Structure algebriques.

I groupes

1 Definitions

Soit E un ensemble ; une loi de composition interne sur E est une application : $E \times E \longrightarrow E$

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

Exemple : (1) $(\mathbb{Z}, +)$; est une loi de composition interne ;

(2) si X est un ensemble ; $E = \mathcal{F}(X, X)$ l'ensemble des applications de X dans X ;

$E \times E \longrightarrow E$

$(f, g) \longmapsto f \circ g$.

On dit qu'une loi de composition interne est associative si $(a * b) * c = a * (b * c)$, $\forall (a, b, c) \in E^3$

Remarque : associative on peut "enlever les parenthèses) ou les mettre ou on veut, il faut par contre garder l'ordre a b c.

1) l'addition, la multiplication, sur $\mathbb{N}$, $\mathbb{Z}$ ... est associative

2) la composition $f \circ g$ est aussi associative

— $e \in E$ est dit est élément neutre si :

$\forall a \in E, \quad a * e = e * a = a,$

On remarque si $(E, *)$ possède un élément neutre, celui-ci est unique.

<u>preuve</u> : Supposons que e, e' sont des éléments neutre

~~Soit $a \in E, \quad a * e$~~

$$e * e' = e \quad (e' \text{ élément neutre})$$
$$= e' \quad (e \text{ élément neutre})$$

<u>Exemple</u> 0 est un élément neutre pour l'addition dans $\mathbb{Z}$;

1 est un élément neutre pour la multiplication dans $\mathbb{Z}$.

l'application $I_X : \begin{array}{l} X \longrightarrow X \\ x \longmapsto x \end{array}$ est un élément neutre pour $(\mathcal{F}(X, X), \underset{\text{composition}}{\underset{\shortparallel}{\circ}})$.

Quand on considère que $(E, *)$ (loi interne) possède un élément neutre ; Soit $a \in E$, on dit que a est inversible s'il existe $b \in E$, $a * b = b * a = e$

b est appelé l'inverse de a (parfois le symétrique ou l'opposé).

<u>Remarque</u>: si $(E, *)$ associative, e élément neutre, l'inverse de a est unique:

<u>preuve</u>: Soit b, b' inverses de a.

$$a * b' = e.$$

$$b * a * b' = b * e = b = e * b' = b'.$$

<u>Exemple</u>: l'inverse de a dans $(\mathbb{Z}, +)$ est $-a$ (on l'appelle souvent l'opposé ou le symétrique).

$(\mathbb{Q}, \times)$; On n'a pas d'inverse.

$$\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}, \quad [p \neq 0, q \neq 0]$$

On dit que x et y commutent si

$$x * y = y * x;$$

On dit que $(E, *)$ est commutatif si tous les éléments de E commutent deux à deux, i.e

$$x * y = y * x \text{ pour tout } (x, y) \in E^2$$

Exemple : $(+, \times)$ sont des lois commutatif (dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$)

La composition n'est pas commutative

Définition de groupe Soit G un ensemble non vide muni d'une loi de composition interne $*$;

On dit que G est un groupe si :

1) $*$ est associative

(2) G possède un élément neutre.

(3) $\forall x \in G$, x est inversible.

si la loi est commutative, On dit que G est commutatif ou Abélien.

Exemples de groupes :

(1) $(\mathbb{Z}, +)$ est un groupe ; 0 est l'élément neutre l'inverse de a (ici l'opposé ou le symétrique) est $-a$.

(2) $(\mathbb{Q}, +)$ est un groupe.
$(\mathbb{Q}^*, \times)$ est un groupe, 1 est l'élément neutre ; l'inverse de $a \in \mathbb{Q}^*$ est $\frac{1}{a}$.

(3) $(\mathbb{Z}, \times)$ n'est pas un groupe ; seuls 1 et -1 possèdent un inverse

④ $n\mathbb{Z}$ l'ensemble des multiple de n est un groupe.

⑤ $U = \{ z \in \mathbb{C},\ |z| = 1 \}$, $(U, \times)$ est un groupe.

⑥ $G = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ;\ a, b, c, d \text{ dans } \mathbb{Z} \right.$

$\left. \text{et } ad - bc = 1 \right\}$;

$(G, \times)$ est un groupe (multiplication des matrices)

Vérifier que $(G, \times)$ est un groupe.

~~Des exempls vus~~ Tous les groupes sont infinis,

~~Voi~~ Voici quelques exemples de groupes finis.

① $G = \{ 1, -1, i, -i \}$, $G \subset \mathbb{C}$;

$(G, \times)$ est un groupe : $\times$ est associative, 1 est l'élément neutre ; $1^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = -i$ et $(-i)^{-1} = i$

G est un groupe commutatif à 4 éléments

On note $|G| =$ cardinal de G ;

② S_n = groupe symétrique :

S_n = {ensemble des bijections de $\{1, 2, \dots, n\}$}.

$(S_n, \circ)$ est un groupe (S_n n'est pas abélien pour $n \geq 3$)

$n = 2$; $\sigma \in S_n$; $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$: i.e

$\sigma(1) = 2$; $\sigma(2) = 1$;

$S_2 = \{ I_d, \sigma \}$.

$n = 3$; $|S_3| = 6$

plus généralement ; $|S_n| = n!$

<u>Notation</u> : On utilise deux notations pour les groupes :

additive : $a * b = a + b$

multiplicative ~~a.b ou s~~ $a * b = a \cdot b$ ou simplement ab.

On utilise souvent la notation additive pour un groupe abélien.

notation	multiplicative	additive
$x * y$	xy	$x + y$
$\underbrace{x * x * \dots * x}_{n \text{ facteurs}}$	$x x \dots x = x^n$	$x + x + \dots + x = nx$
l'inverse	x^{-1}	$-x$ (opposé)
élément neutre	1	0

- pour $a \in G$; $a^0 = 1$ (par convention).

- $a^n (a^{-1})^n = (aa \dots a)(a^{-1} \dots a^{-1}) = 1$

$(a^{-1})^n = (a^n)^{-1}$, qu'on note a^{-n}.

On a les règles de calcul :

$$a^n a^m = a^{n+m}. \quad \text{(multiplication)}$$

$$(nb) + (mb) = (n+m) b \quad \text{(additive)}.$$

② Sous-groupe.

<u>Définition</u> : Soit $(G, \times)$ un groupe, $H \subset G$ une partie de G. On dit que H est un sous groupe de G ssi :

(i) $1 \in H$, (en particulier, H est non vide).

(ii) $\forall x \in H, \forall y \in H$; $xy \in H$ (H est stable par multiplication).

iii). $\forall x \in H$, $x^{-1} \in H$.

Ainsi H muni de la multiplication est lui même un groupe.

Par exemple, $\{1\}$ et G sont sous-groupes de G. On parlera d'un ~~sougo~~ sous groupe H de G comme sous groupe propre si $H \neq \{1\}$ et $H \neq G$.

<u>proposition</u> (a) si H est un sous groupe de G, alors H est lui même un groupe (même loi).

(b) une partie $K \subset G$ est un sous groupe ssi K est un groupe pour la même loi.

(c) si H et K sont des sous-groupe de G; alors $H \cap K$ est un sous groupe de G.

preuve. (laissée aux etudiants).

<u>Remarque</u>: On ~~se sert souvent pour~~ souvent pour montrer qu'un ensemble est un groupe, on montre que c'est un sous-groupe (On évite ainsi de verifier toutes les conditions en nous servant du fait que G est un groupe, en particulier, l'associativité.

<u>Exemples de sous-groupes</u>:

(1) $\{-1, 1\}$ est un sous groupe multiplicatif de $\mathbb{R}^*$ et $\{-1, 1, i, -i\}$ est un sous groupe de $(\mathbb{C}^*, \times)$

(2) $U_n = \{ z \in \mathbb{C},\ z^n = 1 \} = \{$ racines $n$ième de l'unité $\}$ est un sous groupe de $\mathbb{C}^*$ et également un sous-groupe de U. , $|U_n| = n$

(3) $SL_2(\mathbb{Z})$ est un sous groupe de $GL_2(\mathbb{R})$;

$GL_n(\mathbb{R}) = \{$ matrices inversibles $\}$ est un groupe non abélien.

3) Morphisme de groupes

Définition : Soit G, G' deux groupes.
Une application $f : G \longrightarrow G'$ est un morphisme de groupe (on dit parfois homomorphisme) si : pour tout x, y éléments de G on a :

$$f(xy) = f(x)\, f(y).$$

⚠. Ici on a ~~omis de~~ choisit pour faire simple une notation multiplicative pour G et G'.
de manière plus détaillée, $f : (G, *) \longrightarrow (G', *')$

on doit avoir $f(\underbrace{x * y}_{\text{dans } G}) = f(x) \underbrace{*'}_{\text{dans } G'} f(y)$

La notation multiplicative adoptée simplifie l'écriture.

Exemples de morphismes de groupes

1) $e : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$

$x \longmapsto e^x$ est un morphisme de groupes,

$$e^{x+y} = e^x \cdot e^y$$

(2) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$

$$\det(AB) = \det A \cdot \det B$$

(3) $f : \mathbb{R} \longrightarrow \mathbb{C}^*$

$\theta \longmapsto e^{2i\pi\theta}$

$$e^{2i\pi(\theta+\theta')} = e^{2i\pi\theta} \cdot e^{2i\pi\theta'}$$

Un peu de vocabulaire : $f : G \longrightarrow G'$ un morphisme de groupe ou simplement morphisme

si f est bijective, on dit que f est un isomorphisme
si de plus $G = G'$, f est un automorphisme.

~~Propriétés des m~~

On va voir quelques propriétés de morphismes.

(P) $f : G \longrightarrow G'$ est un morphisme.

① l'image par f de l'élément neutre de G est l'élément neutre de G' ; $f(1_G) = 1_{G'}$

preuve : Soit $a \in G$; $1_{G'} f(a) = f(a)$

$$= f(1_G a)$$

$$= f(1_G)\, f(a)$$

On a donc : $f(a) = f(1_G)\, f(a)$.

On va simplifier par $f(a)$, voici comment on fait.

On multiplie par l'inverse de $f(a)$ à droite dans l'égalité :

$$f(a)(f(a))^{-1} = f(1_G)\, f(a)\, f(a)^{-1}$$

$$1_{G'} = f(1_G)\left(f(a) \cdot f(a)^{-1}\right)$$

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

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

② soit $a \in G$; $f(a^{-1}) = (f(a))^{-1}$

preuve : $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1_{G'}$

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

③ Soit $a \in G$, $n \in \mathbb{Z}$.

$f(a^n) = (f(a))^n$.

preuve : (par récurrence) (laissée aux étudiants).

<u>Image de Noyau.</u>

Soit $f : G \longrightarrow G'$ un morphisme

On définit ~~Im f = image de~~

$$\ker f = \{a \in G,\ f(a) = 1_{G'}\}$$
$$= f^{-1}(1_{G'}).$$

si H un sous groupe de G ; $f(H)$ = image de H par $f = \{f(a),\ a \in G\}$.

$f(G) = \operatorname{Im} f$

<u>proposition</u> :

ⓐ $\ker f$ est un sous groupe de G (noyau de f)

ⓑ $f(H)$ est un sous groupe G.

<u>preuve</u> :

ⓐ $f(1_G) = 1_{G'}$, donc $1_G \in \ker f$.

si $a, b \in \ker f$; $f(ab) = f(a) f(b) = 1_{G'} \cdot 1_{G'} = 1_{G'}$

donc $ab \in \ker f$. et enfin.

si $a \in G$; $f(a^{-1}) = (f(a))^{-1} = 1_{G'}^{-1} = 1_{G'}$

donc : $a^{-1} \in 1_{G'}$, cela montre que $\ker f$ est un sous groupe de G.

ⓑ $1_{G'} = f(1_G)$ ~~donc~~ et $1_G \in H$,

donc $f(1_G) = 1_{G'} \in f(H)$. (contient l'element neutre)

soient a, b élements de $f(H)$;

$a = f(a')$ et $b = f(b')$ avec $a' \in H$, $b' \in H$

$ab = f(a') f(b') = f(a'b') \in f(H)$ car $a'b' \in H$.

$a = f(a') \in H$;

$a^{-1} = (f(a'))^{-1} = f(a'^{-1}) \in f(H)$ car

$a'^{-1} \in H$. (H est un sous groupe de G).

Exemples :

1) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$.

Le noyau de ce morphisme est le sous groupe

$SL_n(\mathbb{R}) = \{$ matrice de $\det = 1\}$.

2) $f : \mathbb{R} \longrightarrow \mathbb{C}^*$
$\theta \longmapsto e^{2i\pi\theta}$.

$\operatorname{Ker} f = \{\theta \in \mathbb{R},\ e^{2i\pi\theta} = 1\} = \{\theta \in \mathbb{Z}\} = \mathbb{Z}$

$\operatorname{Im} f = \mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$.

② Groupe monogène, ~~gg~~ cyclique.

Soit G un groupe, $a \in G$;

On note $\langle a \rangle = \{ a^k, k \in \mathbb{Z} \}$.

<u>proposition</u>: $\langle a \rangle$ est un sous groupe de G.

<u>preuve</u>: On considère $f : \mathbb{Z} \longrightarrow G$, $k \longmapsto a^k$;

f est un morphisme de groupe et $\langle a \rangle = \operatorname{Im} f$

Le sous groupe $\langle a \rangle$ s'appelle le sous-groupe engendré par a.

<u>Exemple ①</u> $G = \mathbb{Z}$; le sous groupe engendré par n, $\langle n \rangle = n\mathbb{Z}$ (les multiples de n).

<u>Remarque</u>: $\langle a \rangle$ est un groupe abelien (même si G ne l'est pas) ; $a^k a^{k'} = a^{k+k'} = a^{k'} \cdot a^k$.

<u>Exemple 2</u>: $G = \mathbb{C}^*$; $\langle i \rangle = \{ 1, -1, i, -i \}$.

<u>th</u>: si H est un sous groupe de $\mathbb{Z}$; ~~$H = n\mathbb{Z}$~~ ; il existe $n \geq 0$ tel que $H = n\mathbb{Z}$

preuve : si $H = \{0\}$, $H = 0\mathbb{Z}$.

On suppose que $H \neq \{0\}$; il existe $h \in H$, $h \neq 0$;

On peut supposer que $h \geq 0$ (quitte à prendre $-h$).

On considère $H \cap \mathbb{N}$; $h \in H \cap \mathbb{N}$; $h \neq 0$;

Soit n le plus petit élément strictement positif de $H \cap \mathbb{N}$; $n \in H$; donc $n\mathbb{Z} \subset H$.

soit $m \in H$; on divise m par n :

$$m = qn + r \, ; \quad 0 \leq r < n$$

$r = m - qn \in H$; et $r < n$; par définition de n

On a $r = 0$; Ainsi $m = qn$; $m \in n\mathbb{Z}$.

i.e. $H \subset n\mathbb{Z}$ et enfin $H = n\mathbb{Z}$.

Rem Exo : $n\mathbb{Z} \subset m\mathbb{Z} \iff m \mid n$.

et $n\mathbb{Z} = m\mathbb{Z} \iff n = \pm m$.

Reprenons le morphisme $f : \mathbb{Z} \longrightarrow G$
$k \longrightarrow a^k$.

on a vu que $\langle a \rangle = \operatorname{Im} f$ est un sous groupe de G

$\operatorname{Ker} f$ est un sous groupe de $\mathbb{Z}$; il est donc de la forme $n\mathbb{Z}$.

Distinguons les deux cas:

1 Cas : $n=0$; f est donc injectif ;

et $f : \mathbb{Z} \longrightarrow \langle a \rangle$ est un isomorphisme

2 Cas : $n \neq 0$; $k \in \cancel{\mathrm{Imf}}$ Kerf. $\Leftrightarrow a^k = 1 \Leftrightarrow k \in n\mathbb{Z}$.

$\Leftrightarrow n \mid k$.

dans ce cas : n est le plus petit entier k tel que $a^k = 1$.

Ceci nous amène à la définition

Définition Soit G un groupe, $a \in G$.
s'il existe $k \neq 0$ tel que $a^k = 1$, on dit que a est d'ordre fini, on définit l'ordre a comme étant le plus petit ~~élément~~ entier k tel que $a^k = 1$;
s'il n'existe pas de k tel que $a^k = 1$, on dit que a est d'ordre infini.

Remarque 1 le seul élément de G d'ordre 1 est l'élément neutre.

2 si $|G|$ est fini, tout élément de G est d'ordre fini.

Définition : un groupe G est dit monogène, s'il est engendré par un seul élément ;

$G = \langle a \rangle$.

Si de plus G est fini ; on l'appelle groupe cylique.

Proposition : Soit G un groupe, $a \in G$ d'ordre n

1) pour tout $k \in \mathbb{Z}$; $a^k = 1$ ssi k est un multiple de n

2) $k, \ell \in \mathbb{Z}$, $a^k = a^\ell \Leftrightarrow$ $k - \ell$ est ~~un~~ multiple de n

3) des éléments, $1, a, a^2, \ldots, a^{n-1}$ sont deux à deux distincts ; le sous-groupe engendré par a contient n éléments.

$\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$,

preuve :

1) Soit $k \in \mathbb{Z}$, $a^k = 1$; $k = qn + r$; $r \in \{0, 1, \ldots, n-1\}$, (division euclidienne de k par n).

$1 = a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r = 1$

n est l'ordre de a, donc c'est le plus petit ~~tq~~ $a^n = 1$

donc $r = 0$;

2) si $a^k = a^\ell \Leftrightarrow a^{k-\ell} = 1 \Leftrightarrow k - \ell \equiv 0 \, [n]$

(3). d'après (2), $1, a, \ldots, a^{n-1}$ sont deux à deux distincts, il ~~a~~ reste à montrer que
$\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$.

$b \in \langle a \rangle \Leftrightarrow b = a^k, k \in \mathbb{Z}$, comme pour (1)
$k = qn + r$; $b = a^{qn+r} = a^r \in \{1, a, \ldots, a^{n-1}\}$

Corollaire : Soit G un groupe, $a \neq 1$ ~~un élément d'ordre~~ ~~p, p premier~~; $a^p = 1$; avec p premier;
l'ordre de $a = p$.

preuve : Soit n = ordre de a; $n \mid p$ donc $n = 1$ ou $n = p$, si $n = 1 \Rightarrow a = 1$ (élément neutre)
Cas exclu, donc $n = p$.

~~Coro~~ Corollaire. Soit G un groupe, $a \in G$. a est d'ordre ~~fini~~ n ssi $\langle a \rangle$ contient n éléments.

preuve : n = ordre $a \Rightarrow \langle a \rangle$ contient n éléments
(proposition précédente)
Supposons que $\langle a \rangle$ contient n éléments, a est donc d'ordre fini, soit p ~~son~~, et
$\langle a \rangle = p = n$.

(5)

Exemples :

1) dans $\mathbb{C}^*$; (-1) est d'ordre 2 ; i est d'ordre 4

$<(-1)> = \{1, -1\}$ (2 élément).

$<i> = \{1, i, i^2, i^3\} = \{1, i, -1, -i\}$.

$z = e^{\frac{2i\pi}{n}}$; $n \geq 1$;

z est d'ordre n ;

$<z> = \{1, z, z^2, \ldots, z^{n-1}\}$ est l'ensemble des racines $n$ième de l'unité ; c'est un groupe cyclique.

$n = 4$, on retrouve le sous-groupe $<i>$

(2) dans S_3 ; $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$:

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ = élément neutre !

$<\sigma> = <1, \sigma, \sigma^2>$; σ est d'ordre 3.

proposition : Soit $f : G \longrightarrow G'$ un morphisme

$a \in G$ d'ordre fini

1) $f(a)$ est d'ordre fini, son ordre divise l'ordre a

2) si f est bijective (isomorphisme) a et $f(a)$ ont même ordre.

preuve : 1) Soit n = ordre a ;

$$f(a^n) = f(1_G) = 1_{G'} = (f(a))^n.$$

il s'en suit que ordre de $(f(a))$ divise n.

2) si f est bijective, f^{-1} est un morphisme (vérifier le !)

On applique le résultat (1) ; on trouve que :

ordre $f(a) \mid n$ et $n \mid$ ordre de $f(a)$; ce qui permet de conclure que ordre $f(a) = n$ (les deux sont positifs).