104 . Groupes abéliens et non abéliens finis

Dans cette leçon, G désigne un groupe <u>fini</u>. On supposera connues les notions de sous-groupe, morphisme de groupes, quotient, sous-groupe distingué, ... Eventuellement notat° $(G,\cdot)$ ou $(G,+)$ si abélien

I . Ordre

Déf ①: On appelle ordre de $(G,\cdot)$ son cardinal, noté $|G|$

Soit $x \in G$. On appelle ordre de x, noté $o(x)$, le plus petit entier $n>0$ tel que $x^n = 1$ (s'il existe).

Ex. ②: $\bar{1}$ est d'ordre n dans $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$

Th. ③ : (Lagrange)

Si H est un sous-groupe de G, alors $|G| = |H| \times |G/H|$

Coro ④: • $H \leq G \Rightarrow |H| \mid |G|$

• si $x \in G$, alors $o(x) \mid |G|$

Appli. ⑤: Si G est de cardinal p premier, alors G est cyclique

Déf. ⑥: On appelle exposant de G, noté $\exp(G)$, le plus petit entier $n>0$ tel que : $x^n = 1$ pour tout $x \in G$

Rq ⑦: $\exp(G)$ n'existe pas nécessairement pour un groupe infini !

Prop. ⑧: $\exp(G) = \mathrm{ppcm}(o(x), x \in G)$

En particulier, $\exp(G) \mid |G|$

Rq ⑨: On n'a pas nécessairement $\exp(G) = G$

voir : $\{(1,1)\ (-1,1)\ (1,-1)\ (-1,1)\} \subset (\mathbb{R}^*,\cdot)\times(\mathbb{R}^*,\cdot)$

II . Action d'un groupe sur un ensemble

Déf. ⑩: Soient G un groupe, X un ensemble. On dit que G agit sur X, noté $G \curvearrowright X$ s'il existe une application $\bullet : G\times X \to X$ telle que : $1.x = x$ pour tout $x \in X$

$(gg').x = g\cdot(g'.x)$ pour tout $g, g' \in G$ et $x \in X$

Ex ⑪: i) translation à gauche de G sur G : $g\cdot x = gx$

ii) conjugaison de G sur G : $g \cdot x = gxg^{-1}$

Th ⑫: L'ensemble des actions de G sur X est en bijection avec $\mathrm{Hom}(G, S(X))$ où $S(X)$ est l'ensemble des permutations de X

Th. ⑬ : (Cayley)

Si $|G| = n$, alors G est isomorphe à un sous-groupe de S_n

Déf. ⑭: Soit X un ensemble sur lequel G agit, et $x \in X$. On définit

. l'orbite de x par $\omega(x) = \{g\cdot x, g \in G\} \subset X$

. le stabilisateur de x par $\mathrm{Stab}(x) = \{g \in G, g\cdot x = x\} \subset G$

. $X^G = \{x \in X \mid \forall g \in G, g\cdot x = x\} \subset X$ l'ensemble des points fixes pour l'action

Prop. ⑮: Pour tout $x \in X$, $\mathrm{Stab}(x)$ est un sous-groupe de G.

De plus, l'application $G/\mathrm{Stab}(x) \longrightarrow \omega(x)$, $\bar{g} \longmapsto g\cdot x$ est une bijection

Prop. ⑯: La relation "être dans la même orbite" est une relation d'équivalence sur X.

Th. ⑰: (Equation aux classes)

Soit X un ensemble fini sur lequel agit G. On a alors

$$|X| = \underbrace{\sum_{x\in X}}_{\text{un } x \text{ dans chaque orbite}} \left|G/\mathrm{Stab}(x)\right| \underset{G \text{ fini}}{=} \sum_{\substack{x\in X\\(\dots)}} \frac{|G|}{|\mathrm{Stab}(x)|}$$

III . Groupes abéliens finis

1) Groupes cycliques

Prop. ⑱: G est cyclique d'ordre n si et seulement si $G \simeq \mathbb{Z}/n\mathbb{Z}$

Prop. ⑲: Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$. Alors $o(\bar{k}) = \dfrac{n}{\mathrm{pgcd}(k,n)}$ dans $\mathbb{Z}/n\mathbb{Z}$

Coro. ⑳: Soit G groupe fini et $x \in G$.

Alors pour tout $d \in \mathbb{N}$, $o(x^d) = \dfrac{o(x)}{\mathrm{pgcd}(d, o(x))}$

Prop (20bis): G abélien

i) $\langle x\rangle \cap \langle y\rangle = \{1\} \Rightarrow o(xy) = \mathrm{ppcm}(o(x), o(y))$

ii) $o(x) \wedge o(y) = 1 \Rightarrow o(xy) = o(x)o(y)$

Coro (20ter): G abélien fini $\Rightarrow \exists x \in G \mid o(x) = \exp(G)$

Prop (21) : Soit $n \geq 2$. Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont $\{\bar{k} \mid 0 \leq k \leq n-1 \text{ et } k \wedge n = 1\}$. Il y en a $\varphi(n)$ où φ désigne l'indicatrice d'Euler.

Prop. (22) : Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont exactement de la forme $\langle \frac{\bar{n}}{d} \rangle$ où $d \in \mathbb{N}^*$ et $d \mid n$

Th. (23) : (restes chinois)

Soient $a, b \in \mathbb{N}^*$. $\psi : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $x \bmod ab \longmapsto (x \bmod a, x \bmod b)$ est un morphisme d'anneaux bien défini.

De plus, ψ est un isomorphisme si et seulement si a et b sont premiers entre eux

Corollaire (24) : Soit $n \in \mathbb{N}, n \geq 2$. On note $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. Alors, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

2) Théorème de structure des groupes abéliens finis

Déf. (25) : Soit G un groupe abélien. On appelle caractère linéaire de G tout morphisme de groupes $\chi : G \to \mathbb{C}^*$.

On note $\hat{G}$ l'ensemble des caractères linéaires de G, qui est un groupe muni de la multiplication des fonctions

Th. (26) : (Lemme de prolongement des caractères)

Soit G un groupe abélien et H un sous-groupe de G.

Alors l'application $\rho_H : \hat{G} \to \hat{H}$, $\chi \mapsto \chi_{|H}$ est un morphisme de groupes de noyau canoniquement isomorphe à $\widehat{G/H}$

DVP 1

De plus, si $[G:H]$ est fini, alors ρ_H est surjectif

Th. (27) : (Structure des groupes abéliens finis)

Soit G un groupe abélien fini de cardinal $|G| \geq 2$

Alors il existe des entiers $d_1, \dots, d_s \geq 2$ où $d_1 \mid d_2 \mid \dots \mid d_s$ tels que

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$$

De plus, la suite $(d_1 \dots d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

Déf. (28) : Les entiers $d_1 \dots d_s$ du théorème 27 s'appellent les invariants de similitude de G.

Coro. (29) : Deux groupes abéliens finis sont isomorphes si et seulement si ils ont mêmes invariants de similitude

Coro. (30) : Soit G abélien, $|G| = p^n$ où p premier. Alors il existe des entiers $1 \leq r_1 \leq \dots \leq r_k$ tels que $G \simeq \prod_{i=1}^{k} \mathbb{Z}/p^{r_i}\mathbb{Z}$

Coro (31) : Soit G abélien fini.

Alors $G \simeq \prod_{p \in \mathcal{P}} \prod_{k \geq 1} \mathbb{Z}/p^{n_{p,k}}\mathbb{Z}$

où : $\mathcal{P}$ désigne l'ensemble des entiers premiers

. $n_{p,k}$ sont des entiers presque tous nuls, et uniques à isomorphisme près

. pour tout $p \in \mathcal{P}$, $(n_{p,k})_{k \geq 1}$ est une suite décroissante

Ex (32) :

i) $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/8\mathbb{Z}$

ii) $G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$

IV. Théorèmes de Sylow

1) p-groupes

Déf. (33) : Soit p un nombre premier. Un p-groupe est un groupe fini dont le cardinal est une puissance de p

Prop. (34) : Soit G un p-groupe agissant sur un ensemble fini X. Alors $|X| \equiv |X^G| \; [p]$.

Coro. (35) : Le centre d'un p-groupe non trivial est non trivial

Appli. (36) : Soit p un nombre premier et G un groupe d'ordre p^2. Alors, G est abélien.

Prop. (37) : Si $|G| = p^n$, p premier et $n \geq 1$, Alors pour tout $0 \leq k \leq n$, G admet un sous-groupe d'ordre p^k (Théorème de Cauchy admis)

Coro 38 : Soit G un groupe abélien fini de cardinal $n \geq 1$. Alors pour tout $d | n$, G admet un sous-groupe d'ordre d.

Rq. 39 : FAUX si G n'est pas abélien !

2) Théorème de Sylow

Déf. 40 : Soit G un groupe fini de cardinal $p^m q$ où p premier, $m, q \in \mathbb{N}^*$ et $p \nmid m$. Un sous-groupe H de G est appelé p-Sylow de G si $|H| = p^\alpha$.

Lemme 41 : Soit G un groupe fini avec $|G| = p^m q$, $m \geq 0$, $p \nmid q$ et H un sous-groupe de G. On suppose que G admet un p-Sylow S. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ est un p-Sylow de H.

DVP 2

Th. 42 : (Sylow)
Si $|G| = p^m q$, $m \geq 0$ et $p \nmid q$, alors
i) G admet (au moins) un p-Sylow
ii) Si H est un p-sous-groupe de G, il existe S un p-Sylow tel que $H \subset S$
iii) Les p-Sylow sont conjugués
iv) Si n_p est le nombre de p-Sylow, alors $n_p \equiv 1\ [p]$ et $n_p | q$

Appli. 43 : Un groupe de cardinal 63 n'est pas simple

IV. Groupe symétrique $n \in \mathbb{N}, n \geq 2$

On rappelle que pour tout ensemble X, $S(X)$ désigne les bijections de X dans X, et que si $|X| = n$, $S(X) \simeq S_n$ où $S_n = S(\{1 \ldots n\})$.
On supposera connues les définitions de cycle, transposition, support.

1) Générateurs de S_n

Prop. 44 : Soit $1 \leq k \leq n$. Un k-cycle est d'ordre k dans S_n

Prop. 45 : Deux cycles à support disjoints commutent

Prop. 46 : Soient $\sigma \in S_n$, $(a_1 \ldots a_p)$ un p-cycle. Alors
$$\sigma (a_1 \ldots a_p) \sigma^{-1} = (\sigma(a_1) \ldots \sigma(a_p))$$

Th. 47 : Toute permutation $\sigma \in S_n$ se décompose en un produit de cycles à support disjoint. Cette décomposition est unique à l'ordre des facteurs près.

Prop. 48 : Les systèmes suivants engendrent S_n :
i) les transpositions
ii) les transpositions $(1\ i)$ où $2 \leq i \leq n$
iii) les transpositions $(i\ i+1)$ où $1 \leq i \leq n-1$
iv) $(1\,2)$ et $(1\,2 \ldots n)$

2) Groupe alterné A_n

Déf./Prop. 49 : Il existe un unique morphisme de groupes surjectif $\varepsilon : S_n \to \{\pm 1\}$ appelé morphisme signature.
De plus, ε vaut -1 sur les transpositions

Déf. 50 : On note $A_n = \ker \varepsilon$ le groupe alterné d'ordre n

Ex. 51 : $A_2 = \{1\}$, $A_3 = \{1, \sigma, \sigma^2\}$ où $\sigma = (123)$

Th. 52 : Pour $n \geq 3$, A_n est engendré par les 3-cycles

Lemme 53 : Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n

Th. 54 : A_n est simple pour $n \geq 3$ et $n \neq 4$.

Prop. 55 : A_5 est l'unique groupe simple d'ordre 60 (à isomorphisme près)