Def : Perrin p. 19

Théorème de Sylow :

(par les actions de groupe)

leçons 101
103
104
190

Def : Un p-Sylow H de G (où $|G| = p^{\alpha}.m$, et $p \wedge m = 1$) est un p-sous groupe de G tq $[G : H]$ premier avec p.

Lemme : Soit G groupe de cardinal $n = p^{\alpha}.m$ où $p \nmid m$. Soit $H < G$. Soit S un p-sylow de G. Alors $\exists\, a \in G$ tq $a S a^{-1} \cap H$ soit un p-sylow de H.

Preuve du lemme :

Le groupe G opère sur G/S par translation à gauche :

$$\begin{aligned} G \times G/S &\longrightarrow G/S \\ (g, aS) &\longmapsto g.(aS) = (ga)S \end{aligned}$$

(définition de l'action à gauche)

Il est alors facile de voir que le stabilisateur de aS est le sous groupe aSa^{-1}, conjugué de S :

$$\begin{aligned} \mathrm{Stab}_G(aS) &= \{ g \in G ;\ g.(aS) = aS \} \\ &= \{ g \in G ;\ a^{-1} g a S = S \} \end{aligned}$$

et $a^{-1} g a S = S \Leftrightarrow a^{-1} g a \in S$

d'où $\mathrm{Stab}_G(aS) = \{ g \in G ;\ g \in aSa^{-1} \}$

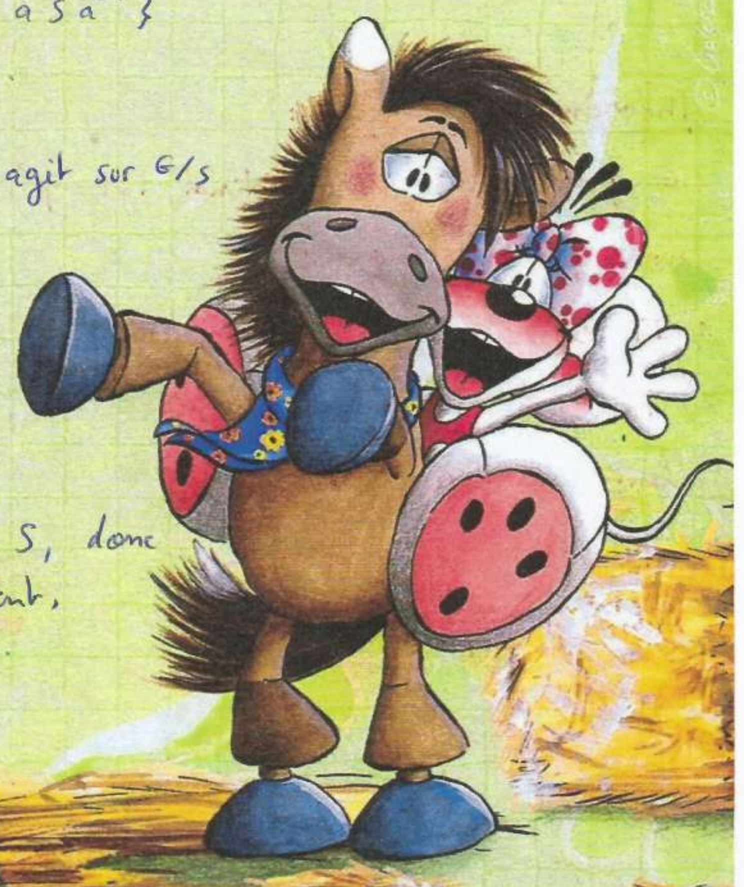
donc $\mathrm{Stab}_G(aS) = aSa^{-1}$.

Ainsi, par restriction, le groupe H agit sur G/S

et $\mathrm{stab}_H(aS) = H \cap \mathrm{Stab}_G(aS)$
$= H \cap aSa^{-1}$

Nous voulons mq $\exists\, a \in G$ tq $H \cap aSa^{-1}$ soit un p-Sylow de H.

- S p-Sylow et aSa^{-1} conjugué de S, donc est aussi un p-Sylow. Particulièrement, $H \cap aSa^{-1}$ est un p-groupe $\forall a \in G$.



• Montrons $\exists a \in G$ tq $[H : H \cap aSa^{-1}]$ soit premier avec p, i.e. $\frac{|H|}{|H \cap aSa^{-1}|}$ premier avec p.

On l'application $\underbrace{\frac{H}{H \cap aSa^{-1}}}_{\mathrm{stab}_H(aS)} \longrightarrow \underbrace{\mathrm{orb}(aS)}_{\text{orbite de } aS \text{ pour l'action de } H \text{ sur } G/S}$ est une bijection

$\bar{g} \longmapsto g.aS$

(car on quotiente par la relation d'équivalence :

$$\begin{aligned} gg'^{-1} \in aSa^{-1} \cap H &\Leftrightarrow gg'^{-1} \in \mathrm{stab}(aS) \\ &\Leftrightarrow (gg'^{-1}).aS = aS \\ &\Leftrightarrow g.aS = g'.aS \\ &\Leftrightarrow g \sim g' \quad) \end{aligned}$$

Ainsi $\frac{|H|}{|H \cap aSa^{-1}|} = |\mathrm{orb}(aS)|$. Par l'absurde, si tout ces nombres étaient divisibles par p, il en serait de même de $\frac{|G|}{|S|}$ car G/S est la réunion des orbites de aS. Donc $\frac{|G|}{|S|}$ divisible par p, ce qui contredit directement le fait que S soit un p-Sylow de G. ▪

Théorèmes de Sylow :

G groupe fini de cardinal $|G| = p^\alpha . m$ avec $p \nmid m$. Alors :

1) Il existe un p-Sylow de G

2) Tous les p-Sylow de G sont conjugués entre eux.

3) $H < G$ et H p-groupe. Alors $\exists S$ p-Sylow de G tq $H \subset S$

Preuve : On va utiliser le théorème de Cayley : "G groupe fini d'ordre $n \Rightarrow G$ isomorphe à un sous groupe de S_n". Preuve : Soit $g \in G$. On définit $t_g : \begin{array}{l} G \to G \\ x \mapsto gx \end{array}$ translation à gauche. On remarque $t_{gh} = t_g \circ t_h$ donc t_g est une permutation (car bijection de G dans G). Ceci définit $t : \begin{array}{l} G \to S(G) \\ g \mapsto t_g \end{array}$. (i) c'est un morphisme (ii) noyau $= \{e\}$ (iii) thm d'isomorphisme $\Rightarrow G \cong S(G)$ ∎ Par le théorème de Cayley, on plonge G dans S_n, puis on plonge S_n dans $GL_n(\mathbb{F}_p)$ via :

$$\begin{array}{l} S_n \to GL_n(\mathbb{F}_p) \\ \sigma \mapsto (U_\sigma : e_i \mapsto e_{\sigma(i)}) \end{array}$$

où $\{e_i\}$ base canonique de $\mathbb{F}_p^{\,n}$. Ainsi, G est un sous groupe de $GL_n(\mathbb{F}_p)$. (en effet : $f : G \to G'$ morphisme. Alors $\forall H' < G'$, $f^{-1}(H') < G$)

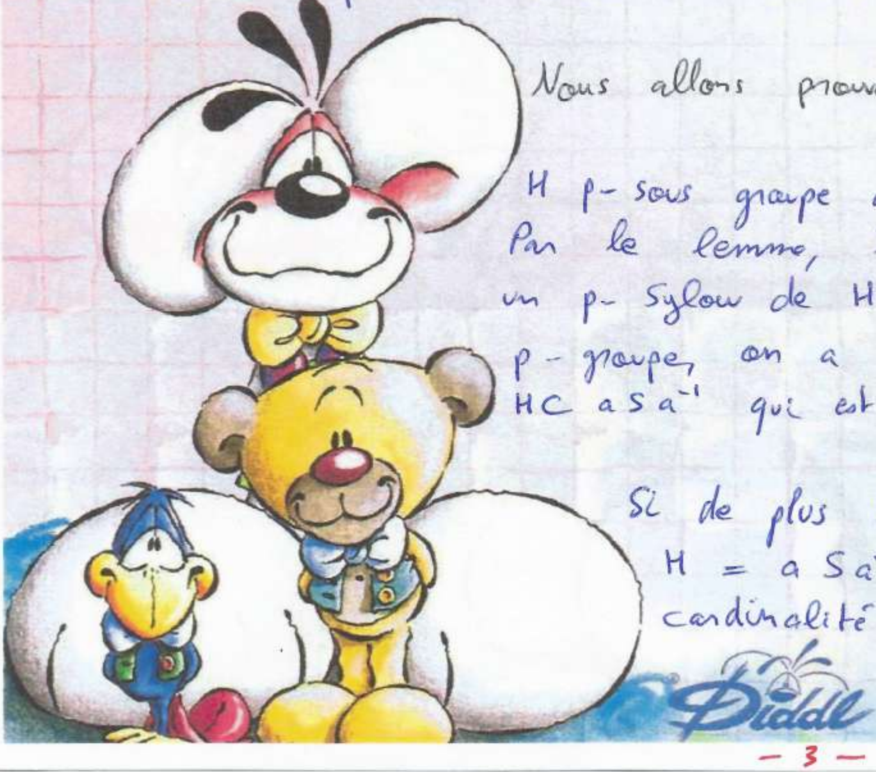
On $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

$$= p^{\frac{(n-1)n}{2}} \cdot (p^n - 1)(p^{n-1} - 1) \cdots (p-1)$$

$$= p^{\frac{n(n-1)}{2}} \cdot m \quad \text{où } p \nmid m \text{ (se voit en développant)}$$

On cherche un sous groupe de $GL_n(\mathbb{F}_p)$ d'ordre $p^{\frac{n(n-1)}{2}}$, un tel groupe est donné par les matrices triangulaires supérieures strictes $\begin{bmatrix} 1 & \cdots & * \\ 0 & \ddots & \vdots \\ & & 1 \end{bmatrix}$. Il s'agit bien d'un sous groupe de $GL_n(\mathbb{F}_p)$ dont l'ordre est $p^{\frac{n(n-1)}{2}}$, c'est un p-sylow de $GL_n(\mathbb{F}_p)$.

On conclut par le lemme : Il existe un p-Sylow de G. $\boxed{1}$



Nous allons prouver 2) et 3) simultanément :

H p-sous groupe de G et S p-Sylow de G. Par le lemme, $\exists a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, on a $aSa^{-1} \cap H = H$ donc $H \subset aSa^{-1}$ qui est un p-Sylow (preuve 3).

Si de plus H est un p-sylow, on a $H = aSa^{-1}$ pour raison de cardinalité. (preuve 2). ∎

© Colette

Cor: $N_p \equiv 1 \; [p]$ pour $|G| = m . p^\alpha$

$N_p \mid m$

- G opère par conjugaison sur $\overbrace{Syl_p(G)}^{\{p\text{-sylow de } G\}}$ car les p-sylow sont conjugués.

Soit S un p-sylow de G. S agit sur $Syl_p(G)$ par restriction.

On a $|Syl_p(G)| \equiv |Syl_p(G)^S| \; [p]$

> en effet: $G \curvearrowright X$, G p-groupe. donc de card p^α
> $|\text{orb } x| \mid |G| \Rightarrow |\text{orb } x| = \begin{cases} 1 \\ p \\ p^2 \\ \dots \end{cases}$
> donc $|\bigcup \text{orb } x| \equiv \# \{\text{orb de card } 1\} \; [p]$
> $\overset{\parallel}{|X|} \equiv |X^G| \; [p]$

Mq $|Syl_p(G)^S| = 1$

- $S \in Syl_p(G)^S$ car $\forall s \in S$, $s . S . s^{-1} = S$. Donc $|Syl_p(G)^S| \geq 1$.
- Soit $T \in Syl_p(G)^S$ et N le ss groupe engendré par S et T. $N = \langle S, T \rangle$.

$\forall s \in S \cup T$, $s T s^{-1} = T$ $\left(\begin{array}{l} \text{car si } s \in T \text{, ok.} \\ \text{sinon, } T \text{ stable sous} \\ \text{l'action de } S \text{ par def de } T \end{array} \right)$ donc $T \trianglelefteq N$ $\left(\begin{array}{l} \forall s \in N, \\ s T s^{-1} = T \end{array} \right)$

Donc T est l'unique p-sylow de N d'où $T = S$ et $|Syl_p(G)^S| = 1$.

Ainsi $N_p \equiv 1 \; [p]$.

- Soit S un p-sylow de G.

$m = |G| = |\text{Stab}(S)| . |\text{orb}(S)|$ par l'action de G par conjugaison sur $Syl_p(G)$

Or $|\text{orb}(S)| = N_p$. Ainsi $N_p \mid m$.

De plus, par point précédent, $p \wedge N_p = 1$ donc $N_p \mid m$ par Gauss.

A savoir pour ce dev : G agit sur E

Cours :

1) L'ensemble des orbites forme une partition de E $\quad |E| = \sum_{x \in E} |\text{orb}\, x|$

2) $\text{Stab}_G(x) < G$

3) $\dfrac{|G|}{|\text{Stab}_G(x)|} = |\text{orb}\, x|$

4) $|E| = \sum_{i=1}^{m} \dfrac{|G|}{|\text{Stab}_G(x_i)|}$ où $\text{orb}(x_1), \dots, \text{orb}(x_m)$ orbites de E.

5) Le nbre d'orbites $= \dfrac{1}{|G|} \cdot \sum_{g \in G} |E^g|$

6) $|X| = \sum_{x \in X} |\text{orb}\, x| = |X^G| + \sum_{\substack{x \in X \\ \text{Stab}_G(x) \neq G}} \dfrac{|G|}{|\text{Stab}_G\, x|}$ donc $|X| \equiv |X^G|\ [p]$.

Questions :

1) Qu'est ce qu'un p-sylow ? (de G) $\quad |G| = p^n \cdot m$

→ élément maximal pour l'inclusion parmi les p-groupes de G

→ sous p groupe de G tq $[G : S]$ premier avec p.

→ les sous groupes d'ordre p^n.

2) Comment appelle-t-on G/S ?

→ L'ensemble des classes à gauche

3) Un groupe quotienté par un p-sylow S a-t-il tjrs une structure de groupe ?

→ non, il faut que $S \trianglelefteq G$. Si le p-sylow est unique, c'est le cas.

4) Quels sont les p-sylow de $G = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ avec $n = p^\alpha m$?

. si $p \nmid n$, alors il n'y en a pas.

. Soit S_1, S_2 deux p-sylow. Alors ils sont conjugués, i.e. $\exists a \in G$ tq $S_1 = a + S_2 - a$
$= S_2$

↳ l'unique p-sylow est $\{km ;\ k \in [\![0, p-1]\!]\}$.

5) p-sylow de S_p ? (groupe des permutations)

→ S_p étant de cardinal $p!$, un p-sylow de S_p doit être de card p.

c'est donc le groupe engendré par un p-cycle.

En effet p premier $\Rightarrow (p-1)! \wedge p = 1$ donc les p-sylow sont d'ordre p^1.

$\boxed{\text{⚠ les } p\text{-sylow sont les sous groupes d'ordre } p^n}$ pour $|G| = p^n \cdot m$.

6) Mq G d'ordre 63 n'est pas simple :

$63 = 7 \times 3^2$. $\begin{cases} N_7 \mid 9 \\ N_7 \equiv 1\ [7] \end{cases} \Rightarrow N_7 = 1$. Donc N_7 unique 7-sylow donc $N_7 \trianglelefteq G$.