

## 104: Groupe fini. Exemples et applications

### I- Généralités sur les groupes finis

#### 1) Notion d'ordre [Ber] 130 146 137 151

- def ordre groupe et éléments
- classe à gauche
- Th Lagrange
- def ss groupe distingué
- conséquence Lagrange

#### 2) Action de groupe [Ber] 171 174 178 [Rom] 21

- def action, orbite, stabilisateur
- équation aux classes

### II- Un groupe fini abélien $\mathbb{Z}/n\mathbb{Z}$

#### 1) Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et cyclicité [Rom] 13 16 18

- def monogène cyclique
- ss groupe de  $\mathbb{Z}/n\mathbb{Z}$
- application groupe d'ordre  $p^2$

#### 2) Théorème de structure [Ber] 483 366

- Th Chinois
- Th structure

#### 3) $(\mathbb{Z}/n\mathbb{Z})^\times$ [Ber] 504

- def card

### III- Groupes finis non abélien

#### 1) $S_n$ [Ber] 201 179 208 216 140

- def

- Cayley
- ordre
- permutation
- générateurs de  $S_n$
- $A_n$  + générateurs de  $A_n$
- $A_n$  simple 217

DEV1

## 2) Probabilité de commutativité

DEV2

- Th de Dixon

## 104: Groupe fini. Exemples et applications

### I- Généralités sur les groupes finis

#### 1) Notion d'ordre

Définition 1: si  $G$  est un groupe fini, son nombre d'éléments  $|G|$  est fini et est appelé l'ordre de  $G$

Exemple 2:  $S_n$  est d'ordre  $n!$

$\mathbb{Z}/n\mathbb{Z}$  est d'ordre  $n$

Théorème 3: Soit  $G$  un groupe et  $H$  un sous-groupe. Pour tout  $a \in G$ , on note  $aH = \{aR \mid R \in H\}$ .

La relation  $\sim$  sur  $G$  définie par  $x \sim y \Leftrightarrow x^{-1}y \in H$  est une relation d'équivalence

Définition 4: Un ensemble de la forme  $xH$ ,  $x \in G$  est appelé classe à gauche modulo  $H$ . L'ensemble des classes à gauche modulo  $H$  est noté  $G/H$

Théorème 5 (Lagrange): Soit  $G$  un groupe fini, et soit  $H$  un sous-groupe de  $G$ . Alors, on a:

$$|G| = [G:H] \times |H|$$

avec  $[G:H] = |G/H|$  appelé indice.

En particulier  $|H|$  divise  $|G|$ .

Application 6: • si  $g \in G$ , alors l'ordre de  $g$  divise l'ordre de  $G$

• les sous-groupes de  $S_3$  sont:  $\{id\}$ ,  $\{id, (12)\}$ ,  $\{id, (13)\}$ ,  $\{id, (23)\}$ ,  $\{id, (123), (132)\}$ ,  $S_3$  de cardinaux respectifs 1, 2, 3 et 6

Définition 7: Soit  $G$  un groupe et  $H < G$ . On dit que  $H$  est distingué dans  $G$  si  $gRg^{-1} \in H \quad \forall R \in H \quad \forall g \in G$

Définition 8: Soit  $g \in G$ , l'ordre de  $g$  est  $o(g) = | \langle g \rangle |$

Corollaire 9: Conséquence de Lagrange:  $\forall g \in G \quad o(g) \mid |G|$

#### 2) Actions de groupes

Définition 10: Soit  $E$  un ensemble et  $G$  un groupe.

Une action à gauche de  $G$  sur  $E$  est une application

$$G \times E \rightarrow E \quad \text{vérifiant: } 1) \forall x \in E \quad 1_G \cdot x = x$$

$$(g, x) \mapsto g \cdot x$$

$$2) \forall g, g' \in G \quad \forall x \in E \quad g \cdot (g' \cdot x) = (gg') \cdot x$$

Remarque 11: Il est équivalent de se donner un morphisme de groupes de  $G$  dans  $S(E)$

Définition 12: L'ensemble  $\text{stab}_G(x) = \{g \in G \mid g \cdot x = x\}$  est appelé le stabilisateur de  $x$  sous l'action de  $G$ .

$$\text{stab}_G(x) < G$$

• Soit  $x \in E$ , l'ensemble  $O_x = \{g \cdot x \mid g \in G\} \subset E$  est appelé orbite de  $x$  sous l'action de  $G$ .

Théorème 13: Si  $G \curvearrowright E$ , soit  $x \in E$ . Si  $G$  fini, on a  $|O_x| = [G : \text{stab}_G(x)] = \frac{|G|}{|\text{stab}_G(x)|}$

En particulier  $|O_x| \mid |G|$

Théorème 14: (Equation aux classes)

Soit  $G$  un groupe fini agissant sur  $E$  fini. En notant  $O_1, \dots, O_r$  les orbites  $\neq \emptyset$  distinctes, on a:

$$|E| = \sum_{i=1}^r |O_i| = \sum_{i=1}^r \frac{|G|}{|\text{stab}_G(x_i)|}$$

Proposition 15: (Formule de Burnside) DEV 1) a)

Soit  $G \curvearrowright E$  tout deux finis. On note  $\Omega$  l'ensemble des orbites de  $E$  sous l'action de  $G$ . Alors on a

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| \text{ où } \text{Fix}(g) = \{x \in E \mid g \cdot x = x\}$$

II - Un groupe fini abélien  $\mathbb{Z}/n\mathbb{Z}$  1) Groupe  $\mathbb{Z}/n\mathbb{Z}$  et cyclique

Définition 16: On dit que  $G$  est (monogène) s'il existe un élément  $g \in G$  tel que  $G = \langle g \rangle$ .

Si de plus  $G$  est fini, on dit qu'il est cyclique

Théorème 17: Soit  $G$  un groupe cyclique d'ordre  $n$ . Alors  $G$  est isomorphe à  $(\mathbb{Z}/n\mathbb{Z}, +)$

Théorème 18: Si  $G = \langle g \rangle$  est cyclique d'ordre  $n$ , ses générateurs sont alors les  $g^k$ ,  $k \in [1, n-1]$  premiers avec  $n$ .  $G$  possède  $\varphi(n)$  générateurs avec  $\varphi$  l'indicatrice d'Euler

Théorème 19: Soit  $G = \mathbb{Z}/n\mathbb{Z}$  avec  $n \geq 2$ .  $\forall$  diviseur positif  $d$  de  $n$ ,  $\exists$  sous groupe d'ordre  $d$  de  $G$ .

$H = \langle \bar{q} \rangle$  où  $q = \frac{n}{d}$

Exemple 20:  $(\mathbb{Z}/10\mathbb{Z}, +) = \langle \bar{1} \rangle$  est cyclique d'ordre 10. Ses générateurs sont  $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ . Ses sous groupes:  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$ ,  $\mathbb{Z}/10\mathbb{Z}$  et  $\{0\}$

Théorème 21 (de Cauchy): Soit  $G$  commutatif fini d'ordre  $n \geq 2$ . Pour tout diviseur premier  $p$  de  $n$ , il existe dans  $G$  un élément d'ordre  $p$

## 2) Théorèmes de structure

Théorème 22: (Théorème Chinois) Soient  $n_1, \dots, n_r$  des entiers premiers entre eux  $\geq 2$ . Alors

$$\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z} \cong \mathbb{Z}/n_1 n_2 \dots n_r\mathbb{Z}$$

(admis)

Théorème 23: (Structure des groupes abéliens finis)

Soit  $G$  un groupe abélien fini.

Alors il existe des entiers  $d_1, \dots, d_s \geq 2$  vérifiant  $d_1 \mid d_2 \mid \dots \mid d_s$  tels que  $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

$$3) (\mathbb{Z}/n\mathbb{Z})^\times$$

Définition 24:  $(\mathbb{Z}/n\mathbb{Z})^\times$  est l'ensemble des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$ .

Proposition 25:  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$  inversible  $\Leftrightarrow a \wedge n = 1$

Lemme 26: Pour  $n \geq 2$   $|( \mathbb{Z}/n\mathbb{Z} )^\times| = \varphi(n)$

## II - Groupes finis non abéliens

### 1) Le groupe symétrique $S_n$

Définition 27: Le groupe des permutations  $S_n$  est l'ensemble des bijections de  $[1, n]$  dans  $[1, n]$ .

Un élément de  $S_n$  est appelé permutation.

$\text{Card } S_n = n!$

Théorème 28: (Caley) Soit  $G$  un groupe fini d'ordre  $n$ . Alors  $G$  est isomorphe à un sous-groupe de  $S_n$ .

Théorème 29: Toute permutation de  $S_n$  se décompose en produit de cycles ou produit de cycles à support disjoint

Théorème 30: L'ordre d'une permutation est la ppcm des longueurs des cycles à supports disjoints qui la compose

Théorème 31:  $S_n$  est engendré par les transpositions

Corollaire 32:  $S_n$  est engendré par chacune des familles suivantes:

- 1) les transpositions  $(i, i+1)$   $i \in [1, n-1]$
- 2) les transpositions  $(i, i+1)$   $i \in [1, n-1]$
- 3)  $\langle (12), (12 \dots n) \rangle$

Théorème 33: Soit  $n \geq 2$ . Alors il existe un unique morphisme  $\varepsilon: S_n \rightarrow \mathbb{C}^*$  non trivial. Si  $\sigma \in S_n$  s'écrit comme un produit de  $s$  transpositions, alors on a  $\varepsilon(\sigma) = (-1)^s$

On appelle ce morphisme, le morphisme signature

Définition 34: Le groupe alterné, noté  $A_n$ , est l'ensemble des permutations de  $S_n$  de signature 1. C'est un sous groupe distingué de  $S_n$ .

Proposition 35: Si  $n = 2$   $A_2$  est trivial, si  $n \geq 3$   $A_n$  est engendré par

- 1) les 3-cycles
- 2) les produits de 2 transpositions

Définition 36: Un groupe  $G$  est simple s'il n'a pas de sous-groupes distingués autres que  $\{Id\}$  et lui-même

Théorème 37: Pour  $n = 3$  ou  $n \geq 5$ ,  $A_n$  est simple.

DEV 2

2) Commutativité dans un groupe

Théorème 38: (Dixon) DEV 1) b)

Soit  $G$  un groupe fini d'ordre  $n$ , non abélien.

On note  $k$  le nombre de classe de conjugaison de  $G$   
 $p(G)$  la probabilité que 2 éléments de  $G$  tirés uniformément et indépendamment commutent

$$\text{Alors } p(G) = \frac{k}{n} \leq \frac{5}{8}$$

Notion de groupe  
omniprésente en mathématiques  
racines d'un polynôme  
...

→ + compliqué  
Non abélien  
Th de Dixon  
DEV2

Un simple  
DEV1

$S_n$  important avec le th de Cayley

104: Groupes finis  
Ex et applications

Abélien cyclique → facile  
 $\mathbb{Z}/n\mathbb{Z}$

Th de Structure

quotient distingué

info sur le card  
Lagrange

ordre des éléments d'un groupe

actions de groupe  
→ relation entre cardinaux  
→ info sur les groupes distingués

On a besoin d'outils

Motivations

- caractériser les groupes abéliens
- savoir les lister
- lois interne d'un groupe
- caractériser les groupes de Galois
- (+ facile avec les groupes abéliens)
- étudier des groupes connus d'ordre petit des familles de groupe fini