Théorème de Cauchy et théorèmes de Sylow

1 Introduction

Le théorème de Lagrange nous apprend que l'ordre d'un élément dans un groupe fini est un diviseur de l'ordre du groupe. Le théorème de Lagrange peut s'énoncer encore sous la forme suivante: l'ordre d'un sous groupe d'un groupe engendré par un élément de ce groupe est un diviseur de l'ordre du groupe. Il est alors naturel de se poser le problème de la réciproque:

- Si p est un diviseur de l'ordre d'un groupe existe-t-il un élément d'ordre p dans ce groupe?
- Si p est un diviseur de l'ordre d'un groupe, existe-t-il un sous groupe d'ordre p dans ce groupe?

Le théorème de Cauchy, puis ceux de Sylow qui sont une généralisation du premier, apporteront des éléments de réponse à ces questions.

2 Théorème de Cauchy

Théorème de Cauchy Soit (G,.) un groupe fini et p un diviseur premier de l'ordre de G. Alors il existe un élément d'ordre p dans G.
Démonstration Soit p un diviseur premier de |G|. Considérons l'ensemble

$$X = \{(x_1,...,x_p) \in \underbrace{G \times ... \times G}_{p\ fois}; x_1.x_2.....x_p = e\}$$

où e désigne le neutre de G. Pour choisir un élément x de X, nous devons faire p-1 choix d'éléments dans G, donc le cardinal de X est $|G|^{p-1}$. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X de la façon suivante: (*On commettra sans aucun scrupule l'abus de notation qui consiste à identifier la classe d'équivalence de* $i \in \mathbb{Z}$ *et l'élément de* $\mathbb{Z}$ *compris entre 0 et p-1 qui est un représentant de cette classe d'équivalence. Autrement dit, on ne sera pas gêné par l'égalité* $\overline{i}=k$ *où k est le représentant de* $\overline{i}$ *qui est compris entre 0 (compris) et p (non compris)). Si x est l'élément* $(x_1,...,x_p)$ *de X et si* $\overline{i}$ *est la classe d'équivalence de i* $(0 \leq i < p)$ *dans* $\mathbb{Z}/p\mathbb{Z}$*, alors* $\overline{i}.x=(x_{\overline{1+i}},...,x_{\overline{p+i}})$. On vérifie sans peine que ceci définit bien une action sur X. Supposons que G ne possède aucun élément d'ordre p.
Remarquons que l'orbite de (e,...,e)∈X n'a qu'un élément. Si un autre élément x de X n'a que lui même dans son orbite, alors en particulier, $x=(x_{\overline{1}},...,x_{\overline{p}})= (x_{\overline{1+1}},...,x_{\overline{p+1}})=(x_2,...,x_p,x_1)=(x_3,...,x_1,x_2)=...$. Et donc $x_1=x_2=...=x_p$ et $x_1{}^p$=e, ce qui implique que G possède un élément x_1 d'ordre p et est contraire à notre hypothèse de départ. On suppose donc que (e,...,e) est le seul élément de X possèdant une orbite ne contenant que lui même. Si x est un élément de X, |w(x)| est alors un diviseur de $|\mathbb{Z}/p\mathbb{Z}|$=p différent de 1. Comme p est premier,

ceci implique que |w(x)|=1. Choisissons alors des éléments x de X dont les orbites respectives partitionnent X. La formule des classes nous donne:

$$|X| = |X^G| + \sum_{x\ partitionnant\ X} |w(x)|.$$

Donc |X| est de la forme 1+m.p où m désigne le nombre d'orbites de taille plus grande que 1 et partitionnant X. Ceci contredit le fait que |X| est de cardinal $|G|^{p-1}$ qui est divisible par p. Nous venons alors de démontrer par l'absurde que G possèdait au moins un élément d'ordre p.

3 Théorèmes de Sylows

Définition On dit que le groupe fini (G,.) est un **p-groupe** si p est premier et si le cardinal de G est une puissance de p.

Proposition Si G est un p-groupe agissant sur un ensemble X et si X^G=$\{x \in X; \forall g \in G, g.x = x\}$ alors on a:

$$|X| \equiv |X^G| \ (mod\ p)$$

Démonstration Soient x_1,...,x_k des éléments de X tels que { X^G,$w(x_1)$,...,$w(x_k)$ } définit une partition de X. X^G est en fait l'ensemble des éléments de X dont l'orbite est constituée d'un unique point. On suppose donc que pour tout i=1,...,k $|w(x_i)|>1$. Comme $|w(x_i)|$ est un diviseur de $|G|=p^\alpha$ et que p est premier, $|w(x_i)|$ est de la forme $p^{\alpha'}$ avec $\alpha' \geq 1$. Donc p divise $|w(x_i)|$ pour tout i=1,...,k. Mais comme X est la réunion disjointe des éléments de { X^G,$w(x_1)$,...,$w(x_k)$ } alors son cardinal est la somme des cardinaux de tout ces éléments et comme p divise chaque $|w(x_i)|$, $|X| \equiv X^G$ (mod p).

Définition Soit G un groupe de cardinal $n=p^\alpha.m$ avec p premier et p ne divisant pas m. On dit que le sous groupe H de G est un **p-Sylows** de G si $|H|=p^\alpha$.

Voici un exemple de p-Sylow.

Proposition Soit le corps fini $\mathbb{F}^p \simeq \mathbb{Z}/p\mathbb{Z}$ (p est un nombre premier). Considérons l'ensemble des matrices inversibles de rang n à coefficient dans $\mathbb{F}^p$. Cet ensemble, noté $GLn(\mathbb{F}^p)$, est un groupe de cardinal $m.p^{\frac{n(n-1)}{2}}$ où m et n sont des entiers non nuls. Si l'on note T le sous ensemble de $GLn(\mathbb{F}^p)$ des matrices triangulaires supérieures de rang n, à coefficients dans $\mathbb{F}^p$ et à éléments diagonaux tous égaux à 1, alors T est un p-Sylow de $GLn(\mathbb{F}^p)$.

Démonstration On ne démontrera pas que $GLn(\mathbb{F}^p)$ est un groupe. Ceci est un résultat de base d'algèbre linéaire. On ne démontrera pas non plus que T est un sous

groupe de GLn($\mathbb{F}^p$) car c'est relativement facile. Calculons par contre le cardinal de GLn($\mathbb{F}^p$). Etudions la première colonne d'une matrice de GLn($\mathbb{F}^p$). On peut choisir n'importe quelle valeur pour les éléments de cette colonne. La seule éventualité à éviter est que tout les éléments de cette colonne soient nuls simultanément. Cela nous fait donc p^n-1 possibilités pour cette première colonne. Etudions maintenant la deuxième colonne. Les éléments de cette colonne peuvent prendre n'importe quelles valeurs. Les seules conditions à vérifier sont que cette colonne ne soit pas dépendante de la première et qu'elle ne soit pas nulle. Il y a p-1 colonnes possibles dépendantes de la première et qu'une colonne nulle possible. Cela nous fait alors p^n-p possibilités pour la deuxièmre colonne. De même, par récurrence, on établit qu'il y a p^n-p^k possibilités pour la k^{ime} colonne. Donc $|GLn(\mathbb{F}^p)|=(p^n-1)(p^n-p)...(p^n-p^{n-1})$. Ce cardinal peut se re-écrire sous la forme: $p.p^2...p^{n-1}.(p^n-1)(p^{n-1}-1)...(p-1)=p^{1+2+...+n-1}.(p^n-1)(p^{n-1}-1)...(p-1)=p^{\frac{n(n-1)}{2}}.(p^n-1)(p^{n-1}-1)...(p-1)$
Donc, en posant m égal à la partie du produit précédent qui est après le premier facteur, on vient de montrer que $|GLn(\mathbb{F}^p)|=m.p^{\frac{n(n-1)}{2}}$.
Calculons maintenant le cardinal de T. Pour cela remarquons qu'il y a p^{n-1} choix possibles pour la première ligne, p^{n-k} choix possibles pour la k^{ime} ligne. Au total, cela nous fait $p.p^2...p^{n-1}$ choix possibles pour une matrice de T. Ceci prouve que $|T|=p^{\frac{n(n-1)}{2}}$ et que T est un p-Sylow de GLn($\mathbb{F}^p$).

Avant d'énoncer les théorèmes de Sylow, démontrons le lemme suivant qui nous sera fort utile pour la suite.

Lemme Soit G un groupe de cardinal n, p un diviseur premier de n tel que $n=p^\alpha.m$ et p ne divisant pas m, soit H un sous groupe de G et S un p-sylow de G. Alors il existe g dans G tel que $g.S.g^{-1}\cap H$ soit un p-sylow de H.

Démonstration Considérons le quotient G/S qui est en fait l'ensemble des classes à gauche de G relativement au sous groupe S: $G/S=\{a.H; a \in G\}$. G agit sur G/S par translation à gauche: g.aS=(ga)S.

L'élément $g\in$ G est élément du stabilisateur de aS si et seulement si g.aS=aS. C'est à dire si et seulement si g est élément de aSa^{-1}. Réciproquement, on montre que si g est élément de aSa^{-1} alors $g \in$Stab(aS).
H agit sur G/S par restriction de l'action de G. Le stabilisateur d'un élément aS pour cette nouvelle action est alors de la forme $aSa^{-1}\cap H$.

S étant un p-Sylow de G, $|S|=p^\alpha$. Comme aSa^{-1} est un sous groupe conjugué de S, il a même cardinal que S. De plus, comme H est un sous groupe de G, son cardinal est, d'après le théorème de Lagrange, de la forme $m'.p^{\alpha'}$ où m' divise m et où $\alpha' \leq \alpha$. L'intersection de deux sous groupes d'un groupe est encore un sous groupe. Donc $aSa^{-1}\cap H$ est un sous groupe de G. C'est de plus un sous groupe de H et de S. Son cardinal, toujours d'après le théorème de Lagrange, divise à la fois p^α et $m'.p^{\alpha'}$. Il est donc de la forme $p^{\alpha''}$ où α'' est à la fois plus petit (ou égal) à α et à α'. Notons que α dépend a priori de a. Supposons que pour tout a dans G, $\alpha''(a) < \alpha'$. Cette hypothèse

revient à supposer que $aSa^{-1} \cap H$ n'est jamais un p-Sylow de H. Alors, comme l'orbite d'un élément aS de G/S par l'action de H vérifie la formule |w(aS)|=|H|/|Stab(aS)| et que Stab(aS)=$aSa^{-1} \cap H$, on a |w(aS)|=m'.$p^{\alpha'-\alpha''}$. Comme pour tout a de G, on a supposé que $\alpha''(a) < \alpha'$ alors p divise |w(aS)| et ce $\forall a \in$G.
Mais $\{w(aS); a \in G\}$ définit une partition de G/S. La réunion de toutes ces orbites est égale à G/S. Le cardinal de G/S est donc divisible par p. Mais ceci est impossible car d'après le théorème de Lagrange |G/S|=m qui n'est pas divisible par p.
Nous avons donc abouti à une contradiction. Ceci nous permet d'affirmer qu'il existe un élément a de G tel que $aSa^{-1} \cap H$ est un p-Sylow de H.

Théorème (Premier théorème de Sylow) Si G est un groupe de cardinal n et que n vérifie n=p^{α}.m avec p premier et p ne divisant pas m, alors G possède un p-Sylow.

Démonstration Soit G un groupe comme dans l'énoncé du théorème. Le théorème de Cayley nous permet d'affirmer l'existence d'un morphisme injectif de G dans le groupe symétrique à n éléments Sn. Mais on a une injection évidente de Sn dans GLn($\mathbb{F}^p$): a toute permutation ϕ de Sn, on fait correspondre l'application linéaire f définie par : si $(ei)_{i=1..n}$ est une base de $(\mathbb{F}^p)^n$ alors f(ei)=$e_{\phi(i)}$.
On réalise ainsi une injection de G dans GLn($\mathbb{F}^p$). Ainsi, l'image d'un groupe par un morphisme étant un sous groupe du groupe d'arrivée du morphisme, et notre morphisme étant injectif (et surjectif sur son image) G est isomorphe à un sous groupe H de GLn($\mathbb{F}^p$). De plus, comme on l'a vu dans l'exemple précédent, GLn($\mathbb{F}^p$) possède un p-Sylow S. D'après le lemme précédent, il existe alors un élément a de GLn($\mathbb{F}^p$) tel que $aSa^{-1} \cap H$ est un p-Sylow de H. H contient donc un p-Sylow. Ce p-Sylow se transporte par l'application inverse de notre isomorphisme vers un p-Sylow du groupe G. Cqfd.

Théorème Soit G un groupe de cardinal n, n vérifiant n=p^{α}.m avec p premier et p ne divisant pas m. G contient, d'après le premier théorème de Sylow, un ou des p-Sylows.

- **(Second théorème de Sylow)** Les p Sylows de G sont tous conjugués. De plus, leur nombre k divise n.
- **(Troisième théorème de Sylow)** Le nombre k de p-Sylow dans G vérifie: $k \equiv 1 \pmod{p}$.

Démonstration Considérons $\mathcal{A} = \{S_1,...,S_k\}$ l'ensemble des p Sylows de G. D'après le premier lemme de ce paragraphe, pour tout i=1..k, il existe un élément a de G tel que $aS_1a^{-1} \cap S_i$ soit un p-Sylow de S_i. Mais en raison de ce fait et des cardinaux respectifs de aS_1a^{-1} et de S_i, on en déduit que $aS_1a^{-1}=S_i$. On démontre ainsi que tout les p-Sylows sont conjugués.
Remarquons à ce stade de la démonstration que si un p-Sylow est normal dans le groupe qui le contient, alors nécessairement, il est l'unique p-Sylow de ce groupe.
Faisons maintenant agir G par conjugaison sur $\mathcal{A}$: $g.S_i=gS_ig^{-1}$. Cette action est , avec ce qui vient d'être établi, bien définie. De plus, comme tout les p-sylows de G sont conjugués, cette action n'engendre qu'une et une seule orbite sur $\mathcal{A}$. Comme le cardinal

de l'orbite d'un point par une action est un diviseur du cardinal du groupe définissant cette action, on en déduit que k est un diviseur du cardinal de G.
S_1 agit de même sur $\mathcal{A}$ par restriction de l'action de G sur $\mathcal{A}$.
Etudions le sous ensemble $\mathcal{A}^{S_1}$ de $\mathcal{A}$. S_i est un élément de $\mathcal{A}^{S1}$ si et seulement si pour tout g de S_1, $g.S_i.g^{-1}$ est inclus dans S_i. Si on considère le sous groupe H de G engendré par S_i et S_1, on en déduit que $S_i \triangleleft H$. Mais S_i et S_1 sont deux p-Sylows de H. Donc, d'après la remarque faite précédemment, ceci implique que ces deux p-Sylows n'en forment qu'un: $S_1=S_i$. Le seul p-Sylow contenu dans $\mathcal{A}^{S_1}$ est donc S_1. Mais S_1 est un p groupe. Donc d'après la proposition établie tout au début de ce thème, $|\mathcal{A}| \equiv |\mathcal{A}^{S_1}|=1$ (mod p). Donc $k\equiv 1$ (mod p), Cqfd.

Voici un corollaire immédiat de ce qui vient d'être démontré.

Corollaire Soit G un groupe de cardinal n, n vérifiant $n=p^{\alpha}.m$ avec p premier et p ne divisant pas m. Soit k le nombre de p-Sylow dans G. Alors k divise m et k est premier avec p.

Démonstration Cela découle directement des deux théorèmes précédents.

Remarquons avant d'en terminer avec ce thème que le premier théorème de Sylow implique le théorème de Cauchy.