

101
104
105

Théorème de Cauchy + sous groupes distingués

- Groupes, DELCOURT
p 75 et 82, p 74 et 81
- Théorie des groupes, ULMER,
p 69 et 72

Théorème de Cauchy

Soit G un groupe fini et p un facteur
premier de n . Alors il existe un élément
d'ordre p dans G .

DELCOURT

Dém: on considère l'ensemble

$$X = \{ (x_1, x_2, \dots, x_p) ; x_1 x_2 \dots x_p = e \}$$

On observe que X est de cardinal n^{p-1} car
on a n choix pour les $(p-1)$ premiers et le
dernier est déterminé: $x_p = (x_1 \dots x_{p-1})^{-1}$.

On va faire agir le groupe $\mathbb{Z}/p\mathbb{Z}$ sur X
par permutations circulaires par:

$$\bar{k} \cdot (x_1, \dots, x_p) = (x_{k+1}, x_{k+2}, \dots, x_{k+p})$$

(les indices sont modulo p)

On peut vérifier que c'est une action de groupes:

• on doit avoir $x_{k+1} x_{k+2} \dots x_{k+p} = e$

On comme $x_1 = (x_2 \dots x_p)^{-1}$ alors

$$x_2 x_3 \dots x_p x_1 = e$$

et donc par récurrence on a bien l'identité
pour n'importe quelle permutation.

• $\bar{1} \cdot (x_1, \dots, x_p) = (x_1, \dots, x_p)$

• $(\bar{k} \bar{h}) \cdot (x_1, \dots, x_p) = \bar{k} \cdot (\bar{h} \cdot (x_1, \dots, x_p))$

G pas
forcément
abélien

ULMER

Comme le cardinal d'une orbite divise le
cardinal de $\mathbb{Z}/p\mathbb{Z}$, alors les orbites sont
de cardinal 1 ou p .

On d'après un lemme sur les points fixes
grâce à la formule des classes, on a que:

$$|X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| [p]$$

On $p \mid |X| = n^{p-1}$ car $p \mid n$ donc p divise le

nombre de points fixes.

On peut qu'un élément soit un point fixe, il faut qu'il reste inchangé par n'importe quelle permutation circulaire.

Le sont donc les éléments de la forme $(g, \dots, g)$ avec $g^p = e$

On $(e, \dots, e) \in X^{2p^2}$ donc il y a au moins $p > 1$ points fixes.

Donc il existe $g \neq e$ dans G tq $g^p = e$.

Donc il existe un élément d'ordre p .

DELCOURT

Prop • Soit G un groupe fini et p le plus petit nombre premier divisant $|G|$. Alors tout sous-groupe H d'indice p est distingué dans G .

Dém: on considère l'action de G sur G/H par translation or H est un sous-groupe d'indice p .

On a alors un morphisme de groupes

$$\ell: G \rightarrow S(G/H).$$

$$\text{Car } [G:H] = |G/H| = p, \quad S(G/H) \cong S_p.$$

$$\text{On } \text{Ker}(\ell) = \{g \in G; g \cdot (xH) = xH \quad \forall x \in G\}$$

$$\text{donc } \text{Ker}(\ell) = \bigcap_{x \in G} \text{Stab}(xH)$$

$$\text{On } H = \text{Stab}(eH) \text{ donc } \text{Ker}(\ell) \subset H.$$

On d'après le 1^{er} théorème d'isomorphisme, $G/\text{Ker}(\ell)$ est isomorphe à un sous-groupe de S_p .
Ainsi l'indice de $\text{Ker}(\ell)$ divise $p!$.

Mais l'indice de $\text{Ker}(\ell)$ divise aussi $|G|$.

Ainsi $[G:\text{Ker}(\ell)] = 1$ ou p (car p est le seul nb premier commun aux deux cardinaux).

On $\text{Ker}(\ell) \subset H$ donc son indice dans G est

G/H n'est pas forcément un groupe
(car on ne sait pas encore que H est distingué)

Supérieur à celui de H .

Donc $\text{Ker}(e) \subset H$ et ont le même indice dans G , donc $H = \text{Ker}(e)$.

Donc H est distingué dans G .

Corollaire: Tout sous-groupe d'indice 2 est distingué.

On peut le montrer directement car alors il y a 2 classes à gauche: H et xH ou $x \notin H$.

Mais il y a aussi 2 classes à droite:

H et Hx . Or $0 \leq 2$: $G = H \cup xH = H \cup Hx$.

Donc $xH = Hx$. Donc H est distingué dans G .

Remarque: avoir une idée des théorèmes de Sylow qui généralisent le théorème de Cauchy.

Def: Soit G groupe fini de cardinal $n = p^h m$ où p est premier et $\text{pgcd}(p, m) = 1$. On appelle alors p -Sylow de G un sous-groupe d'ordre p^h .

Théorème: Soit G groupe fini de card $n = p^h m$ où p est premier et $p \nmid m = 1$. Alors G contient au moins un p -Sylow.

DELCOURT

Ainsi sous les hypothèses du théorème de Cauchy, on a au moins un p -Sylow. Dans celui-ci, on prend un élément différent de e . Il engendre alors un groupe cyclique d'ordre une puissance de p (p^2), qui contient un élément d'ordre p (prendre $x^{p^{h-1}}$).