Les sous-groupes transitifs de S_5

Soit G un sous-groupe de S_5 qui agit transitivement sur $\{1,2,3,4,5\}$.

L'ensemble $\{1,2,3,4,5\}$ est une orbite de G donc $5|G$. Soit n_5 le nombre de $5-$Sylow de G. Comme $n_5 = 1 \bmod 5$ et $n_5||G|/5$, on a $n_5|24 = |S_5|/5$ et donc $n_5 = 1$ ou 6.

Si $n_5 = 6$, alors G contient 24 $5-$cycles (en effet, chaque $5-$Sylow contient 4 $5-$cycles et l'intersection de 2 $5-$Sylow distincts est réduite à l'identité).

Or, dans S_5, il y a 24 $5-$cycles. Donc G contient tous les $5-$cycles de S_5.

Dans S_5, les $5-$cycles engendrent le groupe alterné A_5 (il suffit de voir que tout $3-$cycle est un produit de $5-$cycles : par exemple : $(123) = (13254)(13452)$). Donc $G = A_5$ ou S_5.

Si $n_5 = 1$, ...

Comme les $5-$ Sylow de S_5 sont d'ordre 5 et sont conjugués dans S_5, il existe $\sigma \in S_5$ tel que $\sigma G \sigma^{-1}$ contienne le $5-$cycle (12345). Supposons que G contient (12345). Comme $n_5 = 1$, le $5-$Sylow $\langle(12345)\rangle$ est distingué dans G. Donc $G \subseteq N$ où N est le normalisateur de $\langle(12345)\rangle$ dans S_5.

Notons $\mathrm{GLA}(\mathbb{F}_5)$ le groupe des bijections affines de $\mathbb{F}_5$ de la forme :

$$s_{a,b} : x \mapsto ax + b$$

$a \in \mathbb{F}_5^\times$, $b \in \mathbb{F}_5$.

On identifie $\{1,2,3,4,5\}$ avec $\mathbb{F}_5$ (i avec $i \bmod 5$). Ainsi, on peut identifier $\mathrm{GLA}(\mathbb{F}_5)$ avec un sous-groupe de S_5.

On a par exemple : $t := s_{1,1} = (12345)$ et $s := s_{2,0} = (1243)$. Comme $\mathrm{GLA}(\mathbb{F}_5)$ est d'ordre 20, $\mathrm{GLA}(\mathbb{F}_5)$ est engendré par s et t. Comme $sts^{-1} = t^2$, on voit que $\langle(12345)\rangle$ est distingué dans $\mathrm{GLA}(\mathbb{F}_5)$ donc $\mathrm{GLA}(\mathbb{F}_5) \subseteq N$. Réciproquement, si $n \in N$, alors $n(12345)n^{-1} = (12345)^a$ pour un $a \in \mathbb{F}_5^\times$. Comme 2 engendre $\mathbb{F}_5^\times$ pour la multiplication, il existe k tel que :

$$s^k(12345)s^{-k} = (12345)^{2^k} = (12345)^a = n(12345)n^{-1} \ .$$

Mais alors, $g := n^{-1}s^k$ commute avec (12345). Donc $g \in \langle(12345)\rangle$. En effet, soit i tel que $g(1) = i$. On a $f := g^{-1}(12345)^i$ qui commute avec (12345) et $f(1) = 1$. Donc $f(12345)f^{-1} = (f(1)f(2)f(3)f(4)f(5)) = (12345) \Rightarrow f = \mathrm{Id}$. D'où $g = (12345)^i$.

On a donc $n \in s^k\langle(12345)\rangle \subseteq \mathrm{GLA}(\mathbb{F}_5)$.

Par conséquent G est un sous-groupe de $\mathrm{GLA}(\mathbb{F}_5)$ qui contient t. On vérifie facilement que les sous-groupes de $\mathrm{GLA}(F_5)$ qui contiennent t sont :

$$\langle t\rangle, \langle s^2, t\rangle, \langle s, t\rangle \ .$$

De plus, $\langle t\rangle \simeq \mathbb{Z}/5\mathbb{Z}$, $\langle s^2, t\rangle = \mathrm{GLA}(\mathbb{F}_5) \cap A_5 \simeq D_5$ le groupe diédral d'ordre 10.

Le groupe de Galois de $X^5 - 5X + 12$ sur $\mathbb{Q}$

Posons $P = x^5 - 5X + 12$. Le discriminant de P est :

$$\Delta = 2^{12}5^6$$

qui est un carré dans $\mathbb{Q}$. Donc le groupe de Galois G de P sur $\mathbb{Q}$ est un sous-groupe de A_5.

Or, $P = X(X^2 - X - 1)(X^2 + X - 1) \bmod 3$. Donc G contient une double transposition. Modulo 7, P n'a pas de racines. Et P n'est pas un produit de deux facteurs irréductibles de degrés 2 et 3 car sinon, G contiendrait le produit d'une transposition et d'un $3-$cycle, chose impossible car $G \subseteq A_5$. Donc P est irréductible $\bmod 7$ et donc G est irréductible sur $\mathbb{Q}$.

Par conséquent G est isomorphe à un sous-groupe transitif de A_5.

Il y a trois possibilités :

$G = A_5$, $g \simeq D_5$ ou $G \simeq \mathbb{Z}/5\mathbb{Z}$. Comme G contient une double transposition, G n'est pas isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Notons $r_1, ..., r_5$ les racines distinctes de P. Soit $R := \prod_{1 \leq i < j \leq 5}(X - r_i - r_j)$.

Les $r_i + r_j$ sont deux à deux distincts (*cf.* le lemme qui suit).

Les coefficients de R sont des polynômes à coefficients entiers symétriques en les r_i donc ce sont des polynômes à coefficients entiers en les coefficients de P. Donc $R \in \mathbb{Z}[X]$.

À l'aide d'un ordinateur, on peut vérifier que :

$$R = (X^5 - 5X^3 - 10X^2 + 30X - 36)(X^5 + 5X^3 + 10X^2 + 10X + 4)$$

En particulier, le groupe de Galois de R n'agit pas transitivement sur ses racines. Or, $\mathbb{Q}(r_1, ..., r_5) = \mathbb{Q}(r_i + r_j \ : \ 1 \leq i < j \leq 5)$. Donc le groupe de Galois de R est aussi celui de P. Comme l'action de A_5 sur $\{1, 2, 3, 4, 5\}$ est $2-$transitive, si $G = A_5$, alors G agirait transitivement sur les racines $r_i + r_j$ de R, *absurde !*

Donc $G \simeq D_5$.

Lemme : Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible dont le groupe de Galois sur $\mathbb{Q}$ contient un sous-groupe isomorphe à D_5. Soient $r_1, ..., r_5$ les racines de P dans $\mathbb{C}$. Alors les $r_i + r_j$, $1 \leq i < j \leq 5$ sont deux à deux distincts.

démo : On peut supposer que G, le groupe de Galois sur $\mathbb{Q}$ de P, contient $\langle (12345), (14)(23) \rangle$. Supposons par exemple que $r_1 + r_2 = r_i + r_j$ avec $1 \leq i < j \leq 5$, $(i, j) \neq (1, 2)$. Si $i = 1$ ou 2, alors $r_j = r_2$ ou $r_j = r_1$: absurde car les r_i sont deux à deux distincts. Si $i \leq 3$, alors on a :

$$r_1 + r_2 = r_3 + r_4, r_3 + r_5, \text{ ou } r_4 + r_5 \ .$$

Si $r_1 + r_2 = r_3 + r_4$, alors en appliquant successivement (12345) on trouve : $r_2 + r_3 = r_4 + r_5$ puis : $r_3 + r_4 = r_5 + r_1$. Mais alors $r_1 + r_2 = r_5 + r_1$ et $r_2 = r_5$ absurde !

Si $r_1 + r_2 = r_3 + r_5$, on trouve de même :

$$r_2 + r_3 = r_4 + r_1$$

$$r_3 + r_4 = r_5 + r_2$$

$$r_4 + r_5 = r_1 + r_3$$

$$r_5 + r_1 = r_2 + r_4 \ .$$

On a obtenu un système de 5 équations à 5 inconnues : r_i, $1 \leq i \leq 5$. Si on résout ce système, on trouve qu'il est de rang 4 et que toutes les solutions vérifient $r_1 = r_2 = r_3 = r_4 = r_5$: *absurde !.*

Enfin, si $r_1 + r_2 = r_4 + r_5$, on trouve :

$$r_2 + r_3 = r_5 + r_1$$

$$r_3 + r_4 = r_1 + r_2$$

d'où : $r_3 + r_4 = r_4 + r_5$ et $r_3 = r_5$ *absurde !*