Applications aux p-groupes

Déf. Soit p un nombre premier. Un <u>p-groupe</u> est un groupe de cardinal une puissance de p.

Ex. 1). $\mathbb{Z}/p^n\mathbb{Z}$ est un p-groupe pour tout $n \in \mathbb{N}$ et p premier

2) le produit cartésien $G \times H$ de 2 p-groupes G et H est encore un p-groupe

3) Soit $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}$ c'est un sous-groupe multiplicatif de $\mathbb{H}^*$. Rappelons que $\mathbb{H} = \{ a+bi+cj+dk \mid a,b,c,d \in \mathbb{R}\}$

la multiplication sur $\mathbb{H}$ est déterminée par

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1$$
$$ij = k, \quad jk = i, \quad ki = j$$
$$ji = -k, \quad kj = -i, \quad ik = -j$$

L'addition sur $\mathbb{H}$ est définie par

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) =$$
$$= (a+a') + (b+b')i + (c+c')j + (d+d')k$$

$(\mathbb{H}, +, \times)$ est un corps gauche i.e. un corps non commutatif ($\mathbb{H}$ comme Hamilton)

En particulier, $\mathbb{H}^* = \mathbb{H}\setminus\{0\}$ est un groupe non commutatif.
Or, le sous-ensemble $Q_8 \subseteq \mathbb{H}^*$ est clairement un sous-groupe de $\mathbb{H}^*$ (exo). Comme $|Q_8| = 2^3$, Q_8 est un 2-groupe non-commutatif.

Proposition Soit p un nombre premier et G un p-groupe. Soit E un G-ensemble fini. Notons $E^G = \{x \in E \mid \forall g \in G,\ gx = x\}$ l'ensemble des points fixes de G. Alors

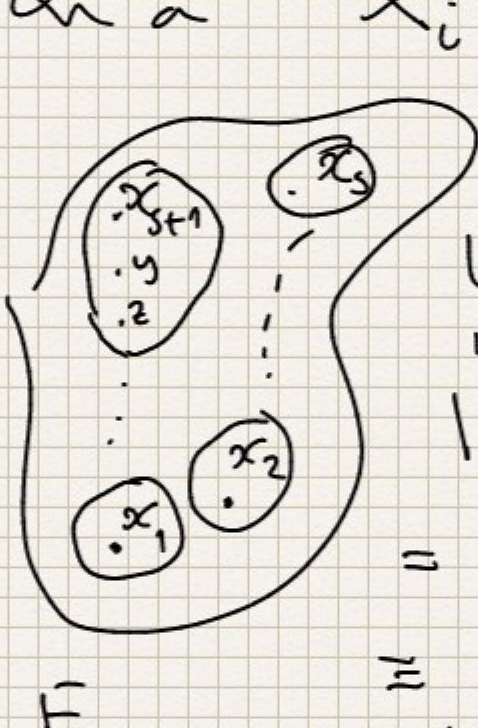
$$|E^G| \equiv |E| \mod p.$$

__Démo.__ Comme G est un p-groupe, toute orbite dans E est de cardinal une puissance de p. Soient $X_1, \dots, X_r \subseteq E$ les orbites de E, et $x_i \in X_i$. Supposons que

$E^G = \{x_1, \dots, x_s\}$ où $1 \leq s \leq r$

On a $X_i = Gx_i = \{x_i\}$ pour $i = 1, \dots, s$

et $|X_i| = p^{n_i}$, $n_i \neq 0$, pour $i = s+1, \dots, r$.



La formule des orbites nous donne alors

$$|E| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{s} |X_i| + \sum_{i=s+1}^{r} |X_i| =$$

$$\equiv s \mod p. \equiv |E^G| \mod p$$

car $|X_i| \equiv 0 \mod p$ pour $i = s+1, \dots, r$ ∎

Déf. Soit G un groupe. Le centre de G est le sous-ensemble

$$C(G) = Z(G) = \{ g \in G \mid \forall h \in G : gh = hg \}$$

Exo. 1) $C(G)$ est un sous-groupe distingué de G

2) G est commutatif $\Leftrightarrow C(G) = G$

Corollaire (de la prop. précédente)

Un p-groupe non trivial possède un centre non trivial.

Démo. Soit G un p-groupe. Soit $E = G$. On fait agir G sur E par conjugaison :

$$g * x := g x g^{-1} \quad \text{où } g \in G \text{ et } x \in E = G$$

Ceci définit bien une action à gauche de G sur E, c-à-d sur lui-même. D'après la proposition précédente

$$\begin{aligned} |E^G| &\equiv |E| \mod p \\ &\equiv |G| \mod p \\ &\equiv 0 \mod p. \end{aligned}$$

Or, $E^G = \{ x \in E \mid \forall g \in G : g * x = x \} =$

$$= \{ g \in G \mid \forall h \in G : hgh^{-1} = g \} = C(G).$$

On a donc

$$|C(G)| \equiv 0 \mod p$$

Or, $1 \in C(G)$ et donc $|C(G)| \neq 1$ i.e. $C(G) \neq \{1\}$. $\square$

Ex. Vérifions que $C(Q_8) \neq \{1\}$

En effet, $C(Q_8) = \{+1, -1\}$.

§2 Les Théorèmes de Sylow

Dans la suite, p désignera un nombre premier

Déf. Soit G un groupe fini. Un <u>p-sous-groupe</u> de G est un sous-groupe de G qui est un p-groupe, i.e, un sous-groupe de G de cardinal une puissance de p

Ex. 1) $G = S_3$ $\{1, (1\,2)\}$ est un 2-sous-groupe de G. Ou encore $\{1, (1\,2\,3), (3\,2\,1)\}$ est un 3-sous-groupe de G

2) Soit G fini et $x \in G$ d'ordre p. Alors $\langle x \rangle$ est un p-sous-groupe de G

3) $G = S_4$ et $H = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. H est un sous-groupe de S_4 (exo) isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (exo)
H est un 2-sous-groupe de G

On notera n le cardinal d'un groupe fini G. On écrira

$$n = mp^r$$

où $m, r \in \mathbb{N}$ et $p \nmid m$.

Remarque Si $H \leq G$ est un p-sous-groupe, $|H| = p^s$ où $s \in \{0, 1, 2, \dots, r\}$.
En effet, $|H|$ divise n et $\mathrm{pgcd}(|H|, m) = 1$

Déf. Un <u>p-sous-groupe de Sylow</u> ou <u>p-sylow</u> de G est un p-sous-groupe de G de cardinal maximal, c-à-d, de cardinal p^r.

Ex. 1) Le 2-sous-groupe $H = \{1, (12)\}$ de S_3 est un 2-sylow de S_3 car $n = |S_3| = 6 = \underset{m \times p^r}{3 \times 2^1}$ et $|H| = 2^1$

De même, $\{1, (13)\}$ et $\{1, (23)\}$ sont des 2-sylows de S_3

Le 3-sous-groupe $K = \{1, (123), (321)\}$ est un 3-sylow de S_3. En effet $|S_3| = 2 \times 3^1$ et $|K| = 3^1$

C'est l'unique 3-sylow de S_3 !

2). Soit H le sous-groupe de S_4 des double transpositions. $|H| = 4 = 2^2$. et $|S_4| = 24 = 3 \times 2^3$. H n'est pas un 2-sylow de S_4. Remarquons que $H \leq A_4$; le sous-groupe alterné de S_4.

Or $|A_4| = \frac{1}{2}|S_4| = 3 \times 2^2$. Donc H est un 2-sylow de A_4.

3) $G = \mathbb{Z}/n\mathbb{Z}$, $n = mp^r$

les sous-groupes de $G = \mathbb{Z}/n\mathbb{Z}$ sont

$$d\mathbb{Z}/n\mathbb{Z} \quad \text{où} \quad d | n, \quad d \in \mathbb{N}.$$

(liste sans répétition). De plus,

$$|d\mathbb{Z}/n\mathbb{Z}| = \frac{n}{d} = \frac{mp^r}{d}$$

Donc les p-sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont

$$mp^i\mathbb{Z}/n\mathbb{Z} \quad \text{où} \quad i = 0, 1, 2, \ldots r$$

de cardinal p^{r-i} resp^t.

En particulier, $\mathbb{Z}/n\mathbb{Z}$ contient un p-sylow et un seul, pour tout nombre premier p.

Théorèmes de Sylow Soit G un groupe fini de cardinal n. Soit p un nombre premier. Ecrivons $n = mp^r$ où $m, r \in \mathbb{N}$ et $p \nmid m$. Soit X_s l'ensemble des p-sous-groupes de G de cardinal p^s, pour $s = 0, \dots, r$.
Alors,

(i) $\forall s \in \{0, \dots, r\}$, $|X_s| \equiv 1 \mod p$. En particulier, G contient un p-sous-groupe de cardinal p^s pour tout $s = 0, \dots, r$.

(ii) Pour tout p-sous-groupe H de G et tout p-sylow S de G, il existe $g \in G$ tq $H \subseteq gSg^{-1}$.

(iii) tout p-sous-groupe de G est contenu dans un p-sylow de G

(iv) le nombre de p-sylows de G est congru à $1 \mod p$ et divise m. Deux p-sylows de G sont conjugués.

Avant de démontrer cet énoncé, vérifions-le sur les exemples précédents.

Ex 1) $G = S_3$, $p = 2$. On a vu que S_3 contenait 3 2-sylows. Or, 3 est bien congru à $1 \mod 2$ et 3 divise bien $m = 3$.
Notons H_1, H_2, H_3 les 3 2-sylows de S_3.
On a bien $H_1 = gH_2g^{-1}$, $H_1 = hH_3h^{-1}$ pour certains $g, h \in S_3$.
Puis $G = S_3$ et $p = 3$. On a vu que S_3 ne contient qu'un seul 3-sylow.
Or $1 \equiv 1 \mod 3$ et $1 | 2 = m$, comme il fallait.

2) $G = \mathbb{Z}/n\mathbb{Z}$ $n = mp^r$. On a vu que G contient un et un seul p-sous-groupe de cardinal p^s, pour $s = 0, \dots, r$.
De plus

$$n\mathbb{Z}/n\mathbb{Z} \subseteq \dots \subseteq mp\mathbb{Z}/n\mathbb{Z} \subseteq \underbrace{m\mathbb{Z}/n\mathbb{Z}}_{p\text{-sylow de } \mathbb{Z}/n\mathbb{Z}}$$

i.e, les p-sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ constituent une chaîne dans $\mathbb{Z}/n\mathbb{Z}$.
Les Théorèmes de Sylow sont donc bien vérifiés pour $\mathbb{Z}/n\mathbb{Z}$