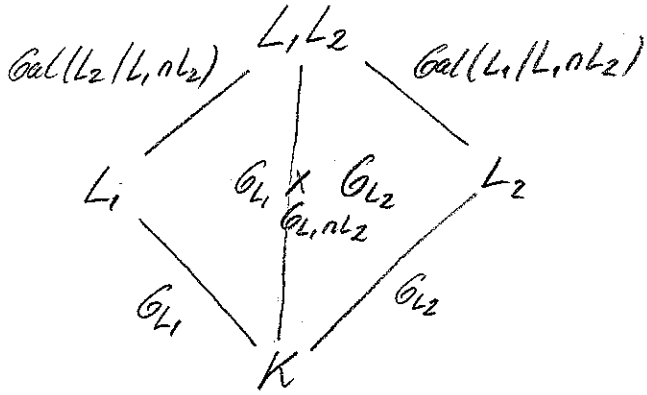
2) Pour tout $g \in G$, la fibre $(f_1\varphi_1)^{-1}(g) = (f_2\varphi_2)^{-1}(g)$ s'identifie au produit $f_1^{-1}(g) \times f_2^{-1}(g)$ (produit d'ensembles). D'où le nom.

Thm 6: Soient $L_1 \supseteq K$ et $L_2 \supseteq K$ des extensions galoisiennes. Alors $L_1L_2 \supseteq K$ et $L_1 \cap L_2 \supseteq K$ sont galoisiennes et l'on a un isom. can.
$$Gal(L_1L_2/K) \xrightarrow{\sim} Gal(L_1/K) \times_{Gal(L_1\cap L_2/K)} Gal(L_2/K)$$

Résumé graphique:



Rque : En particulier, si L_1 et L_2 sont galoisiennes et $L_1 \cap L_2 = K$, alors $Gal(L_1L_2/K) \xrightarrow{\sim} Gal(L_1/K) \times Gal(L_2/K)$.

Dém. : On utilise les notations et la méthode de la démonstration du thm 5. L'affirmation se traduit en : l'application canonique
$$\varphi : G/G_1 \cap G_2 \longrightarrow G/G_1 \times_{G/G_1G_2} G/G_2$$
est un isomorphisme. Effectivement, le noyau de la composée
$$G \longrightarrow G/G_1 \times_{G/G_1G_2} G/G_2 \hookrightarrow G/G_1 \times G/G_2$$
est bien égal à $G_1 \cap G_2$. Donc φ est injective. Supposons que $(\bar{g}, \bar{h})$ appartient au produit fibré. Alors il existe $g_1 \in G_1$ t.q. $h = gg_1g_2$. Mais alors $(\bar{g}, \bar{h})$ est l'image par φ de la classe de $hg_2^{-1} = gg_1$. Donc φ est surjective. ✓

2.9 Résolubilité par radicaux

Soit K un corps de caractéristique nulle (pour simplifier).

Déf. : Une extension finie $E \supseteq K$ est <u>radicale</u> s'il existe une tour d'extensions

$$K = E_0 \subseteq E_1 \subseteq \dots \subseteq E_n = E$$

et, pour tout $1 \leq i \leq n$, un élément $x_i \in E_i$ et un entier $d_i > 0$ tels que $E_i = E_{i-1}(x_i)$ et $x_i^{d_i} \in E_{i-1}$.

Rque : On dira que E est obtenu à partir de K "par adjonction des racines $x_1, x_2, \dots, x_n$".

Déf. : Soit $P \in K[X]$. On dira que "l'équation $P=0$ est résoluble par radicaux" (ou "P est résoluble par radicaux") si P se scinde dans une extension finie radicale.

Rque : Cela signifie que toutes les solutions de $P=0$ sont obtenues à partir d'éléments de K grâce aux opérations $+, -, \cdot, /$ et $\sqrt[d]{\ }$, $d>0$. On sait que c'est le cas si P est de degré 1, 2, 3 (del Ferro, Tartaglia, début 16e) et 4 (Ferrari, 1545)

Solution de $x^3 + mx = n$ d'après Cardan (Ars Magna, 1545) :

On a $(a-b)^3 + 3ab(a-b) = a^3 - b^3$.

Donc si $m = 3ab$ et $n = a^3 - b^3$, alors $x = a-b$ est solution.

On pose donc $b = \frac{m}{3a}$ et on obtient $n = a^3 - \frac{m^3}{27a^3}$

ou encore $a^6 - a^3 \cdot n - \frac{m^3}{27} = 0$, quadratique en a^3.

On calcule a^3, puis a et $b = \frac{m}{3a}$, puis $x = a-b$.

But : Construire des $P \in K[X]$ t.q. $P=0$ ne soit pas résoluble par radicaux.

Lemme 1 : La clôture normale d'une extension radicale (finie) de K est encore une extension radicale de K.

Dém. : Si $E \supseteq K$ et $F \supseteq K$ sont deux extensions radicales, alors $EF \supseteq K$ est encore une extension radicale. En effet, si $E \supseteq K$ est obtenue par adjonction des racines $x_1, \dots, x_n$ et $F \supseteq K$ par adjonction des racines $y_1, \dots, y_m$, alors $EF \supseteq K$ est obtenue par adjonction des racines $x_1, \dots, x_n, y_1, \dots, y_m$. Soit $E \supseteq K$ une extension finie radicale. Soit $L \supseteq E$ une clôture normale. Alors L est la composée des $\sigma(E)$, $\sigma \in Gal(L/K)$ (Prop. 2.8.1). Donc L est encore radicale (récurrence). ✓

Déf : Une extension $E \supseteq K$ est résoluble si elle est contenue dans une extension radicale (finie) $L \supseteq K$.

Thm 2 (Galois) : Soit $E \supseteq K$ une extension finie.
a) Si $E \supseteq K$ est résoluble, $Gal(E/K)$ est résoluble.
b) Si $E \supseteq K$ est galoisienne et $Gal(E/K)$ résoluble, alors $E \supseteq K$ est résoluble.

Déf (rappel) : Un groupe G est résoluble s'il existe une tour de ss-groupes

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G \qquad (*)$$

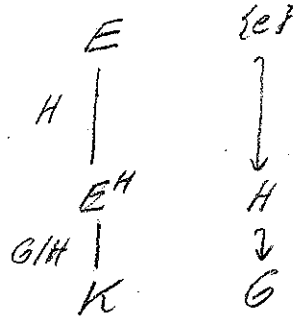
telle que G_i est distingué dans G_{i+1} et G_{i+1}/G_i abélien pour tout $0 \leq i < n$. Le groupe dérivé $DG = [G,G]$ est le ss-groupe engendré par les commutateurs $g_1 g_2 g_1^{-1} g_2^{-1}$, $g_1, g_2 \in G$.

Rques : 1) G est résoluble ssi $D^N G = \{e\}$ pour tous $N \gg 0$.

2) Si $H \subseteq G$ est un ss-groupe et G est résoluble, alors H est résoluble.
Si $H \subseteq G$ est un ss-gr. distingué, alors G résoluble $\Leftrightarrow$ H et G/H résolubles.

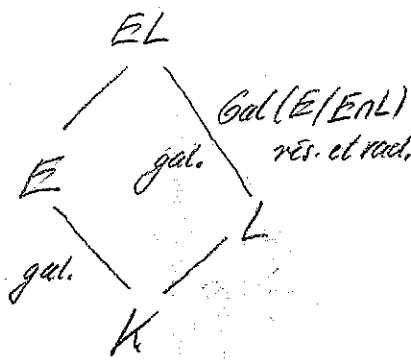
3) Un groupe fini G est résoluble ssi il existe une tour (*)
t.q. G_i est distingué dans G_{i+1} et G_{i+1}/G_i est cyclique, $0 \le i < n$.

Dém. : 6) 1er cas : K contient toutes les racines n-ièmes de l'unité,
où $n = [E : K]$.



Comme $G = Gal(E/K)$ est résoluble, il contient un ss-groupe distingué H t.q. G/H est cyclique et non trivial. Alors $E^H \supseteq K$ est galoisienne de groupe G/H et K contient toutes les racines d-ièmes de l'unité, où $d = [E^H : K] = |G/H|$, car $|G/H|$ divise $|G| = n$. Par le thm de Kummer (2.6.3), il existe $a \in K$ t.q. E^H est un corps de décomposition de $X^d - a$. Donc $E^H \supseteq K$ est radicale. L'extension $E \supseteq E^H$ est galoisienne de groupe H, qui est résoluble, et E^H contient toutes les racines $|H|$-ièmes de l'unité. Par récurrence, l'extension $E \supseteq E^H$ est radicale. Donc $E \supseteq K$ est radicale.

2e cas : cas général.
On travaille dans une clôture algébrique Ω de E.
Soit L le corps de décomps. de $X^n - 1$ dans Ω.
Comme $E \supseteq K$ est galoisienne, $EL \supseteq L$ est galoisienne et $Gal(EL/L)$ est résoluble car isomorphe au ss-groupe $Gal(E/E\cap L)$ de $Gal(E/K)$.
Le degré $[EL : L]$ divise $n = [E : K]$ donc L contient toutes les racines $[EL : L]$-ièmes de l'unité.



Par le 1er cas, l'extension $EL \geq L$ est radicale. En outre, $L \geq K$ est radicale. Donc $EL \geq K$ est radicale et $E \geq K$ est bien une extension résoluble.

a) Soit $L \geq K$ une extension radicale finie contenant E. On travaille dans une clôture alg. Ω de L. On procède par étapes :

1) Réduction au cas où $E \geq K$ est galoisienne.
Soit $K' \geq K$ le corps des points fixes de $Gal(E/K)$ dans E.
Alors $E \geq K'$ est galoisienne de groupe de Galois $Gal(E/K)$ (Lemme d'Artin) et $L \geq K'$ est encore radicale.

2) Réduction au cas où $L \geq K$ est galoisienne.
Soit L' une clôture normale de L. Alors $L' \geq K$ est encore radicale par le Lemme 1 et $L' \geq E \geq K$.

3) Réduction au cas où $L = E$.
Grâce à 1) et 2), on peut supposer que $L \geq K$ et $E \geq K$ sont galoisiennes. Alors $Gal(E/K)$ est un quotient de $Gal(L/K)$. Comme tout quotient d'un gr. résoluble est résoluble, il suffit de montrer que $Gal(L/K)$ est résoluble.

Il reste à démontrer que si $L \geq K$ est galoisienne et radicale, alors $Gal(L/K)$ est résoluble.

4) Cas où K contient toutes les racines n-ièmes de l'unité, $n = [L:K]$.
On a une tour d'extensions

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_m = L,$$

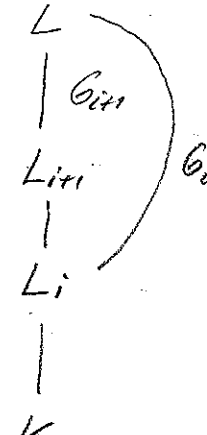
où L_{i+1} est obtenue à partir de L_i par l'adjonction d'une racine. Le degré $[L_{i+1} : L_i]$ divise n. Donc L_i contient toutes les racines $[L_{i+1} : L_i]$-ièmes de 1. ① Par la théorie des extensions cyclotomiques (Lemme 2.6.1), $L_{i+1} \geq L_i$ est galoisienne de groupe de

① Quitte à rajouter des étapes, on peut supposer que $[L_{i+1} : L_i]$ est premier et égal à d_i.

Galois cyclique. Il en résulte une tour de sous-groupes:

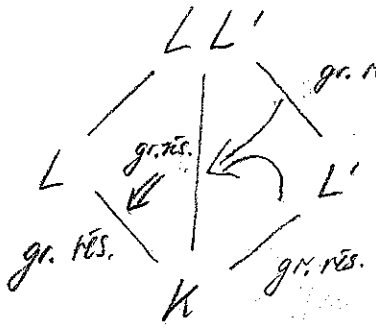
$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = e, \quad G_i = \mathrm{Gal}(L/L_i),$$

telle que G_{i+1} est distingué dans G_i et G_i/G_{i+1} est cyclique (donc abélien). Par conséquent, G est bien résoluble.



5) Cas général: $L \geq K$ galoisienne et radicale.

Soit $n = [L:K]$ et $L' \geq K$ le corps de décomposition de $X^n - 1$ dans Ω. Alors $LL' \geq K$ est galoisienne car $L \geq K$ et $L' \geq K$ le sont. Le groupe $\mathrm{Gal}(L/K)$ est quotient de $\mathrm{Gal}(LL'/K)$. Donc il suffit de montrer que $\mathrm{Gal}(LL'/K)$ est résoluble. Or son ss-groupe dist. $\mathrm{Gal}(LL'/L')$ est résoluble par 4) et le quotient par ce ss-groupe est isomorphe à $\mathrm{Gal}(L'/K)$, qui est abélien par la théorie des extensions cyclotomiques (Prop. 2.5.1). ✓



Cor. 3 (Abel,*) 1824): Pour $n \geq 5$, "l'équation générale"

$$X^n + a_1 X^{n-1} + \dots + a_n = 0$$

n'est pas résoluble par radicaux, i.e. le polynôme

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

n'est pas résoluble par radicaux.

Dém.: On sait (section 2.7), qu'on a un isomorphisme

*) Niels Henrik Abel, 1802 (Stavanger) – 1829 (Froland, Norvège)