Chap 23 : Quelques compléments sur les groupes

$(G,\cdot)$ désignera un groupe

I. Groupes monogènes, cyclique, ordre d'un élément

$a \in G \quad \theta_a \begin{cases} (\mathbb{Z},+) & \to (G,\cdot) \\ n & \mapsto a^n = \begin{cases} \overbrace{a\cdot\ldots\cdot a}^{n \text{ fois}} & \text{si } n>0 \\ e & \text{si } n=0 \\ \overbrace{a^{-1}\cdot\ldots\cdot a^{-1}}^{|n| \text{ fois}} & \text{si } n<0 \end{cases} \end{cases}$ est un morphisme de groupe de $(\mathbb{Z},+)$ dans $(G,\cdot)$

$\mathrm{Im}(\theta_a)=\{a^n, n\in\mathbb{Z}\}$ est un sous groupe engendré par a : on le note $<a>=\{a^n, n\in\mathbb{Z}\}$

On dit que G est monogène s'il existe $a\in G$ tel que $G=<a> \Leftrightarrow \theta_a$ surjectif

$\ker(\theta_a)$ est un sous groupe de $\mathbb{Z}$: $\ker\theta_a=\alpha\mathbb{Z}$ avec $\alpha\in\mathbb{Z}$

* Si θ_a injectif, $\alpha=0$
* Sinon, $\alpha\in\mathbb{N}^*$

Si θ_a n'est pas injectif, on dit que a est d'ordre fini. On définit $ord(a)=\alpha\in\mathbb{N}^*$ tel que $\ker\theta_a=\alpha\mathbb{Z}$

$$\mathrm{ord}(a)=\min\{k\in\mathbb{N}^*, a^k=e\}$$

$a\in G$ d'ordre n $\quad \overline{\theta_a}\begin{cases} \mathbb{Z}/n\mathbb{Z} & \to <a>\subset G \\ \bar{k} & \mapsto a^k \end{cases}$ est un isomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ dans $<a>$

Si a est d'ordre n, $<a>=\{a^k, k\in[\![0,n-1]\!]\}$ et $card(a)=n$

Un groupe cyclique est un groupe monogène et fini : $\mathrm{card}\,G$ est l'ordre du groupe G

Tout sous-groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$

Pour tout $x\in G$, $\mathrm{ord}(x)\,|\,\mathrm{ord}(G)$ $\qquad$ Si $x=a^k$, $\mathrm{ord}(x)=\dfrac{n}{k\wedge n}$

II. Résultats plus généraux sur les groupes finis

(Plus on avancera dans cette partie, plus on s'éloignera du programme)

$(G,\cdot)$ groupe fini de cardinal n

Pour tout H sous groupe de G, $\mathrm{card}\,H\,|\,\mathrm{card}\,G$

Preuve : $\mathfrak{R} : (x\mathfrak{R}y) \Leftrightarrow x\in yH$ est une relation d'équivalence

Les classes d'équivalences pour $\mathfrak{R}$ ont toutes le cardinal de H

Elles sont en union disjointe dans G : $\mathrm{card}\,H\,|\,\mathrm{card}\,G$

Théorème de Lagrange : $a \in G$ avec G fini de cardinal n $\quad a^n = e$

Soit φ morphisme de groupes de G dans G' : $\quad \operatorname{card} G = \operatorname{card}(\ker \varphi) \times \operatorname{card}(\operatorname{Im} \varphi)$

Preuve : $H_0 = \ker \varphi$ $\quad$ On pose $G/H_0 = \{\overline{x}, x \in G\} = \{$classes d'équivalences de $\mathfrak{R}$ pour $H_0\}$

On montre $a \cdot H_0 = H_0 \cdot a$: $\quad x \in \ker \varphi, \varphi(a \cdot x \cdot a^{-1}) = \varphi(a) \cdot \varphi(x) \cdot \varphi(a^{-1}) = e \Rightarrow a \cdot x \cdot a^{-1} \in \ker \varphi$

On en déduit que si $x\mathfrak{R}x'$ et $y\mathfrak{R}y'$, alors $xy\mathfrak{R}x'y'$ et $\overline{xy} = \overline{x'y'}$ $\quad$ (Car $xy = x'h_1y'h_2 = x'y'h_1'h_2$)

On définit une lci $\cdot$ sur G/H_0 : $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$: $\quad (G/H_0, \circ)$ est un groupe

On construit un unique $\overline{\varphi} : G/H_0 \to G'$ tel que pour tout $x \in G, \overline{\varphi}(\overline{x}) = \varphi(x)$

On vérifie qu'il existe et que c'est un isomorphisme de groupes dans $\operatorname{Im} \overline{\varphi}$

$\operatorname{card} G/H_0 = \operatorname{card}(\operatorname{Im} \varphi)$ $\quad \operatorname{card}(G) = \operatorname{card}(H_0) \operatorname{card}(G/H_0) = \operatorname{card}(\ker \varphi) \operatorname{card}(\operatorname{Im} \varphi)$

Si, pour H sous-groupe de G, et pour tout $a \in G$, $a \cdot H = H \cdot a$, on dit que H est distingué

III. Retour sur les groupes cycliques (et au programme)

Rappel : $(\mathbb{Z}/n\mathbb{Z})^* = \{$inversibles de $\mathbb{Z}/n\mathbb{Z}\} = \{\overline{k}, \ k \wedge n = 1\}$

Pour tout $n \in \mathbb{N}^*$, on définit la caractéristique d'Euler : $\varphi(n) = \operatorname{card}((\mathbb{Z}/n\mathbb{Z})^*) = \operatorname{card}\{k \in [\![0, n-1]\!], k \wedge n = 1\}$

Pour tout p premier, $\varphi(p) = p - 1$

Pour tout $(m,n) \in \mathbb{N}^2$ tels que $m \wedge n = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$

Preuve : Lemme chinois : $\mathbb{Z}/mn\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ si $m \wedge n = 1 \Rightarrow$ $\quad$ isomorphisme

G et H deux groupes cycliques $\quad G \times H$ est cyclique *ssi* $\operatorname{card} G \wedge \operatorname{card} H = 1$

Preuve : Mq $\operatorname{ord}(a,b) = \operatorname{ord}(a) \vee \operatorname{ord}(b)$ *Si* $m \wedge n \neq 1 \Rightarrow$ pas d'élément d'ordre mn $\quad$ non cyclique

IV. Groupe symétrique

$n \in \mathbb{N}^*$ $\quad \mathfrak{S}_n = \{$permutations de $[\![1, n]\!]\} = \{f$ bijective de $[\![1, n]\!]$ dans $[\![1, n]\!]\}$

$(\mathfrak{S}_n, \circ)$ est un groupe de cardinal $n!$

$\sigma \in \mathfrak{S}_n$ $\quad$ Pour tout $(x, y) \in [\![1, n]\!]^2$, on dit que $x\mathfrak{R}y$ s'il existe $k \in \mathbb{Z}, x = \sigma^k(z)$

$\mathfrak{R}$ est une relation d'équivalence. L'orbite d'un élément $x \in [\![1, n]\!]$ est la classe d'équivalence de x

$orb(x) = \{\sigma^k(x), k \in \mathbb{Z}\} = \{x, \sigma(x), \ldots \sigma^{d-1}(x)\}$ avec $d = \operatorname{ord}(x)$

Un cycle est une permutation σ de $\mathfrak{S}_n$ qui a une unique orbite non réduite à un point

On note $\sigma = (x_1, \sigma(x_1) \ldots \sigma^k(x_1))$

On appelle support du cycle l'orbite unique non réduite à un point de σ

$\sigma,\tau \in \mathfrak{S}_n$ deux cycles à supports disjoints. On a alors $\sigma\circ\tau=\tau\circ\sigma$

Soit $\sigma \in \mathfrak{S}_n$ Il existe $\sigma_1 ... \sigma_p \in \mathfrak{S}_n$ des cycles à supports 2 à 2 disjoints tels que :

$\sigma=\sigma_1\circ...\circ\sigma_p$ cette décomposition est unique à l'ordre près

Preuve : Existence : on considère les orbites non réduites à un point $\Rightarrow$ 2 à 2 disjointes...

Unicité : on suppose qu'on en a une autre : $\sigma=\tau_1\circ...\circ\tau_p$ On considère leurs orbites

On distingue à chaque fois le cas où l'orbite de x n'est pas réduite à un point de celui où elle l'est

On montre que les cycles des τ_j obt pour support les orbites $\Rightarrow$ comme les σ_j

On appellera $p-cycle$ un cycle dont le support a p éléments ($p\geq 2$)

On appellera transposition les $2-$cycles : $\tau=(i,j)=(j,i)$ avec $j,i\in[\![1,n]\!]$ et $j\neq i$

$\sigma=(a_1...a_p)\Leftrightarrow\sigma^{-1}=(a_p,a_{p-1},...a_1)$

On dit que σ inverse i et j si $i<j$ et $\sigma(i)>\sigma(j)$

Soit $\sigma=(a_1...a_p)\in\mathfrak{S}_n$ un $p-cycle$. Soit $\tau\in\mathfrak{S}_n$ $\tau\circ\sigma\circ\tau^{-1}=(\tau(a_1),...,\tau(a_p))$

Les transpositions engendrent $\mathfrak{S}_n$: Toute permutation s'écrit comme produit de transpositions (non unique)

Preuve : Récurrence sur n : montrer le cas où $\sigma(n+1)=n+1$, puis s'y ramener avec une transposition dans le cas général

Soit $\sigma\in\mathfrak{S}_n$ La signature de σ : $\varepsilon(\sigma)=\displaystyle\prod_{(i,j)\in\mathbb{N}^2}\frac{\sigma(i)-\sigma(j)}{i-j}$

$\varepsilon(\sigma)\in\{-1,1\}$ et $\varepsilon(\sigma)=(-1)^{N_0}$ où N_0 est le nombre d'inversions de σ

Preuve : $\{i,j\}\mapsto\{\sigma(i),\sigma(j)\}$ bijection de $\mathcal{P}_2(\mathbb{N}_n)$. Valeur absolues $\Rightarrow$ dissociation dividende/diviseur

$\Rightarrow|\varepsilon(\sigma)|=1$ + Le signe change quand dividende et diviseur sont de signes $\neq$

ε est un morphisme de groupes (Preuve : comme la dérivation composée + bijectivité)

Soit τ transposition : $\varepsilon(\tau)=-1$ (Compter les inversions)

Soit σ p-cycle : $\varepsilon(\sigma)=(-1)^{p-1}$ (Conséquence de $\varepsilon(\tau)=-1$)

$\mathcal{A}_n=\ker\varepsilon$ est le groupe alterné, sous groupe de $\mathfrak{S}_n$

$\mathrm{card}(\mathcal{A}_n)=\dfrac{card(\mathfrak{S}_n)}{2}=\dfrac{n!}{2}$

Les $3-cycles$ engendrent $\mathcal{A}_n$ (Utiliser les 2-cycles)