



Morphismes de G -esp

DÉFINITION 2.8. Soient $(G, \star)$ et $(H, *)$ deux groupes, un morphisme de groupes $\varphi : G \mapsto H$ est une application telle que

$$\forall g, g' \in G, \varphi(g \star g') = \varphi(g) * \varphi(g').$$

On notera

$$\text{Hom}_{Gr}(G, H)$$

l'ensemble des morphismes de G vers H .

Noyau - Image

PROPOSITION 2.4. (*Invariance des sous-groupes par morphismes*) Soit $\varphi \in \text{Hom}_{Gr}(G, H)$ un morphisme de groupes.

(1) Soit $K \subset G$ un sous-groupe alors $\varphi(K) \subset H$ est un sous-groupe. En particulier l'image de φ ,

$$\text{Im}(\varphi) = \varphi(G) \subset H$$

est un sous-groupe de H .

(2) Soit $L \subset H$ un sous-groupe de H , alors la preimage

$$\varphi^{(-1)}(L) = \{g \in G, \varphi(g) \in L\} \subset G$$

est un sous-groupe de G . En particulier $\varphi^{(-1)}(\{e_H\})$ est un sous-groupe de G .

DÉFINITION 2.9. Le sous-groupe $\varphi^{(-1)}(\{e_H\})$ s'appelle le noyau de φ et est noté

$$\ker(\varphi) = \varphi^{(-1)}(\{e_H\}) = \{g \in G, \varphi(g) = e_H\}.$$

THÉORÈME 2.7 (Critère d'injectivité). Soit $\varphi \in \text{Hom}_{Gr}(G, H)$ un morphisme de groupes alors les propriétés suivantes sont équivalentes

- (1) φ est injectif,
- (2) $\ker(\varphi) = \{e_G\}$.

THÉORÈME 2.8. Soit $\varphi : G \mapsto H$ un morphisme de groupes et $\ker(\varphi) \subset G$ son noyau. Alors pour tout $g \in G$ on a l'égalité suivante entre ensembles

$$g \cdot \ker(\varphi) \cdot g^{-1} = \{g \cdot k \cdot g^{-1}, k \in \ker(\varphi)\} = \ker(\varphi).$$

PROPOSITION 2.5. (*Invariance par composition et par reciproque*) Soient $(G, \star), (H, *), (K, \otimes)$ des groupes et

$$\varphi : G \mapsto H \text{ et } \psi : H \mapsto K$$

des morphismes de groupes alors la composee $\psi \circ \varphi : G \mapsto K$ est un morphisme de groupes.

Supposons que $\varphi : G \mapsto H$ un morphisme de groupes bijectif alors l'application reciproque

$$\varphi^{-1} \in \text{Hom}_{\text{Gr}}(H, G)$$

est un morphisme de groupe bijectif.

COROLLAIRE 2.4. *L'ensemble des automorphismes de G*

$$\text{Aut}_G(G) \subset \text{Bij}(G) = G_6$$

est un sous-groupe pour la composition $\circ$.

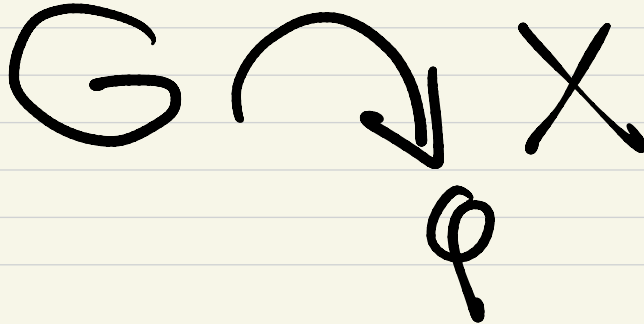
Action d'un gpe sur un
ensemble

$$(G_X, \circ)$$

DÉFINITION 2.11. Soit $(G, \star)$ un groupe, X un ensemble et $(\text{Bij}(X), \circ)$ le groupe symétrique de X (des bijections de X sur lui-même). Une action (à gauche) de G sur X est la donnée d'un morphisme

$$\varphi : G \mapsto \text{Bij}(X).$$

On dit alors que G agit sur X (à gauche) à travers le morphisme φ et on le note $G \curvearrowright_{\varphi} X$.



PROPOSITION 2.6. La donnée d'une action $G \curvearrowright_{\varphi} X$ est équivalente à la donnée d'une application (appelée loi de composition externe)

$$\bullet \odot \bullet : \begin{array}{ccc} G \times X & \mapsto & X \\ (g, x) & \mapsto & g \odot x \end{array} \quad (= \varphi(g)(x))$$

verifiant

(1) neutralité de l'élément neutre:

$$\forall x \in X, e_G \odot x = x,$$

(2) associativité: $\forall x \in X, g, g' \in G,$

$$(g \star g') \odot x = g \odot (g' \odot x).$$

(3) simplification: en combinant les deux propriétés précédentes on a $\forall x \in X, g \in G,$

$$g \odot (g^{-1} \odot x) = g^{-1} \odot (g \odot x) = x.$$

THÉORÈME 2.10. L'application translation à gauche

$$t_{\bullet} : \begin{array}{ll} G & \mapsto \text{Bij}(G) \\ g & \mapsto t_g : g' \mapsto g.g' \end{array}$$

est un morphisme de groupes de $(G, \cdot)$ vers $(\text{Bij}(G), \circ)$. Le morphisme $t_{\bullet}$ définit donc une action à gauche de G sur G qu'on appellera action par translations à gauche et qu'on notera $G \curvearrowright_t G$.

EXERCICE 2.6. Soit G un groupe et

$$t_{\bullet} : \begin{array}{ll} G & \mapsto \text{Bij}(G) \\ g & \mapsto t_g : G \mapsto G \end{array}$$

l'action par translation à gauche de G vers G .

(1) Montrer que $t_{\bullet}$ est injective.

En conséquence le gpe G est isomorphe à son image $t_G = \{t_g \mid g \in G\} \subset \text{Bij}(G)$ et donc G peut être identifié à un sous-groupe de $\text{Bij}(G)$.

Conjugaison : $g \in G$

$$\text{Ad}_g : g' \in G \longrightarrow g g' g^{-1} \in G$$

est un morphisme de G vers G (pour g ds G fixé).

Il est injectif : $\underset{\{e_G\}}{g' \in G} \text{ tq } g g' g^{-1} = e_G$ c'est

et fait il est bijective et sa
reciproque c'est $\text{Ad}_g^{-1}: g' \rightarrow g^{-1}g'g$.

On regarde

$$\begin{array}{ccc} \text{Ad} \cdot : G & \longrightarrow & \text{Bij}(G) \\ g & \longmapsto & \text{Ad}_g \end{array}$$

PROPOSITION 2.7. Pour tout g , l'application $\text{Ad}_g : G \mapsto G$ est un isomorphisme de groupes (ie $\text{Ad}_g \in \text{Aut}_{Gr}(G)$) dont l'application reciproque vaut

$$\text{Ad}_g^{-1} = \text{Ad}_{g^{-1}} : G \xrightarrow{\sim} G.$$

De plus l'application

$$\text{Ad}_\bullet : \begin{array}{ccc} G & \mapsto & \text{Bij}(G) \\ g & \mapsto & \text{Ad}_g \end{array}$$

est un morphisme de groupes.

Preuve: (que $\text{Ad}_\bullet$ st un morphisme de gres)

On veut mq $\forall g_1, g_2 \in G$

$$\text{Ad}_{g_1 g_2} = \text{Ad}_{g_1} \circ \text{Ad}_{g_2} ?$$

$$\text{Ad}_{g_1 g_2} = \text{Ad}_{g_1} \circ \text{Ad}_{g_2}$$

on prend $g' \in G$ et on calcule

$$\text{Ad}_{g_1 g_2}(g') = g_1 g_2 g' (g_1 g_2)^{-1}$$

$$= g_1 g_2 g' g_2^{-1} g_1^{-1}$$

$$= g_1 \text{Ad}_{g_2}(g') g_1^{-1}$$

$$= \text{Ad}_{g_1}(\text{Ad}_{g_2}(g')) = \text{Ad}_{g_1} \circ \text{Ad}_{g_2}(g')$$



DÉFINITION 2.12. *L'application de conjugaison*

$$\begin{array}{lll} \text{Ad} : & G & \mapsto \text{Bij}(G) \\ & g & \mapsto \text{Ad}_g \end{array}$$

étant un morphisme de groupes, elle définit une action à gauche de G sur G (par automorphismes de groupes) qu'on appelle action par conjugaison et qu'on notera $G \curvearrowright_{\text{Ad}} G$.

L'image de ce morphisme

$$\text{Ad}_G = \{\text{Ad}_g, g \in G\} \subset \text{Aut}_{Gr}(G) \subset \text{Bij}(G)$$

(formée d'automorphismes de groupe) et est appelée groupe des automorphismes "intérieurs" de G et est notée

$$\text{Ad}_G = \text{Int}_{Gr}(G) = \text{Inn}_{Gr}(G).$$

("Inn" pour "Inner").

$$\ker \text{Ad} = \{g \in G \mid \text{Ad}_g = \text{Id}_G\}$$

$$\ker \text{Ad}_\bullet = \{g \in G \mid \text{Ad}_g = \text{Id}_G\} = \underset{\text{"}}{\mathbb{Z}}_G$$

$$g \in G \mid \text{Ad}_g = \text{Id}_G \quad \swarrow \text{le centre de } G$$

$$\iff \forall g' \in G \quad gg'g^{-1} = g'$$

$$\iff \forall g' \in G \quad gg' = g'g$$

$\ker \text{Ad}_\bullet =$ l'ensemble de elts de G qui commutent avec tous les elts de G

Action à droite: Cas de la translation

à dr: $g \in G$

$$td_g: g' \rightarrow g'g$$

td_g une bij de G sur G de réciproque

$$td_{g^{-1}}.$$

$$\text{td}_{g_1 g_2}(g') = g' g_1 g_2$$

$$= \text{td}_{g_2}(\text{td}_{g_1}(g'))$$

$$\text{td}_{g_1 g_2} = \text{td}_{g_2} \circ \text{td}_{g_1}$$

DÉFINITION 2.13. Soient $(G, \star)$ et $(H, *)$ deux groupes, un anti-morphisme de groupes $\varphi : G \mapsto H$ est une application telle que

$$\forall g, g' \in G, \varphi(g \star g') = \varphi(g') * \varphi(g).$$

PROPOSITION 2.7. Une application entre groupes $\varphi : G \rightarrow H$ est un anti-morphisme de groupes ssi

$$\varphi \circ \bullet^{-1} : g \mapsto \varphi(g^{-1})$$

est un morphisme de groupes ou bien ssi

$$\bullet^{-1} \circ \varphi : g \mapsto \varphi(g)^{-1}$$

est un morphisme de groupes.

Preuve: Exercice.

□

DÉFINITION 2.14. Soit $(G, \star)$ un groupe, X un ensemble et $(\text{Bij}(X), \circ)$ le groupe symétrique de X (des bijections de X sur lui-même). Une action à droite de G sur X est la donnée d'un antimorphisme de groupes

$$\varphi : G \mapsto \text{Bij}(X).$$

On dit alors que G agit sur X à droite à travers φ et on le note $X \curvearrowright_{\varphi} G$.

PROPOSITION 2.8. La donnée d'une action à droite $X \curvearrowright_{\varphi} G$ est équivalente à la donnée d'une application

$$\bullet \odot \bullet : \begin{array}{ll} X \times G & \mapsto X \\ (x, g) & \mapsto x \odot g \end{array}$$

verifiant

- (1) neutralité de l'élément neutre: $\forall x \in X, x \odot e_G = x$,
- (2) associativité: $\forall x \in X, g, g' \in G, x \odot (g \star g') = (x \odot g) \odot g'$.
- (3) simplification: en combinant les deux propriétés précédentes on a $\forall x \in X, g \in G$,

$$(x \odot g) \odot g^{-1} = (x \odot g^{-1}) \odot g = x.$$

Exemples: translation à dte ds G

$td_\bullet: G \longrightarrow td_g \in \text{Bij}(G)$
est une action à dte.

$td_\bullet$ est un antimorphisme de G
vers $\text{Bij}(G)$

on peut fabriquer à l'aide de la
translation à dte une action à
gauche:

on pose

$$\widetilde{td}_g = td_{g^{-1}}: g^1 \longrightarrow g^1 g^{-1}$$

$\widetilde{\text{td}}$ est un morphisme de SpkS et
 définit une action à gauche
 de $G \curvearrowright G$.

$$\begin{aligned}\widetilde{\text{td}}_{g_1 g_2}(g') &= g'(g_1 g_2)^{-1} = g'^{-1} g_2^{-1} g_1^{-1} \\ &= \widetilde{\text{td}}_{g_1}(\widetilde{\text{td}}_{g_2}(g'))\end{aligned}$$

Autre exemple d'action à droite:

Soit $G \curvearrowright X$ l'action est donnée par

$$g \odot \bullet : x \longrightarrow g \odot x$$

Considérons $\mathcal{F}(X; \mathbb{R})$

$$= \{ f : x \in X \rightarrow f(x) \in \mathbb{R} \}$$

l'action $G \curvearrowright X$ induit une action à droite $\overline{f}(X; \mathbb{R}) \curvearrowright G$

$$(f, g) \longrightarrow f^g : x \longrightarrow f(g \odot x)$$

• $^g : f \longrightarrow f^g$ est une action à droite de G sur $\overline{f}(X, \mathbb{R})$

ie.

$$\int g_1 * g_2$$

$$= \left(\int g_1 \right) g_2$$

$$= (\bullet) \int g_2 \left(\int g_1 \right) \bullet$$



Anneaux

Հիմա՛ պահքը՛նք. հիմա՛ պահքը՛նք
հիմա՛ պահքը՛նք. պահ՛նք հիմա՛նք

Three rings for the Elven-kings under the sky,

$\mathbf{B}_{\text{cris}}, \mathbf{B}_{\text{st}}, \mathbf{B}_{\text{dR}},$

Seven for the Dwarf-lords in their halls of stone,

$\mathbf{E}_{\mathbf{Q}_p}, \mathbf{A}_{\mathbf{Q}_p}, \mathbf{B}_{\mathbf{Q}_p}, \mathbf{E}, \mathbf{A}, \mathbf{B}, \tilde{\mathbf{A}},$

Nine for mortal Men doomed to die,

$\mathbf{Q}_p, \mathbf{Z}_p, \mathbf{F}_p, \overline{\mathbf{Q}}_p, \overline{\mathbf{F}}_p, \mathbf{C}_p, \mathcal{O}_{\mathbf{C}_p}, \mathbf{Q}_p^{\text{nr}}, \mathbf{B}_{\text{HT}},$

One ring to rule them all,

$\mathbf{A}_{\text{inf}}.$

DÉFINITION 3.1. *Un anneau $(A, +, \cdot, 0_A, 1_A)$ est la donnée, d'un groupe commutatif $(A, +)$ (note additivement) d'élément neutre note 0_A , d'une loi de composition interne (dite de multiplication)*

$$\bullet \bullet : \begin{array}{ll} A \times A & \mapsto A \\ (a, b) & \mapsto a \cdot b \end{array}$$

et d'un élément unité $1_A \in A$ ayant les propriétés suivantes

(1) Associativité de la multiplication:

$$\forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c.$$

(2) distributivité:

$$\forall a, b, c \in A, (a + b) \cdot c = a \cdot c + b \cdot c, c \cdot (a + b) = c \cdot a + c \cdot b.$$

(3) Neutralité de l'unité:

$$\forall a \in A, a \cdot 1_A = 1_A \cdot a = a.$$

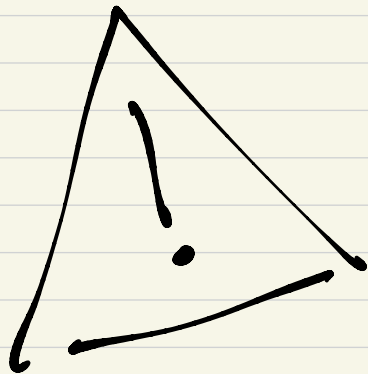
Un anneau est dit commutatif si de plus la multiplication est commutative:

$$\forall a, b \in A, a \cdot b = b \cdot a.$$

Exemples $(\mathbb{Z}, +, 0, \times, 1)$

$(\mathbb{Q}, +, 0, \times, 1)$ $(\mathbb{R}, +, 0, \times, 1)$

$(\mathbb{C}, +, 0, \times, 1)$



la multiplication ne donne
pas forcément une loi de
gpe (d'elt neutre)
1A

- L'anneau nul: $Nul = \{0\}$
avec $1_{Nul} = 0$ et les lois $+$ et $\times$
étant évidente.

- Produit d'anneaux

A, B est anneaux le produit

$(A \times B, (+_A, +_B), (0_A, 0_B), (\times_A, \times_B), (1_A, 1_B))$
forme un anneau.

$$\mathbb{Z}/q\mathbb{Z} = \{ a(q) = a + \mathbb{Z}q \mid a \in \mathbb{Z} \} \subset \mathcal{P}(\mathbb{Z})$$

$(\mathbb{Z}/q\mathbb{Z}, +, 0(q) = \mathbb{Z}q)$ est un gpe commutatif

La multiplication est définie comme suit

$$a(q) \times b(q) := a.b \ (q)$$

On doit vérifier que cette définition ne
depend pas des choix des $a, b \in \mathbb{Z}$
qui permettent d'écrire $a(q)$ et $b(q)$

ie: si $a'(q) = a(q)$ et $b'(q) = b(q)$

alors $a'b'(q) = ab(q)$.

→ on vérifie que on obtient un
anneau (fini de cardinal q)

et d'unité

$$1_{\mathbb{Z}/q\mathbb{Z}} = 1(q) = 1 + \mathbb{Z}q.$$

L'anneau $\mathbb{Z}/q\mathbb{Z}$ est commutatif

$$a(q) \times b(q) = ab(q) = ba(q) = b(q) \times a(q).$$

Anneau de fcts: $X = \text{ens}$

$$\mathcal{F}(X; \mathbb{R}) = \{ f: x \mapsto f(x) \in \mathbb{R} \}$$

$\mathcal{F}(X; \mathbb{R})$ a une structure d'anneau
provenant de celle de $\mathbb{R}$:

$$f_1, f_2: X \rightarrow \mathbb{R}$$

$$f_1 + f_2: x \mapsto f_1(x) + f_2(x)$$

$$f_1 \cdot f_2: x \mapsto f_1(x) \cdot f_2(x)$$

$$0_{\mathcal{F}(X; \mathbb{R})} = \underline{0} = \int d \text{ cst} = \tilde{a} 0.$$

$$1_{\mathcal{F}(X; \mathbb{R})} = \underline{1} = \int d \text{ cst} = \tilde{a} 1.$$

Si A est un anneau qque
 $F(X; A)$ a une structure
canonique d'anneau.

- Anneaux de Polynomes:

$A = \mathbb{R}$ $\mathbb{R}[X] =$ set polynomiales
de $\mathbb{R}$ vers $\mathbb{R}$.

- Si A est un anneau commutatif que
on peut définir son anneau de
polynômes $A[X] =$ anneau des poly-
nômes à coeffs ds A mais c'est un
peu plus formel.

Anneaux de Matrices 2×2 :

A anneau commutatif.

$$M_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in A \right\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

Produit de matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

$(M_2(A), +, \times)$ forme un anneau
(non-commutatif)

$$0_{M_2(A)} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$1_{M_2(A)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Anneaux d'endomorphismes

$(M, +)$ un gpe commutatif.

$$\text{End}(M) = \text{End}_G(M) = \text{Hom}_G(M, M)$$

$$- \varphi, \psi \in \text{End}_G(M)$$

$$\varphi + \psi: m \in M \mapsto \varphi(m) + \psi(m) \in M$$

on doit vérifier que $\varphi + \psi$ est bien un morphisme

$$\begin{aligned}(\varphi + \psi)(m + m') &= \varphi(m + m') + \psi(m + m') \\&= \varphi(m) + \varphi(m') + \psi(m) + \psi(m') \\&= \varphi(m) + \psi(m) + \varphi(m') + \psi(m') \\&= (\varphi + \psi)(m) + (\varphi + \psi)(m') .\end{aligned}$$

Le produit de $\text{End}(M)$ est donné par la composition :

$$(\varphi, \psi) \in \text{End}(M) \rightarrow \varphi \circ \psi \in \text{End}(M)$$

On vérifie que $\underline{0}_M : m \in M \rightarrow 0_M$
est neutre pour $+$, on sait que l'identité
 $\text{Id}_M : m \rightarrow m$ est neutre pour $\circ$

distributive: $\varphi, \psi, \theta \in \text{End}_{\text{Gr}}(M)$

on veut m q

$$- (\varphi + \psi) \circ \theta \stackrel{?}{=} \varphi \circ \theta + \psi \circ \theta$$

$$- \theta \circ (\varphi + \psi) \stackrel{?}{=} \theta \circ \varphi + \theta \circ \psi$$

$$m \in M$$

$$(\varphi + \psi) \circ \theta(m) = (\varphi + \psi)(\theta(m))$$

$$= \varphi(\theta(m)) + \psi(\theta(m))$$

$$= \varphi \circ \theta(m) + \psi \circ \theta(m)$$

A commutatif

Rmq: si $M = (A \times A, (+, +))$ alors l'anneau $\square$
 $M_2(A)$ s'identifie avec $\text{End}_G(A^2)$

pour le voir on note que

$\varphi \in \text{End}(A^2)$ est complètement déterminé
par $\varphi(1_A, 0)$ et $\varphi(0, 1_A)$

on écrit $\varphi(1_A, 0) = (a, c) \quad a, c \in A$
 $\varphi(0, 1_A) = (b, d) \quad b, d \in A$

LEMME 3.1. Pour tout $a, b \in A$, on a

$$0_A \cdot a = a \cdot 0_A = 0_A,$$

(on dit que l'élément neutre de l'addition 0_A est absorbant). Pour l'opposé, on a

$$(-a) \cdot b = -(a \cdot b) = a \cdot (-b).$$

Preuve: on sait que $\forall a \in A$

$$a = a \cdot 1_A = 1_A \cdot a$$

$$a = 1_A \cdot a = (1_A + 0_A) \cdot a = 1_A \cdot a + 0_A \cdot a$$

$$= a + 0_A \cdot a$$

$$\Rightarrow 0_A \cdot a = 0_A.$$

pour l'opposé on écrit que

$$(a + (-a)) \cdot b = 0_A \cdot b = 0_A$$

$$a \cdot b + (-a) \cdot b = 0_A$$

$$\Rightarrow -(a \cdot b) = (-a) \cdot b \dots$$



Exo: $\forall 1_A$ est unique

si $1'_A$ vérifie $a = a \cdot 1'_A = 1'_A \cdot a$ alors $1'_A = 1_A$

Exo: $\forall$ si $0_A = 1_A \Rightarrow A = \{0\}$.

Elements Inversibles

Unités

DÉFINITION 3.2. Soit A un anneau. Un élément $a \in A$ est inversible si il existe $b \in A$ tel que

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse (à gauche et à droite) de a (pour la multiplication).

Ex: 0_A n'admet pas d'inverse sauf si $A = \{0\}$

PROPOSITION 3.1. (Unicité de l'inverse) Soit A un anneau et $a \in A$ un élément inversible et soit b tel que $a.b = b.a = 1_A$.

Soit b' vérifiant

$$a.b' = 1_A$$

alors $b' = b$; de même si b' vérifie

$$b'.a = 1_A$$

alors $b' = b$

Preuve: soit b' tq $a.b' = 1_A$

$$a.b' = 1_A \Rightarrow b.a.b' = b.1_A = b$$

$\times b \text{ a}$
gauche

$$1_A.b' = b$$
$$b' = b$$



NOTATION 3.1. Par la Proposition precedente si un element $a \in A$ est inversible son inverse est unique. On notera cet inverse

$$a^{-1}.$$

Notons que a^{-1} est egalement inversible et on a

$$(a^{-1})^{-1} = a.$$

On deduit de cette discussion que

PROPOSITION 3.2. Soit $A^\times$ l'ensemble des elements inversibles d'un anneau A , alors

$$(A^\times, \cdot, 1_A, \bullet^{-1})$$

forme un groupe: le groupe des elements inversibles de A .

$A^\times$ s'appelle aussi le
gpe des unites de l'anneau

Attention: $\mathbb{R}^* = \mathbb{R} - \{0\}$
 $\quad \quad \quad = \mathbb{R}^\times$

$\mathbb{Z}^* = \mathbb{Z} - \{0\}$
 $\quad \quad \quad \neq$
 $\mathbb{Z}^\times = \{+1, -1\}$

Examples $\mathbb{L}^* = \{\pm 1\} \neq \mathbb{L} - \{0\}.$

$$\mathbb{Q}^* = \mathbb{Q}^* = \mathbb{Q} - \{0\}$$

$$\mathbb{R}^* = \mathbb{R}^* = \mathbb{R} - \{0\} \quad \mathbb{C}^* = \mathbb{C}^* = \mathbb{C} - \{0\}.$$

$$- \{0\}^* = \{0\}$$

$$(\mathbb{Z}/q\mathbb{Z})^* = \{ a(q) = a + q\mathbb{Z} \mid (a, q) = 1 \}$$

Preuve: $\subset$: soit $a(q)$ inversible il existe

$$b \in \mathbb{Z} \text{ tq } a(q) \cdot b(q) = 1(q)$$

$$\parallel$$

$$ab(q) = 1(q)$$

$$ab + q\mathbb{Z} = 1 + q\mathbb{Z}$$

$$\text{il existe } c \in \mathbb{Z} \text{ tq } ab = 1 + qc$$

$$\Rightarrow ab - qc = 1$$

$\Rightarrow a \wedge q = 1$: si p premier divise a

et q
on aura que $p \mid ab - qc = 1$.

$\supset$: si $a \wedge q = 1$ alors $q(q)$ est inversible
dans $\mathbb{Z}/q\mathbb{Z}$

Par Bezout: comme $a \wedge q = 1$ il existe
 $b, c \in \mathbb{Z}$ tq

$$ab + qc = 1 \implies ab(q) = 1(q)$$

(ab et 1 différent par
un multiple de q)

U

□

- Si A, B sont des anneaux
le groupe des elts inversible de
 $A \times B$:

$$(A \times B)^{\times} = A^{\times} \times B^{\times}.$$

EXERCICE 3.2. Soit A un anneau commutatif et $M_2(A)$ l'anneau des matrices à coefficients dans A . Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$, la transposée de la matrice des *cofacteurs* de M est la matrice définie par

$$\text{tcof}(M) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(1) Montrer que

$$M \cdot \text{tcof}(M) = \text{tcof}(M) \cdot M = \det(M) \cdot \text{Id}_2 = \begin{pmatrix} \det(M) & 0 \\ 0 & \det(M) \end{pmatrix}$$

ou $\det(M)$ (le déterminant de M) est défini par

$$\det(M) := ad - bc \in A.$$

(2) En déduire que

$$M_2(A)^\times =: \text{GL}_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in A, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in A^\times \right\}.$$

$$\text{si } \det(M) = ad - bc \in A^\times \quad M^{-1} = (\det(M))^{-1} \cdot \text{tcof}(M).$$

$$M_2(\mathbb{Z})^{\times} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ tq } ad - bc = \pm 1 \right\}.$$

$M =$ gpe commutatif

$$\text{End}_{Gr}^{\times}(M) = \text{Aut}_{Gr}(M) = \text{ls morphismes. de } M \text{ vers } M \text{ bijectifs}$$

DÉFINITION 3.3. Soit $(A, +, \cdot)$ un anneau commutatif et $a, c \in A$, on dit que a divise c et on le note

$$a|c$$

si il existe $b \in A$ tel que

$$c = a.b.$$

On dit également que a est un diviseur de b .

- EXERCICE 3.3.
- (1) Montrer que la relation de divisibilité est réflexive et transitive.
 - (2) Montrer que tout élément du groupe des unités $A^\times$ est un diviseur de tout élément de A .
 - (3) Quels sont les diviseurs de 0_A ? de 1_A ?

Sous - Anneau

DÉFINITION 3.4. Soit $(A, +, \cdot)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A, +)$ qui est

- soit le sous-groupe trivial $\{0_A\}$,
- soit qui contient l'unité 1_A et qui est stable par multiplication:

$$\forall b, b' \in B, \quad b.b' \in B.$$

Ainsi $(B, +, \cdot, 0_A, 1_A)$ est un anneau.

PROPOSITION 3.3. (Critère de sous-anneau) Soit $(A, +, \cdot)$ un anneau et $B \subset A$ un sous-ensemble non-vidé; alors B est un sous-anneau ssi $B = \{0_A\}$, ou bien $1_A \in B$ et

$$(3.1.1) \quad \forall b, b', b'' \in B, \quad b.b' - b'' \in B$$

Preuve: Exercice.

□

Exemples $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

— les seuls ss anneaux de $\mathbb{Z}$ sont $\{0\}$ et $\mathbb{Z}$.

— les seuls ss anneaux de $\mathbb{Z}/_q\mathbb{Z}$ sont $\{0(q)\}$ et $\mathbb{Z}/_q\mathbb{Z}$.

— $M_2(\mathbb{Z}) \subset M_2(\mathbb{Q}) \subset M_2(\mathbb{R}) \subset M_2(\mathbb{C})$

- A commutatif $M_2(A)$

- Matrices scalaires

$$A \cdot \text{Id}_2 = \left\{ a \text{Id}_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in A \right\}$$

- Matrices diagonales

$$\text{Diag}_2(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in A \right\}$$

- Matrices triangulaires supérieures

$$T_{\text{sup},2}(A) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in A \right\}$$

- Matrices triangulaires inférieures

$$T_{\text{inf},2}(A) = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, c, d \in A \right\}$$

Anneau engendré: si $B, B' \subset A$ sont des ssanneaux $B \cap B'$ est un ssanneau.

et si on a une collection de ss-anneaux $(B_i)_{i \in I}$ $B_i \subset A$ ssanneaux

$\bigcap_{i \in I} B_i$ est un ssanneau.

$X \subset A$ un sous-ensemble

le sous-anneau engendré par X est

le + petit sous-anneau contenant X

ie. l'intersection des sous-anneaux contenant X

$$\langle X \rangle_{\text{Ann}} \subset A.$$

Morphismes

DÉFINITION 3.5. Soient $(A, +, \cdot)$, $(B, +, \cdot)$ des anneaux. Un morphisme d'anneaux $\varphi : A \mapsto B$ est un morphisme de groupes commutatif $\varphi : (A, +) \mapsto (B, +)$ tel que

$$\varphi(1_A) = 1_B \text{ ou bien } \varphi(1_A) = 0_B,$$

$$\forall a, a' \in A, \varphi(a \cdot a') = \varphi(a) \cdot \varphi(a').$$

Rmq: si $\varphi(1_A) = 0_B$ alors $\varphi = \underline{0}_B$

$$\begin{aligned} \forall a \in A \quad \varphi(a) &= \varphi(a \cdot 1_A) \\ &= \varphi(a) \cdot_B \varphi(1_A) = \varphi(a) \cdot 0_B = 0_B \end{aligned}$$

Exemple: Le morphisme canonique.

Soit A un anneau

$$\text{Can}_A: \mathbb{Z} \longrightarrow A$$

$$\begin{aligned} n &\longrightarrow n \cdot 1_A = \underbrace{1_A + \dots + 1_A}_{n \text{ fois}} \quad (n \geq 0) \\ &= \underbrace{(-1_A) + \dots + (-1_A)}_{|n| \text{ fois}} \quad \text{si } n \leq 0 \end{aligned}$$

Can_A qui est un morphisme de gres additifs
est en fait un morphisme d'anneaux:

$$\begin{aligned}\text{Can}_A(m.n) &= (m.n)1_A = (m.1_A) \cdot_A (n.1_A) \\ &= \text{Can}_A(m) \cdot_A \text{Can}_A(n) .\end{aligned}$$

$$\ker(\text{Can}_A) = q_A \mathbb{Z} \quad q_A \in \mathbb{Z}$$

$q_A = \text{Caractéristique de } A.$

Exemple:

$$\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$$

$$a \longrightarrow a(\text{mod } q)$$

c'est un morphisme d'anneaux et
c'est le morphisme canonique de $\mathbb{Z}/q\mathbb{Z}$
et la caractéristique de $\mathbb{Z}/q\mathbb{Z}$ c'est q .