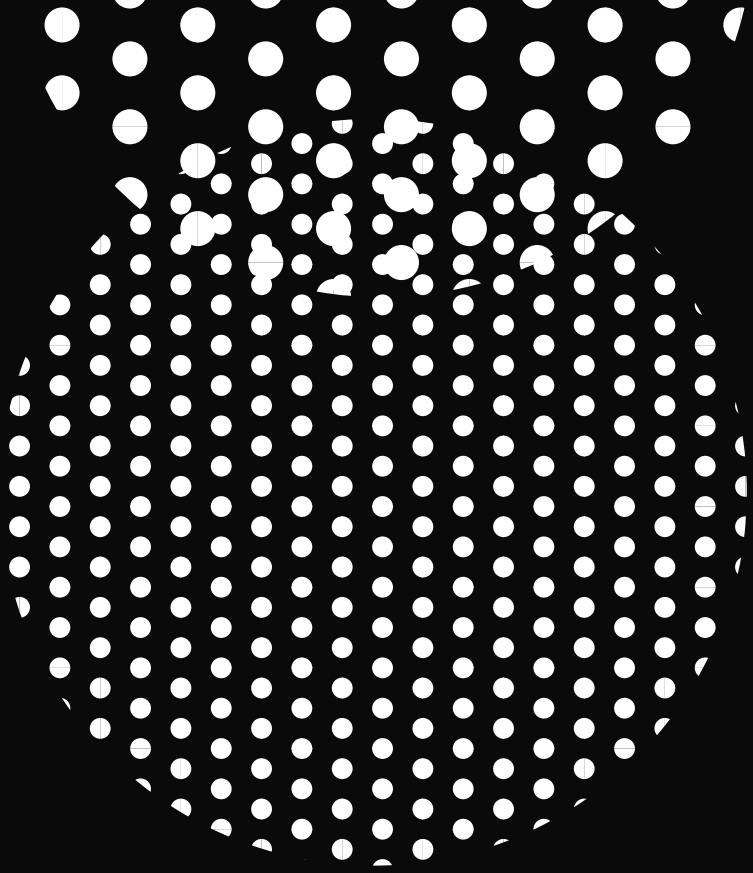

groupe est cyclique si il est généré par un élément

Prp: Si $H \overset{\text{ss gpe}}{\triangleleft} G^{\text{gpe}}$ $\boxed{\text{distingué}}$, alors $\forall x \in G\ \forall h \in H$

$xhx^{-1} \in H$

$xHx^{-1} \subset H$

Alors $\forall x \in H$ on a:

$xH = Hx$

classe à gche = classe à dte

pr: Soit $x \in G$, $h \in H$, alors $xhx^{-1} \in H$

$xhx^{-1} =: h \in H$

$xh = h'x$

$xH \subset Hx$

inversement

$\supset$ pareil $\square$

CCL: $\{xH = Hx : x \in G\}$ ensemble des classes à gche ou à dte, pareil

$X \sim_g Y$ si $x^{-1}y \in H$ $\Updownarrow$ si $H \triangleleft G$ est distingué

$X \sim_d Y$ si $xy^{-1} \in H$

$G \backslash H = H / G$

Q: G/H gpe?

$$G/H \times G/H \longrightarrow G/H$$
$$(\bar{x}, \bar{y}) \longmapsto ? \quad \overline{xy}$$

$*$ de G

classe mod H

Non, si H pas distingué

CEX POLY SECTION 15

$\bar{x}$ classe de x mod H

$= xH = \{xh : h \in H\} \overset{\text{distingué}}{=} Hx = \{h'x : h' \in H\}$

Thm: Si $H \triangleleft G$ est dist. G/H ($\mathbb{Z}/n\mathbb{Z}$) est un gpe pour la loi

$$(\bar{x}, \bar{y}) \longmapsto (\overline{xy})$$
$$(xH, yH) \longmapsto (xyH)$$

pv: La loi ne dépend pas des représentations choisis dans chaque classe.

$\bar{x}_1 = \bar{x}_2 \qquad \bar{y}_1 = \bar{y}_2$

$\overline{x_1 y_1} = \overline{x_2 y_2}$ $\qquad$ x_1 et x_2 sont de m̂ classe.
y_1 et y_2 ——————

$\exists h \in H \qquad x_2 = x_1 h$
$\exists h' \in H \qquad y_2 = y_1 h'$

partiel

Calc: $x_2 y_2 = x_1 h y_1 h'$ $\qquad$ $\forall x \in G, \forall h \in H, \; xhx^{-1} \in H \Leftrightarrow x^{-1}hx \in H$

$= x_1 y_1 \underbrace{y_1^{-1} h y_1}_{\in H} h'$

H distingué

$\underbrace{\qquad\qquad}_{\in H}$

$=: h''$ ss-gpe

$=: x_1 y_1 h''$ $\qquad$ cela dit bien que $x_2 y_2 \sim x_1 y_1 \bmod H$

La loi sur G/H est bien définie

El' neutre: $\bar{1}_G = 1_G H$ car $\bar{x} \cdot \bar{1}_G \overset{\text{déf}}{=} \overline{x 1_G} = \bar{x}$
OK

Associativité: $\forall \bar{x}, \bar{y}, \bar{z} \in G/H$

$$(\bar{x}\bar{y})\bar{z} \overset{\text{df}}{=} (\overline{xy})\bar{z} \overset{\text{df}}{=} \overline{xyz} \underset{\text{dans } G}{\overset{\text{assté}}{=}} \overline{x(yz)} \overset{\text{déf}}{=} \bar{x}(\overline{yz}) \overset{\text{déf}}{=} \bar{x}(\bar{y}\bar{z})$$

Inverse: $\bar{x} \cdot \bar{x}^{-1} = \overline{x x^{-1}} = \bar{1}_G = \overline{x^{-1} x} = \bar{x}^{-1} \bar{x}$

l'inverse de classe x est la classe de x^{-1} $\square$

Déf: G/H avec $H \triangleleft G$ appelé gpe quotient de G par H

Ex canonique: $\underset{G/H}{\mathbb{Z}/n\mathbb{Z}}$ gpe !

Ex: $\mathbb{Z}/3\mathbb{Z}$
$\bar{x} = \bar{6} = \bar{1}_G$
$6 \in 3\mathbb{Z} = \{\underset{1_G}{0}, \underset{1_G}{3}, \underset{1_G}{6}, \underset{1_G}{12} \dots\}$

Rmq: $\bar{x} = \bar{1}_G$ $\quad x = 1_G H \quad x \in H$ les él's de H "disparaissent"

On "force" les él's de H à devenir triviaux.

Appl: $G \xrightarrow{f} G'$ morph de gpes

Prp: $\mathrm{Ker}\, f \triangleleft G$ est distingué, donc le quotient $G/\mathrm{Ker}\, f$ est gpe.

Si: $x \in \mathrm{Ker}\, f$ on a $f(xy) = f(x)f(y) = 1_{G'} f(y)$
$\forall y \in G$

f ne voit pas son noyeau:

Introduire: $\bar{f} : G/\mathrm{Ker}\, f \longrightarrow G'$
$\bar{x} = x\,\mathrm{Ker}\, f \longmapsto f(x)$
$\bar{x} = xH$

Aff°: Cette application $\bar{f}$ est bien définie

pv: Avec $x_1 = x_2$ càd $x_1 h\, x_2$ avec $h \in \mathrm{Ker}\, f$
$\Rightarrow f(x_1 h) = f(x_1) f(h) = f(x_1)\, 1_{G'} = f(x_1)$

$\square$

Prp: $\mathrm{Ker}\, f \triangleleft G$ est dist.
pv: $\forall x \in G \quad \forall h \in \mathrm{Ker}\, f$
$x h x^{-1} \overset{!}{\in} \mathrm{Ker}\, f$

Oui: $f(x h x^{-1}) = f(x) f(h) f(x^{-1}) = f(x)\, 1_{G'}\, f(x^{-1}) = f(x x^{-1}) = f(1_G) = 1_{G'}$

$\square$

Résumé:

$$\begin{tikzcd}
x \arrow[rr, mapsto] \arrow[d, mapsto, "\pi"] & & f(x) \\
G \arrow[r, "f"] \arrow[d, "\pi"] & G' & \\
\bar{x} & G/\mathrm{Ker}\, f \arrow[ur, "\bar{f}"] & \bar{f}(\bar{x}) \arrow[ul, mapsto]
\end{tikzcd}$$

$x \bmod \mathrm{Ker}\, f$

déf
$\boxed{\bar{f}(\bar{x}) = f(x)}$

Thm: Avec $\pi\ G \to G/\mathrm{Ker} f$, $x \mapsto \bar{x} = x\,\mathrm{Ker} f$

Avec $\bar{f} : G/\mathrm{Ker} f \longrightarrow G'$

$x\,\mathrm{Ker} f \longmapsto f(x) = \bar{f}(\bar{x})$

$\bar{x} = xH$

(1) $\bar{f}$ est un morphisme de gpes

(2) $\bar{f}$ est injective

(3) $G/\mathrm{Ker} f \xrightarrow[\sim]{\bar{f}} \mathrm{Im}\, f \subset G'$ est un isomorph de gpes

pv: (1) Soient $\bar{x} = x\,\mathrm{Ker} f$ $\quad \bar{y} = y\,\mathrm{Ker} f$

Alors $\bar{f}(\bar{x}) = f(x)$ $\quad \bar{f}(\bar{y}) = f(y)$

$$\Rightarrow \bar{f}(\bar{x})\bar{f}(\bar{y}) = f(x)f(y) \underset{\text{morph}}{\overset{f}{=}} f(xy) \overset{\text{def}}{=} \bar{f}(\bar{x}\bar{y})$$

(2) Soit $\bar{x} \in G/\mathrm{Ker} f$ avec $1_{G'} = \bar{f}(\bar{x}) = f(x)$

$1_{G'} = f(x)$

$\mathrm{Ker} f \ni x$

$\bar{1}_G = \bar{x}$ donc $\bar{f}$ injective.

(3) Rappel: $\mathrm{Im} f \subset G'$ est un ss-gpe

$\bar{f} : G/\mathrm{Ker} f \longrightarrow \mathrm{Im}\, \bar{f} = \mathrm{Im}\, f$ $\quad \bar{f}(\bar{x}) = f(x)$

injective $\quad$ surjective trivialet

donc bijective

$\bar{f}$ morphisme de gpes = isomorphisme $\square$

Déf: Pour $x \in G^{\text{gpe}}$, regarder $\langle x \rangle := \{x^i \in G,\ i \in \mathbb{Z}\} = \{\dots, x^{-2}, x^{-1}, 1_G, x^1, x^2, \dots\}$ (gpe engendré)

ss-gpe $\quad x^i x^j = x^{i+j}$

L'ordre de x: $o(x) = \mathrm{Card}(\langle x \rangle) = |\langle x \rangle| = \begin{cases} \infty \\ \text{fini} \end{cases}$ 2 cas

Obs: Si $|G| < \infty$, necesst les x^i pas tout $\neq$

$\Rightarrow \exists i \neq j \in \mathbb{Z}$ avec $x^i = x^j$

$\Rightarrow 1_G = x^{j-i}$

$\Leftrightarrow x^{i-j} = 1_G$ $\quad \Rightarrow \exists m \geq 1$ tq $x^m = 1_G$

Déf: L'ordre de x c'est $o(x) := \min\{m \geq 1 : x^m = 1_G\}$

Thm: $|\langle x \rangle| = o(x) = \min\{m \geq 1 : x^m = 1_G\}$

Morphisme de gpes: $h_x : \mathbb{Z} \longrightarrow G$, $i \longmapsto x^i$

$x \in G$ fixé

oui:

$h_x(i) h_x(j) = x^i x^j$ *

$= x^{i+j}$

$= h_x(i+j)$

$h_x(0) = x^0 = 1_G$

Regarder $\operatorname{Ker} h_x$

Prp: Éqults

(i) h_x pas injective — VU POUR $G \xrightarrow{f} G'$ QLCQUE

Vu $\Updownarrow$

(ii) $\operatorname{Ker} h_x \neq \{0\}$

(iii) $\exists m \geq 1$ avec $x^m = 1_G$

pv:

(ii) $0 \neq \operatorname{Ker} h_x$ — $0 \xrightarrow{h_x} 1_G$

$\Updownarrow$

(iii) $\exists i \in \mathbb{Z} \setminus 0$ avec $x^i = 1_G$ — $\operatorname{Ker} h_x = \{i \in \mathbb{Z} \;\; h_x(i) = 1_G\}$

Càd gpe engendré par x

Thm:* (1) $|\langle x \rangle| < \infty \iff \exists\, m \geq 1$ avec $x^m = 1_G$

(2)* Dans ce cas $|\langle x \rangle| = o(x) = \min\{m \geq 1 : x^m = 1_G\}$ et alors $\langle x \rangle = \{1_G, x, x^2, \dots, x^{m-1}\}$ on voit $\mathbb{Z}/n\mathbb{Z}$

$1_G = x^m$

(3) $x^m = 1_G \iff o(x) \mid m$

(4) $o(x) \mid |G|$ — pv: $\langle x \rangle = H \subset G$ ss-gpe Lagrange $|H| \mid |G|$

pv: (1) $\operatorname{Ker} h_x = \{ m \in \mathbb{Z} : x^m = 1_G \}$

Si $\operatorname{Ker} h_x = \{0\}$ tous les x^i sont distincts

Si $\operatorname{Ker} h_x \neq \{0\}$, c'est un ss-gpe de $\mathbb{Z}$

donc thm vu $\operatorname{Ker} h_x = n\mathbb{Z}$ avec $n \geq 1$

pv (2) Dans le cas où $\operatorname{Ker} h_x = n\mathbb{Z}$, on a $x^n = 1_G$

Att°: $\{1_G, x, x^2, \dots, x^{n-1}\}$ n éléments distincts.

pv: $\{x^i\}_{0 \leq i \leq n-1}$

Si pour $0 \leq i \neq j \leq n-1$ on avait $x^i = x^j$

OPS $i < j$ $\qquad 1_G = x^{j-i}$

Mais $0 < j-i \leq n-1$ contredit que

$n = \min\{ m \geq 1 : x^m = 1_G \}$

$-(n-1) \leq -i \leq 0$

$0 \leq j \leq n-1$

$-(n-1) \leq j-i \leq (n-1)$

pv (3): $x^m = 1_G$

$\iff \exists\, m \in \operatorname{Ker} h_x$

$\in n\mathbb{Z}$

$\iff n \mid m$

Ici $o(x) = n$

$$h_x : \underset{(\mathbb{Z},+)}{\mathbb{Z}} \longrightarrow \underset{(G,*)}{G}$$
$$i \longmapsto x^i$$

Thm: Pour ce morphisme h_x

h_x injectif, surjectif sur son image ss-gpe

TRIVIAL ou bien $\operatorname{Ker} h_x = \{0\}$ et alors $\mathbb{Z} \cong \{x^i : i \in \mathbb{Z}\}$

ou bien $\operatorname{Ker} h_x = n\mathbb{Z}$ avec $n \geq 1$ et alors $\mathbb{Z}/n\mathbb{Z} \overset{\text{isom.}}{\cong} \{x^i : i \in \mathbb{Z}\}$

$E \xrightarrow{f} F$ application

$\operatorname{Im} f = \{ f(x) \in F : x \in E \}$

$E \xrightarrow{f} \operatorname{Im} f$ est surjct.

Fait: Une application est toujours surjective sur son image.

pv: h_x

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ i & \longmapsto & x^i \\ x & & i \\ \downarrow & & \downarrow \\ \bar{x} = x\,\mathrm{Ker}\, f & & i \bmod n = \bar{i} \end{array}$$

HYP: $\mathrm{Ker}\, h_x = n\mathbb{Z}$ avec $n \geq 1$ donnée

$$\begin{tikzcd} \overset{G}{\mathbb{Z}} \arrow[r, "h_x"] \arrow[d, "\pi_n"'] & \overset{G'}{G} \\ \mathbb{Z}/n\mathbb{Z} \arrow[ur, "\bar{h}_x"'] & \end{tikzcd}$$

$G/\mathrm{Ker}\, f$

thm vu dans un cadre général

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/\mathrm{Ker}\, f \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Redémontrer "à la main"

S'applique avec $G = \mathbb{Z}$
$G' = G$

pv:

$x^n = 1_G$

$$x^{i \bmod n} = x^{i+kn} = x^i (x^n)^k = x^i$$

$i \bmod n \xrightarrow{\bar{h}_x}$ bien défini

$$\bar{h}_x(\bar{i})\,\bar{h}(\bar{j}) = x^{i \bmod n}\, x^{j \bmod n} = x^{i+j} = h_x(\bar{i}+\bar{j})$$

$\bar{h}_x$ bijectif car $n\mathbb{Z} = \mathrm{Ker}\, h_x$

Résumé: $\{x^i : i \in \mathbb{Z}\}$ pour $x \in G$ fixé

Cas 1: Toutes $\neq$ alors $\{x^i\}_{i\in\mathbb{Z}} \cong \mathbb{Z}$

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \{x^i\}_{i\in\mathbb{Z}} \\ i & \longmapsto & x^i \end{array}$$

est un isomorph. de gpes infinis

Cas 2: Si $\mathrm{Ker}\, h_x = n\mathbb{Z}$ avec $n \in \mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} \simeq \{x^i : i \in \mathbb{Z}\} = \{1_G, x, \dots, x^{n-1}\}$$

Jouer avec les x^i comme avec $i \bmod n$ car

$$x^1 \neq 1_G,\ x^2 \neq 1_G, \dots, x^{n-1} \neq 1_G,\ x^n = 1_G$$

$$x^{2+5n} = x^2 x^{5n} = x^2 (x^n)^5 = x^2 \cdot 1_G = x^2$$

$$\boxed{x^i = x^{i \bmod n}}$$

QUE du $\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow[\text{ISOM}]{\sim} \mathbb{Z}/n\mathbb{Z}$$

$|x^{i \bmod n}|$

Thm: (1) Si G gpe avec $|G| < \infty$, tout $x \in G$ satisfait $x^{|G|} = 1_G$

(2) Si $H \subset G$ ss gpe, alors $\forall y \in H$ $y^{|G|} = 1_G$

gpe engendré par x

pv (1): On a $|\langle x \rangle| \subset G$ ss-gpe, Lagrange: $|\langle x \rangle| \mid |G|$

$$|\langle x \rangle| = o(x) \mid |G|$$

donc $o(x) d = |G|$ mais $(x^{o(x)} = 1_G)^d$

$$x^{|G|} = x^{d \cdot o(x)} = 1_G$$

pv (2): H est un gpe, par (1) $y^{|H|} = 1_H = 1_G$

Thm Lagrange $|H| \mid |G|$

$$|H| \cdot r = |G|$$

$$y^{|G|} = y^{r \cdot |H|} = 1_G$$

Thm: Soit G un gpe, soit $x \in G$, avec $o(x) < \infty$. Alors, pour $c \in \mathbb{N}_{\geq 1}$

$$o(x^c) = \frac{o(x)}{\text{pgcd}(c, o(x))}$$

En particulier:

(1) Si $c \mid o(x)$ alors $o(x^c) = \frac{o(x)}{c}$

(2) si $c \wedge o(x) = 1$ alors $o(x^c) = o(x)$

pv: Par def $\{x^i\}_{i \in \mathbb{Z}} = \{1_G, x^1, x^2, \dots, x^i, \dots, x^{o(x)-1}\}$ avec $x^{o(x)} = 1_G$

Poser $d := \text{pgcd}(c, o(x))$

Ecrire $c = d \cdot r$ $o(x) = d s$ avec $r, s \in \mathbb{N}$ $r \wedge s = 1$

m minimal

Alors $(x^c)^m = 1_G = x^{c \cdot m}$ par thm vu $o(x) \mid cm$

$\iff d s \mid d r m$

$\iff s \mid r m$ mais $s \wedge r = 1$

$\iff s \mid m \Rightarrow s \leq m$

Donc m minimal $= s$

CCL: $o(x^c) = \min\{m \geq 1 : (x^c)^m = 1_G\} = s = \frac{o(x)}{\text{pgcd}(c, o(x))}$ $\square$

Déf: Un gpe est cyclique si $G = \langle x \rangle$ et si $|G| < \infty$.
Dans ce cas $n := |\langle x \rangle| = |G|$ $G = \{1_G, x, x^2, \dots, x^{n-1}\}$

Thm: Si G est fini, si $|G| = p \in \mathbb{P}$ est premier, alors G est cyclique.

+ Thm 14.5