Chap 10 : Groupes

$(G,\cdot)$ est un groupe

I. Généralités

La lci est en général notée $+$ lorsque $\cdot$ est commutative, on parle alors de groupe abélien

$H \subset G$ est un sous-groupe de G s'il est non vide, stable par $\cdot$ et tel que $(H,\cdot)$ est un groupe

H sous-groupe de $G \Leftrightarrow (H \neq \varnothing,$ et $\forall (x,y) \in H^2, xy^{-1} \in H)$

$a \in G$. On définit les translations $\gamma_a : x \mapsto ax$ et $\delta_a : x \mapsto xa$. Ce sont des bijections (mais pas des morphismes)
Puissance : pour $a \in G$, on définit par récurrence $a^0 = e,\ \forall n \in \mathbb{N}, a^{n+1} = a \cdot a^n$ et pour $n < 0, a^n = (a^{-1})^n$
$(G,\star),(G',\square)$ groupes. $f : G \to G'$ est un morphisme (de groupes) lorsque : $\forall (x,y) \in G^2, f(x \star y) = f(x) \square f(y)$

$f : G \to G'$ morphisme $\quad f(e_G) = e_{G'}$ || $\forall x \in G, f(x^{-1}) = f(x)^{-1}$ || $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = f(x)^n$

$\varphi \begin{cases} \mathbb{Z} \to G \\ n \mapsto a^n \end{cases}$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,\cdot)$

Un isomorphisme est un morphisme bijectif. Un automorphisme est un isomorphisme de G dans G

Les morphismes se composent, les isomorphismes s'inversent
$(Aut(G),\circ)$ (ensemble des automorphismes de G dans G) est un sous-groupe de $(\mathfrak{S}(G),\circ)$
$f \in Mor(G,G')$ $\quad H$ ss-gpe de $G \Rightarrow f(H)$ ss-gpe de G' || K ss-gpe de $G' \Rightarrow f^{-1}(H)$ ss-gpe de G
f injective *ssi* $\ker f = \{e_G\}$

$f \in Mor(G,G') \Rightarrow \ker f = \{x \in G / f(x) = e_{G'}\}$ || Le centre de G $Z(G) = \{a \in G / \forall x \in G, ax = xa\}$

Automorphismes intérieurs : $a \in G \quad \varphi_a : x \mapsto axa^{-1} \in Aut(G) \quad \forall (a,b) \in G^2, \varphi_a \circ \varphi_b = \varphi_{ab}$
$\psi \begin{cases} G \to Aut(G) \\ a \mapsto \varphi_a \end{cases}$ est un morphisme où $\ker f = Z(G)$

H ss-gpe de G est distingué/normal/invariant lorsque : $\forall a \in G, \varphi_a(H) \subset H \Leftrightarrow \forall a \in G, aHa^{-1} \subset H$
Un groupe est dit simple lorsque ses seuls sous-groupes distingués sont $\{e_G\}$ et G

Si H est distingué, $aHa^{-1} = H$ $\quad {}^{(I)} f \in Mor(G,G') \Rightarrow H = \ker f$ est distingué dans G

G_1, G_2 deux groupes. L'ensemble $G_1 \times G_2$ muni de la lci $\star : (x_1,x_2) \star (y_1,y_2) = (x_1y_1, x_2y_2)$ est un groupe.
Ce groupe est appelé groupe produit de G_1 et G_2

La projection $G_1 \times G_2 \to G_1$ sont des morphismes surjectifs || $f : \begin{cases} G_1 \to G_1 \times G_2 \\ x_1 \mapsto (x_1, e_2) \end{cases}$ est un morphisme injectif

A, B sous-groupes de G. On note $AB = \{ab / a \in A, b \in B\}$

H, K sous-groupes de G $\quad$ Si $HK = KH$, HK est un sous-groupe de G

H, K ss-gpes de G. $N(K) = \{a \in G, aKa^{-1} \subset K\}$ est le normalisateur de K

$h \in H, k \in K$ $[h,k] = hkh^{-1}k^{-1}$ est le commutateur de h et k

$N(K) = G \Leftrightarrow K$ est distingué $^{(I)}$Si $H \subset N(K)$, alors $HK = KH$

Cas particulier : H distingué $\Rightarrow HK$ sous-groupe de G

$H \cap K = \{e\}$, alors $f \begin{cases} H \times K \to HK \\ (h,k) \mapsto hk \end{cases}$ est bijective. $\Rightarrow$ Si G est fini, $|HK| = |H| \times |K|$

$^{(VI)} H \cap K = \{e\}, K \subset N(H)$ et $H \subset N(K) \Rightarrow H$ et K commutent, HK est un ss-gpe de G isomorphe à $H \times K$

II. $\mathbb{Z}/n\mathbb{Z}$

H sous-groupe de $(\mathbb{Z},+) \Rightarrow \exists! n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

$n \in \mathbb{N}^*$ $\equiv [n]$ définie sur $\mathbb{Z} \times \mathbb{Z}$ par $x \equiv y [n] \Leftrightarrow x - y \in n\mathbb{Z}$ est une relation d'équivalence.

On note $\bar{x}$ la classe de x pour cette relation. $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes déquivalences pour $\equiv [n]$

L'application $(\bar{x}, \bar{y}) \mapsto \overline{x+y}$ est correctement définie et fait de $\mathbb{Z}/n\mathbb{Z}$ un groupe additif

$\pi : x \mapsto \bar{x}$ est un morphisme de groupe surjectif de noyau $n\mathbb{Z}$

$m \in \mathbb{Z} \Rightarrow \mathbb{Z}/n\mathbb{Z} = \{\bar{m}, \overline{m+1}, \ldots, \overline{m+n-1}\}$, ces classes étant 2 à 2 distinctes. $\left|\mathbb{Z}/n\mathbb{Z}\right| = n$

III. Ordre d'un élément

$a \in G. A = \{n \in \mathbb{N}^* / a^n = e_G\}$ Si $A = \varnothing$, on dit que a est d'ordre infini

Si $A \neq \varnothing$, le nombre $\omega(a) = \min A$ est appelé ordre de a

$j : n \mapsto a^n$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,\cdot)$. a d'ordre infini $\Leftrightarrow j$ injective. Sinon, $\ker j = \omega(a)\mathbb{Z}$

a d'ordre fini, $m = \omega(a)$ $\forall n \in \mathbb{Z}, a^n = e \Leftrightarrow m \mid n$ || $\omega(a) = pq \Rightarrow \omega(a^p) = q$

$f \in Mor(G,G'), a' = f(a)$ est d'ordre fini et $\omega(a') \mid \omega(a)$ || $\underline{\forall k \in \mathbb{Z}, \omega(a^k) = \dfrac{m}{k \wedge m}}$

$a, b \in G$ d'ordres fini m, n. si $ab = ba$ $\begin{cases} \omega(a) \wedge \omega(b) = 1 \Rightarrow \omega(ab) = \omega(a)\omega(b) \\ \exists c \in G \text{ tq } \omega(a) \vee \omega(b) = \omega(c) \end{cases}$ $(m = \Pi p_i^{a_i}, n = \Pi p_i^{b_i}, u = \prod_{b_i > a_i} p_i^{a_i}, c = a^u b^v)$

IV. Groupe engendré par une partie

$(G,\cdot)$ groupe, $A \subset G$

Il existe un unique plus petit sous-groupe H de G contenant A, on le note $\langle A \rangle = \bigcap_{\substack{K \text{ ss-gpe de } G \\ A \subset K}} K$

Il est appelé groupe engendré par la partie A. Si $\langle A \rangle = G$, A est une partie génératrice de G

Le sous groupe H de G est dit monogène lorsqu'il existe $a \in G$ tel que $\langle a \rangle = H = \{a^n\}_{n \in \mathbb{Z}}$

$H = \langle a \rangle$ Si H est infini, il est isomorphe à $\mathbb{Z}$. Sinon, a est d'ordre fini, et H est isomorphe à $\mathbb{Z}/\omega(a)\mathbb{Z}$

Un sous-groupe monogène fini est dit cyclique

//HP// $G=\langle a\rangle$ groupe cyclique d'ordre $n(=|G|)$ $\quad G'=\langle b\rangle$ groupe cyclique de cardinal q

$\forall k\in\mathbb{Z}, a^k$ est générateur de G *ssi* $k\wedge n=1$ $\quad\|\quad$ $G\times G'$ est cyclique *ssi* $n\wedge q=1$

H est un sous-groupe de G *ssi* $\exists d\,|\,n$ tq $H=\langle a^d\rangle$, et alors $|H|=\dfrac{n}{d}$

$\langle A\rangle$ est l'ensemble des mots créés sur $A\cup A^{-1}$: $\langle A\rangle=\{a_1^{\alpha_1}...a_m^{\alpha_m}\ /\ a_i\in A,\alpha_i\in\mathbb{Z},m\in\mathbb{N}\}$

/!\ Il n'y a pas d'unicité de l'écriture des mots, même sur les mots réduits.

/!\ Si $\langle A\rangle=G$ et si f et $g\in Mor(G,G')$ qui coincident sur A, $f=g$ mais on ne peut en général pas définir arbitrairement un morphisme sur une partie génératrice

V. Compléments

$(G,\cdot)$ groupe, H sous-groupe de G

Une classe à gauche modulo H est un ensemble de forme aH, $a\in G$

La relation "à gauche selon H" R_H est définie par : $aR_Hb\Leftrightarrow ab^{-1}\in H$.

C'est une relation d'équivalence, et on a : $\forall x\in G,\overline{x}=xH$

//HP// Thm de Lagrange : Si G est fini : $\operatorname{card}H\,|\,\operatorname{card}G$ $\quad$ et $\forall x\in G,\omega(x)\,|\,(|G|)\Leftrightarrow x^{\operatorname{card}G}=e$

$a_1H...a_rH$ (2 à 2 disjointes) $\to$ partition. $\quad h\mapsto a_ih$ est une bij de H dans $a_iH\Rightarrow|aH|=|H|$

Le nombre $\dfrac{|G|}{|H|}$ est appelé index de H dans G

H sous-groupe distingué de G : $aH=Ha$

Groupe quotient : G/H est l'ensemble des classes à gauche selon H

C'est un groupe pour la loi $\star$: $(aH)(bH)=(ab)H$

$s:\begin{cases}G\to G/H\\ a\mapsto aH\end{cases}$ est un morphisme de groupes.

Si $f\in Mor(G,G')$, de noyau H, il existe un unique $\overline{f}\in Hom(G/H,G)$ tel que $f=\overline{f}\circ s$

G opère sur E (ensemble) s'il existe une application $\begin{cases}G\times E\to E\\ (g,x)\mapsto g\cdot x\end{cases}$ telle que :

$-\ \forall x\in E, e\cdot x=x$ $\qquad$ $-\ \forall(g,g')\in G^2,\forall x\in E, g'\cdot(g\cdot x)=(gg')\cdot x$

$\forall g\in G,\varphi_g\begin{cases}E\to E\\ x\mapsto g\cdot x\end{cases}$ est une bijection. $\quad\|\quad$ $Stab(x)=\{g\in G\ /\ g\cdot x=x\}$ est un sous-groupe de G

La relation : $\forall(x,y)\in E^2, x\mathcal{R}y\Leftrightarrow\exists g\in G, g\cdot x=y$ est d'équivalence.

La classe de x pour $\mathcal{R}$ est l'orbite de x sous l'action de G : $\mathcal{O}(x)=\{g\cdot x\ /\ g\in G\}$

Actions de G sur lui-même : $g\cdot x=gx$ ou bien $g\cdot x=gxg^{-1}$ (conjugaison)