calcule pour $v_\mathfrak{b}(\log(x))$

$$\begin{aligned} v_\mathfrak{b}(x^n/n!) &= v_\mathfrak{b}(x^n) - v_\mathfrak{b}(n!) \\ &= nv_\mathfrak{b}(x) - \frac{v_\mathfrak{p}(N_{L/K}(n!))}{f} \\ &= nv_\mathfrak{b}(x) - \frac{v_\mathfrak{p}((n!)^{ef})}{f} \\ &= nv_\mathfrak{b}(x) - \frac{efv_\mathfrak{p}(n!)}{f} \\ &> n - e(n\sum_{i \geq 1} 1/p^i) \\ &\geq n(1 - e\frac{1}{p-1}). \end{aligned}$$

Ainsi il faut que $e \leq p - 1$.. Ainsi seules les extensions dont l'indice de ramification est inférieur ou égal à $p-1$ possèdent un isomorphisme de groupe entre $(\mathfrak{o}_L)^+$ et $(1 + \mathfrak{o}_L)^\times$.

Bibliographie

[1] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

Bilan personnel

Ce travail m'a beaucoup apporté sur un point intellectuel, notamment sur des notions ausi et seulement si importantes que le corps des p-adiques qui peut fournir un grande quantité d'exemples et de contre-exemples. D'un point personnel, j'ai eu d'excellent rapport avec Erik Pickett, qui a su conserver intacte ma motivation des premiers jours, en me donnant les défis que constituent les exercices présents en fin de travail.