

Corps locaux

(Par Qing Liu)

Introduction

Le but c'est d'abord de décrire les extensions finies de corps locaux comment dans [cassels].

Chapitre 1

Corps ultramétriques complets

1.1 Valuations et valeurs absolues

Le but là c'est de classer les valuations, d'abord sur des corps premiers comme \mathbb{Q} . D'abord l'équivalence entre valuations et valeurs absolues.

Définition 1.1.1 (Valuation). Une valuation v (de rang 1) est un morphisme de groupe (multiplicatif vers additif)

$$K \rightarrow \mathbb{R} \cup \{\infty\}$$

tel que $v(x + y) \geq \min\{v(x), v(y)\}$ quand $x + y \neq 0$ avec $v(x + y) = \infty$.

Définition 1.1.2 (Valeur absolue). Une valeur absolue $|\cdot|$ est un morphisme de groupes multiplicatifs $K \rightarrow \mathbb{R}$ étendu avec $0 \mapsto 0$ et qui vérifie une inégalité triangulaire.

Le passage aux valeurs absolues : étant donné un réel $0 < t < 1$ on peut définir une valeur absolue

$$x \mapsto t^{v(x)}$$

Bon ensuite la caractérisation archimédienne :

Définition 1.1.3 (Valeur absolue archimédienne). Un corps valué $(K, |\cdot|)$ est archimédien si pour tout $(x, c) \in K \times \mathbb{R}$ il existe n t.q

$$c \leq |n \cdot x|$$

et pas $n|x|$ attention.

Ensuite la première partie de la caractérisation :

Proposition 1.1.4. *Être archimédien c'est équivalent à*

1.1 Valuations et valeurs absolues

- $(|n|)_{n \in \mathbb{Z}}$ est bornée.
- $(|n|)_{n \in \mathbb{Z}}$ est ≤ 1 .
- $|\cdot|$ est ultramétrique!

Preuve. La première équivalence est directe. La deuxième aussi via $x \mapsto x^k$ et la troisième se ramène à la deuxième en regardant $|1+x| \leq 1$ et la flèche $x \mapsto x^k$ à nouveau ! (Ça caractérise les éléments inférieurs à 1) \square

Proposition 1.1.5 (Valuations et valeurs absolues). *Il y a une bijection entre valeurs absolues ultramétriques et valuations. L'inverse de la flèche du dessus est juste*

$$|\cdot| \mapsto \frac{1}{\log(1/2)} \log(|\cdot|)$$

On s'approche du théorème d'Ostrowski. Avant on déf les équivalences de valeurs absolues.

Proposition 1.1.6 (La topologie induite). *On obtient une distance à partir d'une valeur absolue puis la topologie de la distance.*

Dans le cas ultramétrique c'est très bizarre.

Proposition 1.1.7. *On a les propriétés suivantes.*

- Si $|x| \neq |y|$ alors $|x+y| = \max(|x|, |y|)$.
- Avec l'inégalité ultramétrique, les boules ont un seul centre.
- Puis deux disques qui s'intersectent forment en fait une chaîne.

Proposition 1.1.8 (Anneau de valuation). *On peut déf l'anneau de valuation de $(K, |\cdot|)$ par $\mathcal{O} := \bar{D}(0, 1)$ les éléments de valuations plus petites que 1. Et son idéal maximal la boule ouverte $D(0, 1)$. Les inversibles sont dans la frontière.*

Définition 1.1.9 (Équivalence de valeurs absolues). Deux valeurs absolues sont équivalentes si elles définissent la même topologie.

Lemme 1.1.10 (Caractérisation). *Deux valeurs absolues sont équivalentes ssi il existe $s \in \mathbb{R}_+^*$ t.q $|\cdot|_1 = |\cdot|_2^s$.*

Preuve. La bonne idée c'est la caractérisation de $D(0, 1)$ par les trucs qui tendent vers 0 par $x \mapsto x^k$. Faut comprendre que prendre des limites dans \mathbb{R} donne la même chose pour $|\cdot|_1$ et $|\cdot|_2$. \square

Ça suffit à prouver le théorème d'Ostrowski :

Théorème 1.1.11 (Ostrowski). *Une valeur absolue non triviale sur \mathbb{Q} est équivalente soit à $|\cdot|_\infty$ ou à une valeur absolue p -adique $|\cdot|_p$.*

Preuve. Pour la partie non archimédienne, on regarde $\mathfrak{m} \cap \mathbb{Z}$ pour obtenir un p . Ensuite, on montre via $|uk| = |1 - vp|$ que $|k| = 1$ dès que $k \wedge p = 1$, $|vp| < 1$ parce que $vp \in \mathfrak{m}$. Ensuite y reste à comparer $|p|$ et $|p|_p$. Vu que $|x| = |p|^r |k| = |p|^r$.

Pour le cas archimédien l'idée c'est d'écrire a en base b pour comparer a^n et b^l où $l \sim n$. En particulier montrer que $|a| \geq 1$ implique $b \geq 1$ dès que $a \geq 2$ ET $|a| = |b|^{\log(a)/\log(b)}$, via la comparaison et par symétrie. Puis remplacer b par 2. On a montré que seul $|2|$ détermine le lien entre $|\cdot|$ et $|\cdot|_\infty$. \square

Définition 1.1.12 (Places). On définit une place comme une classe d'équivalence de valeurs absolues. Une place est finie/infinie si elle est ultramétrique/archimédienne.

1.2 Complétions et corps complets

Dès qu'on a un corps valué $(K, |\cdot|)$, on peut construire une distance

$$d_{|\cdot|} : (x, y) \mapsto |x - y|$$

puis définir des suites de Cauchy.

Définition 1.2.1. Un corps valué $(K, |\cdot|)$ est complet si les suites de Cauchy pour $d_{|\cdot|}$ convergent dans K .

Définition 1.2.2 (Complétion). Pour tout corps valué $(K, |\cdot|)$ il existe un corps valué complet $(\hat{K}, |\cdot|)$ tel que $|\cdot|$ s'étend à \hat{K} .

Preuve. L'idée c'est de regarder l'ensemble des suites de Cauchy $\mathcal{C}(K) \subset K^\mathbb{N}$, de voir que c'est un anneau puis de quotienter par l'idéal maximal des suites qui convergent vers 0. \square

Définition 1.2.3 (Morphismes dans la catégorie des corps valués). Un morphisme de corps valués est un morphisme d'anneau et une isométrie.

On peut étendre les morphismes vers des corps complets en morphismes de corps valués unique à unique isomorphisme près.

1.2 Complétions et corps complets

Remarque 1. Si $(K, |\cdot|)$ est ultramétrique et non triviale, \hat{K} peut-être construit algébriquement. On fixe $t \in K$ t.q $0 < |t| < 1$. Dans l'anneau de valuation, on regarde

$$\hat{O}_K = \varprojlim_n (O_K/t^n O_K)$$

C'est un anneau intègre muni d'une valuation t.q

$$\hat{v}((x_n)_n) = v(y)$$

où $(x_n) = \pi(y)$ et $\pi: O_K \rightarrow \hat{O}_K$; $x \mapsto (x)_n$. C'est une valuation par densité. On l'étend au corps de fraction de la manière évidente. On peut montrer que c'est complet **à faire**. Pareil en général $I \subset A$.

Exercices 1.2.4. Rayon de convergence de $\exp(z) = \sum_n \frac{z^n}{n!}$ dans \mathbb{Q}_p ? Sachant que en métrique p -adique $1/n! \rightarrow_{n \rightarrow \infty} +\infty$. Faut calculer la valuation de $n!$.

Plus généralement, si A est intègre et $\mathfrak{m}_A = tA$ est maximal on peut définir la valuation t -adique associée et l'étendre au corps de fractions et c'est une valuation discrète. Je crois que l'idée c'est que

$$I = \cap t^n A = \{0\}$$

parce que $tI = I$ puis Nakayama dans un anneau noethérien.

Apparemment il fait une construction de \mathbb{R} sans complétion parce que c'est tautologique? Ah bah oui les valuations c'est dans \mathbb{R} , mais en fait on peut d'abord juste les prendre dans \mathbb{Q} .

Il regarde un corps K avec un ordre total compatible archimédien et la topologie de l'ordre.

Alors on demande enfin que $\iota: \mathbb{Q} \rightarrow K$ soit dense, on a nécessairement que ι est croissante. Par densité de \mathbb{Q} dans K , on peut remplacer toute les suites de Cauchy dans K par des suites de Cauchy dans \mathbb{Q} .

En particulier, y'a équivalence entre les suites de Cauchy de K et \mathbb{Q} . On regarde maintenant $C(\mathbb{Q})$ les suites de Cauchy dans \mathbb{Q} et $I(\mathbb{Q})$ les suites qui tendent vers 0. Dans

$$\pi: C(\mathbb{Q}) \rightarrow C(\mathbb{Q})/I(\mathbb{Q})$$

on définit un ordre à droite via $\pi(x_n)_n \geq \pi(y_n)_n$ ssi on a égalité où il existe $r \in \mathbb{Q}_+^*$ t.q $x_n \geq y_n + r$. On obtient un corps totalement ordonné $C(\mathbb{Q})/I(\mathbb{Q})$ (totalement car $\pm \pi(x_n)_n \geq 0$). Bon maintenant faut juste conclure en montrant que le quotient est complet. **à faire?**

Remarque 2. On a bel et bien utilisé que \mathbb{Q} .

Proposition 1.2.5. \mathbb{R} est unique à unique isomorphisme près en tant que corps totalement ordonné complet archimédien où \mathbb{Q} est dense.

1.3 Espaces de Banach

Une norme K sur un espace vectoriel V est une flèche $x \mapsto \|x\|$ qui est nulle qu'en 0, a une inégalité triangulaire et qui transforme l'action de K en action de \mathbb{R} via $|\cdot|$.

Définition 1.3.1. Un e.v.n est un Banach si il est complet pour sa norme.

Remarque 3. *Un k -espace vectoriel de dimension finie sur un corps complet est un Banach. L'inverse est faux!*

Définition 1.3.2. Deux normes sont équivalentes si elles définissent la même topologie. Ou immédiatement si il existe c_1, c_2 t.q

$$c_1\|x\|_1 \leq \|x\|_2 \leq c_2\|x\|_1$$

L'intérêt c'est maintenant qu'étant donné une extension de corps L/k et une valeur absolue sur k , qu'est-ce qu'il se passe quand on l'étend à L ? En fait c'est des normes sur L en tant que k -ev, et elles sont équivalentes en tant que norme ssi elles le sont en tant que v.a par définition!

Théoreme 1.3.3. *Si k est complet, et V est un k -ev de dimension finie, alors toutes les normes sur V sont équivalentes et V est un Banach.*

Démonstration. La norme du max donne une structure de Banach grâce à la convergence normale. Il reste à montrer que toutes les normes sont équivalentes à la norme du max $\|\cdot\|_\infty$. Un côté est simple, l'autre par induction **Faire? Ah la preuve est non triviale mdr.** \square

1.4 Lemme de Hensel

Soit $(K, |\cdot|)$ un corps complet ultramétrique. On note $k = \mathcal{O}_K/\mathfrak{m}$ le corps résiduel.

Lemme 1.4.1 (Lemme de Hensel). *Soit $P(X) \in \mathcal{O}_K[X]$, on suppose que $P \equiv f.g \pmod{\mathfrak{m}}$ tels que $\gcd(f, g) = 1$. Alors il existe $F, G \in \mathcal{O}_K[X]$ tels que*

$$P = F.G$$

et $F \equiv f \pmod{\mathfrak{m}}$, $G \equiv g \pmod{\mathfrak{m}}$, avec $\deg(F) = \deg(f)$. La décomposition est unique à inversible près.

1.4 Lemme de Hensel

Démonstration. On commence par prendre un lift F_0 de f et G_0 de g de degrés minimaux. On a $(f, g) = k[X]$ d'où $1 \in (F_0, G_0) + \mathfrak{m}[X]$, il existe donc $t \in K$ t.q $0 < |t| < 1$ et $\begin{cases} P - F_0 G_0 \in t\mathcal{O}_K[X] \\ 1 \in (F_0, G_0) + t\mathcal{O}_K[X] \end{cases}$. On a déjà augmenté la précision. Soit $F_1 = F_0 + tV_1$ et $G_1 = G_0 + tU_1$. On veut $P - F_1 G_1 \in t^2\mathcal{O}_K[X]$ t.q $\deg(F_1) = m$ et $\deg(G_1) \leq d - m$. On regarde

$$\begin{aligned} P - (F_0 + tV_1)(G_0 + tU_1) &= P - (F_0 G_0 + t(F_0 U_1 + G_0 V_1) + t^2 U_1 V_1) \\ &= (P - F_0 G_0) + t(F_0 U_1 + G_0 V_1) + t^2 * \\ &= tE_0 + t(-) + t^2 * \\ &= t(E_0 + F_0 U_1 + G_0 V_1) + t^2 * \end{aligned}$$

On prends $E_0 = H_0 F_0 + R_0 G_0 + t*$. **Revoir la preuve ailleurs.** \square

Corollaire 1.4.2. *On garde les hypothèses sur K . Étant donné un polynôme irréductible $P \in K[X]$, on a*

$$\max_i |a_i| = \max\{|a_0|, |a_d|\}.$$

En particulier si $a_d = 1$ et $a_0 \in \mathcal{O}_K$ alors $P \in \mathcal{O}_K[X]$.

Démonstration. Supp $|a_{i_0}| > |a_0|, |a_d|$. Alors $P' = P/a_{i_0} \in \mathcal{O}_K[X]$. On a

$$P' = X^r g(X) \pmod{\mathfrak{m}_K}$$

avec $r > 0$ et $g(0) \neq 0$. On a $r \leq \deg(P' \pmod{\mathfrak{m}_K}) < d$ et par le lemme de Hensel $P(X) = FG$ avec $0 < \deg(F) = r < d$ par déf, c'est contradictoire. \square

Corollaire 1.4.3 (Lemme de Hensel). *Si $P \in \mathcal{O}_K[X]$ a une racine simple modulo \mathfrak{m}_K . Alors P a une unique racine congrue à elle modulo \mathfrak{m}_K .*

Démonstration. Clair par l'unicité du relèvement. \square

Corollaire 1.4.4 (Lemme de Newton). *Pour $P \in \mathcal{O}_K[X]$, on suppose qu'il existe $\alpha \in \mathcal{O}_K$ tel que*

$$|P(\alpha)| < |P'(\alpha)|^2$$

alors il existe un unique $\tilde{\alpha} \in \mathcal{O}_K$ tel que

$$\begin{cases} P(\tilde{\alpha}) = 0, \\ |\tilde{\alpha} - \alpha| < |P'(\alpha)| \end{cases}$$

Démonstration. Soit $\lambda = P'(\alpha)$, l'expansion de Taylor de P en α est

$$P(X + \alpha) = P(\alpha) + P'(\alpha)X + X^2 R(X)$$

avec $R(X) \in \mathcal{O}_K[X]$. Soit $H(X) = \lambda^{-2}P(\lambda X + \alpha)$, on a

$$P(\lambda X + \alpha)/\lambda^2 = P(\alpha)/\lambda^2 + X + X^2 R_1(X)$$

et $|P(\alpha)/\lambda^2| < 1$ par hypothèse. Donc on a $H(X) \in \mathcal{O}_K[X]$ et $\bar{H}(X) = X(1 + XG(X))$ pour un G . Et 0 est une racine simple de \bar{H} . Par le corollaire précédent on a une unique racine t de H telle que $|t| < 1$. D'où $\lambda t + \alpha$ est une racine de P et c'est la seule dans $D(\alpha, |\lambda|)$. \square

Exemple 1. Dans \mathbb{Q}_p , si $\alpha \in \mathbb{Q}_p$ et $|\alpha|_p < 1$ alors $1 + \alpha$ a une racine n -ème dans \mathbb{Z}_p si n est premier à p . On peut considérer $X^n - (1 + \alpha) \in \mathbb{Z}_p[X]$, dans \mathbb{F}_p : $X^n - (1 + \alpha) = X^n - 1$ a une racine simple $X = 1$ puis lemme de Hensel.

Exemple 2. Si $n = p - 1$, $P = X^{p-1} - 1$ est décomposé dans \mathbb{F}_p d'où on a les racines $p - 1$ -èmes de l'unité dans \mathbb{Z}_p .

Exemple 3. Si $n = p$, $(1 + p\alpha)^p = 1 + p^2\alpha^*$ et $(1 + X)^p = 1 + pX + p(p - 1)/2X^2 + pX^{p-1} + X^p$ et $p \mid \binom{p}{k}$ pour $1 \leq k \leq p - 1$. Enfin

$$(1 + p\alpha)^p = 1 + p^2\alpha^*$$

et $(1 + p) \neq (1 + \alpha)^p, \alpha \in \mathbb{Z}_p$.

Exemple 4. Enfin par exemple $X^2 - p$ peut pas avoir de racines dans \mathbb{Z}_p parce que $\equiv X^2 \pmod{p}$ et $v_p(\alpha^2) = 2v_p(\alpha) \neq 1 = v_p(p)$.

Théoreme 1.4.5 (Lemme de Hensel multivarié). *Soit $F(X, Y) \in \mathcal{O}_K[X, Y]$. On suppose que \bar{F} a un zéro (a, b) . On suppose que $\bar{F}'_X(a, b) \neq 0$. Alors*

$$\{(x, y) \in \mathcal{O}_K^2 \mid F(x, y) = 0, \bar{x} = a, \bar{y} = b\}$$

est en bijection avec

$$\{t \in \mathcal{O}_K \mid |t| < 1\}.$$

Démonstration. Soit $t \in \mathfrak{m}_K$. On considère $P = F(X, \tilde{b} + t) \in \mathcal{O}_K[X]$ où $\tilde{b} \equiv b$ et $\bar{P}(X) = \bar{F}(X, b)$, $\bar{P}'(X) = \bar{F}'_X(X, b)$. Par le lemme de Hensel, P a une unique racine $\alpha(t) \in \mathcal{O}_K$, telle que $\bar{\alpha}(t) \equiv a$. Alors

$$\{|t| < 1\} \rightarrow \{(x, y) \in \mathcal{O}_K^2 \mid F(x, y) = 0, \bar{x} = a, \bar{y} = b\}$$

est injective car $t \mapsto b + t$ est injective.

Inversement, si (x, y) est dans l'ensemble de droite. On pose $t = y - b$ d'où $P_t(x) = 0$, $\bar{x} = a$ implique $x = \alpha(t)$. En fait,

$$\{|t| < 1\} \rightarrow \{F^{-1}(0) \dots\}$$

est continue et même analytique. \square

Exemple 5. Soit $E: y^2 = x^3 + 1$ sur \mathbb{Q}_p , $p > 3$. On regarde $F = Y^2 - (X+1)^3$. On a $F_X = 3X^2$ et $F_Y = 2Y$. Pour tout $(a, b) \in \mathbb{F}_p^2$ tel que $b^2 = a^3 + 1$, au moins l'un des $\bar{F}_X(a, b)$ et $\bar{F}_Y(a, b)$ est non nul. Alors $E(\mathbb{Z}_p)$ est une union disjointe de disques ouvert de \mathbb{Z}_p indexés par $E(\mathbb{F}_p)$.

1.5 Extension de valeurs absolues

On considère L/K une extension finie de corps quelconques. Pour rappel la norme

$$N_{L/K}(\alpha): L \rightarrow K$$

est définie comme le déterminant de $x \mapsto \alpha x$ dans L .

Proposition 1.5.1. *Pour $\alpha \in L$,*

- $N(\alpha) = \alpha^{[L:K]}$ si $\alpha \in K$.
- La norme est multiplicative.
- Étant donné $L/E/K$, on a $N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha))$. (dur)
- Si $P(X) = X^d + \dots + a_0$ est le polynôme minimal de α sur K , alors, $N_{K[\alpha]/K}(\alpha) = (-1)^d a_0$.

En particulier, le cas $E = K[\alpha]$ est intéressant.

Théoreme 1.5.2. *Si K est complet ultramétrique. Soit L/K une extension finie. Alors $|\cdot|$ s'étend uniquement en une valeur absolue sur L via*

$$|\alpha| = |N_{L/K}(\alpha)|^{1/[L:K]}.$$

Démonstration. L'existence consiste à vérifier que c'est bien une valeur absolue. On sup $|\alpha|_L \leq 1$. On doit vérifier que

$$|1 + \alpha|_L \leq 1$$

mais $|\alpha|_L \leq 1$ dit que $|N_{L/K}(\alpha)| \leq 1$. Si P est le polynôme minimal de α alors $|a_0| \leq 1$ d'où par le corollaire de Hensel $P \in \mathcal{O}_K[X]$. En plus, $P(X-1)$

Corps ultramétriques complets

est le pol minimal de $1 + \alpha$. D'où $|N_{K[\alpha]/K}(1 + \alpha)| = |1 + \alpha|_L \leq 1$. Enfin l'unicité est due à l'unicité des normes sur L en tant que K -ev. (**regarder**)

Si $|\cdot|$ est triviale les extensions définissent des topologies discrètes donc sont triviales. \square

Ça c'est pour les extensions finies.

Corollaire 1.5.3. *Une valeur absolue sur un corps ultramétrique complet K s'étend uniquement en une valeur absolue sur \bar{K} !*

Démonstration. L'idée c'est de définir

$$|\alpha| := |N_{K[\alpha]/K}(\alpha)|^{1/[K[\alpha]:K]}$$

et tout se vérifie localement. En fait dès que $\alpha \in L$, on a $|N_{K[\alpha]/K}(\alpha)|^{1/[K[\alpha]:K]} = |\alpha|_L$. \square

Proposition 1.5.4. *Soit $(K, |\cdot|)$ un corps ultramétrique et L/K une extension finie. Alors il existe au plus $[L : K]$ extensions de $|\cdot|$ à L .*

Sans les valeurs absolues, on a tjr un diagramme

$$\begin{array}{ccccc} L & & & & \\ | & \searrow & & & \\ K & \xrightarrow{\quad} & \hat{K} & \xrightarrow{\quad} & \hat{K}^c \\ & & |\cdot| & & |\cdot|_c \end{array}$$

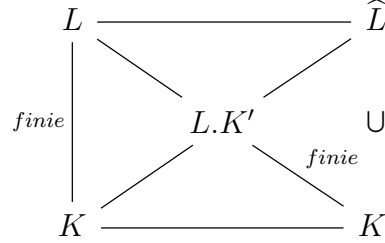
Démonstration. On commence par remarquer qu'on en a une manière d'en avoir $[L : K]$ via $x \mapsto |\sigma(x)|_c$ et qu'on a $|Aut(L/K)| \leq [L : K]$. On montre que toute extension est donnée par un plongement $\sigma: L \rightarrow \hat{K}^c$. Étant donné le diagramme

$$\begin{array}{ccc} (L, |\cdot|_L) & \xrightarrow{\quad} & \hat{L} \\ | & & \cup \\ (K, |\cdot|) & \xrightarrow{\quad} & K' \xrightarrow{\sim} \hat{K} \end{array}$$

où K' est la cloture topologique de K dans \hat{L} , on obtient un isomorphisme $K' \rightarrow \hat{K}$. On veut maintenant montrer que \hat{L} est finie sur K' . Si c'est le cas alors on a un τ tel que $|\tau(x)|' := |x|_{\hat{L}}$ pour tout $x \in \hat{L}$. C'est une valeur absolue sur $\tau(\hat{L}) \subset \hat{K}^c$ qui étend celle de \hat{K} ! L'unicité sur \hat{K}^c implique que $|\cdot|' = |\cdot|_c$ d'où $|\cdot|_{\hat{L}} = |\cdot|_c \circ \tau$.

1.6 Extension de $|\cdot|$ à une extension quelconque

On prouve maintenant que \widehat{L} est finie sur K' .



On remarque que $L.K'$ est complet donc fermé dans \widehat{L} . On conclut en remarquant que c'est dense parce que L est dense dans \widehat{L} . \square

1.6 Extension de $|\cdot|$ à une extension quelconque

Il suffit de savoir étendre à une extension purement transcendante. On regarde dans

$$K(x_i)_{i \in I} = \bigcup_{J \subset I; \#J < \infty} K(x_j)_{j \in J}$$

si on a une manière de définir des normes de manières canoniques sur les extensions finiment générées. On a sur $K[X_1, \dots, X_n]$ la norme de Gauss

$$\|\sum \lambda_{k_1 \dots k_n} X_1^{k_1} \dots X_n^{k_n}\| = \max |\lambda_{k_1 \dots k_n}| \in \mathbb{R}$$

est multiplicative! Et s'étend donc en une valeur absolue de $K(X_1, \dots, X_n)$.

Remarque 4. En analyse p -adique on a besoin de corps algébriquement clos. Mais \mathbb{Q}_p^c n'est pas complet mdr, donc on complète à nouveau en $\widehat{\mathbb{Q}_p^c}$, et cette fois c'est complet et clos.

Théoreme 1.6.1. Soit $(K, |\cdot|)$ un corps ultramétrique. Alors

$$\widehat{\widehat{K^c}}$$

est complet et algébriquement clos.

On prouve d'abord une proposition, comme dans le cas réel ou complexe, soit $(K, |\cdot|)$ un corps valué. On ajoute la norme 1 (au cas où c'est archimédien) sur $K[X]$. On étend $|\cdot|$ à K^c (\mathbb{C} si archimédien).

Proposition 1.6.2 (Continuité des racines). Soit $P \in K[X]$ un polynôme unitaire de degré n , alors pour tout $\epsilon > 0$, $\exists \delta > 0$ dépendant uniquement de P est ϵ tel que pour tout $Q \in K[X]$ unitaire de degré n avec $\|P - Q\|_1 < \delta$ on a, pour toute racine $\alpha \in K^c$ de P il existe $|\alpha - \beta| < \epsilon$.

Corps ultramétriques complets

Démonstration du théorème. On peut supposer K complet. Soit $P \in \widehat{K^c}[X]$ et α une racine dans une extension finie. Pour tout $m \geq 1$ et $\epsilon = 1/m$, on a $Q_m \in K^c[X]$ tel que

$$\|P - Q_m\| < \delta_m$$

implique qu'il existe une racine β_m de $Q_m(X)$ telle que $|\alpha - \beta_m| < 1/m$. Clairement, $(\beta_m)_m$ est de Cauchy et $\beta_m \in K^c$ d'où $\alpha = \lim_m \beta_m \in \widehat{K^c}$ et on a fini. \square

Démonstration de la proposition. On peut noter que $\|P\| \geq 1$ implique $|\alpha| \leq \|P\|$ si $|\alpha| \leq 1$. On suppose donc $\|\alpha\| \geq 1$. On a

$$|\alpha^n| = |-a_{n-1}\alpha^{n-1} - \dots - a_0| \leq \left(\sum_{0 \leq i \leq n-1} |a_i| \right) |\alpha|^{n-1}$$

puis

$$\leq \|P\| \cdot |\alpha|^{n-1} \implies |\alpha| \leq \|P\|.$$

Maintenant $|Q(\alpha)| \leq \|Q - P\| \max\{1, |\alpha|^n\}$ et $Q(X) = \prod (X - \beta_i) \implies \prod |\alpha - \beta_i| \leq \|Q - P\| \max\{1, |\alpha|^n\}$ c'est équivalent à ce qu'il existe $\beta - \beta_{i_0}$ t.q

$$|\alpha - \beta|^n \leq \|Q - P\| \cdot \|P\|^n \implies |\alpha - \beta| \leq \|Q - P\|^{1/n} \cdot \|P\|.$$

\square

1.7 À l'aide d'anneaux artiniens

On peut commencer à discuter les propriétés du point de vue topologique. Si on considère \widehat{K} on peut regarder la \widehat{K} -algèbre $B_L = L \otimes_K \widehat{K}$. En tant qu'ev, c'est de dimension $[L : K]$. Elle a qu'un nombre fini d'idéaux maximaux, $\leq [L : K]$ car si on prends une suite décroissante $\mathfrak{m}_1, \mathfrak{m}_1 \cap \mathfrak{m}_2, \dots, \cap_{j=1}^i \mathfrak{m}_j$ alors c'est une suite décroissante d'espaces vectoriels! D'où la finitude.

On voudrait maintenant construire une bijection entre

$$\{\text{Idéaux maximaux de } B_L\} \leftrightarrow \{\text{extensions de } |\cdot|_K \text{ à } L\}$$

Démonstration. On commence avec $\mathfrak{m}_0 \subset B_L$, alors B_L/\mathfrak{m}_0 est une extension finie de \widehat{K} . Il existe une unique extension $|\cdot|_{\mathfrak{m}_0}$ de $|\cdot|_K$ à B_L/\mathfrak{m}_0 . Via le morphisme canonique

$$L \rightarrow L \otimes_K \widehat{K} \rightarrow B_L/\mathfrak{m}_0$$

le pullback de $|\cdot|_{\mathfrak{m}_0}$ à L est une extension de $|\cdot|_K$ à L . On montre maintenant que si \mathfrak{m}_1 en est un autre on obtient une extension différente. L'espace $L \otimes_K \widehat{K}$

est un Banach dans lequel L est dense c'est assez clair. Si $\hat{x} \in \mathfrak{m}_0 \setminus \mathfrak{m}_1$ et $L \ni a \sim \hat{x}$ alors $|a|_{\mathfrak{m}_0} \sim 0$ dans le quotient car $\hat{x} \mapsto 0$ mais $|a|_{\mathfrak{m}_1} \neq 0$ parce que $\hat{x} \mapsto \neq 0$ dans B_L/\mathfrak{m}_1 . On a montré que $\mathfrak{m} \mapsto |\cdot|_{\mathfrak{m}}$ est injective. À l'inverse si on regarde $\hat{L} = (\hat{L}, |\cdot|_L)$ où $|\cdot|_L$ étend $|\cdot|_K$. On regarde

$$\begin{array}{ccc}
 L & \xrightarrow{\quad} & \hat{L} \\
 \searrow & & \nearrow \\
 & L \otimes_K \hat{K} & \\
 \nearrow & & \nwarrow \\
 K & \xrightarrow{\quad} & \hat{K}
 \end{array}$$

Où $B_L \rightarrow L$ est le produit. Faut montrer que c'est bien défini, on sait que l'image est dense car L est dense, et l'image est fermée, simplement par exemple parce que e.v. de dim finie sur \hat{K} donc Banach donc complet donc fermé. On déf ensuite $\mathfrak{m} = \ker(L \otimes_K \hat{K} \rightarrow \hat{L})$ alors $\hat{L} = B_L/\mathfrak{m}$. (\mathfrak{m} dépend de la clôture choisie donc c'est bon) \square

Exemple 6. Si on pose $L = \mathbb{Q}[\sqrt{2}]$ et qu'on regarde $|\cdot|_p$, on a

$$L \otimes_K \hat{K} = \mathbb{Q}_p[X]/(X^2 - 2)$$

dans \mathbb{Q}_2 , $X^2 - 2$ est irréductible (regarder la valuation), de sorte que $|\cdot|_2$ s'étend de manière unique à $\mathbb{Q}[\sqrt{2}]$! Dans \mathbb{Q}_7 ça split et on a deux extensions de $|\cdot|_7$ à $\mathbb{Q}[\sqrt{2}]$.

1.8 Cas archimédien

On appelle $r_1, 2r_2$ le nombre de plongement réels, complexes de L/\mathbb{Q} dans \mathbb{C} . Si $L = \mathbb{Q}[\theta]$ et P est le polynôme minimal de θ alors r_1 est le nombre de racines réelles et $2r_2$ le nombre de racines complexes de P .

Proposition 1.8.1. *Il y'a exactement $r_1 + r_2$ extensions de $|\cdot|_{\infty}$ à L .*

Exemple 7. Si $L = \mathbb{Q}[i]$ alors $r_2 = 1$ et $r_1 = 0$. Faut montrer que la conjugaison complexe change pas la valeur absolue dans ce cas, on dirait qu'il faut étendre à \mathbb{C} puis remarquer que la restriction à \mathbb{R} n'est pas invariante. Faut aussi utiliser que $z \mapsto \bar{z}$ est linéaire donc continue (**à faire**).

1.9 Corps local

Si $(K, |\cdot|)$ est complet ultramétrique. On veut montrer que si le corps résiduel est fini alors K est localement compact, i.e. \mathcal{O}_K est compact. On suppose $|\cdot|$ non triviale.

Démonstration. Soit $0 < |t| < 1$, on considère \mathcal{O}_K comme d'hab et $\Sigma \subset \mathcal{O}_K$ un système de représentants de $\mathcal{O}_K/t\mathcal{O}_K$. On considère l'ensemble $\mathcal{E} \subset \Sigma^{\mathbb{Z}}$ des suites éventuellement nulle à gauche. On met la topologie discrète sur Σ et produit sur $\Sigma^{\mathbb{Z}}$.

Proposition 1.9.1. *On a un homéomorphisme*

$$f: \mathcal{E} \rightarrow K; (x_n)_n \mapsto \sum x_n t^n$$

Preuve de la proposition. Faut montrer que c'est bien déf, suffit de voir que $|x_n||t|^n \leq |t|^n \rightarrow 0$. Ensuite la "norme" de f , si $x \neq y \in \mathcal{E}$ on déf $|f(x) - f(y)|$ comme le plus petit entier t.q $x_{n_0} \neq y_{n_0}$. On montre que $|f(x) - f(y)| = |x_{n_0} - y_{n_0}||t|^{n_0}$, on peut pas supposer $y = 0$ parce que $x_{n_i} - y_{n_i}$ est pas nécessairement un représentant. Il suffit de remarquer que comme $x_{n_0} - y_{n_0} \neq 0$ dans le quotient, alors $|x_{n_0} - y_{n_0}| > |t|$. Ensuite on factorise, $(x_{n_0} - y_{n_0})t^{n_0}$ et on conclut.

Soit maintenant $\alpha \in K^*$, on a un n_0 t.q. $|t|^{n_0+1} < |\alpha| \leq |t|^{n_0}$. On a $|t| < |\alpha/t^{n_0}| \leq 1$ d'où dans \mathcal{O}_K , il existe $x_{n_0} \in \Sigma$ t.q

$$|\alpha/t^{n_0} - x_{n_0}| \leq |t|$$

d'où

$$|\alpha - x_{n_0}t^{n_0}| \leq |t|^{n_0+1}$$

on peut alors construire de manière inductive α . On a montré la bijection. Enfin, l'histoire des normes montre que c'est continu et même un homéo par la topologie produit (faire). \square

Corollaire 1.9.2. *Si $\mathcal{O}_K/t\mathcal{O}_K$ est fini, alors \mathcal{O}_K est compact et K est localement compact.*

Démonstration. On a $\mathcal{E}_0 = \Sigma^{\mathbb{N}} \subset \mathcal{E}$. On doit étudier les suites de $\mathcal{E}_0 = f^{-1}\mathcal{O}_K$. On a $|f(x)| = |x_{n_0}||t|^{n_0} > |t|^{n_0+1}$ si $x_{n_0} \neq 0$ car $|x_{n_0}| > |t|$ d'où $1 \geq |f(x)| > |t|^{n_0+1} \implies n_0 \geq 0$. Maintenant, Σ est compact puis $\Sigma^{\mathbb{N}}$ est compact. Enfin $K = \cup(\lambda + \mathcal{O}_K)$. \square

\square

1.9 Corps local

Chapitre 2

Théorie algébrique

On utilise des anneaux de valuations discrètes plutôt que des valeurs absolues.

2.1 Anneaux de Dedekind

Si on prends deux anneaux intègres $A \subset B$, B intégralement clos alors la clôture intégrale de A dans B est intégralement close. Si on note \tilde{A} la clôture intégrale de A dans B et $\lambda \in \text{Frac}(\tilde{A})$, entier sur $\tilde{A} \subset B$ alors entier sur A . Maintenant, $\lambda \in \text{Frac}(B)$ entier sur B implique $\lambda \in B \cap \tilde{A} = \tilde{A}$.

Proposition 2.1.1. *Si $b \in B$ algébrique sur $\text{Frac}(A) = K$ et P son polynôme minimal est unitaire. Alors b est entier sur A si $P[X] \in A[X]$. L'inverse est vrai si A est intégralement clos.*

Démonstration. On prouve l'inverse, si b est entier sur A alors toutes les racines sont entières sur A par galois sur l'équation. D'où les coefficients sont entiers sur A et dans $\text{Frac}(A)$ on conclut avec l'hypothèse en plus sur A . \square

Corollaire 2.1.2. *Si $b \in B$ est entier sur A intégralement clos, $N_{L/K}(b), \text{Tr}_{L/K}(b) \in A$ où L est juste une extension finie tq $b \in L$ et $K = \text{Frac}(A)$.*

Démonstration. On regarde $N_{K[b]/K}(b)^{[L:K[b]]}, \text{Tr}(\dots)$. \square

Théoreme 2.1.3. *Soit A un anneau noethérien intégralement clos. Et soit une extension séparable finie L de $\text{Frac}(A) = K$. Alors la clôture intégrale de A dans L , B , est un A -module de type fini, en particulier noethérien.*

Démonstration. On regarde les traces $\text{Tr}_{L/K}: L \times L \rightarrow K$ qui sont bilinéaires sur K . Maintenant si L/K est séparable alors $\text{Tr}_{L/K}$ est non dégénérée (voir dans le Samuel). Soit e_1, \dots, e_n une base de L sur K . On peut prendre $e_i \in B$

via le coefficient dominant de leur polynôme minimal. On prend les bases duales **pour** \mathbf{L} $e_i^* \in L$ et on regarde

$$Tr_{L/K}(e_i e_j^*) = \begin{cases} 1, & i = j \\ 0 & \end{cases}$$

Maintenant soit $b \in B$, on a $b = \sum \lambda_i e_i$ avec $\lambda_i \in K$. En plus, $\lambda_i = Tr_{L/K}(b e_i^*)$ et e_i^* étant algébrique il existe $t \in A \setminus 0$ t.q $t e_i^* \in B$ pour chaque i . Maintenant,

$$\lambda_i = (1/t) Tr_{L/K}(b(t e_i^*)) \in (1/t)A$$

d'où $b \in \sum_{i=1}^n (1/t) A e_i$ qui est un A -module de type fini, or A est noethérien donc ce truc est noethérien donc B est de type fini sur A car inclut dedans. \square

2.2 Anneaux de Dedekind

Définition 2.2.1. Un anneau de dedekind A est un anneau t.q

- A est noethérien.
- A est intégralement clos.
- A est de dimension 1.

Théoreme 2.2.2 (Décomposition en idéaux premiers). *Il existe une décomposition unique de $(0) \neq I \subset A$ en idéaux premiers*

$$I = \prod_{i=1}^r \mathfrak{m}_i^{r_i}$$

où les $r_i \geq 1$.

Comment on obtient des anneaux de Dedekind maintenant ? On peut localiser un anneau de Dedekind. Ça reste un anneau de Dedekind.

Remarque 5. *Si on regarde topologiquement, $\text{Spec}(S^{-1}A) \subset \text{Spec}(A)$ d'où la dimension est \leq .*

Corollaire 2.2.3. *Si A est de dedekind, la localisation en \mathfrak{p} est un anneau de valuation discrète.*

Définition 2.2.4. Un anneau de valuation discrète est un anneau de Dedekind local qui n'est pas un corps.

Proposition 2.2.5. *Un anneau de valuation discrète est un anneau local principal qui n'est pas un corps.*

Démonstration. Comme on admet le théorème de décomposition : si $\mathfrak{m} \neq 0$ alors $\mathfrak{m} \neq \mathfrak{m}^2$ par Nakayama. Ensuite si $t \in \mathfrak{m} - \mathfrak{m}^2$ alors $tA = \mathfrak{m}^k$ par le théorème de décomposition mdr, $t \notin \mathfrak{m}^2$ implique $k \leq 1$. \square

on peut construire une valuation sur (A, \mathfrak{m}) puis sur $\text{Frac}(A)^*$. On réobtient $A = \{v(K^*) \geq 0\}$.

Théoreme 2.2.6. *Soit A un anneau de Dedekind et $L/K = \text{Frac}(A)$ finie séparable. Alors la clôture de A dans L , B , est un anneau de Dedekind fini sur A .*

Démonstration. Via l'exo du td B est entier sur A implique tout. \square

Exemple 8. Si on prends $L/k(T)$, la clôture intégrale dans L de $k[T]$ fournit un morphisme fini $C \rightarrow \mathbb{P}^1$. Pareil, si on prends $k((t))$ c'est transcendant sur $k(t)$. Si $k = \mathbb{F}_q$ alors $k(t)$ est dénombrable contrairement à $k((t))$. On prends s transcendant et la valuation t -adique. On regarde

$$k(t) \subset K = k(t, s^p) \subset L = k(t, s) \subset k((t))$$

On a $[L : K] = p$, $\mathfrak{m}_K = t\mathcal{O}_K$ et $\mathfrak{m}_L = t\mathcal{O}_L$ de corps résiduels k avec les valuations restreintes. Alors,

$$\mathcal{O}_L \text{ est un a.v.d, pas fini sur } \mathcal{O}_K$$

On verra la preuve plus tard. Le point c'est que c'est inséparable donc la dimension est pas finie.

Théoreme 2.2.7 (Krull-Akizuki). *Si A est de Dedekind et $L/K = \text{Frac}(A)$ finie. Alors la clôture de A dans L est de Dedekind.*

Théoreme 2.2.8. *Si A est un a.v.d avec les hyp du dessus. Alors la clôture est d'Artin.*

Lemme 2.2.9. *Si L/K est purement insép finie. Alors on obtient un anneau de valuation discrète.*

Démonstration. Soit $p = \text{char}(K) > 0$. Il existe $e > 0$, $L^{p^e} \subset K$. On note $A = \mathcal{O}_K$ et \mathcal{O}_L la clôture dans L . On construit une valuation sur L^* via $v(x^{p^e})/p^e$. C'est une valuation. Et maintenant $v_L(x) \geq 0$ est équivalent à $x^{p^e} \in \mathcal{O}_K$ est entier sur \mathcal{O}_K . À l'inverse si $x \in \mathcal{O}_L$ t.q. $x^{p^e} \in K$ est entier sur \mathcal{O}_K comme \mathcal{O}_K est de dedekind on a fini. \square

2.2 Anneaux de Dedekind

Chapitre 3

Ramification

On étudie les extensions d'anneaux de valuations discrètes. On prends \mathcal{O}_K un d.v.r, k son corps résiduel, K son corps de fractions. Et π_K une uniformisante.

3.1 Définitions

Définition 3.1.1. Une extension de d.v.r est un morphisme d'anneaux locaux.

Définition 3.1.2 (Indice de ramification). C'est l'exposant $e_{L/K}$ tel que $\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L^{e_{L/K}}$. On peut le voir sur les uniformisantes.

On définit, pour $|\cdot|_K$ associée à \mathcal{O}_K et étendue à L . La valuation normalisée $v_K: K^* \rightarrow \mathbb{Z}$ via $v_K(\pi_K) = 1$. Alors

$$v_L(\pi_K) = e$$

.

Définition 3.1.3 (Degré résiduel). On déf $f_{L/K} := [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}_K/\mathfrak{m}_K]$ la dimension de l'extension résiduelle.

Exemple 9. Si on pose $K = \mathbb{C}(z)$ et $L = K[t]$ avec $t^d = z$. Alors $\mathbb{C}[t]$ est entier sur $\mathbb{C}[z]$ et un PID donc la clôture intégrale de $\mathbb{C}[z]$ dans L . Les idéaux au dessus, $(z - c)\mathbb{C}[z]$, y'a deux cas :

- $c \neq 0$ et la le polynôme se scinde à racines simples et indice de ramification 1.
- $c = 0$, les racines de l'unité sont inversibles. Donc seulement (t) contient (z) et indice de ramification d .

Si c est proche de 0, les branches se "ramifient".

Exemple 10. Si on regarde $K = \mathbb{Q}[\sqrt{d}]$ avec d sans facteurs carrés. On peut voir avec la trace que $\mathbb{Z}[\sqrt{d}]$ est d'indice au plus 2 dans \mathcal{O}_K .

Proposition 3.1.4. *L'indice de ramification et le degré résiduel sont multiplicatifs pour les sous-extensions.*

Proposition 3.1.5. *L'indice de ramification et le degré résiduel sont invariants par complétions.*

Théoreme 3.1.6. *Pour une extension finie L/K . Avec $\tilde{\mathcal{O}}_K$ la clôture de \mathcal{O}_K dans L . En notant $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ les idéaux maximaux de $\tilde{\mathcal{O}}_K$, $\mathcal{O}_K \rightarrow (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}$ est une extension de d.v.r. Alors*

$$\sum_i e_i f_i \leq [L : K]$$

et les propriétés suivantes sont équivalentes

1. l'inégalité est une égalité.
2. $\tilde{\mathcal{O}}_K$ est fini sur \mathcal{O}_K .
3. $L \otimes_K \hat{K}$ est réduite.

En particulier, on a une égalité si L/K est séparable ou si K est complet.

Lemme 3.1.7. *Si $\mathcal{O}_K \rightarrow \mathcal{O}_L$ est une extension de d.v.r alors*

$$\dim_k \mathcal{O}_L / \mathfrak{m}_K \mathcal{O}_L = e \cdot f \in \mathbb{N} \cup \{\infty\}$$

Démonstration. Voir cours. En gros on considère la famille $\{\pi_L^i b_j | 0 \leq i \leq e-1, 1 \leq j \leq r\}$ pour $b_1, \dots, b_r \in \mathcal{O}_L$ une famille libre dans le quotient. On montre que la famille est libre puis que $r = f$ quand les quantités sont finies. Pour ça on lift une base de k_L , b_1, \dots, b_f , et on a $\mathcal{O}_L \subset \sum_j b_j \mathcal{O}_K + \pi_L \mathcal{O}_L$. On a plus qu'à itérer e fois. On obtient

$$\mathcal{O}_L \subset \left(\sum_{0 \leq i \leq e-1; 1 \leq j \leq f} b_j \pi_L^i \mathcal{O}_K \right) + \pi_K \mathcal{O}_L$$

. Si on appelle M le gros truc à gauche. En quotientant par $\pi_K \mathcal{O}_L$ on obtient une famille génératrice du quotient de taille ef . \square

Remarque 6. *Si \mathcal{O}_L est fini sur \mathcal{O}_K alors $\mathcal{O}_L = M$ par Nakayama!*

Ramification

Lemme 3.1.8.

$$\dim_k \tilde{\mathcal{O}}_K / \mathfrak{m}_K \tilde{\mathcal{O}}_K \leq [L : K]$$

Note 1. Dans le premier lemme, on regarde qu'un idéal, là on les regarde tous.

Démonstration. Voir cours. Je crois que c'est juste qu'une famille libre dans le quotient doit être libre au dessus. D'où le résultat. \square

Lemme 3.1.9. Si K est complet :

$$\dim_k \tilde{\mathcal{O}}_K / \mathfrak{m}_K \tilde{\mathcal{O}}_K = [L : K]$$

Démonstration. Faut faire attention, \mathcal{O}_L est pas nécessairement fini sur \mathcal{O}_K . Mais on a $\mathcal{O}_L \subset M + \pi_K \mathcal{O}_L$ et en itérant, $\mathcal{O}_L \subset M + \pi_K^N \mathcal{O}_L$ pour tout N . Donc M est dense dans \mathcal{O}_L . Donc $M \otimes_{\mathcal{O}_K} K$ est dense dans L de dimension finie sur K complet donc fermé + complet dans L . D'où on a l'égalité. \square

Lemme 3.1.10. La flèche induite $A/\mathfrak{m}^r \rightarrow A_{\mathfrak{m}}/\mathfrak{m}^r A_{\mathfrak{m}}$ est un isomorphisme dès que \mathfrak{m} est maximal.

Théoreme 3.1.11. On se place dans L/K finie, \mathcal{O}_K un d.v.r et $\tilde{\mathcal{O}}_K$ la clôture de \mathcal{O}_K dans L . On considère $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ les idéaux maximaux de $\tilde{\mathcal{O}}_K$. Puis via les $(\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i} / \mathcal{O}_K$ on a les e_i, f_i et alors

$$\sum_i e_i f_i \leq [L : K]$$

En plus on a égalité ssi $\tilde{\mathcal{O}}_K$ est fini sur \mathcal{O}_K ssi $L \otimes_K \hat{K}$ est réduite.

Preuve de l'inégalité. Comme on est dans un anneau de Dedekind on a

$$\mathfrak{m}_K \tilde{\mathcal{O}}_K = \prod_i \mathfrak{m}_i^{r_i}$$

et par localisation on voit que $r_i = e_i$. Enfin par CRT et le dernier lemme on a $\tilde{\mathcal{O}}_K / \mathfrak{m}_K \simeq \prod (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i} / \mathfrak{m}_i^{e_i} (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}$ avec $\mathfrak{m}_i^{e_i} (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i} = \mathfrak{m}_K (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}$. D'où par le premier lemme et le deuxième lemme on obtient l'inégalité. \square

Preuve des équivalences. Si maintenant on a l'égalité on veut montrer que $\tilde{\mathcal{O}}_K$ est fini sur \mathcal{O}_K . Il montre qu'une base relevée de $\tilde{\mathcal{O}}_K / \mathfrak{m}_K$ est libre sur \mathcal{O}_K et K , donc une base de L . En plus par unicité de la décomposition et via l'écriture dans le quotient c'est une base de $\tilde{\mathcal{O}}_K$ sur \mathcal{O}_K . Si $\tilde{\mathcal{O}}_K$ est fini à l'inverse, alors il est libre car d.v.r sont principaux et son rang est le même après $\otimes K$. \square

3.2 Trouver les indices de ramification/degrés résiduels

Proposition 3.2.1. *On suppose que $\tilde{\mathcal{O}}_K = \mathcal{O}_K[\alpha]$ pour un α . Soit $P \in K[X]$ le polynôme minimal unitaire de α . Alors $P \in \mathcal{O}_K[X]$ et soit $\bar{P}(X) = \prod_i p_i(X)^{r_i} \bmod \tilde{\mathfrak{m}}_K$ la décomposition irréductible dans $k[X]$. Soit $P_i = p_i \bmod \tilde{\mathfrak{m}}_K$ des lifts alors*

1. *Les idéaux maximaux de $\tilde{\mathcal{O}}_K$ sont exactement les \mathfrak{m}_i où $\mathfrak{m}_i = (\mathfrak{m}_K, P_i(\alpha))$.*
2. *$(\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}/(\mathfrak{m}_i) \simeq k[X]/(P_i(X))$.*
3. *$e_i = e_{(\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}/\mathcal{O}_K} = r_i$.*

Démonstration. Les idéaux maximaux de $(\tilde{\mathcal{O}}_K)$ contiennent tous \mathfrak{m}_K d'où on a une bijection avec les idéaux du quotient \tilde{k} . On conclut en prenant les images inverses qui sont maximales parce que le quotient par elles est un corps. Ça prouve 1. et 2., pour 3. on a $P(X) = \prod P_i(X)^{r_i} + \epsilon(X)$ avec $\epsilon(X) \in \mathfrak{m}_K[X]$. Alors $0 = P(\alpha) = \prod P_i(X)^{r_i} + \epsilon(\alpha)$. D'où $\prod_i P_i(\alpha)^{r_i} = -\epsilon(\alpha) \in \mathfrak{m}_K \tilde{\mathcal{O}}_K$. Ensuite

$$\prod \mathfrak{m}_i^{r_i} \subset \mathfrak{m}_K \tilde{\mathcal{O}}_K + P_i(\alpha)^{r_i} \tilde{\mathcal{O}}_K$$

d'où $\prod \mathfrak{m}_i^{r_i} \subset \mathfrak{m}_K \tilde{\mathcal{O}}_K$. Comme on est dans un anneau de Dedekind $e_i \leq r_i$. Ensuite comme $\sum r_i f_i \geq \sum e_i f_i = [L : K]$, et qu'à gauche on a le degré de \bar{P} qui est monique donc pareil que le degré de $P = [K[\alpha] : K]$. \square

Note 2. Voir pq y contiennent tous \mathfrak{m}_K c'était dans le dernier cours.

On suppose tjr maintenant que $\tilde{\mathcal{O}}_K$ est finie sur \mathcal{O}_K .

Définition 3.2.2. $\mathcal{O}_K \rightarrow \mathcal{O}_L$ une extension de d.v.r est non ramifiée si $\begin{cases} e = 1 \\ k_L/k \text{ est finie séparable} \end{cases}$ Dans le cas général, L/K est non ramifiée si $\mathcal{O}_K \rightarrow (\tilde{\mathcal{O}}_K)_{\mathfrak{m}_i}$ est non ramifiée pour tout $\mathfrak{m} \subset \tilde{\mathcal{O}}_K$.

Topologiquement, ça ressemble à un revêtement.

Corollaire 3.2.3. *On suppose que $L = K[\alpha]$ et P le polynôme minimal de α est dans $\mathcal{O}_K[X]$ ainsi que \bar{P} est séparable. Alors $\tilde{\mathcal{O}}_K = \mathcal{O}_K[\alpha]$ et L/K est non ramifiée (si k est parfait).*

Ramification

Démonstration. On pose $B = \mathcal{O}_K[X]/(P(X)) \simeq \mathcal{O}_K[\alpha] \subset \tilde{\mathcal{O}}_K$. Alors $B \otimes_{\mathcal{O}_K} K = K[\alpha] = L$ est int gralement clos, le quotient $B/\mathfrak{m}_K B = k[X]/(\bar{P}(X))$ est r duit car $\bar{P}(X)$ est s parable. Par l'exercice 1 du td4, $B = \mathcal{O}_K[\alpha]$ est int gralement clos d'o  l' galit . Enfin par la prop pr c dente la s parabilit  de \bar{P} force $e_i = 1$. \square

Exemple 11. On consid re pour $p > 2$: $\mathbb{Q}_p \rightarrow L = \mathbb{Q}_p[\zeta_p]$ avec $\zeta_p \in \mathbb{C}_p$. On note $\tilde{\mathbb{Q}}_p$ la cl ture de \mathbb{Z}_p dans L , c'est un d.v.r \mathcal{O}_L . On a $\lambda_p = \zeta_p - 1 \in \mathfrak{m}_L$ puis

$$(\lambda_p + 1)^p = 1$$

et

$$\mathfrak{m}_L^{p-1} \ni \lambda_p^{p-1} = p(-1 - \lambda_p c) \in \mathfrak{m}_L^e$$

avec $c \in \mathcal{O}_L$. Comme $\lambda_p \in \mathfrak{m}_L$, le terme   droite est inversible, on obtient $e_{\mathcal{O}_L/\mathbb{Z}_p} \geq p - 1$. Comme $ef \leq [L : \mathbb{Q}_p] \leq p - 1$, $f = 1$ et on a pas de racines p - mes de l'unit  dans \mathbb{Q}_p .

Exemple 12. Si p est premier et n est premier   p . En notant $\phi_n(X)$ le n - me polyn me cyclotomique et F_n le polyn me minimal de ζ_n sur \mathbb{Q}_p on a $F_n \mid \phi_n$ d'o  F_n est dans $\mathbb{Z}_p[X]$ monique car $\phi_n \in \mathbb{Z}[X]$ est monique. En plus, \bar{F}_n est s parable car ϕ_n l'est. En particulier $\mathcal{O}_L = \mathbb{Z}_p[\zeta_n]$ et est non ramifi e sur \mathbb{Z}_p par le corollaire pr c dent.

3.3 Extensions monog nes

  rattaper :  tant donn  $K - L$ finie de corps valu s discrets. Supp. $\mathcal{O}_K - \tilde{\mathcal{O}}_K$ est finie. Sous des hypoth ses modestes, $\tilde{\mathcal{O}}_K$ est monog ne sur \mathcal{O}_K . Par exemple,

1. Si K est complet et L est totalement ramifi e ($[L : K] = e$, et l'extension r siduelle est triviale). Alors $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ pour un α annul  par un polyn me d'Eisenstein ($v(a_i) > 0, v(a_0) = 1$). Si en plus L/K est mod r e, ($e_{L/K} \wedge \text{char}(k) = 1$ ou $\text{char}(k) = 0$). On peut prendre $\alpha^n - \pi_K = 0$).

Lemme 3.3.1. *Si K est complet, et on a une extension*

$$\begin{array}{ccccc} K & \longrightarrow & & & L \\ | & & & & | \\ k & \longrightarrow & k' & \longrightarrow & k_L \end{array}$$

avec k'/k s parable. Alors il existe une unique extension $L/K'/K$ t.q $k_{K'} = k'$. Avec K'/K non ramifi e.

3.3 Extensions monogènes

Lemme 3.3.2. *On prends maintenant $e' | e_{L/K}$, avec e' premier à $\text{char}(k)$. Avec $k_K - k_L$ purement inséparable. Alors il existe un lift unique $L/K'/K$ t.q. $k_K = k_{K'}$ et K'/K est de degré e' totalement ramifiée.*

Théoreme 3.3.3. *Soit K un corps complet et L/K finie. On considère*

$$\begin{array}{ccc} K & \longrightarrow & L \\ | & & | \\ k & \xrightarrow{\text{sep}} k' & \longrightarrow k_L \end{array}$$

On a

1. *Pour tout $k' \subset k_L$ séparable sur k il existe une unique $K - K' - L$ une unique sous extension non ramifiée $K - K' - L$ de corps résiduel $= k'$.*
2. *Il existe une plus grande sous-extension non ramifiée $K \subset K^u \subset L$ de K .*
3. *Il existe une plus grande sous-extension modérément ramifiée de L .*

On obtient $K - K^{un} - K^{tam} - L$ avec $[L : K^{tam}]$ une puissance de p .

Preuve de 1.. **Existence** : on trouve un élément primitif de k'/k séparable finie. D'où $k' = k(\theta)$, on trouve $P \in \mathcal{O}_K[X]$ t.q θ est une racine de \bar{P} . Comme P irréd sur k . Alors irréd sur \mathcal{O}_K (TD6). Comme \bar{P} est séparable, en regardant $P \in \mathcal{O}_L[X]$ on peut lift θ par Hensel. Disons en α . On a en plus $K' = K[\alpha]/K$ et $\mathcal{O}_K[\alpha] = \mathcal{O}_{K'}$ car non ramifiée et $k' = k(\theta) = k_{K'}$.

Unicité : Si K''/K est une autre extension t.q $k_{K''} = k' = k(\theta)$. Alors θ lift en une racine $\alpha' \in K'' \subset L$. Le lemme dans Hensel dans L fournit le même $\alpha' = \alpha$. Maintenant K' et K'' ont la même dimension,

$$[K' : K] = [k' : k] = [K'' : K]$$

□

Preuve de 2.. Soit $k' = k^s$ la clôture séparable de k dans k_L . Alors on pose K^{un} l'unique extension non ramifiée t.q. $k_{K^{un}} = k^s$. Si $K - K' - L$ est une extension non ramifiée, alors $k \subset k_{K'} \subset k^s \subset k_L$. Il existe

$$K \subset K'' \subset K^{un}$$

t.q. $k_{K''} = k_{K'}$. On obtient deux sous-extensions non ramifiée de corps résiduels $k_{K'}$ on conclut par 1.. □

Ramification

Preuve de 3.. On a tjr $e_{L/K} = e_{L/K^{un}}$. On supp $\text{char}(k) > 0$ sinon $K^{tam} = L$. Soit e' le plus grand diviseur de e non divisible par p . Par le lemme précédent on a

$$\begin{array}{ccccc} K^{un} & \xrightarrow{-e'} & K^{tam} & \longrightarrow & L \\ | & & & & | \\ k^s & \longrightarrow & k^s & \longrightarrow & k_L \end{array}$$

On a K^{tam}/K^{un} est totalement modérément ramifiée. Et K^{un}/K est non ramifiée sur K . D'où K^{tam}/K est modérément ramifiée. On montre que c'est la plus grande, si on a F/K modérée et $F \subset L$ on considère F^{un}/K non ramifiée et remplacer F par F^{un} . On a $k_F = k^s$ et par 1. on obtient

$$K^{un} \subset F \subset L$$

par la preuve précédente le lift de θ le générateur K^{un} est dans F (on peut prendre le pol a coeff dans $\mathcal{O}_F[X]$.)

Maintenant la preuve découle de l'unicité dans le lemme précédent. \square

Corollaire 3.3.4. *Soit L/K finie et K complet. On a*

$$\begin{array}{ccccccc} K & \xrightarrow{\text{non ramifiée}} & K^{un} & \xrightarrow{\text{mod}+\text{tot}} & K^{tam} & \xrightarrow{[L:K^{tam}]=p^r} & L \\ & & & & | & & | \\ & & & & k_{K^{tam}} & \xrightarrow{\text{tot insep}} & k_L \end{array}$$

Exemple 13. Soit $K = \mathbb{Q}_p, L = \mathbb{Q}_p(\zeta_{p^r})$ et $r \geq 1$. On a $\mathbb{Q}_p - \mathbb{Q}_p(\zeta_p)$ est modérément totalement ramifiée de degré $p-1$. Maintenant par l'exam

$$[L : \mathbb{Q}_p(\zeta_p)] = p^{r-1}$$

est sauvagement totalement ramifiée. On pouvait écrire explicitement $\lambda_p^{p^{r-1}} = \lambda_p(1 + \epsilon)$ avec $1 + \epsilon$ une unité.

On obtient $\mathbb{Q}_p^{un} = \mathbb{Q}_p$ et $\mathbb{Q}_p^{tam} = \mathbb{Q}_p(\zeta_p)$. Le polynôme d'Eisenstein est donné par

$$1 + \lambda_p = (1 + \lambda_{p^r})^{r-1}$$

3.4 Théorie de Galois

Si on a $L/F/K$ avec L/F galoisienne alors F/K est galoisienne ssi $\text{Gal}(L/K).F \subset F$. Et cette dernière condition fournit la suite exacte

$$1 \rightarrow \text{Gal}(L/F) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(F/K) \rightarrow 1$$

3.4 Théorie de Galois

Maintenant L/K est normale ssi K^s/K est galoisienne. Et $\text{Aut}_K(L) = \text{Gal}(K^s/K)$. Aussi $K \subset L \subset \tilde{L}$ avec \tilde{L}/K normale est galoisienne si L/K est séparable. Il existe de telles extensions minimales.

Maintenant si on regarde une extension galoisienne finie L/K et K de valuation discrète. Alors

$$\mathcal{O}_K \rightarrow \tilde{\mathcal{O}}_K$$

et finie et $\tilde{\mathcal{O}}_K$ est semi-local de Dedekind. Maintenant $G = \text{Gal}(L/K)$ agit sur $\text{Spm}(\tilde{\mathcal{O}}_K)$ et on a

Proposition 3.4.1. *G agit transitivement sur $\tilde{\mathcal{O}}_K$.*

Lemme 3.4.2 (Lemme d'évitement). *Soit A un anneau commutatif et $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ des idéaux premiers. $\text{Supp } \mathfrak{p}_1 \not\subseteq \mathfrak{p}_i$ pour tout $i \geq 2$. Alors $\mathfrak{p}_1 \not\subseteq \cup_i \mathfrak{p}_i$.*

Preuve du lemme. Dans le cas des idéaux maximaux, c'est un CRT direct. Le cas $n = 3$ est plutôt simple ? Sinon, par induction. \square

Preuve de la proposition. On fixe un idéal maximal \mathfrak{m} et on suppose qu'il existe \mathfrak{m}' t.q. $\mathfrak{m} \neq \sigma(\mathfrak{m}')$ pour tout σ . On obtient $x \in \mathfrak{m} - \cup \sigma(\mathfrak{m}')$. Maintenant $N_{L/K}(x) \in \mathfrak{m}_K \subset \mathfrak{m} \cap \sigma(\mathfrak{m}')$ d'où on a pour un \mathfrak{m}' , $\sigma_0(x) \in \mathfrak{m}'$ d'où $x \in \sigma_0^{-1}(\mathfrak{m}')$. Ce qui contredit l'hypothèse. \square

Définition 3.4.3. Soit \mathfrak{m} un idéal maximal de $\tilde{\mathcal{O}}_K$, on définit $D_{\mathfrak{m}} = \{\sigma(\mathfrak{m}) = \mathfrak{m}\}$ le groupe de décomposition de \mathfrak{m} .

On remarque que $D_{\mathfrak{m}}$ agit sur $(\tilde{\mathcal{O}}_K)_{\mathfrak{m}}$ d'où sur le corps résiduel $\tilde{\mathcal{O}}_K/\mathfrak{m} =: k_{\mathfrak{m}}$. Si $\sigma \in D_{\mathfrak{m}}$ et $\alpha \in \tilde{\mathcal{O}}_K$ alors

$$\sigma(\bar{\alpha}) = \bar{(\sigma(\alpha))}$$

est bien défini. On obtient $D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}})$ et on note $I_{\mathfrak{m}}$ le noyau tel que

$$1 \rightarrow I_{\mathfrak{m}} \rightarrow D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}})$$

c'est le groupe d'inertie en \mathfrak{m} .

Corollaire 3.4.4. *Il existe une bijection entre les idéaux maximaux et les cosets $G/D_{\mathfrak{m}}$ donnée par*

$$\begin{aligned} G &\rightarrow \text{Spm}(\tilde{\mathcal{O}}_K) \\ \sigma &\mapsto \sigma(\mathfrak{m}) \end{aligned}$$

Remarque 7. Si $\sigma_0(\mathfrak{m}) = \mathfrak{m}'$ alors

$$D_{\mathfrak{m}'} = \sigma_0 D_{\mathfrak{m}} \sigma_0^{-1}$$

et

$$I_{\mathfrak{m}'} = \sigma_0 I_{\mathfrak{m}} \sigma_0^{-1}$$

Ramification

Corollaire 3.4.5. *Les indices de ramifications et les degrés résiduels sont égaux à tout les premiers.*

On va montrer qu'en fait

$$1 \rightarrow I_{\mathfrak{m}} \rightarrow D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}})$$

s'étend en

$$1 \rightarrow I_{\mathfrak{m}} \rightarrow D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}}) \rightarrow 1$$

Lemme 3.4.6. *L'extension $k_{\mathfrak{m}}/k$ est normale.*

Démonstration. On montre que pour tout $\theta \in k_{\mathfrak{m}}$, ses conjugués sont dans $k_{\mathfrak{m}}$. On lift en un α dans $\tilde{\mathcal{O}}_K$. G agit sur le polynôme $\min P$ d'où $P \in \mathcal{O}_K[X]$. Puis $\bar{P} \in k[X]$ (car unitaire). D'où le polynôme minimal de θ divise P qui est split dans $k_{\mathfrak{m}}$ par réduction. \square

Proposition 3.4.7. *On montre que la s.e.c est exacte.*

Démonstration. On a vu que $k_{\mathfrak{m}}/k$ est normale. On note $k_{\mathfrak{m}}^s$ la clôture séparable. Alors $k_{\mathfrak{m}}^s/k$ est galoisienne et $\text{Aut}_k(k_{\mathfrak{m}}) = \text{Gal}(k_{\mathfrak{m}}^s/k)$. On écrit $k_{\mathfrak{m}}^s = k[\theta]$. Soit $\tau \in \text{Gal}(k_{\mathfrak{m}}^s/k)$, τ est déterminé par $\tau(\theta)$. On note $r: D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}})$, on montre qu'il existe $\sigma \in D_{\mathfrak{m}}$ tq

$$r(\sigma)(\theta) = \tau(\theta)$$

. On lift θ en $\alpha \in \tilde{\mathcal{O}}_K$. Alors $r(\sigma)(\alpha) = \overline{\sigma(\alpha)}$.

On prends $P = \prod (X - \sigma(\alpha)) \in \mathcal{O}_K[X]$, et on a $\bar{P}(\theta) = 0$. Maintenant les conjugués de θ sont des racines de \bar{P} , qui sont des conjugués de α . On a $\tau(\theta) = \sigma(\alpha)$ pour un $\sigma \in G$, reste à trouver $\sigma \in D_{\mathfrak{m}}$. On peut le trouver en choisissant α mieux.

Plutôt que la flèche du haut dans

$$\tilde{\mathcal{O}}_K \longrightarrow k_{\mathfrak{m}}$$

$$\tilde{\mathcal{O}}_K \longrightarrow \prod_{\mathfrak{m}} \tilde{\mathcal{O}}_K/\mathfrak{m}$$

on la factorise par la flèche du bas. Et on prends α tel que $\alpha = 0$ modulo les autres premiers. Reste à voir que les $\sigma \in G$ tels que $\overline{\sigma(\alpha)} = \tau(\theta)$ sont dans $D_{\mathfrak{m}}$. Par construction, $\alpha \in \mathfrak{m}'$ pour $\mathfrak{m}' \neq \mathfrak{m}$. D'où si $\sigma \notin D_{\mathfrak{m}}$ alors $\sigma^{-1}\mathfrak{m} = \mathfrak{m}' \neq \mathfrak{m}$ puis $\sigma^{-1}\sigma\alpha \in \mathfrak{m}'$, d'où $\sigma(\alpha) = 0 \pmod{\mathfrak{m}}$. Ce qui est contradictoire si $k_{\mathfrak{m}}^s \neq k$. \square

Maintenant on peut regarder la tour

$$K - L^{D_{\mathfrak{m}}} - L^{I_{\mathfrak{m}}} - L$$

et \mathfrak{m} correspond a une valeur absolue de K à L , $|\cdot|_{\mathfrak{m}}$. On note les deux restrictions par $|\cdot|_D$ et $|\cdot|_I$.

Théoreme 3.4.8. *On a*

1. $(K, |\cdot|_K) - (L^D, |\cdot|_D)$ a indice de ramification 1 et une extension de corps résiduels trivial.
2. $(L^D, |\cdot|_D) - (L^I, |\cdot|_I)$ est non ramifiée et d'extension de corps résiduels $k - k_{\mathfrak{m}}$.
3. $(L^I, |\cdot|_I) - (L, |\cdot|_L)$ est d'indice de ramification $|D_{\mathfrak{m}}|$ et l'extension de corps résiduels est purement inséparable.

Remarque 8. L^I/K est alors non ramifiée et L^I/L^D est galoisienne non ramifiée.

Théoreme 3.4.9. *On a les résultats suivants :*

1. $|\cdot|_{\mathfrak{m}}$ est l'unique extension de $|\cdot|_D$ à L et

$$L \otimes_{L^D} (\widehat{L^D, |\cdot|_D}) \simeq (\widehat{L, |\cdot|_{\mathfrak{m}}})$$

en plus $(\widehat{L, |\cdot|_{\mathfrak{m}}})$ est galoisienne sur $(\widehat{L^D, |\cdot|_D})$ de groupe de Galois D .

2. $(K, |\cdot|_K) - (L^D, |\cdot|_D)$ a indice de ramification 1 et extension résiduelle triviale. Puis,

$$(\widehat{K, |\cdot|_K}) \simeq (\widehat{L^D, |\cdot|_D})$$

c'est un exercice.

3. $(L^D, |\cdot|_D) - (L^I, |\cdot|_I)$ est galoisienne, non ramifiée, d'extension résiduelle galoisienne de groupe de galois D/I .
4. L'extension résiduelle de $(L^I, |\cdot|_I) - (L, |\cdot|_{\mathfrak{m}})$ est purement inséparable et

$$e_{(L, |\cdot|_{\mathfrak{m}})/(L^I, |\cdot|_I)} = e_{(L, |\cdot|_{\mathfrak{m}})/K}$$

Ramification

Démonstration. Pour 1., on sait que $L^D - L$ est de groupe de galois D et que D fixe \mathfrak{m}_0 par déf. On a prouvé que D agit transitivement sur les extensions de $|\cdot|_D$ à L . D'où il y'a une seule extension $|\cdot|_{\mathfrak{m}_0}$. Maintenant, la surjection canonique

$$L \otimes_K \rightarrow \prod L_i$$

où $L_i = \widehat{(L, |\cdot|_i)}$. Maintenant par le point d'avant y'a qu'un seul $L_i = L_0$ pour :

$$L \otimes_{L^D} \widehat{L^D} \rightarrow \widehat{(L, |\cdot|_{\mathfrak{m}})}$$

d'où à gauche c'est local, puis L est séparable sur L^D d'où c'est réduit. Maintenant à gauche c'est de dimension finie réduit et local sur un corps complet. Donc c'est un corps.

Exercices 3.4.10. Soit L/K galoisienne, et Ω une extension de K t.q. $L_\Omega := L \otimes_K \Omega$ est un corps. Alors

1. L_Ω/Ω est galoisienne et la flèche canonique

$$\text{Gal}(L/K) \rightarrow \text{Gal}(L_\Omega/\Omega)$$

est un isomorphisme. Où $\sigma \in \text{Gal}(L/K)$ agit via $x \otimes y \mapsto \sigma(x) \otimes y$.

2. Pour toute extensions $K \subset F \subset L$:

$$F \rightarrow F \otimes_K \Omega \subset L \otimes_K \Omega$$

est une bijection entre

$$\{\text{Sous-extensions de } L\} \leftrightarrow \{\text{Sous-extensions de } L \otimes_K \Omega\}$$

t.q. $\text{Gal}(L/K) \simeq \text{Gal}(L \otimes_K \Omega / F \otimes_K \Omega)$.

en admettant l'exercice on obtient

$$D \simeq \text{Gal}(L \otimes_{L^D} \widehat{L^D} / \widehat{L^D})$$

et $\widehat{L^D} = L \otimes_{L^D} \widehat{L^D}$.

Pour 2., on a $[L : K] = \sum e_i f_i$ et quand c'est galoisien $= (|G|/|D|)e_{L/K}f_{L/K}$. D'où pour $L^D - L$, on obtient $e_{L/K}f_{L/K} = |D| = [L : L^D] = e_{(L, |\cdot|_{\mathfrak{m}})/L^D} f_{(L, |\cdot|_{\mathfrak{m}})/L^D}$. En regardant $K - L^D - L$ et $e_{L/K}f_{L/K} = e_{L/L^D}e_{L^D/K}f_{L/L^D}f_{L^D/K}$ d'où $e_{L^D/K}f_{L^D/K} = 1$.

Pour 3./4., $L^I - L$ est galoisienne et dessus, $I = D$ d'où $\text{Aut}(k_{\mathfrak{m}}/k_I) = 1$ et $k_I - k_{\mathfrak{m}}$ est purement inséparable. Pareil $L^D - L^I$ est galoisienne de groupe

3.4 Théorie de Galois

de galois $D/I \simeq \text{Gal}(k_{\mathfrak{m}}^s/k) = \text{Aut}(k_{\mathfrak{m}}/k)$ (avec $k_{\mathfrak{m}}^s$ la cloture de k dans $k_{\mathfrak{m}}$). Maintenant comme $k_I - k_{\mathfrak{m}}$ est purement inséparable d'où $k_{\mathfrak{m}}^s \subset k_I$. On a

$$[k_I : k] \geq [k_{\mathfrak{m}}^s : k] = |D/I| = [L^I : L^D] = e_{L^I/L^D}[k_I : k_D] = e_{L^I/L^D}[k_I : k]$$

d'où $e_{L^I/L^D} = 1$ puis $k_{\mathfrak{m}}^s = k_I$. On obtient 3.. Enfin pour 4., on a vu que l'extension résiduelle est purement inséparable et $e_{L/L^I} = e_{L/K}$. \square

Remarque 9. Garder $1 \rightarrow I \rightarrow D \rightarrow \text{Aut}(k_{\mathfrak{m}}/k) \rightarrow 1$ en tête.

Remarque 10. Dans le cas galoisien, $L^I = K^{un}$ dans $(L, |\cdot|_{\mathfrak{m}})$ (pas facile). Aussi, si k est parfait alors $k_{\mathfrak{m}} = k_{\mathfrak{m}}^s$.

Remarque 11. Si D est distingué dans $\text{Gal}(L/K)$ alors $L^D - L^I$ est inerte et $K - L^D$ est split ($e = f = 1$)! Enfin, $K - L^I$ est la plus grande extension non ramifiée.

Corollaire 3.4.11. $K - (L, |\cdot|_{\mathfrak{m}})$ est modérément ramifiée ssi $|I|$ est premier à $p = \text{car}(k)$. Ça implique que

$$(L^I, |\cdot|_I) - (L, |\cdot|_{\mathfrak{m}})$$

est totalement ramifiée.

Démonstration. Dans

$$K - (L^I, |\cdot|_I) - (L, |\cdot|_{\mathfrak{m}})$$

l'extensio est modérément ramifiée ssi $(L^I, |\cdot|_I) - L$ est modérément ramifiée et on conclut avec le dernier thm. \square

Sachant qu'il donne les pdfs, jsp si ca vaut le coup de noter. Jvais commenter. Et noter les thms.

Théoreme 3.4.12. Avec les notations d'avant,

1. si $\text{char}(k) = 0$, alors I est cyclique.
2. si $p = \text{char}(k) > 0$, on a

$$1 \rightarrow P \rightarrow I \rightarrow T \rightarrow 1$$

avec T cyclique, $|T|$ premier à p est $|P| = p^m$ maximal.

en conséquence, P est l'unique p -Sylow de I . Unique car normal.

Ramification

Il utilise le cas complet et $K = K^{tam} = L$. Critère galoisiens à revoir !
je calcule pas du tout assez. ni exos concrets.

Remarque 12. Si L/K est galoisienne on a la décomposition :

$$K = L^D = L^I = L^P = L$$

avec $L^I = L^P$ modérée et $L^P = L$ sauvage.

Maintenant c'est l'étude de P . On regarde une filtration

$$P = G_1 \supseteq G_2 \supseteq \dots$$

Il suppose k parfait. D'où $L^D = L$ a extension résiduelle séparable. Et

$$\mathcal{O}_L = \mathcal{O}_{L^D}[\alpha]$$

.

Définition 3.4.13. $G_{-1} = D$, $\mathfrak{m}_L \subset \mathcal{O}_L$. On pose

$$G_i := \ker(D \rightarrow \text{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{i+1}))$$

on a $G_i = \{\sigma \in D \mid \sigma(x) - x \in \mathfrak{m}_L^{i+1}\}$. Par déf $G_0 = I$.

Lemme 3.4.14. $\sigma \in G_i$ ssi $\sigma(\alpha) - \alpha \in \mathfrak{m}_L^{i+1}$.

On définit

Définition 3.4.15. $U^{(0)} = \mathcal{O}_L^*$ et $U^{(i)} = 1 + \mathfrak{m}_L^i$.

Proposition 3.4.16. Pour tout $i \geq 0$,

$$G_i/G_{i+1} \hookrightarrow U^{(i)}/U^{(i+1)} \simeq k$$

Corollaire 3.4.17. On a

1. G_0/G_1 est cyclique d'ordre premier à p .
2. $G_i/G_{i+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_i}$ pour tout $i \geq 1$.

Proposition 3.4.18. On a $G_i = \{1\}$ pour $i \gg 1$.

Note 3. On note $i_G(\sigma) = v_L(\sigma(\alpha) - \alpha)$. Pour $K = L^I$ et $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Avec $\sigma \neq 1$.