Déf : Le <u>discriminant</u> est l'unique polynôme $\mathrm{disc} \in \mathbb{Z}[Y_1, \dots, Y_n]$ tel que

$$\mathrm{disc}(\sigma_1, \dots, \sigma_n) = D = \prod_{1 \le i < j \le n} (X_i - X_j)^2$$

Pour un polynôme unitaire

$$P = X^n - a_1 X^{n-1} + \dots + (-1)^n a_n \in K[X],$$

on pose

$$\mathrm{disc}(P) := \mathrm{disc}(a_1, \dots, a_n).$$

Exemples : $n = 1 \Rightarrow \mathrm{disc} = 1$

$n = 2 \Rightarrow D = (X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 = \sigma_1^2 - 4\sigma_2$

$\mathrm{disc} = Y_1^2 - 4Y_2$

$n = 3 \Rightarrow D = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2$

$$\underset{\text{MAPLE}}{=} 4\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_2^3 - 27\sigma_3^2$$

$n = 4 \Rightarrow D = \prod_{1 \le i < j \le 4} (X_i - X_j)^2$

$$\underset{\text{MAPLE}}{=} 16\sigma_2^4 - 4\sigma_2^3\sigma_3^2 - 128\sigma_2^2\sigma_4^2 + 144\sigma_2\sigma_3^2\sigma_4 - 27\sigma_3^4 + 256\sigma_4^3 + \sigma_1 \cdot (\dots).$$

Rque : Si P est un polynôme unitaire et $P = \prod_{i=1}^{n} (X - \alpha_i)$ dans une extension $L \supseteq K$, alors

$$\boxed{0 \neq \mathrm{disc}(P) = \prod_{i<j} (\alpha_i - \alpha_j)^2} \iff \boxed{P \text{ séparable.}}$$

Prop. 3 : Si $P' = n \cdot \prod_{j=1}^{n-1} (X - \beta_j)$ (dans une extension assez grande),

alors $\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{j=1}^{n-1} P(\beta_j).$

Dém. : On a

$$P' = \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j) \quad \text{et} \quad P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Donc

$$(-1)^{\frac{n(n-1)}{2}} \operatorname{disc} P = \prod_{i\neq j} (\alpha_i - \alpha_j) = \prod_{i=1}^{n} \prod_{i\neq j} (\alpha_i - \alpha_j) = \prod_{i=1}^{n} P'(\alpha_i)$$

$$= \prod_{i=1}^{n} n \prod_{j=1}^{n-1} (\alpha_i - \beta_j) = n^n \prod_{j=1}^{n-1} \underbrace{\prod_{i=1}^{n} (\alpha_i - \beta_j)}_{(-1)^n P(\beta_j)}$$

$$= n^n \prod_{j=1}^{n-1} P(\beta_j) \quad (\text{car } n(n-1) \text{ est pair}).$$

✓

Lemme 4 : $\operatorname{disc}(X^3 + pX + q) = -4p^3 - 27q^2$

Rques : 1) Si car $k \neq 3$, tout polynôme unitaire P de degré 3 se ramène à cette forme par un changement de var. $X \mapsto X - a$, et $\operatorname{disc}(P(X)) = \operatorname{disc}(P(X-a))$.

2) On peut montrer que, plus généralement,
$\operatorname{disc}(X^n + aX + b) = (-1)^{n(n-1)/2} \left((1-n)^{n-1} a^n + n^n b^{n-1} \right)$.

Dém. du lemme : Le polynôme

$$D = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2 = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2$$

est homogène de degré 6. Donc on a

$$\operatorname{disc}(\sigma_1, \sigma_2, \sigma_3) = \sigma_1 \cdot A + \lambda \sigma_2^3 + \mu \sigma_3^2$$

pour un $A \in \mathbb{Z}[\sigma_1, \sigma_2, \sigma_3]$ et des $\lambda, \mu \in \mathbb{Z}$. Pour trouver λ et μ, on considère des polynômes particuliers :

- $P = X(X-1)(X+1) = X^3 - X \Rightarrow \operatorname{disc}(P) = 4 = -\lambda$
- $P = X^3 - 1 = (X-1)(X-j)(X-j^2)$, $P' = 3X^2$

$$\Rightarrow \operatorname{disc}(P) = (-1)^{\frac{3\cdot 2}{2}} \prod_{i=1}^{3} P'(\alpha_i) = -27 = \mu. \quad ✓$$

Prop. 5 : Soient $P \in K[X]$ un polynôme unitaire séparable, $L \supseteq K$ un corps de décomposition de P et

$$\varphi : Gal(L/K) \hookrightarrow \mathfrak{S}_n$$

le plongement donné par l'action de $Gal(L/K)$ sur l'ensemble des racines $\alpha_1, \dots, \alpha_n$ de P dans L. Alors

$disc(P)$ est un carré dans $K \iff Im\varphi \subseteq \mathfrak{A}_n$.

Rque : A conjugaison près, $Im\varphi$ ne dépend pas de la numérotation des racines.

Dém. : Soit $\delta \in L$ l'élément $\prod_{i<j}(\alpha_i - \alpha_j)$. Pour $g \in Gal(L/K)$ d'image $\sigma \in \mathfrak{S}_n$, on a

$$\frac{g(\delta)}{\delta} = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) \Big/ \prod_{i<j}(\alpha_i - \alpha_j) = sign(\sigma).$$

Donc
$$Im\varphi \subseteq \mathfrak{A}_n \iff \delta \in L^{Gal(L/K)} \ (= K)$$
$$\iff disc(P) \ (= \delta^2) \text{ admet une racine carrée ds } K. \quad \checkmark$$

2.8 Clôture galoisienne, extensions composées

Soient K un corps, $K \hookrightarrow \Omega$ une clôture algébrique.
On suppose que toutes les extensions considérées sont contenues dans Ω.

Rque : Pour toute partie $\mathcal{X} \subseteq \Omega$, il existe un plus petit ss-corps contenant $\mathcal{X}$, à savoir l'intersection de tous les ss-corps contenant $\mathcal{X}$.

Déf : Si L_1, L_2 sont deux extensions, l'extension composée L_1L_2 est le plus petit ss-corps de Ω contenant $L_1 \cup L_2$.

Prop. 1 : Soit $K \subseteq L \subseteq \Omega$ une extension finie et séparable.

a) Il existe une plus petite extension galoisienne $L^g \supseteq K$ telle que $L^g \supseteq L$. On l'appelle la clôture galoisienne de L.

b) Si $M \supseteq K$ est galoisienne et $M \supseteq L$, alors L^g est la composée des $\sigma(L)$, $\sigma \in Gal(M/K)$, et

$$Gal(M/L^g) = \bigcap_{\sigma \in Gal(L/K)} \sigma\, Gal(M/L)\, \sigma^{-1} \quad (*).$$

Dém. : a) Soit $x_1, \dots, x_n$ une base de L sur K. Pour $1 \leq i \leq n$, soit $P_i \in K[X]$ le polynôme minimal de x_i. Soit Q le PPCM des P_i. Alors Q est séparable et le ss-corps de Ω engendré par ses racines est L^g (!).

b) Comme $M \supseteq K$ est galoisienne et $M \supseteq L$, on a $M \supseteq L^g$. Par la correspondance de Galois, L^g doit correspondre au plus grand ss-groupe distingué contenu dans $Gal(M/L)$. D'où la formule $(*)$. Comme $\sigma\, Gal(M/L)\, \sigma^{-1}$ correspond à $\sigma(L)$, l'intersection des $\sigma\, Gal(M/L)\, \sigma^{-1}$ correspond à la composée des $\sigma(L)$. ✓

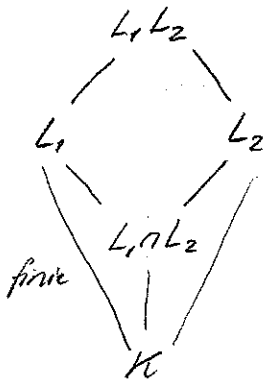
Lemme 2 : Soit A une K-algèbre intègre de dimension finie. Alors A est un corps.

Dém. : Pour $0 \neq a \in A$, l'endomorphisme linéaire $b \mapsto ab$ de A est injectif donc bijectif. De même pour $b \mapsto ba$. ✓

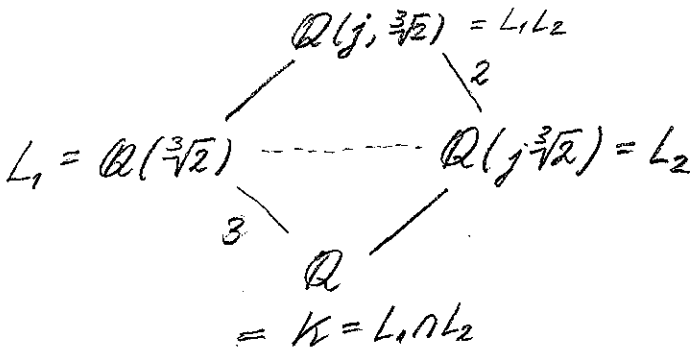
Prop. 3 : Soient $L_1 \supseteq K$ une ext. finie et $L_2 \supseteq K$ une ext. Alors $L_1 L_2 \supseteq L_2$ est finie et

$$[L_1 L_2 : L_2] \leq [L_1 : L_1 \cap L_2] \leq [L_1 : K].$$

Si on a des égalités, alors $L_1 \cap L_2 = K$.

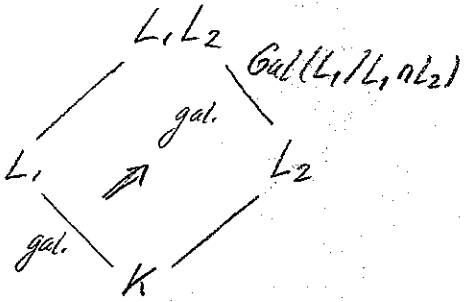


Exemple :



Dém. : La L_2-algèbre $L_2[L_1]$ est un corps (par le lemme) donc égale à $L_2 \cdot L_1$. Une partie génératrice du K-esp. vect. L_1 est aussi une partie gén. du $(L_1 \cap L_2)$-esp. vect. L_1. Et une partie gén. de L_1 sur $L_1 \cap L_2$ est une partie gén. de $L_2[L_1] = L_2L_1$ sur L_2. ✓

Thm 4 : Soient $L_1 \supseteq K$ une ext. galoisienne et $L_2 \supseteq K$ une extension finie



a) Alors $L_1L_2 \supseteq L_2$ est galoisienne et l'application de restriction
$\mathrm{Gal}(L_1L_2/L_2) \longrightarrow \mathrm{Gal}(L_1/L_1 \cap L_2)$
est un isomorphisme.

b) Si, de plus, $L_2 \supseteq K$ est galoisienne, alors $L_1L_2 \supseteq K$ et $L_1 \cap L_2 \supseteq K$ le sont aussi.

Cor. 5 : Sous les hypothèses du thm, on a

a) $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$ et

b) $[L_1L_2 : K] = [L_1 : K][L_2 : K] / [L_1 \cap L_2 : K]$

Par conséquence, on a $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ ssi $L_1 \cap L_2 = K$.

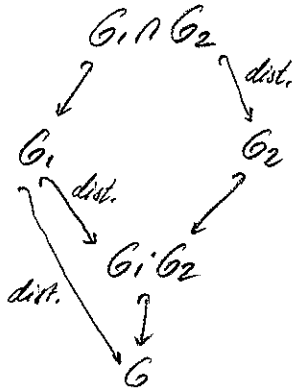
Dém. du thm : Soit $M = (L_1L_2)^g$ la clôture galoisienne. Posons $G = \mathrm{Gal}(M/K)$. Utilisons la correspondance de Galois :

$\mathrm{Gal}(M/?) : \{\text{ext. intermed. } K \subseteq E \subseteq M\} \xrightarrow{\sim} \{\text{ss-gr. de } G\}$.

Posons $G_i = Gal(M/L_i)$, $i=1,2$. Alors $Gal(M/L_1L_2) = G_1 \cap G_2$ (car L_1L_2 est la plus petite ext. intermédiaire contenant L_1 et L_2 et $G_1 \cap G_2$ le plus grand sous-groupe contenu dans G_1 et G_2) et

$$Gal(M/L_1 \cap L_2) = G_1 \cdot G_2 := \{ g_1 g_2 \mid g_1 \in G_1, g_2 \in G_2 \}$$

(puisque G_1 est distingué dans G, l'ensemble $G_1 \cdot G_2$ est bien un ss-groupe et c'est le plus petit ss-gr. contenant G_1 et G_2).
Alors les affirmations résultent des faits suivants (bien connus et faciles à vérifier):



a) G_1 dist. dans $G \Rightarrow G_1 \cap G_2$ dist. dans G_2 et

$$G_2 / G_1 \cap G_2 \xrightarrow{\sim} G_1 G_2 / G_1$$

b) G_1 et G_2 dist. dans $G \Rightarrow G_1 G_2$ et $G_1 \cap G_2$ dist. dans G.

✓

Soit un diagramme de groupes et de morphismes de groupes:

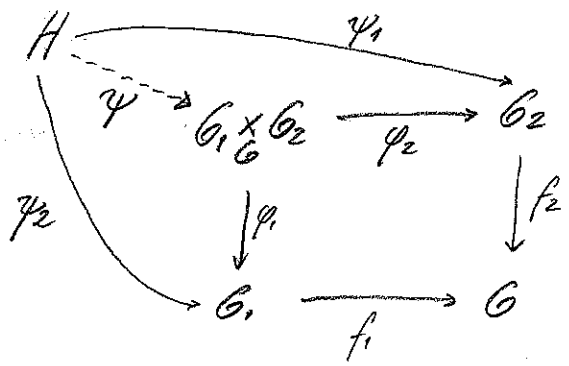
$$\begin{array}{ccc} & & G_2 \\ & & \downarrow f_2 \\ G_1 & \xrightarrow[f_1]{} & G \end{array}$$

Déf: Le produit fibré associé est le groupe

$$G_1 \underset{G}{\times} G_2 := \{ (g_1, g_2) \in G_1 \times G_2 \mid f_1(g_1) = f_2(g_2) \}$$

muni des morphismes can. $G_1 \underset{G}{\times} G_2 \xrightarrow{\varphi_i} G_i$, $(g_1, g_2) \mapsto g_i$, $i=1,2$.

Rques: 1) Cette construction jouit d'une propriété universelle:



Pour tous morph. de groupes $\psi_i : H \to G_i$, $i=1,2$, tels que $f_1 \psi_1 = f_2 \psi_2$, il existe un unique morph. de gr. $\psi : H \to G_1 \underset{G}{\times} G_2$ t.q. $\varphi_i \circ \psi = \psi_i$, $i=1,2$.