Développement : Théorèmes de Sylow

Théorème : $p \in \mathbb{P}$. G est un groupe fini de cardinal $n = p^\alpha m$, avec $m \wedge p = 1$.

1. Historique. — *Ce résultat possède de nombreuses démonstrations. D'une certaine manière il est une réciproque à Lagrange qui dit que l'ordre d'un sous-groupe divise l'ordre du groupe. A l'inverse donc, lorsque nous avons un diviseur en puissance de p qui divise G, alors il existe un sous-groupe de cet ordre. Cauchy est un cas restreint à p^1 dont la démonstration est aussi instructive et que l'on rajoute à ce développement.*

2. Premier Théorème : existence d'un p-Slyow ou p-groupe de puissance maximale. —

- Définitions :
  - Def : un p-groupe est un groupe ayant pour cardinal une puissance de p.
  - Def : un sous-groupe S de G est un p-Sylow s'il a pour cardinal p^α. C'est donc un p-groupe maximal et on a $[G : S] = m$, premier avec p.
- Enoncé : *Tout groupe fini G dont le cardinal est divisible par un nombre premier p possède un p-Sylow.*
- Lemme : Si H est un sous-groupe de G et S un Sylow de G, il existe un sous-groupe de H qui soit un Sylow de H et il est de la forme $aSa^{-1} \cap H$ où $a \in G$.
  - $\forall a \in G$, aSa^{-1} est un p-Sylow.
  - $\forall a$, en notant $F_a = aSa^{-1} \cap H$, F_a est donc un sous-groupe de H qui est un p-groupe.
  - On veut trouver a tel que $Card(H/F_a)$ soit premier avec p.
  - Or, aSa^{-1} est le stabilisateur de aS par l'action de translation par G sur aS et donc F_a est le stabilisateur de aS par la translation limitée à H.
  - Alors $H/(aSa^{-1} \cap H)$ est en bijection avec l'orbite par H de aS.
  - Or, si toutes ces orbites étaient un multiple de p, comme G/S est l'union de ces orbites, son cardinal serait divisible par p ce qui n'est pas le cas (S est un p-Sylow).
  - Donc pour au moins un a nous avons $Card(H/F_a)$ est premier avec p et pour cet a, F_a est un p-Sylow de H.
- Nous avons alors :
  - On plonge G dans $\mathfrak{S}_n$ (par le théorème de Cayley).
  - On plonge ensuite $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ (où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, corps fini de cardinal et de caractéristique p) : si $\sigma \in \mathfrak{S}_n$ et si $(e_i)_{1lei\leq n}$ est une base de $\mathbb{F}_p^n$, on associe à σ la transformation linéaire f définie par $f(e_i) = e_{\sigma(i)}$. Donc G se plonge dans $GL_n(\mathbb{K})$.
  - Se donner un élément de $GL_n(\mathbb{K})$ c'est se donner une base de $\mathbb{F}_p^n$.
  - En dénombrant les choix possibles pour chaque vecteur d'une base, on observe que $Card(GL_n(\mathbb{K})) = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) = (p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1)\cdots(p - 1)pp^2p^{n-1} = mp^{\frac{n(n-1)}{2}}$
  - Il reste à montrer que $GL_n(\mathbb{K})$ a un p-Sylow. Pour cela considérons le groupe P constitué des matrices triangulaires supérieures à coefficients diagonaux égaux à 1.
  - C'est un sous-groupe de $GL_n(\mathbb{K})$ en tant que sous-espace vectoriel.
  - Il est d'ordre $|P| = p^{\frac{n(n-1)}{2}}$.
  - Donc P est un p-Sylow de $GL_n(\mathbb{K})$ et en vertu du lemme il existe $a \in GL_n(\mathbb{K})$ tel que $aSa^{-1} \cap G$ soit un p-Sylow de G.
  - CQFD

3. Corollaire : cas particulier des p-groupes. — Enoncé : Soit P un p-groupe de cardinal p^n. $\forall i \leq n$, il existe un sous-groupe normal/distingué de cardinal p^i.

- On raisonne par récurrence sur n. P lui-même est la réponse lorsque $n = 1$.
- Sq la propriété soit vraie pour les groupes de cardinal p^q où $q < n$.
- Soit P un p-groupe de cardinal p^n.
- Considérons l'action sur P par lui-même par conjugaison.
- $\{e\}$ est une orbite singleton. Si on note Z l'ensemble des éléments de P ayant une orbite singleton, on observe qu'il s'agit du "Centre" de P, qui est le plus grand sous-groupe commutatif de P.
- $Card(P) = Card(Z) + \Sigma_{x \notin Z} Card(\mathscr{O}_x)$.
- Ces cardinaux divisent tous p^n et les $Card(\mathscr{O}_x)$ sont >1 donc sont des multiples de p;
- Donc $p|Card(Z)$ et de ce fait $Card(Z) > 1$. Donc $Card(Z) = p^\alpha$.
- Soit $x \in Z - \{e\}$ avec $\omega(x) = p^\beta$. Alors $y = x^{\beta-1}$ est d'ordre p.
- $G/ < x >$ est d'ordre p^{n-1} et donc, par hypothèse de récurrence, pour chaque $k \leq (n-1)$ il existe un sous-groupe $\mathscr{H}$ de $G/ < x >$, distingué et de cardinal p^{k-1}.
- On considère H son image réciproque par la surjection canonique $G \to G/ < x >$. H est normal/distingué en tant qu'image réciproque d'un sous-groupe distingué et
- Et $Card(H)/p = Card(\mathscr{H}) = p^{k-1}$, ce qui donne le résultat.
- CQFD

4. Deuxième théorème de Sylow. — Soit G un groupe de cardinal $n = p^\alpha m$ avec $p \wedge m = 1$.

1. Si H est un p-groupe de G il est inclus dans un p-Sylow de G.
2. Tous les p-Sylow sont conjugués entre eux.
3. Le nombre de p-Sylow divise n et aussi il est congru à 1 modulo p.

Démonstration :

- Soit S un p-Sylow de G qui existe d'après le théorème 1.
- Pour tout a, aSa^{-1} est aussi un p-Sylow de G.
- En application du lemme, soit $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.
- Comme H est un p-groupe, s'il a un p-Sylow c'est lui même donc $H = aSa^{-1} \cap H$ donc $H \subset aSa^{-1}$, ce qui prouve 1.

- Soit un sous-groupe H de G qui serait un p-Sylow. En tant que p-groupe, on peut lui appliquer le raisonnement ci-dessus et prouver qu'il est inclus dans aSa^{-1} pour certain a. Comme H est un p-Sylow, nous avons donc $H = aSa^{-1}$, ce qui prouve 2.
- Lemme : $Card(X) \equiv Card(X^P) : (mod.p)$
- Démonstration : En effet, si un p-groupe fixe les éléments d'un sous-ensemble X^P de X sur lequel il opère, alors les orbites des éléments de X^P sont des singletons. Toutes les autres orbites, qui divisent $Card(X)$, ont un cardinal divisible par p et l'équation des classes donne alors la conclusion.
- Si S et S' sont des p-Sylow de G et si S' normalise S, alors $S = S'$. Il suffit de considérer $H =< S, S' >$ qui normalise S. Du coup, H aura un seul p-Sylow puisqu'ils sont conjugués les uns des autres et S est un p-Sylow de H et H normalise S. Or, S' est aussi un p-Sylow de H et donc $S = S'$.
- Ainsi, si on revient à l'opération par conjugaison et si on l'applique à l'ensemble X des p-Sylow, comme le stabilisateur de aS est aSa^{-1} et que donc il est réduit au seul S d'après le point précédent. D'après le lemme, on a donc le point 3 du théorème.

5. Cauchy par voie directe. — Soit G un groupe de cardinal $n = p^\alpha m$ avec $p \wedge m = 1$. Il existe un sous-groupe de G de cardinal p.

1. Soit $E = \{(g_1, \cdots, g_p) \in G^p : \Pi g_i = e\}$.
2. Pro : $Card(E) = n^{p-1}$ car, une fois fixés $a_1, \cdots a_{p-1}$, a_p en découle.
3. Pro : E est stable par permutation circulaire.
4. On fait opérer $\mathbb{Z}/p\mathbb{Z}$ sur E par permutation circulaire.
5. Pro : les orbites autres que des singletons ont p éléments.
6. Si on a a orbites réduites à un élément (dont $(e, e, \cdots, e)$) l'équation des classes nous donne $a + pb = n^{p-1}$
7. Donc p divise a qui doit forcément être > 1.
8. Si on a une orbite singleton $(g, \cdots, g)$ avec $g \neq e$ alors $g^p = e$ et $< g >$ est alors un sous-groupe de G à p éléments.

.

Sources : Perrin et polycopié de JP Serre

December 27, 2017

Bruno Nitrosso, EPP et candidat libre