



1 exode partiel : groupes abstraits

Def: Un groupe $(G, *)$ c'est:

$$*: G \times G \longrightarrow G \quad \text{loi interne}$$

$$(x, y) \longmapsto x * y$$

satisfaisant:

$$(1) \text{ Associativité: } \forall x, y, z \in G \quad (x * y) * z = x * (y * z)$$

$$(2) \exists e \in G \text{ él' neutre}$$

$$e * x = x = x * e \quad \forall x \in G$$

$$(3) \forall x \in G \exists x' \in G \text{ avec } x * x' = e = x' * x$$

ON NE SUPPOSE PAS

*** commutative** En général $x * y \neq y * x$

L'élément neutre unique (POLY)

Prop: L'inverse x' de x est unique

pr: Soit x'' un autre inverse de x

$$x' (x * x'' = e) = x'' * x$$

$$x' * x * x'' = x'$$

$$e * x'' = x'$$

$$x'' = x'$$

Similaire

□

Noter x^{-1} l'inverse de x

Noter e ou 1_G l'él' neutre de G

Noter $x^n = x \dots x$ n fois sans $*$

Comme la mult. dans $\mathbb{Z}/n\mathbb{Z}$ sans symbole

souvent, on note la loi de groupe sans symbole

$$x * x \quad x x \quad x^2$$

Rappel: G pas forcément commutatif!!! Donc $x^* y^* \neq y^* x^*$ en général

Mais si deux éléments "spéciaux" x et y de G

commutent, i.e. $xy = yx$ Ex: $ex = xe$

alors on peut changer l'ordre des termes.

$$(xy)^2 \stackrel{\text{dit}}{=} xyxy$$

$$= xxyy$$

$$= x^2 y^2$$

PAS SOUVENT!

Def de gre, e unique, x^{-1} unique

$x * y \neq y * x$ souvent

on multiplie à droite des deux côtés

Pr: (1) $(xz = yz)z^{-1} \Rightarrow x = y$

rv: $xz z^{-1} = yz z^{-1}$
 $xe = ye$
 $x = y$

(2) $(x^{-1})^{-1} = x$

rv: Par déf de x^{-1} , on a $xx^{-1} = e = x^{-1}x$
inverses de x^{-1}

(3) $(xy)^{-1} = y^{-1}x^{-1}$
 $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$

rv: A-t-on:

$xyy^{-1}x^{-1} \stackrel{!}{=} e$

$y^{-1}x^{-1}xy \stackrel{!}{=} e$

$xe x^{-1} = e$

$y^{-1}e y = e$

□

Deux identités
à vérifier
(3) Déf gp

Déf: Si $\text{Card } G < +\infty$, note $|G| < +\infty$

on dit que l'ordre de G c'est son nombre d'el's
(au lie du mot cardinal)

Thm: $(\mathbb{Z}/n\mathbb{Z}, +)$ est un gpe $e = 0$

Thm: $(\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un gpe $e = 1$

Pour le gpe $G := (\mathbb{Z}/n\mathbb{Z}, +)$

$1_G = e = 0$

Pour $G := (\mathbb{Z}/n\mathbb{Z})^\times, \times)$ $1_G = e = 1$

L'ordre de $G = \text{Card } G$

Def: Une application $f: G \longrightarrow G'$ entre deux gres $(G, *)$ et $(G', *')$ est un morphisme de gres si $\forall x \in G, \forall y \in G$
 $f(xy) = f(x) *' f(y)$

f respecte les structures de groupe

Sans étoiles $f(xy) = f(x)f(y)$

Prop: La composée de deux morphismes $G \xrightarrow{f} G' \xrightarrow{f''} G''$ est un morphisme
 Soient $x, y \in G$. Regardons:
Pv: $f''(xy) = f''(f(x)f(y)) = f''(f(x))f''(f(y)) = f''(x)f''(y)$

Prop: Soit $f: G \longrightarrow G'$ morph. alors

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

(2) $f(x^{-1}) = f(x)^{-1}$

Pv: (1): $f(1_G) = f(1_G 1_G) = f(1_G) \cdot f(1_G)$ $\implies f(1_G)^{-1} f(1_G) = f(1_G)^{-1} f(1_G) f(1_G)$
 $f(1_G)^{-1} = 1_{G'}$ $\implies 1_{G'} = f(1_G)$

Pv: (2): $f(x) f(x^{-1}) = f(xx^{-1}) = f(1_G) \stackrel{(1)}{=} 1_{G'}$

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

donc ceci montre que $f(x^{-1})$ est l'inverse (unique) de $f(x)$ de G'

Def: Un isomorphisme = morphisme bijectif

Prop: Si $G \xrightarrow{f} G'$ isomorph
 alors la bijection réciproque
 $G \xleftarrow{f^{-1}} G'$ est aussi un isomorphisme $\square$

Sous groupe est H.C.G.
un groupe où élément
neutre et loi sont ceux
de groupe principal

Def: Un sous-groupe $H \subset G$ d'un gpe G , c'est un ss-ensemble
satis faisant:

- (1) $1_G \in H$
- (2) $\forall x \in H \forall y \in H \quad xy \in H$
- (3) $\forall x \in H \quad x^{-1} \in H$

Alors en définissant

$$1_H := 1_G$$

$$x_H := x_G|_H$$

alors (H, x_H) est un vrai gpe.

Prop: Pour un ss-ensemble $H \subset G$ non-vide, on a:

ok $\Downarrow$ (i) H est un ss-gpe de G

(ii) $xy^{-1} \in H \quad \forall x, y \in H$ **CRITÈRE DIRECTE**

pv 1: Comme $H \neq \emptyset \quad \exists h \in H$ d'où $h h^{-1} = 1_G \in H$ (i)

Ensuite $\forall x \in H$ on a $x^{-1} = 1_G x^{-1} \in H$ (ii)

Enfin, $\forall x, y \in H$

$$xy = x(y^{-1})^{-1} \in H \quad \text{(iii)}$$

Donc (1,2,3) Ok $\square$

Thm: Les ss-gpes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$
avec un nzo entier fixé