FICHE 02-11 : Lemme de Cauchy : ALG1-01 2.10

Yvann Le Fay

Juillet 2019

Enoncé

1. Soit G un groupe fini de cardinal p^m avec $m \in \mathbb{N}^*$ et p premier qui opère sur un ensemble fini non vide E, on note

$$E^G = \{x \in E : \forall g \in G, gx = x\}$$

   Montrer que $|E^G| \equiv |E| \, [p]$
2. Soit H un groupe fini d'ordre n et p un diviseur premier de n. Montrer que H contient un élément d'ordre p. On introduira une opération de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des $(x_1, \dots x_p) \in H^p$ telle que $\prod_{i=1}^{p} x_i = e$.

Solution

E^G n'est rien d'autre que l'ensemble des $x \in E$ tels que $\mathrm{Orb}(x) = \{x\}$. De plus, on sait que les orbites forment une partition de E et on a $\forall x \in G$, $|G| = |\operatorname{Stab}(x)||\operatorname{Orb}(x)|$, on en déduit l'équation aux classes suivante

$$|E| = \sum_{i \in I} \frac{|G|}{|\operatorname{Stab} x_i|} = |E^G| + \sum_{j=1}^{n} |w_j|$$

où les $|w_j|$ pour $1 \leq j \leq n$ sont les termes de la somme de gauche tels que $|\operatorname{Stab} x_i| < |G|$. On en déduit par le théorème de Lagrange que $|\operatorname{Stab} x_i| \in \{1, \dots p^{m-1}\}$ puis que les $|w_j|$ sont des multiples de puissances de p, d'où le résultat.

Introduisons $(x_1, \dots x_p) \in H^p$ tel que $x_1 \dots x_p = 1$ alors $x_2 \dots x_p x_1 = 1$, notons c le cycle $(1,2,\dots p)$. On remarque que $K = \langle c \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et que pour tout $c' \in K$, $\prod_{i=1}^{p} x_{c'(i)} = 1$. Notons E l'ensemble des p-plets de produit égal à 1 et appliquons le résultat de la question précédente à l'opération

$$\begin{cases} K \to E \\ c' \mapsto c(x_1, \dots x_p) = (x_{c(1)}, \dots x_{c(n)}) \end{cases}$$

On obtient donc que

$$|E| \equiv |E^K| \, [p]$$

Or $|E| = n^{p-1}$ par un simple argument combinatoire (au choix $p-1$ éléments de E puis le dernier est l'inverse). Or $p \mid n$ donc $|E^K| \equiv 0 \, [p]$, or E^K est non vide puisque $(e, \dots e)$ en est un élément donc $|E^K| \geq p$. De plus, $E^K = \{(x_1, \dots x_p) \in E : \forall c' \in \langle c \rangle, (x_{c'(1)}, \dots x_{c'(p)}) = (x_1, \dots x_p)\} = \{(x, \dots x) \in H^p : x^p = 1\}$. De plus, s'il existait $x \in H$ tel que $x^p = 1$ et x n'est pas d'ordre p alors l'ordre de x diviserait p sans être égal à p, d'où $x = e$. Donc mis à part e, E^K contient l'ensemble des éléments d'ordre p. Ainsi on a prouvé qu'il y avait un nombre $kp - 1$ éléments d'ordre p. ■