CHAPITRE 2 Structure algébrique

§1 Loi de composition interne (运算)

Déf Soit E un ensemble. On appelle loi de composition (interne) toute application $*$ de $E \times E$ dans E.

Notation l'image de $(a,b) \in E \times E$ par $*$ est notée $a * b$.

On dit que $*$ est commutative (交换).

Si $\forall (a,b) \in E \times E,\ a * b = b * a$.

On dit que $*$ est associative (结合).

Si pour tous éléments x, y, z de E $(x * y) * z = x * (y * z)$

On dit que $e \in E$ est un élément neutre (单位元) pour $*$.

Si $\forall x \in E,\ x * e = e * x = x$

Exemple $(\mathbb{N}, +)$ élément neutre $= 0$

$(\mathbb{N}, \times)$ élément neutre $= 1$

E ensemble $(\mathrm{App}(E,E), \circ)$ (复合) élément neutre Id_E

Prop. Si l'élément neutre existe, alors il est unique.

Preuve Soient e et e' deux éléments neutres. On a $e = e * e' = e'$

§2 Groupe

Déf On appelle semi-groupe (半群) tout ensemble E muni (赋予) d'une loi de composition associative $*$. Si de plus E admet un élément neutre pour $*$, on dit que $(E, *)$ est un monoïde. (幺半群)

Soient $(A,\circ)$ et $(B,*)$ deux {monoïdes / semi-groupes}.

On appelle morphisme de semi-groupes tout application $f: A \to B$ telle que $\forall (x,y) \in A \times A \quad f(x,y) = f(x) * f(y)$

et qui envoie l'élément neutre de A sur celui de B

Si de plus f est une bijection, on dit que f est un isomorphisme (同构) de semi-groupes

Remarque Si f est un isomorphisme de semi-groupes, alors f^{-1} l'est aussi

soit $(B,*)$ un semi-groupe. On appelle sous-semi-groupe (子半群) de $(B,*)$, tout sous-ensemble B_0 de B tel que

$\forall (x,y) \in B_0 \times B_0$, $x * y \in B_0$ et qui contient l'élément neutre de B

(B_0 la restriction de $*$ à $B_0 \times B_0$) est un morphisme de semi-groupe

Remarque $i_{B_0}: B_0 \to B$ est un morphisme de semi-groupe

$(\mathbb{N},+) \to (\mathbb{N},\times)$ $2^{n+m} = 2^n \times 2^m$ morphisme de monoïde

$n \to 2^n$

$(\mathbb{N},\times)$ $\{0\} \subset \mathbb{N}$ sous-semi-groupe

Déf Soit $(A,*)$ un monoïde. Soit e l'élément neutre de A.

On dit que $x \in A$ est inversible s'il existe un élément $x^{-1} \in A$ tel que

$x * x^{-1} = x^{-1} * x = e$ (x^{-1} est unique)

Si tous les éléments de A sont inversibles, on dit que $(A,*)$ est un groupe.

Soient $(A,\circ)$ et $(B,*)$ deux groupes. On appelle morphisme de groupes de $(A,\circ)$ dans $(B,*)$ tout morphisme de monoïdes $f: A \to B$ tel que, pour tout $x \in A$, $f(x^{-1}) = f(x)^{-1}$

Si de plus f est une bijection, on dit que f est un isomorphisme de groupes.

Déf On appelle groupe tout monoïde $(G, *)$ tel que tout élément de G soit inversible.

Notation Sauf mention au contraire (除特殊说明外)
la loi de composition d'un groupe G et noté $(a,b) \mapsto ab$

Lemme Soit G un groupe. Un élément est G est l'élément neutre, si et seulement s'il existe $x \in G$ tel que $ex = x$

Preuve "$\Rightarrow$" résulte de la définition
"$\Leftarrow$" Soit e_0 l'élément neutre de G, On suppose qu'il existe $x \in G$, tel que $ex = x$. Soit y l'inverse de x dans G. On a $xy = e_0$. Donc $e = e\,e_0 = e(xy) = (ex)y = xy = e_0$

(若知 x, y 在同一群 G, 则写一遍 $xy = e$ 表可逆 不然则写 $yx = e$)

② Soient x, y deux éléments de G. Alors y est l'inversible de x Si Es Si $xy = e$
où e est l'élément neutre de G.

Preuve $\Rightarrow$ "résulte de la définition de l'inversible"
$\Leftarrow$ On a $x^{-1} = x^{-1}e = x^{-1}(xy) = \underline{(x^{-1}x)}y = \underline{ey} = y$

(右逆存在, 左逆不存在)
$x^{-1}x = e$ $ey = y$
相同

$(\mathbb{N}, +)$ est un monoïde

Prop Soient A et B deux groupe, $f: A \to B$ un moiphisme de semi-groupes ($\forall (x,y) \in A \times A$, $f(xy) = f(x)f(y)$)
Alors (1) $f(e_A) = e_B$, où e_A et e_B sont des éléments neutres de A et B, respectivement (分别)

群的单群多出来单位的逆

(2) $\forall x \in A$, $f(x^{-1}) = f(x)^{-1}$
f est appelé ainsi un morphisme de groupe

Preuve (1) $f(e_A) = f(e_A e_A) = f(e_A) f(e_A) \overset{\text{Lemme}}{\Rightarrow} f(e_A) = e_B$

(2) $e_B = f(e_A) = f(x x^{-1}) = f(x) f(x^{-1}) \overset{\text{Lemme}}{\Rightarrow} f(x^{-1}) = f(x)^{-1}$

Déf Soit G un groupe. On appelle sous-groupe de G tout sous-monoïde H de G qui est stable par l'inversible ($\forall x \in H,\ x^{-1} \in H$)

eg $G = (\mathbb{Z}, +)$ $H = 2\mathbb{Z} = \{\text{nombres pairs}\}$ est un sous-groupe de G

$0 \in H$ $\forall n \in 2\mathbb{Z}$, $-n \in 2\mathbb{Z}$

Prop Soient G un groupe et H un sous-ensemble non vide de G. Pour que H soit un sous-groupe de G, il faut et il suffit (缺且仅缺) que, $\forall (g,h) \in H^2$, $gh^{-1} \in H$

充分(必要)条件 H是G的子群的充要条件是 $\forall (g,h) \in H^2$, $gh^{-1} \in H$

condition suffisante et nécessaire

Preuve Nécessité (必要性) "$\Rightarrow$"

Si H est un sous-groupe de G. pour $(g, h) \in H \times H$, on a $h^{-1} \in H$ et donc $gh^{-1} \in H$.

Suffisance (充分性) "$\Leftarrow$" Comme H est non vide, il existe $a \in H$. On obtient $e = aa^{-1} \in H$, où e est l'élément neutre de G.

$\forall (g,h) \in H \times H$, on a $h^{-1} = eh^{-1} \in H$ et $gh = g(h^{-1})^{-1} \in H$ ✳

Remarque Si H est un sous-groupe de G, H muni de la restriction de la loi de composition de G forme un groupe, et l'application d'inclusion $i_H : H \to G$ est un morphisme de groupes.

$n \in \mathbb{N}, n \geq 2$

$\forall a \in \mathbb{Z}$ $\exists$ unique $r(a) \in \{0, \cdots n-1\}$

tel que n divise $a - r(a)$
整除

$r(a)$ est appelé le reste de a divise par n

$a \equiv r(a) \pmod n$

$(a,b) \in \mathbb{Z} \times \mathbb{Z}$, $r(a)+r(b) \equiv r(a+b) \pmod n$

Déf Soit M un ensemble. On appelle relation d'équivalence tout relation binaire $\sim$ sur M telle que. (等价关系)

自反 (i) $\forall x \in M$, $x \sim x$

对称 (ii) $\forall (x,y) \in M \times M$, Si $x \sim y$, alors $y \sim x$

传递 (iii) $\forall (x,y,z) \in M \times M \times M$, Si $x \sim y$ et $y \sim z$, alors $x \sim z$

Pour tout $x \in M$, on désigne par $[x]$ l'ensemble des $y \in M$ tel que $x \sim y$. $[x]$ est appelé la classe d'équivalance de x

Proposition (i) $\forall (x,y) \in M \times M$ $[x] = [y]$ Si es Si $x \sim y$

(ii) $\forall (x,y) \in M \times M$, Si $[x] \neq [y]$, alors $[x] \cap [y] = \emptyset$

(iii) M s'écrit comme une union disjointe de classe d'équivalance.

Ex $M = \mathbb{Z}$ $x \sim y$ si et seulement Si $x-y$ est divisible par n. $n \in \mathbb{N}$ $n \geq 2$

Soit $a \in \mathbb{Z}$ on dit que n divise a et on noté n/a s'il existe $b \in \mathbb{Z}$

tel que $a = bn$

$x - x = 0 = 0 \cdot n$

Si $x - y = bn$, alors $y - x = (-b) n$

- Si $x - y = b_1 n$, $y - z = b_2 n$ alors $x - z = (b_1 + b_2) n$

Preuve

(1) "⇒" Comme $[x]=[y]$, on a $y\in[x]$, donc $x\sim y$

"⇐" Soit $z\in[x]$, on a $x\sim z$. Or $x\sim y$ donc $z\sim y$ et $z\in[y]$

On obtient donc $[x]\subset[y]$

De même $[y]\subset[x]$ Donc $[x]=[y]$

(2) Montrons la contraposition (逆否命题) de l'énancé.

On suppose que $z\in[x]\cap[y]$ Comme $z\in[x]$, $x\sim z$.

De même, $y\sim z$ Donc $x\sim y$ par (1) $[x]=[y]$

(3) $M=\bigcup_{x\in M}[x]$ Par (1) et (2) M s'écrit comme

$\bigcup_{\alpha\in\{[x]\mid x\in M\}}\alpha$ qui est une union disjointe.

同余分类.

等价类

On note M/N l'ensemble des classes d'équivalence dans M.

$M/N=\{[x]\mid x\in M\}$

$n\mid(x-y)$

n 整除 $(x-y)$

On a une application surjective $\pi: M\to M/N$

appelée la projection. $x\mapsto[x]$

Ex $M=\mathbb{Z}$ $x\sim y$ si et si $n\mid(x-y)$ $n\in\mathbb{N}$, $n\geq 2$

$M/N=\{n\mathbb{Z}=[0], n\mathbb{Z}+1=[1], \dots n\mathbb{Z}+(n-1)=[n-1]\}=\mathbb{Z}/n\mathbb{Z}$

Ex Soit G un groupe. On dit qu'un sous-groupe H de G est distingué (正规子群) Si, pour tout $g \in G$, on a

$$H = \{a \in H \mid gag^{-1}\} =: gHg^{-1}$$

On note $H \triangleleft G$ Si H est un sous-groupe distingué.

Si G est un groupe abélien, c'est-à-dire la loi de composition de G est commutatif, alors tout sous-groupe de G est distingué.

En effet, $\forall a \in H$, et $g \in G$, $gag^{-1} = agg^{-1} = a$

Prop. Soient G un groupe et H un sous-groupe de G. Alors la relation $x \sim y$ Si $e \leq Si$ $xy^{-1} \in H$ est une relation d'équivalence sur G. L'ensemble quotient $G/\sim$ est noté $H\backslash G = \{Hx \mid x \in G\}$

Preuve Soit e l'élément neutre de G.

- $\forall x \in G \quad xx^{-1} = e \in H$
- $\forall (x, y) \in G \times G$ Si $xy^{-1} \in H$, alors $(xy^{-1})^{-1} = (y^{-1})^{-1}x^{-1} = yx^{-1} \in H$
- $\forall (x, y, z) \in G \times G \times G$. On suppose $xy^{-1} \in H$ et $yz^{-1} \in H$.

  Alors $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xez^{-1} = xz^{-1} \in H$

Prop. Soient G un groupe et H un sous-groupe de G. Alors la relation $x \sim y$ Si $e \leq Si$ $y^{-1}x \in H$ est une relation d'équivalence sur G. L'ensemble quotient $G/\sim$ est noté $G/H = \{xh \mid h \in H\}$

Remarque Si H est distingué, alors $\forall x \in G$ on a $xH = Hx$.

$(ab)^{-1} = b^{-1}a^{-1}$

$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$

$Si \; e \leq Si$ = Si et seulement si

Théorème

Soient G un groupe, et $H \triangleleft G$. Alors l'application

$$G/H \times G/H \longrightarrow G/H$$
$$(xH, yH) \longmapsto xyH$$

est bien définie et munit G/H d'une structure de groupe dont l'élément neutre est $eH = H$, où e est l'élément neutre de G.

De plus, la projection $\pi : G \to G/H$ est un morphisme de groupes.

Ex

$G = (\mathbb{Z}, +)$ $H = n\mathbb{Z}$ $(n \in \mathbb{N}, n \geq 2)$

等价类可做 + 同余类 +

$x \mathcal{R} y$ si et seulement si $x - y \in H$, $(n \mid x-y)$

$\mathbb{Z}/n\mathbb{Z} = G/H = \{[0], \dots [n-1]\}$

$[x] + [y] = [x+y]$ loi sur $\mathbb{Z}/n\mathbb{Z}$

$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ $x \mapsto [x]$

Preuve

Montrons que $(*)$ est bien définie.

Soient x_1, x_2, y_1, y_2 des éléments de G tels que

$x_1 H = x_2 H$ et $y_1 H = y_2 H$

Montrons que $x_1 y_1 H = x_2 y_2 H$

Comme $H \triangleleft G$. $x_1 y_1 H = x_1 H y_1 = x_2 H y_1 = x_2 y_1 H = x_2 y_2 H$

Cette loi est associative on a

$(xH)(yH)(zH) = (xyH)(zH) = (xyz)H = xH(yH)(zH))$

$\forall x \in G$, on a $(eH)(xH) = (xH)(eH) = xH$

$\forall x \in G$, on a $(xH)(x^{-1}H) = (xx^{-1})H = eH = (x^{-1}H)(xH)$

Ex $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$

$[0] + [1] = [1]$

$[1] + [1] = [0]$

Déf On appelle anneau (环) tout ensemble A muni de deux lois de composition internes $(a,b) \mapsto a+b$ et $(a,b) \mapsto ab$ telle que

(1) $(A,+)$ forme un groupe abélien dont l'élément neutre est noté 0.

(2) $(A,\times)$ forme un monoïde dont l'élément neutre est noté 1 et appelé l'unité de A.

(3) $\forall (a,b,c) \in A\times A\times A$

$a(b+c) = ab+ac$

$(b+c)a = ba+ca$

- Si la loi $(a,b) \mapsto ab$ est commutatif, on dit que A est commutatif.
- Si $\forall \dot{a} \in A\setminus\{0\}$, a est inversible pour la loi de multiplication, $0 \neq 1$ et on dit que A est un corps. (体)