

## 5.1 Sous-groupes de Sylow

**Définition :** Soit  $G$  un groupe fini de cardinal  $n = p^\alpha \cdot m$  où  $p$  est un nombre premier ne divisant pas  $m$ . On appelle  $p$ -sous-groupe de Sylow (ou  $p$ -Sylow) un sous-groupe de  $G$  de cardinal  $p^\alpha$ .

On a le premier théorème de Sylow :

**Théorème 1 de Sylow :** Soit  $p$  un nombre premier divisant  $n$  et  $G$  un groupe de cardinal  $n$ . Alors  $G$  contient au moins un  $p$ -groupe de Sylow.

Pour la démonstration on utilise le lemme suivant :

**Lemme :** Soit  $G$  un groupe fini de cardinal  $n = p^\alpha \cdot m$  où  $p$  est un nombre premier ne divisant pas  $m$ , et  $H$  un sous-groupe de  $G$  tel que  $p$  divise  $|H|$ . Soit  $S$  un  $p$ -Sylow de  $G$ . Alors il existe  $a \in G$  tel que :

$$aSa^{-1} \cap H \text{ est un } p\text{-Sylow de } H.$$

**Démonstration du Lemme :** on fait agir le groupe  $G$  sur l'ensemble  $(G/S)_g$  des classes à gauche par translations à gauche  $(g, aH) \mapsto gaH$  (voir exemples). Le stabilisateur de  $a.S$  est l'ensemble des  $g$  de  $G$  tels que  $gaS = aS$ ; cette relation équivaut à :  $a R_g ga$  soit  $a^{-1}ga \in S$  ou  $g \in a.S.a^{-1}$ . Le stabilisateur de  $a.S$  est donc  $a.S.a^{-1}$ . De même  $H$  opère sur  $(G/S)_g$  par restriction et le stabilisateur de  $a.S$  par cette action est  $(a.S.a^{-1}) \cap H$ . D'après l'équation des classes, si  $p$  divise tous les  $|H/(a.S.a^{-1}) \cap H|$  alors  $p$  divise  $|(G/S)_g|$  ce qui est impossible car  $S$  est un  $p$ -Sylow de  $G$ . Par conséquent il existe  $a \in G$  tel que  $p$  ne divise pas  $|H/(a.S.a^{-1}) \cap H|$ . Mais  $(a.S.a^{-1})$  est un  $p$ -groupe (car c'est l'image de  $S$  par l'automorphisme intérieur  $x \mapsto a.x.a^{-1}$ ) donc  $(a.S.a^{-1}) \cap H$  aussi. Comme  $p$  ne divise pas  $|H/(a.S.a^{-1}) \cap H| = |H|/|(a.S.a^{-1}) \cap H|$ ,  $(a.S.a^{-1}) \cap H$  est donc un  $p$ -Sylow de  $H$ .

**Démonstration du théorème 1 de Sylow :** on plonge  $G$  dans  $S_n$  (Théorème de Cayley : voir 4.2) puis  $S_n$  dans  $GL(n)$ , groupe linéaire de  $K^n$  où  $K = \mathbb{Z}/p\mathbb{Z}$ , par l'application  $\sigma \mapsto u$  définie par  $u(e_i) = e_{\sigma(i)}$  où  $e_i$  est la base canonique de  $K^n$ .

Le cardinal de  $GL(n)$  est celui des bases de  $K^n$ . Dénombrons donc le nombre de ces bases. Il y a  $p^n - 1$  façons de choisir le premier vecteur  $e_1$  d'une base. Ce premier vecteur étant choisi, on peut choisir le second vecteur  $e_2$  parmi les vecteurs non colinéaires au premier. Comme ceux-ci s'écrivent  $k.e_1$  il y a  $p$  vecteurs colinéaires à  $e_1$  donc il y a  $p^n - p$  façons de choisir le second vecteurs  $e_2$  d'une base. De même les vecteurs liés avec  $e_1$  et à  $e_2$  s'écrivent  $ke_1 + k'e_2$  et il y en a donc  $p^2$ . Le nombre de choisir  $e_3$  est donc  $p^n - p^2$ . On voit ainsi qu'il y a  $(p^n - 1) \cdot (p^n - p) \cdot \dots \cdot (p^n - p^{n-1})$  bases de  $K^n$  donc  $|GL(n)| = (p^n - 1) \cdot (p^n - p) \cdot \dots \cdot (p^n - p^{n-1})$  qui est un nombre divisible par  $p$ .

Si on identifie  $GL(n)$  à l'ensemble des matrices inversibles à coefficients dans  $K$ , l'ensemble  $S$  des matrices triangulaires inférieures de diagonale 1 est un sous-groupe de  $GL(n)$  de cardinal  $p \cdot p^2 \cdot \dots \cdot p^{n-1} = p^{n(n-1)/2}$ , donc  $|GL(n)|/|S| = (p^n - 1) \cdot (p^{n-1} - 1) \cdot \dots \cdot (p - 1)$  qui n'est pas divisible par  $p$  : donc  $S$  est un  $p$ -Sylow de  $GL(n)$ .

On termine en utilisant le lemme : il existe  $a \in GL(n)$  tel que  $aSa^{-1}$  soit un  $p$ -sylow de  $G$ .

**Théorème 2 de Sylow :** Soit  $p$  un nombre premier et  $n = p^\alpha \cdot m$  ( $\alpha > 1$ ),  $p$  ne divisant pas  $m$ . Soit  $G$  un groupe de cardinal  $n$ .

(i) Soit  $H$  un sous-groupe de  $G$  qui est un  $p$ -groupe. Alors il existe un  $p$ -Sylow  $S$  tel que  $H \subset S$ .

(ii) Les  $p$ -Sylow de  $G$  sont tous conjugués et leur nombre  $k$  divise  $n$ .

(iii) On a :  $k \equiv 1 \pmod{p}$  (donc  $k$  divise  $m$ ).

**Démonstration :**

(i) D'après le théorème précédent il existe un  $p$ -Sylow  $S$  de  $G$ . D'après le lemme il existe  $a \in G$  tel que  $aSa^{-1} \cap H$  soit un  $p$ -Sylow de  $H$ . Mais  $H$  étant un  $p$ -groupe,  $H$  est l'unique  $p$ -Sylow de  $H$  donc  $aSa^{-1} \cap H = H$  soit  $H \subset aSa^{-1}$  et  $aSa^{-1}$  est encore un  $p$ -Sylow de  $G$  comme image de  $S$  par l'automorphisme intérieur  $x \mapsto axa^{-1}$ . D'où le (i).

(ii) Soient  $S$  et  $S'$  deux  $p$ -Sylow de  $G$ . D'après le lemme il existe  $a \in G$  tel que  $(aSa^{-1}) \cap S'$  soit un  $p$ -Sylow de  $S'$ .  $S'$  étant un  $p$ -groupe on a donc  $aSa^{-1} = S'$  et les  $p$ -Sylow de  $G$  sont tous conjugués.

D'autre part  $G$  agit sur les  $p$ -Sylow de  $G$  par automorphismes intérieurs. D'après ce qu'on vient de dire il n'y a qu'une orbite sous cette action. La formule des classes implique alors que le nombre de  $p$ -Sylow divise  $n$ .

(iii) Soit  $S$  un  $p$ -Sylow de  $G$ . Faisons agir  $S$  sur l'ensemble  $X$  des  $p$ -Sylow de  $G$  par automorphismes intérieurs. D'après le (i) de l'exercice 30 on a  $|X| \equiv |I| \pmod{p}$  où  $I = \{p\text{-Sylow } T \text{ de } G / sTs^{-1} = T \text{ pour tout } s \text{ de } S\}$ . Soit  $T \in I$  et  $N$  le sous-groupe de  $G$  engendré par  $S$  et  $T$ . Pour tout  $n$  de  $S$  et tout  $n$  de  $T$  on a  $nTn^{-1} = T$ ; cette relation est donc valable pour tout  $n$  du groupe  $N$ . Comme  $T$  est un  $p$ -Sylow de  $G$  c'est aussi un  $p$ -Sylow de  $N$  et tous les  $p$ -Sylow de  $N$  étant conjugués d'après (ii) on en déduit que  $T$  est l'unique  $p$ -Sylow de  $N$ . Par conséquent  $T = S$  d'où  $|I| = 1$  et  $k = |X| \equiv 1 \pmod{p}$ .

Cette dernière relation prouve que  $k$  est premier avec  $p$ ; comme  $k$  divise  $n = p^\alpha \cdot m$   $k$  divise  $m$  d'après le théorème de Gauss ce qui achève la démonstration du (iii).

### ***Exercice 32***

Déduire du théorème précédent que si  $S$  est un  $p$ -Sylow de  $G$  on a :

$$S \triangleleft G \Leftrightarrow S \text{ est l'unique } p\text{-Sylow de } G$$

En déduire qu'un groupe d'ordre 63 n'est pas simple.