

## Décompositions d'extensions

## 0.1 Non ramifiée, modérément, sauvagement, totalement ramifié

Pour le vocabulaire : Avec  $L/K$  extension de corps de valuations discrètes, i.e.  $v_K$  discrète fixée.

1. Non ramifié : Pour chaque  $i$ ,  $e_i = 1$  et  $k_{L_i}/k_K$  est séparable.
2. Modérément ramifié : pour chaque  $i$ ,  $p \nmid e_i$  et  $k_{L_i}/k_K$  est séparable.
3. Sauvagement ramifié : il existe un  $i$  tq  $p \mid e_i$  ou  $k_{L_i}/k_K$  inséparable.
4. Totalement ramifié :  $[L : K] = e$  et  $\tilde{\mathcal{O}}_K = \mathcal{O}_L$ . (On a la condition de finitude)

Attention y'a pas toujours l'égalité  $\sum e_i f_i = [L : K]$ , dans la plupart des cas qui m'intéressent si quand même.

## 0.2 Lien entre liberté dans $k_K, k_L$ et dans $L/K$

On regarde  $L = K(\alpha)$  et  $P = \mu_\alpha$  unitaire dans  $\mathcal{O}_K[X]$ . Si  $\overline{Q(\alpha)} = 0$  (liberté de  $(\alpha^i)$ ) on a  $Q(\alpha) \in \mathfrak{m}_L$  et pas dans  $\mathfrak{m}_K$ . D'où on peut pas directement comparer les libertés dans ce sens ! À l'inverse, si  $(\bar{e}_i)_i$  est libre dans  $k_L - k_K$  et qu'on a  $\sum a_i e_i = 0$  alors  $a_i \in \mathfrak{m}_L \cap \mathcal{O}_K = \mathfrak{m}_K$ . Si y sont tous non nuls  $0 < |(\sum a_i e_i)|$  on a un problème.

## 0.3 Factorisation de $\bar{P} = F^d$ et $e.f = d \deg F$

Même contexte, dans le cas complet c'est plus simple : Par Hensel  $\bar{P} = F^d$  et  $\deg(F) \mid f$  parce que  $F$  se scinde dans  $k_L$  vu que  $P$  se scinde dans  $\mathcal{O}_L$ . En particulier on peut faire descendre la racine. On déduit

$$e.f = \deg(P) = d. \deg(F)$$

d'où  $e \mid d$  et  $\deg(F) \mid f$ .

**Remarque 1.** Comme Vincent m'a fait remarquer pas d'égalité vu que par exemple si  $K[\alpha]/K$  est non ramifiée et  $\alpha$  engendre l'extension résiduelle alors  $\pi_L^d P(X/\pi_L)$  annule  $\pi_L \alpha$  mais  $F = X^d$ , donc on est dans le pire cas.

## 0.4 Polynômes d'eisenstein et extensions totalement ramifiées

(1)

Si  $P(X) = X^d + \sum a_i X^i$  avec  $v_K(a_0) = 1$  et  $v_K(a_i) \geq 1$  alors  $L = K[X]/(P(X))$  est totalement ramifiée et  $X$  est une uniformisante. Si  $\alpha$  est une racine dans  $L$  de  $P$  :

Y'a deux points,  $B = \mathcal{O}_K[\alpha]$  a un seul idéal maximal car  $a_0$  et  $\alpha$  sont dans le même idéal maximal et y contiennent tous  $a_0$  (!) puis  $(a_0, \alpha) = \alpha B$  est maximal (via le quotient!). Ça prouve que  $B$  est local et principal donc un DVR, i.e.  $\tilde{\mathcal{O}}_K = B$ . Pour la valuation  $e = d = [L : K]$  directement, d'où le résultat.

(2)

Si  $L/K$  est totalement ramifiée, alors  $\pi_L$  est annulé par un Eisenstein. L'idée c'est que si  $P$  l'annule, alors si  $a_{i_0} \notin \mathfrak{m}_K$  alors :

$$\pi_L^{i_0}(a_{i_0}/\pi_L^{i_0} + \sum_{i=i_0}^n a_i \pi_L^{i-i_0})$$

est de valuation  $i_0$ . Si  $v_K(a_j) > 0$  pour  $j < i_0$  alors la valuation est strictement plus grande que  $e = v_L(\pi_K)$ . Sauf que

$$\sum_{i=0}^{i_0-1} a_i \pi_L^i = \pi_L^{i_0}(a_{i_0}/\pi_L^{i_0} + \sum_{i=i_0}^n a_i \pi_L^{i-i_0})$$

d'où c'est eisenstein. En plus

$$a_0/\pi_L^n = -1 + \sum a_i \pi_L^i / \pi_L^n$$

d'où  $v_L(a_0/\pi_L^n) = 0$  vu que  $v_L(a_i) \geq e$  et  $n = e$ .

#### *0.4 Polynômes d'eisenstein et extensions totalement ramifiées*

# Chapitre 1

## Cas complet

### 1.1 Extension totalement modérément ramifiée

Cette fois on peut trouver  $\pi_L$  et  $\pi_K$  tels que  $P(X) = X^e - \pi_K$ . Déjà

$$\mathcal{O}_K/\mathfrak{m}_K \rightarrow \mathcal{O}_L/\mathfrak{m}_L$$

est un iso et donc si  $u\pi_L^e = \pi_K$ , on regarde  $u = v$  dans  $k_L$  (car c'est là que  $u$  vit) avec  $v \in \mathcal{O}_K$ . D'où  $u = v + \epsilon$ ,  $\epsilon \in \mathfrak{m}_L$  (car c'est dans  $k_L$  l'égalité). Ensuite  $u = v(1 + v^{-1}\epsilon)$ . Sauf que  $1 + v^{-1}\epsilon$  a une racine  $e$ -ème par Hensel,  $\zeta$ . D'où  $(\pi_L\zeta)^e = \pi_K/v$ .

### 1.2 Trouver les extensions totalement modérément ramifiées

En gros dans  $L/K$  finie complète telle que  $k_K - k_L$  est purement inséparable (c'est juste une généralisation), On regarde presque le corps engendré par  $\pi_L^{e/e'}$ . On choisit  $e' \mid e/p_p^v(e)$ , il existe  $k_L^{p^r} \subset k_K$  alors  $ap^r + be' = 1$  et

$$\bar{u} = (\bar{u}^{p^r})^a (\bar{u}^b)^{e'} \pmod{\mathfrak{m}_L}$$

et ducoup on relève  $u = \lambda^a (\bar{u}^b)^{e'} (1 + \epsilon)$  avec  $\lambda \in \mathcal{O}_K^\times$  puis comme d'hab le truc à droite a une racine  $e'$ -ème par hensel, disons  $\zeta$ . D'où en notant  $\pi_{e'} = u^b \zeta \pi_L^{e/e'}$  c'est une racine  $e'$ -ème de  $\pi_K/\lambda^a$ . Alors

$$K(\pi_{e'})$$

est totalement ramifiée vu que **engendrée par un eisenstein**.

### 1.2.1 Unicité

C'est pas très satisfaisant.

#### Apparté

Si on regarde  $\mathcal{O}_K \rightarrow \mathcal{O}_L/\mathfrak{m}_L$  ça induit  $i: k_K \rightarrow k_L$ . En particulier dire que  $u \in k_L$  est en fait dans  $k_K$  **ça veut dire que**  $u + \mathfrak{m}_L = v + \mathfrak{m}_L$  avec  $v \in \mathcal{O}_K$ .

#### Preuve

Concrètement,  $\lambda = (\pi_1 \pi_2^{-1})^{e'} \in \mathcal{O}_K^\times$  et en regardant dans  $k_L$  ça engendrerait une sous-extension de degré premier à  $p^r$ , i.e 1. D'où  $\bar{u} = \bar{v} \in k_K$  et  $(\bar{v})^{e'}(1 + \epsilon) = \lambda$  sauf que  $(1 + \epsilon) = \lambda/(v)^{e'}$  d'où est dans  $\mathcal{O}_K$  puis  $1 + \mathfrak{m}_K$  c'est que des puissances  $e'$ -ème. On obtient que  $(\pi_1 \pi_2^{-1})^{e'} = (v')^{e'}$  avec  $v' \in \mathcal{O}_K^\times$ . En particulier comme les racines  $e'$ -ème de l'unité sont dans  $\mathcal{O}_K$   $\pi_1 = u \pi_2$  avec  $u \in \mathcal{O}_K^\times$  d'où unicité.

**Remarque 2.** En résumé, pour tout  $e' \mid e/p^{v_p(e)}$ , on a une sous-extension  $K - L_{e'} - L$ , dans le cas complet sous l'hypothèse d'extension résiduelle purement inséparable.

## 1.3 Trouver les sous-extensions non ramifiée

En dessous de  $K - L$  on regarde  $k_K - k - k_L$  avec  $k_K - k$  séparable. On a une correspondance entre  $k$  et  $K - K_k - L$  où la première est non ramifiée.

### 1.3.1 Existence

$k_K^{sep} = k_K(\bar{\theta})$ . Comme **tout se passe dans**  $k_L$  on lift un polynôme  $P \in \mathcal{O}_L[X]$  de même degré. **Par hensel**,  $\theta$  en est une racine et il est **scindé séparable** dans  $L$ . On regarde  $K(\theta)$ , c'est séparable vu que  $\bar{P}$  est séparable **via la dérivée** mod  $\mathfrak{m}_L$  (!). Et c'est non ramifié vu que  $f = \deg(\bar{P}) = \deg(P) = [K(\theta) : K]$ .

### 1.3.2 Unicité

Donc le détail encore c'est qu'on plonge  $k$  dans  $k_L$ . I.e. on peut faire Hensel QUE dans  $\mathcal{O}_L[X]$  en gros (c'est presque pas un abus). Donc dire qu'on a un sous-corps  $F'$  de  $L$  ou on lift  $\bar{\theta}$  en  $\alpha$ . En fait  $\alpha = \theta$  par unicité dans  $L$ . Parce que par définition le sous-corps  $k$  est considéré dans  $k_L$ . D'où dans  $\mathcal{O}_L$ .

**Remarque 3.** Le seul détail là c'est  $k^{sep} \subset k_L$  par déf.

*Cas complet*

### 1.3.3 Extension non ramifiée maximale

On prend  $k = k_K^{sep}$  et un générateur  $\bar{\theta}$  fournit  $K(\theta) =: K^{un}$  puis pour n'importe quelle sous-extension non ramifiée de  $L, F$ , on applique la partie d'avant dans  $K^{un}/K$  à  $k_F$  pour obtenir  $F' \subset K^{un}$ , sauf que  $k_F = k_{F'}$  dans  $k_L$  d'où  $F = F'$ .

## 1.4 Extensions modérément ramifiée maximale

On prend  $K^{tam}$  qui correspond à  $e/p_p^v(e)$  dans  $L - K^{un}$ . Pour prouver que c'est maximal on prend une extension modérément ramifiée  $L - F - K$ , on peut considérer  $F - F^{un} - L$ . Et on a  $k_{F^{un}} = k_K^{sep}$ , ducoup on remplace  $F$  par  $F^{un}$ . Et on a  $K^{un} \subset F^{un}$  en regardant dans  $F^{un} - K$  puis  $L - K$ . Ensuite,  $K^{un} - F^{un}$  est totalement modérément ramifiée, d'où par construction dans l'autre section  $F^{un} \subset K^{tam}$ .

**Remarque 4.**  $K - F - F^{un}$  est modérément ramifiée! Et  $k_{F^{un}} - k_F - k_K$  est séparable car les deux intermédiaires sont séparable.

## 1.5 Résumé

On a un premier découpage

$$K \rightarrow K^{un} \rightarrow K^{tam} \rightarrow L$$

dans le cas complet et  $L/K$  finie. On peut aussi facilement regarder les extensions intermédiaires des deux premières sous-extensions.

## *1.5 Résumé*



# Chapitre 2

## Cas galoisien

### 2.1 Un peu de théorie de Galois

Peut-être la chose la plus importante. Quand on a une extension normale finie  $L/K$ , on a

$$\text{Aut}(L/K) = \text{Gal}(K^{\text{sep}}/K)$$

Étant donné  $K - L^H = F - L$  galoisienne,  $F/K$  est galoisienne si et seulement si  $H \leq G := \text{Gal}(L/K)$  est distingué. Ou  $F$  est stable par l'action de  $\text{Gal}(L/K)$ .

### 2.2 Groupe de décomposition et groupe de Galois résiduel

Étant donné  $L/K$  finie galoisienne, et  $\mathfrak{m}$  un idéal max. On regarde  $D = D_{\mathfrak{m}}$  et  $I = I_{\mathfrak{m}}$ . Avec pour rappel

$$D_{\mathfrak{m}} = \{\sigma \in \text{Gal}(L/K) \mid \sigma(\mathfrak{m}) = \mathfrak{m}\}$$

et  $I_{\mathfrak{m}} = \ker(D_{\mathfrak{m}} \rightarrow \text{Aut}(k_L/k_K)) = \text{Gal}(k_K^{\text{sep}}/k_K)$ .

#### 2.2.1 $1 \rightarrow I_{\mathfrak{m}} \rightarrow D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}}) \rightarrow 1$ et $k - k_{\mathfrak{m}}$ est normale

L'idée c'est de voir que dans  $\mathcal{O}_K[X]$  on a  $P(X) = \prod (X - \sigma(x))$  et si  $\bar{x} \in k_{\mathfrak{m}}$  de pol min  $p(X)$  alors  $\bar{P}(\bar{x}) = \overline{P(x)} = 0$  d'où

$$p \mid \bar{P}$$

et le deuxième est scindé dans  $L$  donc dans  $k_{\mathfrak{m}}$ . Ensuite faut montrer que  $D_{\mathfrak{m}} \rightarrow \text{Aut}_k(k_{\mathfrak{m}}) = \text{Gal}(k_{\mathfrak{m}}^s/k)$  est surjectif. L'idée c'est de lift un générateur

$$k(\bar{\theta}) = k_{\mathfrak{m}}^s$$

alors si  $\tau \in \text{Gal}(k_{\mathfrak{m}}^s/k)$  on peut trouver  $\sigma \in G$  tel que  $\overline{\sigma(\theta)} = \tau(\bar{\theta})$  parce que  $p \mid P!!!$  Ensuite faut juste lift  $\theta$  intelligemment pour que  $\sigma \in D_{\mathfrak{m}}$ . On lift de

$$\ker(\prod \tilde{\mathcal{O}}_K/\mathfrak{m}' \rightarrow \tilde{\mathcal{O}}_K/\mathfrak{m})$$

i.e.  $\theta \in \prod_{\mathfrak{m} \neq \mathfrak{m}'} \mathfrak{m}' - \mathfrak{m}$  alors  $\sigma^{-1}\mathfrak{m} = \mathfrak{m}'$  force  $\sigma(\theta) \in \mathfrak{m}$  d'où

$$\tau(\bar{\theta}) = 0$$

puis  $k_{\mathfrak{m}}^s = k$ . Suffit d'exclure ce cas (où le résultat est clair).

## 2.3 Résumé bref

**Remarque 5.** On a des nouvelles formules :  $e.f.g = [L : K]$ . ET  $|G| = |\text{Gal}(L/K)| = [L : K]$ . Faut utiliser ça exhaustivement.

Si  $L/K$  est galoisienne, pas forcément complète, on a une décomposition similaire, on fixe  $\mathfrak{m} = \mathfrak{m}_L$  et  $|\cdot|_D, |\cdot|_I$  les restriction de  $|\cdot|_{\mathfrak{m}}$  on a:

$$K - L^D - L^I - L$$

où  $D = D_{\mathfrak{m}}$  et  $I = I_{\mathfrak{m}}$ . Maintenant  $L^D - K$  est inerte en  $\mathfrak{m}$  ( $e = 1 = f$ , d'où  $\hat{K} = \hat{L}^D!$ ) et non ramifiée ( $k_{L^D} - k_K$  est séparable). La raison

- $(|G|/|D|)e_{L/K}f_{L/K} = [L : K]$  et  $|D| = e_{L/L^D}f_{L/L^D}$ .

Le dernier argument c'est qu'on a une unique extension de  $|\cdot|_D$  à  $|\cdot|_L$  vu que le groupe de galois (ici  $D$ ) agit transitivement. En plus,  $L \otimes_{L^D} \hat{L}^D$  est galoisienne sur  $\hat{L}^D$  de même groupe de galois. Maintenant

$$L^D - L^I$$

est non ramifiée,  $k_D = k_K$  et  $k_I = k_{\mathfrak{m}}^s$  la clôture séparable de  $k_K$  dans  $k_L = k_{\mathfrak{m}}$ . Et  $L^I - L$  est totalement ramifiée (elle a toute la ramification), en plus  $k_{\mathfrak{m}}^s = k_I - k_{\mathfrak{m}}$  est purement inséparable. L'argument pour les deux consiste à utiliser exhaustivement l'exactitude de

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

et le fait que  $k_L - k$  est normale dans le cas où  $L/K$  galois (ca se montre bien en liftant etc..).

## 2.4 Résumé très bref

L'extension  $K - L^D$  est immédiate car  $\#\{\mathfrak{m}|\mathfrak{m}_K\} = |G/D| = [L^D : K]$ , et  $efg = |G/D||D| = |G/D|e_D f_D$ . Maintenant  $k_L/k_I$  est purement inséparable car  $\text{Aut}(k_L/k_I) = I/I = 1$  par la suite exacte sur  $L/L^I$ . Enfin,

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

sauf que le truc de gauche c'est  $|D/I|$  par la suite exacte car  $L/K$  est galoisienne d'où  $k_L/k$  est normale et  $|\text{Gal}(k_{\mathfrak{m}}/k)| = k_{\mathfrak{m}}^s$ . Et là  $f_{\text{sep}} = [L^I : L^D]$ . En conclusion  $k_L/k_I$  contient  $f_{\text{insep}}$ ,  $L/L^I$  contient  $e$ , et  $L^I/L^D$  contient  $f_{\text{sep}}$ . Enfin, on regarde  $L^I - L$ , on peut supposer  $L^I$  complet, et  $E = (L^I)^{\text{tam}}$ . D'où la tour

$$L^I - (L^I)^{\text{tam}} - L$$

Là  $(L^I)^{\text{tam}} - L^I$  est totalement modérément ramifiée et fixée par  $I$ , d'où galoisienne de groupe de Galois  $T = I/P$  avec  $P$  le (car normal)  $p$ -sylo. Vu que  $e_{L/(L^I)^{\text{tam}}} = p^{v_p(e)}$  et  $k_L - k_{L^I}^{\text{tam}} = k_{L^I}$  est purement inséparable. Enfin,  $T$  est cyclique car  $L^I$  contient les racines  $e/p^{v_p(e)}$ -eme de l'unité. Le groupe  $T$  est donné par  $T \rightarrow \mu_{e/p^{v_p(e)}}$ . Alors on a

$$K - L^D - L^I - L^P - L$$

## 2.5 Groupes de ramification

On se place dans le cas complet, alors  $G = D$ . On regarde les

$$G_i = \ker(\text{Gal}(L/K) \rightarrow \mathcal{O}_L/\mathfrak{m}_L^{i+1})$$

qu'on peut traduire en  $v_L(\sigma(x) - x) \geq i+1$  pour tout  $x \in \mathcal{O}_L$ . Si  $\mathcal{O}_L = \mathcal{O}_K[\alpha]$  on peut juste regarder sur  $\alpha$ . On déf

$$i_G(\sigma) := v_L(\sigma(\alpha) - \alpha)$$

**Remarque 6.** On pourrait probablement le définir comme un min sinon. On a aussi  $I = G_0$  et  $P = G_1$  (c'est pas trivial le deuxième).

### 2.5.1 Quotients des groupes de ramifications

On regarde les  $G_i/G_{i+1}$ , le cas  $i = -1$  c'est  $D/I = \text{Gal}(k_L/k)$  donc on le saute. Le cas  $i = 0$  est un peu différent. On note  $U^{(i)} = \ker(\mathcal{O}_L^\times \rightarrow (\mathcal{O}_L/\mathfrak{m}_L^i)^\times)$ . On a  $U^{(i)} = 1 + \mathfrak{m}_L^i$  pour  $i > 0$  et  $U^{(0)} = \mathcal{O}_L^\times$ . On a (!)

$$\begin{cases} U^{(i)}/U^{(i+1)} \simeq k, & i \neq 0 \\ U^{(0)}/U^{(1)} \simeq k^\times, & i = 0 \end{cases}$$

## 2.5 Groupes de ramification

le premier donné par  $1 + \pi_L^i x \mapsto x$  le deuxième par  $x \mapsto x$  (oui ça marche). Pour le premier, la multiplicativité modulo  $U^{(i+1)}$  on écrit  $y = 1 + \pi_L^i(x_1 + x_2) + \pi_L^{2i}(x_1 x_2)$  et  $x^{-1} = (1 + \pi_L^{2i}(x_1 x_2)) \in U^{(2i)}$ . Alors  $x^{-1}y = 1 + \pi_L^i(x^{-1}(x_1 + x_2)) \mapsto x^{-1}(x_1 + x_2) = x_2 + x_2 \pmod{\mathfrak{m}_L}$  car  $x^{-1} \in 1 + \mathfrak{m}_L$ . L'isomorphisme est une question de cardinalité. Maintenant on a

$$G_i/G_{i+1} \rightarrow U^{(i)}/U^{(i+1)}$$

donné par  $\sigma \mapsto \sigma(\pi_L)/\pi_L$ . En particulier,  $G_i/G_{i+1}$  est cyclique pour tout  $i \geq 0$ . Et dès que  $i > 0$  c'est un  $p$ -groupe!

**Remarque 7.**  $\sigma \mapsto \sigma(\pi_L)/\pi_L$  c'est l'ami de toujours, c'est un super morphisme de groupes injectifs. Injectif c'est facile mais morphisme de groupe c'est pas évident.

Plusieurs idées dans cette partie : L'idée c'est que  $\sigma(x) - x \in \mathfrak{m}_L^{i+1}$  se traduit en  $\sigma(x)/x - 1 \in \mathfrak{m}_L^{i+1}/x$ . Ducoup avec  $x = \pi_L$ ,

$$\sigma(\pi_L)/\pi_L \in 1 + \mathfrak{m}_L^i = U^{(i)}$$

et avec  $x = u \in U^{(i)}$  (!)

$$\sigma(u)/u \in 1 + \mathfrak{m}_L^{i+1} = U^{(i+1)}$$

trop cool. Ducoup en notant  $\sigma(\pi_L) = \pi_L u$  avec  $u \in U^{(i)}$  on a

$$\sigma_1(\sigma(\pi_L))/\pi_L = \sigma_1(\pi_L)\sigma_1(u)/\pi_L$$

et  $\sigma_1(u) = (\sigma_2(\pi_L)/\pi_L)\sigma_1(u)/u$ . Ducoup modulo  $U^{(i+1)}$  c'est un morphisme de groupe (!).

**Remarque 8.** Pour rappel, on se restreint bien à  $i \geq 0$ . Quand  $i = -1$   $\sigma \mapsto \sigma(\pi_L)/\pi_L$  est pas à valeur dans  $U^{(i)}$ , y'a pas de  $U^{(-1)}$ .