Université Claude Bernard LYON 1
Préparation à l'agrégation de Mathématiques

Présentation du groupe symétrique $\mathfrak{S}_n$

Michel CRETIN

Proposition 1
Le groupe Γ *engendré par des générateurs* γ_i *pour* $1 \leq i \leq n-1$ *soumis aux relations :*

$$\begin{cases} \gamma_i^2 = 1 \text{ pour } 1 \leq i \leq n-1 \\ \gamma_i\gamma_j = \gamma_j\gamma_i \text{ pour } 1 \leq i,j \leq n-1 \text{ tels que } |i-j| \geq 2 \\ \gamma_i\gamma_{i+1}\gamma_i = \gamma_{i+1}\gamma_i\gamma_{i+1} \text{ pour } 1 \leq i \leq n-2 \text{ } \textit{(relations de tresses)} \end{cases}$$

est isomorphe au groupe symétrique $\mathfrak{S}_n$.

Le groupe Γ est *caractérisé* par la *propriété universelle* suivante :
pour tout groupe S et toute famille d'éléments $(s_i)_{1\leq i\leq n-1}$ vérifiant les relations

$$\begin{cases} s_i^2 = 1 \text{ pour } 1 \leq i \leq n-1 \\ s_is_j = s_js_i \text{ pour } 1 \leq i,j \leq n-1 \text{ tels que } |i-j| \geq 2 \\ s_is_{i+1}s_i = s_{i+1}s_is_{i+1} \text{ pour } 1 \leq i \leq n-2 \end{cases}$$

il existe un *unique* homomorphisme de groupes :

$$f : \Gamma \longrightarrow S$$

tel que

$$f(\gamma_i) = s_i \text{ pour tout } 1 \leq i \leq n-1$$

Le groupe symétrique $\mathfrak{S}_n$ et les transpositions simples $\tau_i = (i, i+1)$, $1 \leq i \leq n-1$, vérifient les conditions précédentes, aussi il existe un unique homomorphisme :

$$F : \Gamma \longrightarrow \mathfrak{S}_n$$

tel que

$$F(\gamma_i) = \tau_i \text{ pour tout } 1 \leq i \leq n-1$$

De plus, les transpositions simples $\tau_i = (i, i+1)$, $1 \leq i \leq n-1$, engendrant le groupe $\mathfrak{S}_n$, l'homomorphisme F est *surjectif*. En particulier on a :

$$\text{Card}(\Gamma) \geq \text{Card}(\mathfrak{S}_n)$$

Lemme 1
Pour $0 \leq i \leq n-1$ *désignons par* $\Gamma_i =< r_1, \cdots, r_i >$ *le sous-groupe de* Γ *engendré par* $r_1, \cdots, r_i$ *(*$\Gamma_0 = \{1\}$, $\Gamma_i \subset \Gamma_{i+1}$ *et* $\Gamma_{n-1} = \Gamma$*). On a :*

$$\Gamma_{i+1} = \Gamma_i \cup \Gamma_i\, r_{i+1}\, \Gamma_i \quad \text{et} \quad [\Gamma_{i+1} : \Gamma_i] \leq i+1 \text{ pour } 0 \leq i \leq n-2$$

$\triangledown$ Pour $i=0$, on a $\Gamma_0=\{1\}$ et $\Gamma_1=<r_1>\simeq C_2$ de sorte que $\Gamma_1=\Gamma_0\cup\Gamma_0\, r_1\,\Gamma_0$ et $[\Gamma_1:\Gamma_0]\leq 2$.
Par *hypothèse de récurrence* supposons que $\Gamma_i=\Gamma_{i-1}\cup\Gamma_{i-1}\, r_i\,\Gamma_{i-1}$. et montrons que pour tout $\gamma\in\Gamma_{i+1}$ on a :

$$(\Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i)\gamma\subset\Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i$$

Comme $1\in\Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i$ on aura bien $\Gamma_{i+1}\subset\Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i$.
Puisque $\Gamma_{i+1}=<\Gamma_i, r_{i+1}>$ il suffit d'établir le résultat pour $\gamma=r_{i+1}$.
On a $\Gamma_i\, r_{i+1}\subset\Gamma_i\, r_{i+1}\,\Gamma_i$ et comme chaque élément de Γ_{i-1} commute avec r_{i+1}, que r_{i+1} est d'ordre 2 et que l'on a les relations de tresses on obtient :

$$\begin{aligned}
\Gamma_i\, r_{i+1}\Gamma_i\, r_{i+1} &= \Gamma_i\, r_{i+1}(\Gamma_{i-1}\cup\Gamma_{i-1}\, r_i\,\Gamma_{i-1})\, r_{i+1}\\
&= \Gamma_i(\Gamma_{i-1}\, r_{i+1}^2\cup\Gamma_{i-1}\, r_{i+1}\, r_i\, r_{i+1}\,\Gamma_{i-1})\\
&= \Gamma_i(\Gamma_{i-1}\cup\Gamma_{i-1}\, r_i\, r_{i+1}\, r_i\,\Gamma_{i-1})\\
&\subset \Gamma_i(\Gamma_{i-1}\cup\Gamma_i\, r_{i+1}\,\Gamma_i)\\
&= \Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i
\end{aligned}$$

Supposons *par hypothèse de récurrence* que $r=[\Gamma_i:\Gamma_{i-1}]\leq i$ et considérons $\gamma_1,\cdots,\gamma_r$ un *système de représentants* des classes de G *modulo* H. Tout $\gamma\in\Gamma_i$ s'écrit alors $\gamma=\gamma'\gamma_k$ avec $\gamma'\in\Gamma_{i-1}$ de sorte que :

$$\gamma^{-1}r_{i+1}\gamma=\gamma_k^{-1}\gamma'^{-1}r_{i+1}\gamma'\gamma_k=\gamma_k^{-1}r_{i+1}\gamma_k$$

puisque r_{i+1} commute avec $r_1,\cdots,r_{i-1}$ donc avec Γ_{i-1} qui est d'indice *au plus* i dans Γ_i. Il en résulte que :

$$\mathrm{Card}(\{\gamma\, r_{i+1}\,\gamma^{-1}\,/\,\gamma\in\Gamma_i\})=\{\gamma_k^{-1}r_{i+1}\gamma_k\,/\,1\leq k\leq r\}=r\leq i$$

Pour $\gamma,\widetilde{\gamma}\in\Gamma_i$ on a alors :

$$\gamma\, r_{i+1}\widetilde{\gamma}=\gamma\,\widetilde{\gamma}\;\widetilde{\gamma}^{-1}r_{i+1}\widetilde{\gamma}\gamma\,\widetilde{\gamma}\;\gamma_k^{-1}r_{i+1}\gamma_k$$

de sorte que

$$\Gamma_{i+1}=\Gamma_i\cup\Gamma_i\, r_{i+1}\,\Gamma_i\subset\Gamma_i\cup\bigcup_{k=1}^{r}\Gamma_i\;\gamma_k^{-1}r_{i+1}\gamma_k$$

$\triangle$

Finalement le lemme montre que :

$$\mathrm{Card}(\Gamma)\leq n!=\mathrm{Card}(\mathfrak{S}_n)$$

de sorte que l'unique homomorphisme :

$$F:\Gamma\longrightarrow\mathfrak{S}_n$$

tel que

$$F(\gamma_i)=\tau_i \text{ pour tout } 1\leq i\leq n-1$$

est un isomorphisme

[1] Robert A. Wilson The finite simple groups (p31-32) Graduate texts in Mathematics 251 (Springer 2009)