Lemme 1 (Indépendance des caractères) *Soit G un groupe. Soit Ω un corps. Si $s_1, ..., s_n : G \to \Omega^\times$ sont des morphismes de groupes distincts. Alors $s_1, ..., s_n$ sont Ω linéairement indépendants.*

Démonstration :
On raisonne par récurrence sur $n \geq 1$. Soient $t_1, ..., t_n \in \Omega$ tels que $t_1 s_1 + ... + t_n s_n = 0$. Soit $g \in G$ tel que $s_1(g) \neq s_2(g)$. On a pour tout $x \in G$:

$$t_1 s_1(gx) + ... + t_n s_n(gx) = 0$$

$$t_1 s_1(x) + ... + t_n s_n(x) = 0 \ .$$

On retranche $s_1(g)\times$ la deuxième ligne à la première ligne ci-dessus :

$$t_2(s_2(g) - s_1(g))s_2(x) + ... + t_n(s_n(g) - s_1(g))s_n(x) = 0$$

pour tout $x \in G$. Par hypothèse de récurrence, on a :

$$t_i(s_i(g) - s_1(g)) = 0$$

pour tout i. Donc : $t_2 = 0$. On applique encore l'hypothèse de récurrence à la relation :

$$t_1 s_1 + t_3 s_3 + ... + t_n s_n = 0$$

et on trouve : $t_1 = t_2 = ... = t_n = 0$. q.e.d.

Corollaire : Si $s_1, ..., s_n : K \to \Omega$ sont des morphismes de corps distincts. Alors $s_1, ..., s_n$ sont $\Omega-$linéairement indépendants.
Démonstration : Il suffit d'appliquer le lemme aux restrictions $s_i|_{K^\times} : K^\times \to \Omega^\times$. q.e.d.

Extensions radicales

Lemme 2 *Soit L/K une extension galoisienne cyclique de degré n. On suppose que K est de caractéristique 0 ou p avec p premier à n et que K contient les racines $n-$ièmes de l'unité. Alors, il existe un $\alpha \in L$ tel que :*

i) $a := \alpha^n \in K$;

ii) $L = K(\alpha)$;

iii) *le polynôme $X^n - a$ est irréductible sur K.*

On peut noter sans ambiguïté $L = K(\sqrt[n]{a})$.
Démonstration : Soit σ un générateur du groupe $\mathrm{Gal}(L/K)$. Les automorphismes $1, \sigma, ..., \sigma^{n-1} : L \to L$ sont distincts. Donc d'après le corollaire ci-dessus, on a :

$$\mathrm{Id} + z\sigma + ... + z^{n-1}\sigma^{n-1} \neq 0$$

dans $\mathrm{End}_K(L)$ où $z \in K$ est une racine primitive $n-$ième de l'unité.
Il existe donc $x \in L$ tel que :

$$\alpha := x + z\sigma(x) + ... + z^{n-1}\sigma^{n-1}(x) \neq 0 \ .$$

Comme σ est d'ordre n, on a :

$$\sigma(\alpha) = z^{-1}\alpha \ .$$

On a donc $\sigma(\alpha^n) = \sigma(\alpha)^n = z^{-n}\alpha^n = \alpha^n$. Comme σ engendre $\mathrm{Gal}(L/K)$, $a := \alpha^n$ est fixé par $\mathrm{Gal}(L/K)$ et $\alpha^n \in K$.
De plus si $\sigma^d \in \mathrm{Gal}(L/K(\alpha)) \subseteq \mathrm{Gal}(L/K) = \langle\sigma\rangle$, on a :

$$\sigma^d(\alpha) = \alpha \Leftrightarrow z^{-d}\alpha = \alpha \Leftrightarrow n|d \Leftrightarrow \sigma^d = \mathrm{Id} \ .$$

Donc $\mathrm{Gal}(L/K(\alpha))$ est trivial et $K(\alpha) = L$. Puisque $[L : K] = n$, le polynôme $X^n - a$ est forcément irréductible sur K.

q.e.d.

Lemme 3 *Soit p un nombre premier. Si K est un corps, et si $a \in K$, alors le polynôme $X^p - a$ admet une racine dans K ou est irréductible sur K.*

Démonstration : Soit α une racine de $X^p - a$ dans une extension algébrique de K. Considérons la norme N relative à l'extension $K(\alpha)/K$. On a :

$$N(\alpha) \in K \text{ et } N(\alpha)^p = N(a) = a^d$$

où $d = [K(\alpha) : K]$. Si $X^p - a$ est réductible sur K, alors d est premier à p car $1 \leq d < p$. On en déduit à l'aide d'une relation de Bézout l'existence d'un $b \in K$ tel que $b^p = a$ *i.e.* $X^p - a$ possède une racine dans K. *q.e.d.*

On en déduit le lemme suivant :

Lemme 4 *Soit K un corps qui contient les racines primitives $p-$ièmes de l'unité, p premier, et dont la caracttéristique est différente de p. Soit $0 \neq a \in K$, si α est une racine de $X^p - a$ (dans une extension algébrique de K), alors $K(\alpha) = K$ ou $[K(\alpha) : K] = p$ et l'extension $K(\alpha)/K$ est galoisienne cyclique d'ordre p.*

Caractérisation des équations résolubles par radicaux

Soient K un corps de caractéristique nulle et Ω une clôture algébrique de K.

Définition : On dit que $z \in \Omega$ peut s'exprimer avec des radicaux sur K s'il existe une suite d'extensions de corps :

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n$$

avec : $z \in K_n$ et pour tout $1 \leq i \leq n$, il existe $\alpha_i \in K_i$, p_i un nombre premier tel que : $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{p_i} =: a_{i-1} \in K_{i-1}$ et $X^{p_i} - a_{i-1}$ est irréductible sur K_{i-1}.

Si k est un corps, on dira qu'une extension de la forme $k(\alpha)/k$ où $\alpha^p =: a \in k$ pour un nombre premier p, où $X^p - a$ est irréductible sur k et où p n'est pas la caractéristique de k est une *extension radicale irréductible*.

Par exemple les nombres $j \in \mathbb{Q}(i\sqrt{3}) \supseteq \mathbb{Q}$, $\sqrt[12]{2} \in \mathbb{Q}(\sqrt[12]{2}) \supseteq \mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$ ou $\alpha := \sqrt[4]{2}(1-i) \in \mathbb{Q}(i\sqrt{2}, \alpha) \supseteq \mathbb{Q}(i\sqrt{2}) \supseteq \mathbb{Q}$, $e^{2i\pi/5} \in \mathbb{Q}\left(i\sqrt{(5+\sqrt{5})/2}\right) \supseteq \mathbb{Q}(\sqrt{5}) \supseteq \mathbb{Q}$ peuvent s'exprimer avec des radicaux.

Théorème 1 *Soit $f(X) \in K[X]$ un polynôme irréductible. On suppose que f a une racine dans Ω qui peut s'exprimer avec des radicaux sur K. Alors, le groupe de Galois de f sur K est résoluble.*

Démonstration : Notons $x_1, ..., x_n$ les racines de f dans Ω. Soit $K = K_0 \subseteq ... \subseteq K_N$ une suite d'extensions telles que pour tout i, K_i/K_{i-1} est radicale irréductible, de degré p_i premier, et $x_1 \in K_n$. Notons m le ppcm des p_i et $K_0' := K(z)$ où z est une racine primitive $m-$ième de l'unité. Soient $\alpha_i \in K_i$ tel que $K_i = K_{i-1}(\alpha_i)$ et $\alpha_i^{p_i} \in K_{i-1}$. Notons, pour tout $i > 0$, K_i' le corps engendré par K_i, z et tous les $K-$conjugués de α_i (les images de α_i par les différents $K-$plongements de $K(\alpha_i)$ dans Ω) *.

Par récurrence, on peut montrer que tous les K_i' sont des extensions normales de K et grâce aux lemmes 2 et 4 que l'on peut passer de K_{i-1}' à K_i' par une suite d'extensions radicales irréductibles.

*. Par exemple : si $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}(i\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt[4]{2}(1-i))$. Alors on peut prendre : $\alpha_1 = i\sqrt{2}$, $\alpha_2 = \sqrt[4]{2}(1-i)$, $p_1 = p_2 = 2$. Donc $z = -1$ convient et $K_0' = \mathbb{Q}$, $K_1' = \mathbb{Q}(\pm i\sqrt{2}) = K_1$ et $K_2' = \mathbb{Q}(\alpha_2, i\alpha_2, -\alpha_2, -i\alpha_2) = \mathbb{Q}(i, \sqrt[4]{2})$ qui est une extensiion de degré 2 de K_2.

En effet, si on note par exemple $\alpha_{i,1}, ..., \alpha_{i,n_i}$ les $K-$conjugués de α_i, si on suppose que K'_{i-1}/K est normale, on a :

$$K'_i = K_i(z, \alpha_{i,1}, ..., \alpha_{i,n_i}) = K'_{i-1}(\alpha_{i,1}, ..., \alpha_{i,n_i})$$

donc K'_i/K est normale et on a de plus :

$$K'_{i-1} \subseteq K'_{i-1}(\alpha_{i,1}) \subseteq ... \subseteq K'_{i-1}(\alpha_{i,1}, ..., \alpha_{i,n_i})$$

avec des extensions successives de degré 1 ou p_i d'après le lemme 4 puisque $\alpha_i^{p_i} \in K_{i-1} \Rightarrow \alpha_i^{p_i} \in K'_{i-1} \Rightarrow \alpha_{i,j}^{p_i} \in K'_{i-1}$ pour tous les $K-$conjugués $\alpha_{i,j}$ de α_i.

On a donc une suite d'extensions :

$K \subseteq K' = K"_0 \subseteq ... \subseteq K"q = K'_N$ avec $x_1 \in K"_q$, $K"_q/K$ normale, $K"_i/K"_{i-1}$ normale de degré un nombre premier et K'/K galoisienne de groupe de Galois isomorphe à un sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^\times$, donc abélien.

On considère les sous-groupes $G_i := \mathrm{Gal}(K"_q/K"_i)$ de $G := \mathrm{Gal}(K"_q/K)$ associés :

$$1 = G_q \leq G_{q-1} \leq ... \leq G_0 \leq G \ .$$

Chaque groupe ci-dessus est distingué dans son successeur car les extensions $K"_i/K"_{i-1}$ sont normales. De plus les quotients G_{i-1}/G_i sont d'ordre premier et G/G_0 est abélien (car $\mathrm{Gal}(K'/K)$ l'est. Donc G est résoluble. Or $x_1 \in K"_q \Rightarrow x_1, ..., x_n \in K"_q$ car $K"_q/K$ est normale. Donc le groupe de Galois de f sur K est un quotient de $G = \mathrm{Gal}(K"_q/K)$. Ainsi $\mathrm{Gal}_K(f)$ est résoluble en tant que quotient d'un groupe résoluble. *q.e.d.*

Lemme 5 *Si p est premier, les racines $p-$èmes de l'unité peuvent s'exprimer avec des radicaux sur K.*

Remarque : en particulier, c'est vrai aussi sur $\mathbb{Q}$

Démonstration : Si $p = 2$, c'est évident et on raisonne par récurrence sur p.

Soit z une racine primitive $p-$ième de 1. Le groupe de Galois de $K(z)/K$ est abélien cyclique d'ordre qui divise $p-1$. Soient $p_1, ..., p_r$ les nombres premiers qui divisent $p-1$. Par hypothèse de récurrence, il existe une suite d'extensions radicales irréductibles qui commence à K et se termine à K', le corps engendré par les racines primitives p_i-ième de l'unité pour tout p_i.

Il suffit donc de montrer que z peut s'exprimer avec des radicaux sur K'. On peut donc supposer que pour tout i, K contient les racines primitipves p_i-ièmes de l'unité.

On a : $K \subseteq K(z)$. On montre facilement que l'extension $K(z)/K$ est galoisienne. Soit $G := \mathrm{Gal}(K(z)/K)$. Le groupe G est abélien d'ordre un diviseur de $p-1$. Soit une suite de sous-groupes :

$$G = G_0 > G_1 > ... > G_n = 1$$

tels que G_i est distingué dans G_{i-1} et G_{i-1}/G_i est cyclique d'ordre un nombre premier p_{ν_i}. Comme $|G| = \prod_{i=1}^n |G_{i-1}|/|G_i|$, chaque p_{ν_i} est un diviseur de $p-1$.

Considérons les corps $K_i := K(z)^{G_i}$.

On a : $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = K(z)$ et chaque extension K_i/K_{i-1} est galoisienne de groupe de Galois G_{i-1}/G_i donc est cyclique d'ordre un nombre premier p_{ν_i} qui divise $p-1$. D'après le lemme 2, chaque K_i/K_{i-1} est donc une extension radicale irréductible. Ainsi z peut s'exprimer avec des radicaux sur K. *q.e.d.*

Théorème 2 *Soit K un corps de caractéristique nulle. Soit $f(X) \in K[X]$ un polynôme irréductible. On suppose que le groupe de Galois de f sur K est*

résoluble. Alors toutes les racines de f peuvent s'exprimer avec des radicaux sur K.

Démonstration : Soient $x_1, ..., x_n$ les racines de f dans Ω une clôture algébrique de K. Soit $L = K(x_1, ..., x_n)$. On note $G := \mathrm{Gal}(L/K)$; c'est un groupe résoluble. Donc il existe des sous-groupes :

$$G = G_0 > G_1 > ... > G_N = 1$$

tels que G_i est distingué dans G_{i-1} et G_{i-1}/G_i est cyclique d'ordre premier p_i.

Soit K' une extension de K qui contient toutes les racines p_i-èmes de l'unité et qui est le dernier terme d'une suite d'extensions radicales irréductibles : $K \subseteq ... \subseteq K'$. Une telle suite existe d'après le lemme 5. Il suffit donc de montrer que $x_1, ..., x_n$ peuvent s'exprimer avec des radicaux sur K'. On peut donc supposer que K contient les racines p_i-ièmes de l'unité. On considère $K_i := L^{G_i}$.

Ona une suite d'extensions de corps :

$$K = K_0 \subseteq ... \subseteq K_n = L$$

telle que :

$$x_1, ..., x_n \in K_n$$

et K_i/K_{i-1} est une extension galoisienne de groupe de Galois (isomorphe à) G_{i-1}/G_i. en particulier, les extensions K_i/K_{i-1} sont de degré premier p_i pour tout i. D'après le lemme 2, les extensions K_i/K_{i-1} sont radicales irréductibles et on en conclut que $x_1, ..., x_n$ peuvent s'exprimer avec des radicaux sur K. *q.e.d.*