# Cours 5

Terminologies $G \curvearrowright X$ (action) i.e. $\varphi : G \to \mathfrak{S}_X$

**Déf** • l'action est **transitive** si $\forall x, y \in X$

$$\exists g \in G \quad \text{tq} \quad g.x = y$$

Autrement-dit, il n'y a qu'une seule orbite.

• l'action est **bitransitive** si $\forall (x_1, x_2), (y_1, y_2) \in X \times X$

$$\exists g \in G \text{ tq } \begin{cases} g.x_1 = y_1 \\ g.x_2 = y_2 \end{cases}.$$

**Exemples** • $G \curvearrowright G$ par la translation $\left|\begin{array}{l} \text{à droite} \\ \text{à gauche} \end{array}\right.$ est une action transitive.

• $X = \mathbb{A}^n_{\mathbb{R}}$ un espace affine avec direction $V = \mathbb{R}^n$

$V \curvearrowright X$ par translation

cette action est transitive, mais pas bi-transitive

• $G = \mathbb{R}^n \rtimes GL_n(\mathbb{R})$ le groupe des transformées affines

($\mathbb{R}^n$ : translations ; $GL_n(\mathbb{R})$ : transformée linéaire)

$G \curvearrowright \mathbb{A}^n_{\mathbb{K}}$ par transformées affine

cette action est bi-transitive.

- $G = PGL_2(\mathbb{K}) \curvearrowright \mathbb{P}^1_{\mathbb{K}} := \dfrac{\mathbb{K}^2 \setminus \{(0,0)\}}{\mathbb{K}^\times}$

(Rappel un élément de $\mathbb{P}^1_{\mathbb{K}}$ représenté par $(x,y)$ est noté $[x:y]$)

l'action définie par :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot [x:y] := [ax+by : cx+dy]$$

Cette action ~~est~~ bi-transitive.

En effet, on a mieux : $\forall P, Q, R \in \mathbb{P}^1_{\mathbb{K}}$ distincts

$\exists ! g \in PGL_2(\mathbb{K})$

tq $g.P = [0:1] = "\infty"$

$g.Q = [1:0] = "0"$ (*)

$g.R = [1:1] = "1"$

Rappel : $\forall P, Q, R, W$ le birapport

$[P,Q,R,W] := g(W)$ où $g$ est déterminé par (*)

**Déf** (fidélité)

Une action $G \curvearrowright X$ donnée par $\rho : G \longrightarrow \mathfrak{S}_X$ est dite **fidèle** si $\ker(\rho) = \{e_G\}$.

Autrement-dit, $\forall\, e_G \neq g \in G$ agit non-trivialement sur $X$.

**Non Ex :** $G \curvearrowright X$ l'action triviale n'est pas fidèle (sauf si $G = \{e\}$).

**Ex :** $G \curvearrowright G$ par conjugaison : $\rho : G \to \mathrm{Aut}(G)$

l'action est fidèle $\iff Z(G) = \{e\}$.

**Rq :** Soit $G \curvearrowright X$ une action.

donnée par $\rho : G \longrightarrow \mathfrak{S}_X$.

Alors on a une action **fidèle** de $G/\ker(\rho)$ sur $X$

# Applications d'action de groupe

**Thm** (Cayley) "tout gp est un sous-gp de $\mathfrak{S}_X$"

(i) Soit $G$ un groupe, alors on a un morphisme injectif

$$G \hookrightarrow \mathfrak{S}_G$$

(ii) Si $G$ est fini, alors $G$ est un sous-gp de $\mathfrak{S}_n$ avec $n \geq |G|$.

**Preuve** : $f\ell : G \longrightarrow \mathfrak{S}_G$

$$g \longmapsto \left( f_{\ell(g)} : G \longrightarrow G,\ h \longmapsto g.h \right)$$

est un morphisme injectif.

□

**Déf** ($p$-groupe). Soit $p$ un nombre premier. Un groupe fini $G$ est un $p$-groupe si $|G|$ est une puissance de $p$.

- Un $p$-sous-gp d'un gp $G$ est un sous-gp qui est un $p$-gp.

**Déf** Soit $G$ un groupe fini, $p$ = nb premier

On écrit $|G| = p^r m$ avec $p \nmid m$.

Un **$p$-Sylow** de $G$ est un $p$-sous-gp $H$

avec $|H| = p^r$.

**Lemme** Soit $G$ un $p$-gp (non-trivial), $|G| := p^r$

alors $Z(G) \neq \{e\}$.

**Preuve :** On considère l'action de $G$ sur $G$ par conjugaison,

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto \varphi_g := g \cdot - \cdot g^{-1} \end{aligned}$$

On regarde la **décomposition en orbites**.

$$G = \bigsqcup_i \mathcal{O}_i$$

par la **relation orbite - stabilisateur** :

$$|\mathcal{O}_x| = |G| / |\mathrm{Stab}_G(x)| \quad \text{est une puissance de } p.$$

en particulier $p \mid |\mathcal{O}_x|$ ou $\mathcal{O}_x = \{x\}$.

Or on a au moins une orbite de cardinal 1

à savoir $\{e_G\}$

$\Rightarrow \exists$ une autre orbite de cardinal 1

( Sinon, $|G| = 1 +$ (divisible par $p$) contradiction ! )

On le note $\{x\}$. $(x \neq e_G)$

$\Rightarrow \forall g \in G, \quad gxg^{-1} = x$

$\Rightarrow e_G \neq x \in Z(G)$.

$\Rightarrow Z(G) \neq \{e_G\}$.

Cor $Z(G)$ est un sous-$p$-gp abélien non-trivial.

Thms de Sylow Soit $G$ un gp fini, $p$ = nb premier

On écrit $|G| = p^r m$, avec $p \nmid m$.

(i) $\exists$ un $p$-Sylow

(ii) Deux $p$-Sylow sont conjugués.

(iii) $n_p :=$ nb de $p$-Sylow., alors

$$\begin{cases} n_p \equiv 1 \pmod p \\ n_p \mid m \end{cases}$$

**Preuve** Si $G$ est un $p$-gp, rien à démontrer.
On suppose donc $m > 1$.

(i) On considère $\mathcal{S} := \{ S \subset G \mid |S| = p^r \}$.

$$|\mathcal{S}| = \binom{p^r m}{p^r} \equiv \binom{m}{1} = m \pmod{p}$$

On considère l'action de $G$ sur $\mathcal{S}$ par translation à gauche :

$$g \cdot S := \{ gx \mid x \in S \} \in \mathcal{S}$$

On considère la décomp en orbites.

$$\mathcal{S} = \bigsqcup_i \mathcal{O}_i$$

$$\Rightarrow |\mathcal{S}| = \sum_i |\mathcal{O}_i| \equiv m \pmod{p}$$

Comme $p \nmid m$, $\exists$ une orbite $\mathcal{O}$ tq $p \nmid |\mathcal{O}|$.

Par la relation Stabilisateur-orbite on a $|\mathcal{O}| = |G| / |\mathrm{Stab}_G(S)|$ avec $S \in \mathcal{O}$.

$$\Rightarrow p \nmid [G : \mathrm{Stab}_G(S)] = \frac{|G|}{|\mathrm{Stab}_G(S)|}$$

$\Rightarrow p^r \mid \mid \mathrm{Stab}_G(S) \mid$

car $|S| = p^r < p^{r_m} = |G|$

De plus $\mathrm{Stab}_G(S) \subsetneq G$ car $S \subsetneq G$.

(Raison : On choisit $x \in S$, $y \notin S$
alors $g := yx^{-1}$ envoie $x$ à $y$
donc $g \notin \mathrm{Stab}_G(S)$.)

Par récurrence sur $|G|$
$\exists$ un $p$-Sylow de $\mathrm{Stab}_G(S)$, qui est aussi un $p$-Sylow de $G$.

(ii) Soient $P, Q$ deux $p$-Sylow de $G$.
$|P| = |Q| = p^r$.

On considère l'action de translation à gauche de $Q$ sur $G/P$ :

$$Q \times G/P \longrightarrow G/P$$
$$(q, gP) \longmapsto qgP$$

$$\mathrm{Stab}_Q(gP) = \{ q \in Q \mid qgP = gP \}$$
$$= \{ q \in Q \mid g^{-1}qg \in P \}$$
$$= gPg^{-1} \cap Q$$

Decomp. en orbites : $G/P = \bigsqcup_i \mathcal{O}_i$.

$$m = |G/P| = \sum_i |\mathcal{O}_i|$$

Comme $p \nmid m$, $\exists$ une orbite $\mathcal{O}$ avec $p \nmid |\mathcal{O}|$.

Relation orbite-Stabilisateur :

$$|\mathcal{O}| = \frac{|Q|}{|\mathrm{Stab}_Q(gP)|} = \frac{|Q|}{|gPg^{-1} \cap Q|}.$$

$p \nmid |\mathcal{O}| \Rightarrow |\mathcal{O}| = 1 \Rightarrow gPg^{-1} \cap Q = Q$.

$\Rightarrow Q = gPg^{-1}$ est un conjugué de $P$.

(iii) $n_p := |\{ p\text{-Sylow de } G \}| = |S|$

On considère l'action de conjugaison de $G$ sur

$$S := \{ p\text{-Sylow de } G \}.$$

Plus précisément

$$G \times \mathcal{S} \longrightarrow \mathcal{S}$$
$$(g, P) \longmapsto gPg^{-1}$$

Par (ii), c'est une action transitive !

(i.e. Il n'y a qu'une seule orbite $\mathcal{S}$)

Par la relation Stabilisateur-orbite :

$$n_p = |\mathcal{S}| = \frac{|G|}{|Stab_G(P)|}.$$

$$Stab_G(P) = \{ g \in G \mid gPg^{-1} = P \} = N_G(P)$$

$P \lhd N_G(P)$.

$\Rightarrow n_p = [G : N_G(P)] \mid [G : P] = m$.

$\Rightarrow n_p \mid m$.

On considère $P$ agit sur $\mathcal{S} = \{p\text{-Sylow}\}$ par conjugaison. $|\mathcal{S}| = n_p$.

Décomposition en orbites :

$$|\mathcal{S}| = \sum_{i} |\mathcal{O}_i|$$

Relation stabilisateur-Orbites $|\mathcal{O}_i| = \frac{|P|}{|Stab_P(Q)|}$, $\forall Q \in \mathcal{O}_i$

$$Stab_P(Q) = \{ g \in P \mid gQg^{-1} = Q \}$$
$$= N_G(Q) \cap P$$

Si $\mathrm{Stab}_P(Q) = P$, alors $P \subset N_G(Q)$

or $Q \lhd N_G(Q)$

$\Rightarrow$ $P, Q$ sont des $p$-Sylow de $N_G(Q)$

Thm Sylow (iii) $\Rightarrow$ $P, Q$ sont conjugués dans $N_G(Q)$

$Q \lhd N_G(Q) \Rightarrow P = Q$.

<u>ccl</u> : Si $Q \neq P$, alors $\mathrm{Stab}_P(Q) \subsetneq P$.

Donc $p \Big| \dfrac{|P|}{|\mathrm{Stab}_P(Q)|} = |\mathcal{O}_Q|$

$\Rightarrow$ $n_p = |\mathcal{P}| \equiv |\mathcal{O}_P| \pmod p$

$\{P\}$

$\Rightarrow$ $n_p \equiv 1 \pmod p$.

□

## Preuve alternative du Thm de Sylow

<u>Prop clé</u> Si $H$ est un sous-gp de $G$ (fini).

Si $P$ est un $p$-Sylow de $G$

alors $\exists\, g \in G$ tq $H \cap gPg^{-1}$ est un $p$-Sylow de $H$.

En particulier, $G$ admet $p$-Sylow $\Rightarrow$ $H$ admet $p$-Sylow.

Preuve : On considère l'action de translation de $H$ sur $G/P$.

$$H \times G/P \longrightarrow G/P$$
$$(h, gP) \longmapsto hgP$$

$$\mathrm{Stab}_H(gP) = \{h \in H \mid hgP = gP\} = \{h \in H \mid g^{-1}hg \in P\}$$
$$= H \cap gPg^{-1} < gPg^{-1} \text{ donc un } p\text{-gp}.$$

Relation orbite-stabilisateur $\Rightarrow$ $\dfrac{|H|}{|H \cap gPg^{-1}|} = |\mathcal{O}_{gP}|$.

comme $|G/P| = m$ qui n'est pas divisible par $p$.

$\exists$ une orbite $\mathcal{O}_{gP}$ avec $p \nmid |\mathcal{O}_{gP}|$.

$\Rightarrow \exists g \in G$, $p \nmid \dfrac{|H|}{|H \cap gPg^{-1}|}$ $\Rightarrow$ $H \cap gPg^{-1}$ est un $p$-Sylow de $H$.

□

## Preuve du Thm de Sylow :

Soit $p$ un nb premier
Soit $G$ un gp fini

Par Cayley, $G \hookrightarrow \mathfrak{S}_n$ pour certain $n \geq 1$.

Prop $\Rightarrow$ il suffit de trouver un $p$-Sylow de $\mathfrak{S}_n$.

On a un morphisme injectif

$$\mathfrak{S}_n \hookrightarrow GL_n(\mathbb{F}_p)$$

$$\sigma \longmapsto \left( \sigma : \mathbb{F}_p^n \xrightarrow{\sim} \mathbb{F}_p^n,\ e_i \longmapsto e_{\sigma(i)},\ i = 1, \dots, n \right)$$

Concretement, $(12) \mapsto \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & \\ & & & \ddots \end{pmatrix}$.

Prop $\Rightarrow$ il suffit de trouver un $p$-Sylow de $GL_n(\mathbb{F}_p)$.

Exemple de $p$-Sylow :

$$U_n(\mathbb{F}_p) := \left\{ \begin{pmatrix} 1 & * & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in GL_n(\mathbb{F}_p) \right\}$$

$$|U_n(\mathbb{F}_p)| = |\mathbb{F}_p^{1+2+\dots+(n-1)}| = |\mathbb{F}_p^{\frac{n(n-1)}{2}}| = p^{\frac{n(n-1)}{2}}$$

$$|GL_n(\mathbb{F}_p)| = \left(|\mathbb{F}_p^n| - 1\right)\left(|\mathbb{F}_p^n| - |\mathbb{F}_p^1|\right)\left(|\mathbb{F}_p^n| - |\mathbb{F}_p^2|\right) \cdots \left(|\mathbb{F}_p^n| - |\mathbb{F}_p^{n-1}|\right)$$

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

$$= p^0 \cdot p^1 \cdots p^{n-1} \cdot m \quad \text{avec } p \nmid m.$$

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

$\Rightarrow U_n(\mathbb{F}_p)$ est un $p$-Sylow de $GL_n(\mathbb{F}_p)$. $\square$

# Chapitre 2 Anneaux et Algèbres

**Déf** Un anneau est un groupe abélien $(A, +, 0)$ muni d'une loi de multiplication

$$\cdot : A \times A \longrightarrow A$$

tq (i) (Associativité) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) (Distributivités)

$$\begin{cases} a \cdot (b+c) = a \cdot b + a \cdot c \\ (b+c) \cdot a = b \cdot a + c \cdot a \end{cases}$$

$(\Rightarrow \quad 0 \cdot a = a \cdot 0 = 0)$

On dit que $A$ est <u>unitaire</u> si

(iii) $\exists\, 1 \in A$ tq $1 \cdot a = a \cdot 1 = a \quad \forall a \in A$.

(s'il existe, c'est unique).

On dit que $A$ est <u>commutatif</u> si

$a \cdot b = b \cdot a \quad \forall a, b \in A$.

**Déf.** Un <u>morphisme d'anneaux</u> est un morphisme de gp abélien $f : A \to B$ tq $f(ab) = f(a) f(b)$

$\forall a, b \in A$.

Convention Si $A$, $B$ sont des anneaux unitaires alors on suppose toujours qu'un morphisme d'anneaux entre $A$ et $B$ préserve 1

i.e. $f(1_A) = 1_B$.

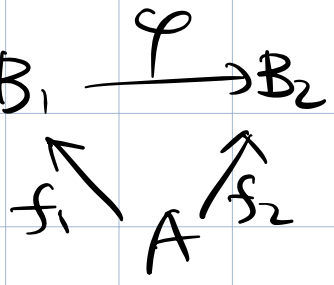
Exercice : Définir la notion d'anneau en utilisant des diagrammes commutatifs (sans parler d'élément).
(Cf. cours 1 en théorie de groupes)

Déf. Si on a un morphisme d'anneaux $A \xrightarrow{f} B$ on dit que $B$ est une A-algèbre.

- Soient $A \xrightarrow{f_1} B_1$ et $A \xrightarrow{f_2} B_2$ deux $A$-algèbres

Un morphisme de $A$-algèbres entre $B_1$ et $B_2$ est un morphisme d'anneaux $B_1 \xrightarrow{\varphi} B_2$ tq $\varphi \circ f_1 = f_2$

i.e.




Commute.

**Déf** (Algèbre à division)

Soit $A \neq 0$ un anneau unitaire.

On dit que $A$ est une algèbre à division si $\forall\, a \neq 0$ dans $A$ $\exists\, b \in A$

tq $ab = ba = 1_A$.

On note $b := a^{-1}$.

**Déf** (Idéaux) Soit $A$ un anneau

Un idéal | à gauche / à droite / bilatère | de $A$ est un ss-gp $I$ de $A$

tq $\forall a \in A$, $x \in I$, on a | $a \cdot x \in I$. / $x \cdot a \in I$ / $a \cdot x \in I$, $x \cdot a \in I$

**Rappel** (Quotient) soit $I$ un idéal bilatère de $A$ alors le gp abél. $A/I$ admet une structure d'anneau naturellement hérité de $A$ :

- $\cdot : A/I \times A/I \longrightarrow A/I$.

$(a+I, b+I) \longmapsto ab+I$.

ou $[a]$

Cl est bien-définie.

**Déf** Un anneau intègre est un anneau commutatif unitaire $A$ tq $A$ n'admet pas de diviseur de zéro non nul :

c-à-d : $\forall x, y \in A$ avec $x \cdot y = 0$

on a $x=0$ ou $y=0$.

**Déf** Un corps est une algèbre à division commutative.

Cl-à-d. un anneau commutatif unitaire $A$ tq

$\forall x \neq 0 \in A \quad \exists\, y \in A$ tq $xy = 1$.

**Exemples**

- $0$
- $\mathbb{Z}$, tout anneau unitaire est canoniquement une $\mathbb{Z}$-algèbre
- $\mathbb{Z}/n\mathbb{Z}$ ann. comm.
- Corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_q$ $(q = p^n)$.

- $A$ = anneau. (commutatif)

  $A[X_1, \dots, X_n]$ est une $A$-algèbre (commutatif)

  $A\langle X_1, \dots, X_n \rangle$ est une $A$-algèbre

  $A[[X_1, \dots, X_n]]$ = = séries formelles à coeff dans $A$.
  est une $A$-algèbre (commutatif)

- $A$ = anneau.

  $M_n(A)$ est un anneau, non-commutatif
  (même si $A$ comm.)

- $V$ = $\mathbb{k}$-espace vectoriel

  $\mathrm{End}(V)$ est une $\mathbb{k}$-algèbre.

(Plus généralement, soit $X$ un objet dans une catégorie additive (e.g. - gp abéliens
- espaces vectoriels
- modules
- faisceaux
⋮)
alors $\mathrm{End}(X)$ est un anneau.)