Les sous-groupes transitifs et résolubles de S_p, p premier

Soit p un nombre premier.

On note Aff_p le sous-groupe de S_p formé par les bijections affines :

$$\mathbb{F}_p \to \mathbb{F}_p,\ x \mapsto ax + b$$

$a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p$ (où l'on identifie $i \in \{1, ..., p\}$ avec $i \bmod p \in \mathbb{F}_p$).

Le sous-groupe Aff_p est le normalisateur du groupe P engendré par le $p-$cycle $(12...p)$.

De plus Aff_p est résoluble car P est distingué dans Aff_p et $\mathrm{Aff}_p/P \simeq \mathbb{F}_p^\times$ (abélien). En particulier, tous les sous-groupes de Aff_p sont résolubles.

Soit G un sous-groupe transitif résoluble de S_p. Comme G est transitif, p divise $|G|$. Donc G contient un élément d'ordre p *i.e.* un $p-$cycle. Comme les $p-$cycles sont conjugués dans S_p, il existe une permutation s telle que $(12...p) \in sGs^{-1}$. Supposons que $(12...p) \in G$.

Comme G est résoluble, il existe une suite strictement croissante de sous-groupes :

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

tels que G_{i-1} est distingué dans G_i et G_i/G_{i-1} est abélien pour tout i.

Supposons que $c := (12...p) \in G_i$ avec $i \geq 2$. Soit $t \neq 1$ dans G_{i-1}. Supposons par exemple $t(1) \neq 1$. Alors $k := t(1) - 1$ est un entier premier à p. On a $c^k(1) = t(1)$. Donc $t^{-1}c^k(1) = 1$. Par conséquent, l'ordre de $t^{-1}c^k$ dans S_p divise $(p-1)!$. A fortiori dans G_i/G_{i-1} l'ordre de $t^{-1}c^k = c^k \bmod G_{i-1}$ divise aussi $(p-1)!$. Comme k, p sont premiers entre eux, comme $c^p = 1$, On trouve que $c = 1 \bmod G_{i-1}$ *i.e.* $c \in G_{i-1}$. On en déduit par récurrence descendante que $c \in G_1$.

Montrons par récurrence ascendante que $P = \langle c \rangle$ est distingué dans G_i.

Comme G_1 est abélien, P est distingué dans G_1. Si P est distingué dans G_i, alors $G_i \leq N(P)$. D'où :

$$N(G_i) \leq NN(P)$$

(la lettre N désigne le normalisateur dans G). Or $G_{i+1} \leq G_i$ car G_i est distingué dans G_{i+1} et $NN(P) = N(P)$ car P est un $p-$Sylow. Donc $G_{i+1} \leq N(P)$.

On a donc $G \leq N_{S_p}(P) = \mathrm{Aff}_p$.

Soit $f \in \mathbb{Q}(X)$ un polynôme irréductible sur $\mathbb{Q}$ de degré p.

Si $f = 0$ est résoluble par radicaux alors le groupe de Galois G de f sur $\mathbb{Q}$ est résoluble. C'est aussi un sous-groupe transitif.

Notons $x_1, ..., x_p$ les racines de f dans $\mathbb{C}$. Le groupe G permute les x_i et s'identifie à un sous-groupe de S_p transitif et résoluble. Montrons que $\mathbb{Q}(x_1, ..., x_p) = \mathbb{Q}(x_1, x_2)$. Il suffit de montrer que $\mathrm{Gal}(\mathbb{Q}(x_1, ..., x_p)/\mathbb{Q}(x_1, x_2))$ est trivial. Soit $\sigma \in G$ qui laisse fixe x_1, x_2. Quitte à conjuguer σ, on peut supposer que σ est un élément de Aff_p qui a deux points fixes. Or la seule bijection affine qui a au moins 2 points fixes distincts est l'identité. D'où $\sigma = 1$.

Réciproquement, supposons que $\mathbb{Q}(x_1, ..., x_p) = \mathbb{Q}(x_1, x_2)$. Montrons que le groupe G est résoluble (et donc que l'équation $f = 0$ est résoluble par radicaux sur $\mathbb{Q}$).

Comme f est de degré p et comme $f/(X - x_1) \in \mathbb{Q}(x_1)[X]$ est de degré $p-1$, on a :

$$|G| = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}] = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}] \leq (p-1)p\ .$$

On en déduit que G ne contient qu'un seul $p-$Sylow (le seul entier égal à $1 \bmod p$ et inférieur à $(p-1)p$ est 1). En particulier, G contient un $p-$cycle.

Quitte à conjuguer G dans S_p, on peut supposer que $(12...p) \in G$ et donc $P = \langle (12...p) \rangle$ est l'unique $p-$Sylow de G. Comme unique $p-$Sylow, P est distingué dans G *i.e.* $G \leq N_{S_p}(P) = \mathrm{Aff}_p$. Et donc G est résoluble comme sous-groupe d'un groupe résoluble.

Le polynôme $X^p - X - a$ en caractéristique p

Soit p un nombre premier. Soit k un corps de caractéristique p. Soit $a \in k$. Le polynôme $X^p - X - a$ est irréductible sur k ou scindé sur k.

En effet, supposons que $X^p - X - a = PQ$ avec $P, Q \in k[X]$ unitaires et de degrés $1 < \deg P, \deg Q < p$. Soit β une racine de P. Les $\beta + i$, $i \in \mathbb{F}_p$ sont aussi racines de $X^p - X - a$ car :

$$(\beta + i)^p - (\beta + i) - a = \beta^p - \beta - a = 0 \ .$$

Les racines de P sont donc de la forme :

$$\beta + i_k$$

pour certains $i_k \in \mathbb{F}_p$, $1 \leq k \leq d := \deg P$.

La somme des racines de P est $\pm$ le coefficient de P de degré $d-1$.

Donc :

$$\beta + i_1 + ... + \beta + i_d = d\beta + (i_1 + ... + i_d) \in k$$
$$\Rightarrow d\beta \in k \ .$$

Or $1 < d < p$, donc $d.1$ est inversible dans k et $\beta \in k$. En particulier, $X^p - X - a = \prod_{i \in \mathbb{F}_p} (X - (\beta + i))$ est scindé sur k.

Soit K/k une extension galoisienne cyclique de degré p premier. Alors il existe $\beta \in K$ dont le polynôme minimal est $X^p - X - a$ pour un certain $a \in k$ et tel que $K = k(\beta)$.

En effet :

Soit $G := \mathrm{Gal}(K/k)$. Soit s un générateur de G. Soit $S : K \to K$, $x \mapsto x - s(x)$. Le $k-$endomorphisme S est nilpotent car dans $\mathrm{End}_k(K)$:

$$S^p = \mathrm{Id}^p - s^p = \mathrm{Id} - \mathrm{Id} = 0 \ .$$

Comme $S \neq 0$, $\ker S \neq \ker S^2$. Soit $x \in \ker S^2 \ \setminus \ \ker S$.

On pose $\beta := \frac{x}{s(x) - x}$.

On a $s(\beta) = -s(x)/s(S(x))$. Or $S^2(x) = 0 \Rightarrow S(x) = s(S(x))$. Donc $s(\beta) = -s(x)/S(x) = s(x)/(s(x) - x) = \beta + 1$.

En particulier $\beta \notin k = K^{\langle s \rangle}$. Donc $k \subsetneq k(\beta) \subseteq K$. Comme $[K : k] = p$ est premier, $k(\beta) = K$. On en déduit que le polynôme minimal de β est de degré p.

Or : $a := \beta^p - \beta \in k$. En effet, $s(\beta^p - \beta) = s(\beta)^p - s(\beta) = (\beta + 1)^p - \beta - 1 = \beta^p - \beta$. Donc $X^p - X - a \in k[X]$ est le polynôme minimal de β sur k. **Q.e.d.**