(en effet, soit c un PPCM des dénominateurs de Q et soit $R = PQ$. Alors $cQ \in A[T]$ est primitif. Donc $(cQ)P = cR$ est primitif. Donc c est inversible dans A).

Dém. du thm de Lüroth : On peut supposer $K \subsetneq L$. Alors il existe un $v \in L \setminus K$. Par le lemme 1, X est algébrique sur $K(v)$, donc aussi sur $L \supseteq K(v)$. Soit

$$\Phi(T) = T^n + a_1 T^{n-1} + \dots + a_n \in L[T]$$

le polynôme minimal de X sur L. Soit $i \in \{1, \dots, n\}$ tel que $a_i \in L \setminus K$ (il existe i car X n'est pas alg. sur K). On va montrer que $L = K(a_i)$. Ecrivons

$$\Phi(T) = \frac{1}{A_0(X)} \underbrace{\left(A_0(X) T^n + A_1(X) T^{n-1} + \dots + A_n(X) \right)}_{=: P(X,T)},$$

où $A_0(X)$ est un PPCM des dénominateurs des $a_i \in K(X)$. Soit $m = \deg_X(P(X,T))$. On a $a_i = A_i(X)/A_0(X)$ et donc $\delta(a_i) \leq \max(\deg A_i, \deg A_0) \leq m$. On va montrer que

$$m = n \quad (= \deg_T P(X,T) = [K(X) : L])$$

Comme $[K(X) : L] = n$ et $[K(X) : K(a_i)] = \delta(a_i)$, cela entraînera $L \subseteq K(a_i)$ et donc $L = K(a_i)$. Le polynôme

$$A_i(T) - a_i A_0(T) \in L[T]$$

admet X pour racine. Donc il est multiple de Φ : il existe $H(T) \in L[T]$ t.q. $A_i(T) - a_i A_0(T) = \Phi \cdot H$. $\quad // \cdot A_0(X)$

Donc on a

$$\underbrace{A_1(T)A_0(X) - A_1(X)A_0(T)}_{=: D(X,T) \in A[X,T]} = P(X,T)\,H(T) \qquad (*)$$

dans $L[T] \subseteq K(X)[T]$. Comme $P(X,T)$ est primitif en T, on a $H(T) \in A[X,T]$ (d'après le rappel). Dans $(*)$, le degré en X est $\leq m$ à gauche et $\geq m$ à droite. Donc il est égal à m des deux côtés et $H(T) \in K[T]$. Nous avons

$$P(X,T)\,H(T) = D(X,T) = -D(T,X) = -P(T,X)\,H(X).$$

Comme $P(X,T)$ et $H(T)$ sont primitifs en X, il s'ensuit que H est une constante inversible. Comme les degrés en X et T de $D(X,T)$ sont égaux, cela vaut aussi pour $P(X,T)$ et on a donc $n = m$ comme promis. ✓

Exemple : $L = \{f \in K(X) \mid f(X) = f(1/X)\}$

$P(T) = (T-X)(T-1/X) = T^2 - (X+1/X)T + 1$

est le polynôme minimal de X sur L (car $[K(X):L] \geq 2$).

Le coeff. $a_1 = (X+1/X)$ est dans $L \setminus K$.

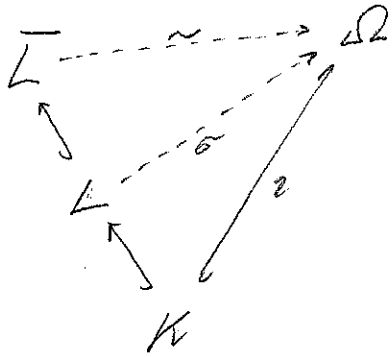
Donc $L = K(X+1/X)$, par la démonstration ci-dessus.

2. Théorie de Galois

2.1 Extensions séparables

Soient K un corps, $K \subseteq L$ une extension finie et $K \hookrightarrow \Omega$ une clôture algébrique de K. On va étudier l'extension $K \subseteq L$ au moyen de l'ensemble des K-morphismes

$$\mathrm{Hom}_K(L, \Omega) = \{\sigma : L \to \Omega \mid \sigma \text{ morph. de } K\text{-algèbres}\}$$



Rque : Cet ensemble est non vide : si $L \subset \bar{L}$ est une clôture algébrique, $\bar{L}$ est aussi une clôture algébrique de K et il existe un K-isomorphisme

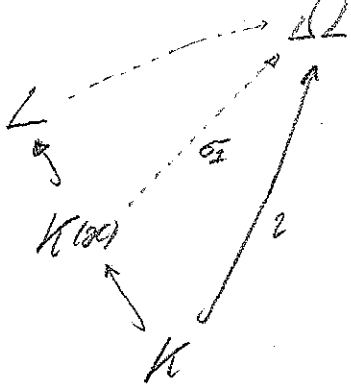
$$\bar{L} \xrightarrow{\sim} \Omega.$$

Déf : Un élément de L est séparable sur K si son polynôme minimal sur K est séparable.

Thm 1 : On a $|\mathrm{Hom}_K(L, \Omega)| \leq [L:K]$ et il y a égalité ssi tous les éléments de L sont séparables sur K.

Dém. : Récurrence sur $d = [L:K]$. Tout est clair pour $d = 1$.

Supposons $d > 1$. Soit $x \in L \setminus K$. Par le lemme 1.1.1, les K-morphismes $K(x) \xrightarrow{\sigma_i} \Omega$ sont en bijection avec les conjugués de x dans Ω, i.e. les racines du polynôme minimal P de x dans Ω. Donc on a



$$|\{i.\ K\text{-morph. } \sigma_i : K(x) \to \Omega\}| \leq \deg P = [K(x):K]$$

et il y a égalité ssi x est séparable.

Par l'hyp. de récurrence, pour tout σ_1, le nombre de $K(x)$-morphismes (= prolongements de σ_1) est borné par $[L:K(x)]$. Donc on a bien l'inégalité

$$|\mathrm{Hom}_K(L,\Omega)| \leq [K(x):K]\cdot[L:K(x)] = [L:K], \quad (*)$$

et on a l'égalité si tous les éléments de L sont séparables sur K (car alors ils le sont sur $K(x)$). Si, par contre, L contient un élément x_0 non séparable, on prend $x = x_0$ et on obtient une inégalité stricte dans $(*)$. ✓

Déf: L'extension $L \supseteq K$ est <u>séparable</u> si tous les éléments de L sont séparables sur K.

<u>Prop 2</u>: On a équivalence entre

i) $|\mathrm{Hom}_K(L,\Omega)| = [L:K]$

ii) $L \supseteq K$ est séparable.

iii) L est engendré par un nombre fini d'éléments séparables sur K.

Dém.: i) $\Rightarrow$ ii) par le thm. 1.

ii) $\Rightarrow$ iii) clair car L est fini sur K.

iii) $\Rightarrow$ i) On écrit $L = K(x_1, \dots, x_n)$ pour des éléments séparables $x_1, \dots, x_n$ et on reprend la dém. du thm 1.

Exercice ! ✓

<u>Rque</u>: Il s'ensuit que les éléments séparables forment un ss-corps de L !

Thm 3 (existence d'un élément primitif) : Supposons que

$$L = K(x, y_1, \dots, y_n),$$

où $x \in L$ est arbitraire et $y_1, \dots, y_n \in L$ sont séparables. Alors il existe un $z \in L$ ("élément primitif") t.q. $L = K(z)$.
En particulier, si $L \supseteq K$ est séparable, L est monogène.

Dém.: Si K est fini, alors L est fini et on peut prendre pour z un générateur du groupe cyclique L^*. Supposons donc que K est infini. Par récurrence sur n, on peut supposer que $n = 1$. On cherche z sous la forme $z = x + t_0 y_1$ pour un $t_0 \in K$ à déterminer. Soient

$$P = \prod_{i=1}^{r} (X - \xi_i) \quad \text{et} \quad Q = \prod_{j=1}^{s} (X - \eta_j)$$

les polynômes minimaux de x et de y_1, où $\xi_1 = x$, $\eta_1 = y$. Notons que les η_j sont distincts 2 à 2. Donc l'équation

$$\xi_1 + t\eta_1 = \xi_i + t\eta_j$$

admet une unique solution $t \in K$ pour tous i et tous $j \neq 1$. Choisissons $t_0 \in K$ distinct de toutes ces solutions (K est infini !) et posons $z = \xi_1 + t_0\eta_1 = x + t_0 y_1$. Par constr., on a

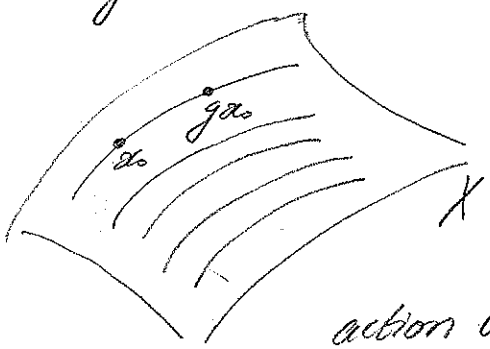
$$Q(\eta_1) = 0 \quad \text{et} \quad P(z - t_0\eta_1) = 0$$
$$\text{et } Q(\eta_j) = 0 \text{ mais } P(z - t_0\eta_j) \neq 0 \quad \text{pour } j \neq 1.$$

Donc le PGCD de $Q(X)$ et $P(z - t_0 X)$ est $X - \eta_1$. Ainsi, η_1 appartient au ss-corps de L engendré par les coeff. de Q et de $P(z - t_0 X)$. Donc $y_1 = \eta_1 \in K(z)$. Mais alors $x = z - t_0 y_1 \in K(z)$. ✓

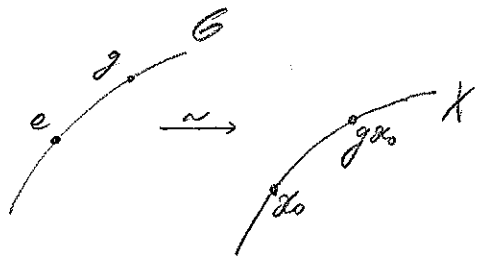
2.2 Extensions normales

Rappel : Soit G un groupe agissant sur un ensemble non vide X.
L'action est
- *libre* si $\forall g \in G, \forall x \in X : gx = x \Rightarrow g = e$
- *transitive* si $\forall x_1, x_2 \in X, \exists g \in G$ t.q. $gx_1 = x_2$.

Si l'action est libre, chacune de ses orbites est en bijection (non canonique !) avec G. Si en outre, elle est transitive, chaque *choix* de $x_0 \in X$, donne une bijection $G \xrightarrow{\sim} X, g \longmapsto gx_0$.



action libre

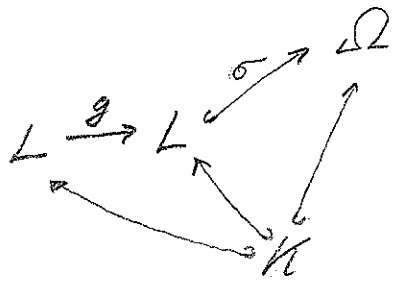


action libre et transitive
= simplement transitive.

Soient $K \subseteq L$ une extension finie et $K \hookrightarrow \Omega$ une clôture algébrique.

Rque : Le groupe $G = Gal(L/K)$ agit (à droite) sur l'ensemble non vide $X = Hom_K(L, \Omega)$ via

$$\sigma . g = \sigma \circ g.$$



Comme chaque $\sigma \in Hom_K(L, \Omega)$ est injectif, cette action est *libre* et on a

$$|Gal(L/K)| \leq |Hom_K(L, \Omega)| \quad \text{(mieux : divise !).}$$

Il y a égalité ssi l'action est transitive.

Lemme 1 : L'action de $Gal(L|K)$ sur $Hom_K(L, \Omega)$ est transitive ssi tous les K-morph. $\sigma : L \to \Omega$ ont même image.

Dém. : "$\Rightarrow$" Soient σ, σ' deux K-morphismes $L \to \Omega$. On a $\sigma' = \sigma \circ g$ pour un $g : L \xrightarrow{\sim} L$. Donc $Im\sigma = Im\sigma'$.

"$\Leftarrow$" Soient σ, σ' deux K-morph. $L \to \Omega$ qui ont même image. Comme σ et σ' sont injectifs, il existe une bijection $g : L \to L$ t.q. $\sigma' = \sigma \circ g$. On vérifie que g est dans $Gal(L|K)$. ✓

Déf : L'extension $K \subset L$ est <u>normale</u> si tout polynôme irréd. $P \in K[X]$ qui admet une racine dans L est scindé dans $L[X]$.

Exemple : L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est pas normale car $P = X^3 - 2$ y admet une racine $\sqrt[3]{2}$ mais ne se scinde pas.

Prop 2 : On a équivalence entre
- i) $K \subset L$ est normale ;
- ii) Tous les K-morph. $\sigma : L \to K$ ont même image ;
- iii) $|Gal(L|K)| = |Hom_K(L, \Omega)|$;
- iv) L est un corps de décomposition d'un polynôme de $K[X]$.

Dém. : iv) $\Rightarrow$ ii) Supposons que L est un corps de décompos. de $P \in K[X]$. Alors l'image de L par tout K-homom. $\sigma : L \to \Omega$ est engendrée sur K par les racines de P dans Ω.

ii) $\Leftrightarrow$ iii) par le lemme 1.