Références :
Cours d'algèbre, Daniel Perrin

Théo (Cayley)**.** *Si G est fini de cardinal n, G est isomorphe à un sous-groupe de $\mathcal{S}_n$.*

Déf. Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \wedge m = 1$, on appelle **p-Sylow** de G un sous-groupe de cardinal p^α.

Théo (Sylow)**.** *Soit G un groupe fini et p un diviseur (premier) de $|G|$, alors*

(i) G contient au moins un p-Sylow.

(ii) Les p-Sylow sont tous conjugués.

Démonstration. Pour montrer le (i) du théorème, nous aurons besoin de deux lemmes.

Lemme 1. *Soit G un groupe avec $|G| = n = p^\alpha m$ et $p \wedge m = 1$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

NB. Ce lemme permet, connaissant un Sylow d'un groupe G d'en trouver un pour un sous-groupe H.

Démonstration. Le groupe H opère sur G/S par translation à gauche. De plus, on a, pour tout $a \in G$:

$$\begin{aligned} Stab_H(aS) &= \{h \in H : h.aS = aS\} \\ &= \{h \in H : a^{-1}haS = S\} \\ &= \{h \in H : a^{-1}ha \in S\} \\ &= aSa^{-1} \cap H \end{aligned}$$

On applique l'équation aux classes

$$|G/S| = \sum_{aS \in \Omega} \frac{|H|}{|aSa^{-1} \cap H|}$$

avec Ω un partie de G/S constitué exactement d'un représentant de chaque orbite.
Par hypothèse, on sait que p ne divise pas $|G/S|$. Ainsi, il existe un $aS \in \Omega$ tel que p ne divise pas $\frac{|H|}{|aSa^{-1} \cap H|}$. On sait, de plus que $aSa^{-1} \cap H$ est un p-groupe, car sous-groupe du p-Sylow aSa^{-1}. D'où le résultat. □

Lemme 2. *Soit $n \in \mathbb{N}^*$. Alors $GL_n(\mathbb{Z}/p\mathbb{Z})$ possède un p-Sylow.*

Démonstration. Pour connaitre le cardinal de $GL_n(\mathbb{Z}/p\mathbb{Z})$, il suffit de connaître le nombre de bases du $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$.
On a donc :

- Pour e_1, on peut choisir tout le monde sauf 0, soit $p^n - 1$ choix.
- Pour e_2, on peut choisir tout le monde sauf $Vect(e_1)$, soit $p^n - p$ choix.
- ...
- Pour e_n, on peut choisir tout le monde sauf $Vect(e_1, ..., e_{n-1})$, soit $p^n - p^{n-1}$ choix.

Ainsi, on a

$$\begin{aligned} |GL_n(\mathbb{Z}/p\mathbb{Z})| &= (p^n - 1)(p^n - p)...(p^n - p^{n-1}) \\ &= (pp^2...p^{n-1})m \text{ avec } m \wedge p = 1 \\ &= p^{\frac{n(n-1)}{2}}m \end{aligned}$$

On exhibe alors un p-Sylow P de $GL_n(\mathbb{Z}/p\mathbb{Z})$. C'est l'ensemble des matrices triangulaires supérieures strictes :

$$P = \{A = (a_{i,j}) : a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1\}.$$

En effet, comme les $a_{i,j}$ pour $i < j$ sont quelconques, on a

$$|P| = p \times p^2 \times ... \times p^{n-1} = p^{\frac{n(n-1)}{2}}.$$

□

Revenons à la preuve du théorème. Soit G un groupe et p un diviseur de $|G| = n$. On plonge d'abord G dans $\mathcal{S}_n$, par le théorème de Cayley, puis on plonge $\mathcal{S}_n$ dans $GL_n(\mathbb{Z}/p\mathbb{Z})$ à l'aide de l'application injective suivante :

$$\begin{array}{ccc} \mathcal{S}_n & \longrightarrow & GL_n(\mathbb{Z}/p\mathbb{Z}) \\ \sigma & \longmapsto & u_\sigma \end{array}$$

avec u_σ définie dans la base canonique par $u_\sigma(e_i) = e_{\sigma(i)}$.
Finalement, on a donc réalisé G comme sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$ qui possède un p-Sylow d'après le lemme 2. Ainsi, G possède un p-Sylow par le lemme 1.

Montrons maintenant (ii).
Soit H et S deux p-Sylow de G. Comme H est un sous-groupe de G, par le lemme 1, il existe un $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Or, comme H est un p-groupe, on a $aSa^{-1} \cap H = H$ et donc H est inclus dans $aSa^{-1} \cap H$. Ainsi, on a $H = aSa^{-1}$.

□

Leçons possibles : 101 - 104

Questions posées :

- Qu'est-ce qu'un p-Sylow ?
- Comment appelle-t-on "G/S" ? Réponse : L'ensemble des classes à gauche.
- Est-ce qu'un groupe quotienté par un p-Sylow a toujours une structure de groupe ? Réponse : Non, il faut que le sous-groupe par lequel on quotiente soit distingué. Si le p-Sylow est unique, alors c'est vrai.
- Quels sont les p-Sylow de $G = \mathbb{Z}/n\mathbb{Z}$ avec $n = p^\alpha m$? Réponse : Si p ne divise pas n, alors G n'admet pas de p-Sylow. Sinon, soit S_1 et S_2 deux p-Sylow de G. Alors, par le théorème de Sylow, ils sont conjugués, ie il existe $a \in G$ tel que $S_1 = a + S_2 - a = S_2$ donc il y a un unique p-Sylow qui est $\{km : k \in [\![0, p-1]\!]\}$.
- Quels sont les p-Sylow de $\mathcal{S}_p$? Réponse : $\mathcal{S}_p$ est de cardinal $p!$. Un p-Sylow de $\mathcal{S}_p$ doit donc être de cardinal p. C'est donc le groupe engendré par un p-cycle.
- Comment calcule-t-on $1 + 2 + ... + (n-1)$? Réponse : En additionnant au premier terme le dernier, puis le deuxième à l'avant-dernier, etc, on arrive à n. On fait $\frac{n}{2}$ sommes d'où le résultat.
- Pourquoi le groupe P est un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$? Réponse : Si on effectue la multiplication de deux matrices de P, on reste dans P. Le calcul de l'inverse est un peu plus subtil. Pour inverser la matrice, on résout un système linéaire échelonné.