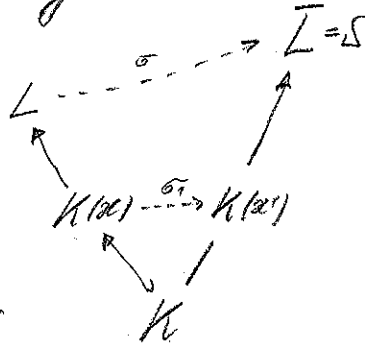
ii) ⇒ i) Soient $P \in K[X]$ irréd., $x \in L$ une racine de P et $x' \in \bar{L}$ une racine de P dans une clôture alg. $\bar{L}$ de L.

On peut supposer $\Omega = \bar{L}$. Le K-isom.

$$\sigma_1 : K(x) \xrightarrow{\sim} K(x'),\ x \longmapsto x'$$

se prolonge en un K-morph. $\sigma : L \longrightarrow \bar{L}$.



Or σ a même image que l'inclusion $L \hookrightarrow \bar{L}$.

Donc $x' \in L$.

i) ⇒ iv) Soit $x_1, \dots, x_n$ une famille génératrice pour L sur K.

Soit $P \in K[X]$ le PPCM des polynômes minimaux des x_i sur K.

Alors P se scinde sur L (car les polynômes minimaux s'y scindent) et L est engendré par les racines de P. ✓

2.3 Extensions galoisiennes

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

Résumé de 2.1 et 2.2 : On a

$$|\mathrm{Gal}(L/K)| \underset{1)}{\leq} |\mathrm{Hom}_K(L, \Omega)| \underset{2)}{\leq} [L:K].$$

On a l'égalité

- dans 1) ssi $K \subseteq L$ est normale
- dans 2) ssi $K \subseteq L$ est séparable

Donc $|\mathrm{Gal}(L/K)| = [L:K] \iff K \subseteq L$ est normale et séparable.

Déf : L'extension $K \subseteq L$ est <u>galoisienne</u> si elle est (finie et) normale et séparable.

Thm 1 : On a équivalence entre

i) $K \subseteq L$ est galoisienne ;

ii) $K \subseteq L$ est séparable et tous les K-morph. $\sigma : L \to \bar{L}$ ont même image ;

iii) L est un corps de décompos. d'un polynôme séparable à coeff. dans K.

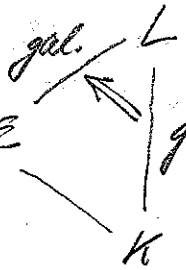
Dém. : i) $\Leftrightarrow$ ii) par déf. et par la caractérisation de la normalité (2.2.

i) $\Rightarrow$ iii) Nous avons $L = K(x_1, \dots, x_n)$ pour des $x_i \in L$ séparables (2.1.

Pour chaque i, soit $P_i \in K[X]$ le polynôme minimal de x_i. Les P_i sont scindés sur L (car $L \supseteq K$ est normale) et ont des racines simples. Soit P le PPCM des P_i. Alors P est scindé sur L, à racines simples et L est un corps de décompos. de P.

iii) $\Rightarrow$ i) $K \subseteq L$ est normale par 2.2.2 et séparable par 2.1.2 ✓

Cor. 2 : Si $L \supseteq K$ est galoisienne, alors $L \supseteq E$ est galoisienne pour toute ext. intermédiaire E.



Dém. : L est un corps de décomp. sur K d'un polynôme séparable $P \in K[X]$. Le polynôme $P \in E[X]$ est encore sép. et L en est un corps de décompos. sur E. ✓

Rque 3 : Supposons que L est un corps de décompos. d'un polynôme $P \in K[X]$. Soient $x_1, \dots, x_n$ les racines de P. Alors tout $\sigma \in \mathrm{Gal}(L/K)$ permute les x_i et l'homomorphisme

$$\mathrm{Gal}(L/K) \to \mathfrak{S}_n$$

est injectif car les racines engendrent L sur K. L'action de $\mathrm{Gal}(L/K)$ sur l'ens. des racines est fidèle. Si $L \supseteq K$ est galoisienne, on obtient $[L:K] = |\mathrm{Gal}(L/K)| \leq n!$.

Prop. 4 : Supposons $K \subset L$ galoisienne de groupe de Galois G.

a) On a $K = L^G$ $(:= \{x \in L \mid \sigma(x) = x, \forall \sigma \in G\})$

b) Pour $x \in L$, le polynôme minimal de x est $\prod_{y \in Gx} (X - y)$.

c) Pour $x \in L$, G agit transitivement sur les racines du polynôme minimal de x (= les conjugués de x).

Dém. : a) L'inclusion "$\subseteq$" est claire. Montrons "$\supseteq$". Soit $x \in L^G$ et soit $P \in K[X]$ son polynôme minimal. P se scinde dans $L[X]$ et est à racines simples. Soit x' une racine de P. Il existe $\sigma \in Gal(L/K)$ t.q. $\sigma(x) = x'$ (Corisme 1.1.2). Or $x = \sigma(x)$. Donc $x' = x$ et P est de degré 1.

b) Clairement, on a $\sigma P = P$ pour tout $\sigma \in Gal(L/K)$. Donc $P \in K[X]$ par a). Soit Q un facteur irréd. unitaire de P. L'ensemble des racines de Q est stable par $Gal(L/K)$. Donc $Q = P$. ✓

Thm 5 (Lemme d'Artin[1]) : Soient L un corps et G un ss-groupe fini du groupe des automorphismes de L. Alors l'extension $L^G \subseteq L$ est finie et galoisienne de groupe de Galois G.

Dém. : Posons $K = L^G$. Soit $x \in L$. Montrons que x est algébrique et séparable de degré $\leq |G|$ sur K. Soit $P = \prod_{y \in Gx} (X - y)$. Alors $\sigma P = P$ pour tout $\sigma \in G$. Donc P est à coeff. dans $L^G = K$. En outre P est séparable et de degré $\leq |G|$ par construction. D'où l'affirmation sur x. Soit $x \in L$ un élément de

---

[1] Emil Artin, 1898 (Vienne) – 1962 (Hambourg)

degré maximal. Je dis que $L = K(x)$. Sinon, soit $y \in L \setminus K(x)$. Comme x et y sont séparables, l'extension $K(x,y)$ de K est monogène (thm de l'élément primitif 2.1.3) et engendrée par un élément z de degré strictement plus grand que le degré de x. Contradiction. Donc L est finie et séparable de degré $\leq |G|$ sur K. On a $|G| \leq |\mathrm{Gal}(L|K)| \leq [L:K] \leq |G|$ ce qui montre que $K \subseteq L$ est galoisienne de groupe de Galois G. ✓

2.4 Correspondance de Galois[1]

Soit $K \subseteq L$ une extension galoisienne de groupe de Galois G.
Soit $\mathcal{G}$ l'ensemble des ss-groupes $H \subseteq G$.
Soit $\mathcal{E}$ l'ensemble des extensions intermédiaires $K \subseteq E \subseteq L$.
Notons que $\mathcal{G}$ et $\mathcal{E}$ sont des ensembles ordonnés (par l'inclusion) et munis d'actions naturelles de G :

$$g.H := gHg^{-1}, \quad g.E = g(E).$$

Thm 1 (Théorème fondamental) :

a) Les applications

$$\mathcal{G} \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \mathcal{E}$$
$$H \longmapsto L^H$$
$$\mathrm{Gal}(L|E) \longmapsto E$$

sont des bijections inverses l'une de l'autre.

b) Si $H_i \in \mathcal{G}$ correspond à $E_i \in \mathcal{E}$, $i = 1,2$, alors

$$H_1 \subseteq H_2 \iff E_1 \supseteq E_2. \qquad (1)$$

$$\forall g \in G: \quad H_2 = gH_1g^{-1} \iff E_2 = g(E_1) \qquad (2)$$

---

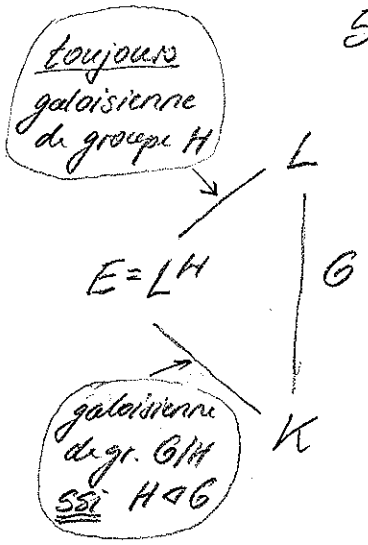
[1] Évariste Galois, 1811 (Bourg-La-Reine) – 1832 (Paris)

c) Soit $H \in \mathcal{G}$. Alors

1) L'extension $L^H \subseteq L$ est galoisienne de groupe de Galois H.

2) L'extension $K \subseteq L^H$ est galoisienne ssi H est un ss-groupe distingué et alors on a l'isom. de groupes

$$G/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K), \quad (\text{classe de } \sigma) \longmapsto \sigma|_{L^H}$$



Rque : Donc si $K \subseteq L$ est galoisienne, il n'existe qu'un nombre fini d'extensions intermédiaires $K \subseteq E \subseteq L$!

Dém. : a) Soit $E \in \mathcal{E}$. Alors $L \supseteq E$ est encore galoisienne (Cor. 2.3.2). Donc on a $E = L^{\mathrm{Gal}(L|E)}$ (Prop. 2.3.4 a)) et $\alpha\beta(E) = E$. Soit $H \in \mathcal{G}$. Alors $L^H \subseteq L$ est galoisienne de groupe H par le lemme d'Artin (thm 2.3.5). Donc on a $\beta\alpha(H) = H$.

b) Comme α et β renversent les inclusions et sont des bijections inverses l'une de l'autre, on a (1). Pour (2), notons que

$$L^{H_2} = L^{gH_1g^{-1}} = g(L^{H_1})$$

ce qui montre que α respecte l'action de G. Donc β la respecte aussi.

c) On a 1) par le lemme d'Artin (thm 2.3.5). Montrons 2). Supposons $L^H \supseteq K$ galoisienne. Alors L^H est le corps de décomp. dans L d'un polynôme sép. $P \in K[X]$. Donc, pour $g \in G$, $g(L^H)$ est le corps de décompos. de $gP = P$. Ainsi $g(L^H) = L^H$ et $gHg^{-1} = H$ par b).

Réciproquement, supposons que H est distingué dans G. Soit $P \in K[X]$ un polynôme irréductible qui a une racine x dans L^H. Alors les autres racines de P sont les éléments de l'orbite $G.x$ (prop. 2.3.4 6). Elles sont dans L^H car $L^H = g(L^H)$ pour tout $g \in G$. Donc L^H est normale. Elle est aussi séparable car contenue dans L. Donc elle est bien galoisienne. On a un morphisme de groupes bien défini

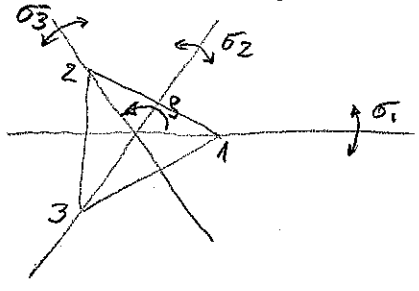
$$G \longrightarrow Gal(L^H/K),\ g \mapsto g|_{L^H}$$

et surjectif (Lemme 1.1.2). Son noyau est formé des éléments $g \in G$ t.q. $g(x) = x$, $\forall x \in L^H$. Donc ce noyau est $Gal(L/L^H) = H$. ✓

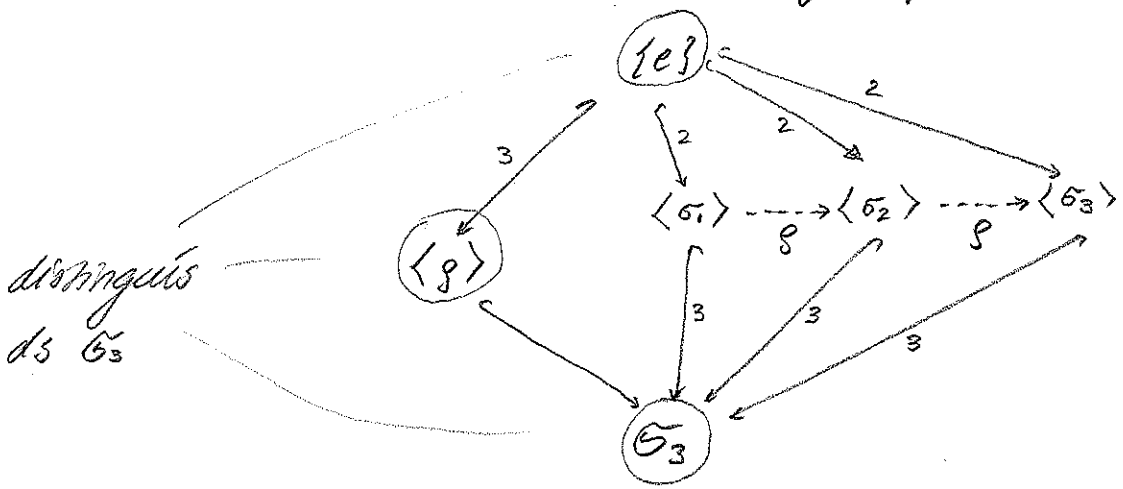
Exemple : Sur $K = \mathbb{Q}$, considérons le corps de décompos. L du polyn. $P = X^3 - 2$. Plongeons L dans $\mathbb{C}$. Nous avons $L = \mathbb{Q}(\sqrt[3]{2}, j)$, où $j = e^{2\pi i/3}$. Nous avons $[L:\mathbb{Q}] = 6$. Numérotons les racines $x_1 = \sqrt[3]{2}$, $x_2 = jx_1$, $x_3 = j^2 x_1$. Nous obtenons un morphisme de groupes injectif

$$G = Gal(L/\mathbb{Q}) \longrightarrow \mathfrak{S}_3$$

et donc bijectif car les deux groupes sont d'ordre 6. Le groupe $\mathfrak{S}_3$ s'interprète géométriquement comme le groupe des isométries d'un triangle équilatéral :



L'ensemble ordonné de ses sous-groupes est :



Dans l'isomorphisme $G \xrightarrow{\sim} \mathfrak{S}_3$, σ_1 correspond à la conjugaison complexe et s à la permutation cyclique des racines. Nous obtenons l'ens. ordonné des ss-corps :