Théorie de Galois et revêtements

Table des matières

Quelques notes et notes de lecture sur le Douady!

0.1 Clôture algébrique

C'est sombre mdr dans le Douady. Y'a une construction explicite dans le pdf de Benois par induction sur des gros anneaux de polynomes. En gros prendre $K[X_f]$

0.2 Bases normales

Représentations régulière isomorphe à représentation de $Gal(L/K)$ naturelle, i.e. dans $GL(L)$. Théorème de Krull-Schmidt sur les modules indécomposables.

Chapitre 1

Théorie de Galois

Y'a plusieurs points où j'suis pas au clair. Le nombre de plongements et la séparabilité. Les extensions successives et la séparabilité/normalité.

1.1 Plongements et séparabilité

Pour les problèmes de compatibilité juste toujours considérer les morphismes induits de $s\colon \varphi\colon K \to L$ à

$$K[X] \to L[X]$$

$P \in K[X]$ a une racine dans E veut dire $s(P)$ a une racine dans E. Toute les notions sont alors relatives au surcorps. Ou à isomorphisme près (pas unique (!)).

1.1.1 Cas monogène

Étant donné $F \to \Omega$ on a $|\mathrm{Hom}_F(F(\alpha), \Omega)| = \{\text{racines de } \mu_{\alpha,F}\}$ Via $F[X] \to \Omega$, $X \mapsto \ \{racines\}$, et on passe au quotient.

Remarque 1. *C'est là qu'on utilise P irréductible. Ca explique que si on regarde $\hat{L}/\hat{K}$ via $L = K[\alpha]$ et $P = \mu_\alpha$ sur K alors le nombre de plongements qui étendent K, $\hat{L} \to (\hat{K})^c$ est pas $[L : K]$, y faut un générateur.*

1.1.2 Subtilité, p.q. pas un polynôme pas irréd

Si f est pas irréductible, ça fait pas sens de regarder le corps engendré par une racine de f. Puisque les corps de facteurs différents ont pas de liens ! $F[X] \to E$ passe au même quotient en le même corps pour des racines distinctes du même pol irred!

1.1.3 Corps de rupture/décomposition

Y'a pas de subtilité c'est des corps de ruptures à la chaîne.

1.1.4 Nombre de morphismes d'une extension algébrique finie vers une extension

On écrit $E = F(\alpha_1, \ldots, \alpha_k)$ et f le produit des polynômes minimaux sur F, étant donné Ω/F on cherche le nombre de plongement $E \to \Omega$. Pour simplifier on peut supposer que f split dans Ω.

On trouve un premier plongement $\varphi_1 \colon F[\alpha_1] \to \Omega$, puis le polynôme minimal de α_2 sur $\varphi_1(F[\alpha_1])$ divise $\varphi_1(f)$ donc split dans Ω. Maintenant faut juste utiliser le cas monogène des prolongements entre :

$$F[\alpha_1, \alpha_2] \to \varphi_1(F[\alpha_1])[\beta_2]$$

avec β_2 une racine du pol min de α_2 dans $\varphi_1(F[\alpha_1])[X]$.

À chaque étape, en notant $F_i = F[\alpha_1, \ldots, \alpha_i]$, on obtient $\leq [F_{i+1} : F_i]$ nouveaux morphismes. Comme on construit le nouveau en fonction du précédent on prend le produit $\leq \prod [F_{i+1} : F_i] = [E : F]$. L'égalité dépend à chaque étape du nombre de racines distinctes de $\varphi_i(\mu_{\alpha_{i+1}, F_i}(X))$ dans Ω.

Remarque 2. *Donc "l'extension" est cachée dans le morphisme $F_i[X] \to \varphi_i(F_i)[X]$. À droite on quotient par la racine et à gauche aussi.*

1.1.5 En résumé

Le cadre type c'est $F \to E = F[\alpha_1, \ldots, \alpha_k]$ et $F \to \Omega$. On cherche à comprendre $\mathrm{Hom}(E, \Omega)$ en fonction des polynômes minimaux des α_i dans F.

La construction de E peut-être et même est dûe soit à des corps de ruptures successifs soit à l'adjonction d'éléments d'un surcorps (!).

Les morphismes/corps sont construits par passage au quotient de $F[X] \to E$.

Il y'a une bijection entre les morphismes $F(\alpha) \to \Omega$ et les racines de $\mu_{\alpha,F}$ dans Ω.

Les racines de $P \in F[X]$ dans un corps L étant donné $F \to L$ veut dire étant donné le morphisme $F[X] \to L[X]$. Et c'est ce même morphisme qui cache "l'extension" de $F \to L$ à $F(\alpha) \to L$. Penser

$$0 \to (\mu_{\alpha,F}) \to F[X] \to L[X]/(X - \beta) = L \to 0$$

pour chaque racine β.

1.2 F-automorphismes et séparabilité

En combinant tout le reste. Dans Ω si on prends E un corps de décomposition de $f \in F[X]$ séparable on a $Aut_F(E) = [E : F]$.

Question : C'est si clair ? Lien dimension du splitting field et nombre de racines ?
En fait c'est bien $[E : F]$ le nombre de plongements même en prenant un polynôme de degré $[F(\alpha_1) : F]$ le point c'est vraiment que $\mu_{\alpha_1}/(X - \alpha_1)$ reste irréductible donc on peut itérer.

Remarque 3. *Y'a un petit détail à éclaircir, pourquoi c'est bien multiplicatif à chaque étape le nombre de plongements ? C'est vraiment qu'on choisit d'envoyer α_i sur un élément spécifique à chaque étape. Ça définit uniquement le morphisme.*

1.3 Extension normales, séparables, galoisiennes.

Donc E/F est galoisienne si elle est finie séparable et normale. Y'a le théorème d'Artin qui dit que pour tout $G \subset Aut(E)$ fini

$$[E : E^G] \leq |G|$$

d'où $Aut(E/E^G) = G$ car $G \subset Aut(E/E^G)$. Et $Aut(|E/E^G)|) \leq [E : E^G]$.

1.3.1 Corps de décomposition et galois

Toute extension galoisienne E/F finie est donnée par le corps de décomposition de $f \in F[X]$ séparable et E/F. On peut écrire $E = F[\alpha_1, \ldots, \alpha_k]$ et f le produit des polynômes minimaux. Comme E/F est normale, f split, et comme les f_i sont séparables, f aussi.

À l'inverse E/E^G est galoisienne pour tout $G \subset Aut(E)$. D'abord séparable, on peut regarder f le polynôme minimal de $\alpha \in E$, on a $f = \prod(X - g\alpha) \in F[X]$ en prenant juste l'orbite (!) et celui de droite est séparable et split. La double divisibilité faut aussi voir que $f(g\alpha) = 0$ pour tout g.

1.3.2 Théorème d'Artin

L'extension E/E^G est galoisienne de groupe de galois G et $[E : F] = |G|$. Le fait que c'est galoisien c'est la sous section d'avant, le groupe de galois c'est le lemme d'Artin, et la dimension c'est le nombre de plongements vu que c'est séparable.

1.3.3 Clôture galoisienne et transitivité

Quand on a une extension séparable on peut split tout les polynômes minimaux, c'est galoisien via avant.

En plus si $E/M/F$ et E/F est galoisienne, E/M aussi via $F[X] \subset M[X]$ est les corps de décompositions nécessitent pas de polynômes irréductibles.

1.3.4 Résumé

Le lemme d'Artin dit que $[E : E^G] = |G|$, elle est galoisienne en construisant des polynômes irréductibles via $\prod(X - g\alpha)$. On peut en faire un corps de décomposition en splittant les pols mins des générateurs de $E = E^G(\alpha_1, \ldots, \alpha_k)$ via les orbites.

Inversement $F = E^{Aut(E/F)}$, et la propriété galoisienne découle directement.

Donc pour résumer quand on a E/F finie, on peut écrire $E = F[\alpha_1, \ldots, \alpha_k]$. Si on a suffisamment d'automorphismes, on peut split les polynômes minimaux et en faire une extension normale (orbites suffisamment grande) ET séparable (automorphismes distincts). Sinon on peut passer au corps de décomposition.

Penser à $Aut(E/F)$ comme $\mathrm{Hom}_F(E, E)$ pour compter les automorphismes comme des plongements.

1.4 Correspondance de Galois

Comme $Gal(E/E^G) = G$ la correspondance est bien bijective. Via le théorème d'Artin, $[E : E^G] = (G : 1)$ d'où

$$[E : E^{H_1}][E^{H_1} : E^{H_2}] = [E : E^{H_2}] = (H_1 : 1)(H_1 : H_2) = (H_2 : 1)$$

enfin les sous-corps isomorphes de E ont des groupes de Galois conjugués d'où un corps correspondant à un sous-groupe distingué est invariant par G d'où $g \mapsto g|_{E^H}$ est bien défini de noyau H.

1.4.1 Remarques

Le foncteur est contravariant pour l'inclusion, d'où le compositum correspond à l'intersection (!). Si $N = \cap gHg^{-1}$ est le plus petit sous-groupe normal de H dans G, alors E^N est la clôture galoisienne de E^H/E^G.

1.5 Résumé général

Étant donné E/F finie, on a toujours $E = F[\alpha_1, \ldots, \alpha_k]$. On a aussi $F[X] \to E[X]$.