PCSI - mathématiques

Structures algébriques

1 Groupes

Définition 1 *Un* groupe *est un couple $(G, \times)$ où G est un ensemble non vide et $\times$ une loi de composition interne sur G vérifiant*

(G1) *$\times$ est associative ;*

(G2) *G possède un élément neutre pour $\times$ noté 1_G ;*

(G3) *Tout élément x de G admet un symétrique x^{-1} dans G pour $\times$.*

Si de plus la loi $\times$ est commutative, le groupe $(G, \times)$ est dit *commutatif* ou *abélien*.

Exemple 1

1. *$G = \{1_G\}$, $\times$ étant définie par $1_G \times 1_G = 1_G$;*
2. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition usuelle ;*
3. *$\{-1, 1\}$, $\mathbb{Q}_+^*$, $\mathbb{Q}^*$, $\mathbb{R}_+^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ munis de la multiplication usuelle ;*
4. *$(\mathrm{Bij}(E, E), \circ)$;*
5. *$(\mathcal{P}(E), \triangle)$, ...*

Rappelons que (*cf.* "vocabulaire ensembliste") :

- Le neutre est unique, ce qui justifie la notation 1_G ;
- Le symétrique d'un élément est unique.
- Le symétrique de xy est $\boldsymbol{y^{-1}x^{-1}}$ ($\neq xy$ en général si G n'est pas abélien).
- Tout élément d'un groupe est simplifiable (car symétrisable).

Lorsque la loi du groupe G est notée $+$, le neutre est noté 0_G et le symétrique d'un élément x est noté $-x$ (*notation additive* — généralement réservée aux groupes abéliens).

Notation 1 *Si $(G, \times)$ est un groupe et si $x \in G$, $n \in \mathbb{Z}$ on note*

$$x^n = \begin{cases} x \times ... \times x \text{ (n facteurs)} & \text{si } n > 0 \\ 1_G & \text{si } n = 0 \\ x^{-1} \times ... \times x^{-1} \text{ ($-n$ facteurs)} & \text{si } n < 0 \end{cases}$$

On vérifie alors l'habituelle règle des exposants. L'écriture x^n devient $n.x$ en notation additive.

1.1 Sous-groupes

Soit $(G, \times)$ un groupe. Soit H une partie de G.

Définition 2 *H est un* sous-groupe *(sg) de $(G, \times)$ si*

(SG1) $1_G \in H$;

(SG2) $\forall x \in H, \forall y \in H, xy \in H$;

(SG3) $\forall x \in H, x^{-1} \in H$.

Compte tenu de (SG2) et (SG3), (SG1) peut être remplacé par

(SG1') $H \neq \varnothing$.

Compte tenu de (SG1), (SG2) et (SG3) peuvent être remplacés par

(SG2') $\forall x \in H, \forall y \in H, xy^{-1} \in H$.

Le résultat de ces hypothèses est que H, muni de la (restriction de la) multiplication de G, est un groupe.

Exemple 2

1. *$\{1_G\}$ et G (sg triviaux) ;*
2. *$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset (\mathbb{C}, +)$;*
3. *$\{-1, 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset (\mathbb{C}^*, \times)$;*
4. *$\mathbb{U}_n \subset \mathbb{U} \subset (\mathbb{C}^*, \times)$, ...*
5. Groupe produit : *si $(G, \times)$ et $(G', \times)$ ([1]) sont deux groupes, l'ensemble $G \times G'$ est canoniquement muni d'une structure de groupe définie par :*
$$(x, x') \times (y, y') = (xy, x'y').$$
Notamment, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $\mathbb{R}^3$, ..., $\mathbb{R}^n$ sont des groupes.
6. Groupe $\mathcal{F}(X, G)$: *si X est un ensemble et G un groupe, $\mathcal{F}(X, G)$ est muni d'une structure canonique de groupe définie par*
$$f \times g : X \to G \ ; \ x \mapsto f(x) \times g(x).$$
Par exemple, $\mathbb{R}^{\mathbb{N}}$, $\mathcal{F}(I, \mathbb{R})$ sont des groupes.

Il est rare qu'on puisse décrire tous les sous-groupe d'un groupe donné lorsque celui-ci est infini. C'est cependant possible dans le cas de $\mathbb{Z}$ grâce à la division euclidienne.

[1] On note $\times$ les *deux* lois. Cela ne signifie pas qu'elles sont les mêmes, mais en pratique il n'y aura pas ambiguïté quant à l'appartenance à G où G' des différents éléments.

Notation 2 *Si $p \in \mathbb{Z}$, on note*

$$p\mathbb{Z} = \{pn \mid n \in \mathbb{Z}\}$$

l'ensemble des multiples de l'entier p.

C'est trivialement un sg de$\mathbb{Z}$. Il n'y en a pas d'autre :

Théorème 1 *Soit H un sous-groupe de $(\mathbb{Z}, +)$. Il existe un unique entier naturel p tel que : $H = p\mathbb{Z}$.*

1.2 Morphismes

Soient $(G, \times)$ et $(G', \times)$ ([1]) deux groupes. Soit $f : G \to G'$ une application.

Définition 3 *f est un* morphisme *(de groupes) de $(G, \times)$ dans $(G', \times)$ si pour tous x, $y \in G$:*

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

Exemple 3

1. *L'application constante $G \to G'$; $x \mapsto 1_{G'}$;*
2. *$\mathrm{Id}_G : G \to G$; $x \mapsto x$;*
3. *$\exp : (\mathbb{R}, +) \to \left(\mathbb{R}_+^*, \times\right)$ (*resp. *$(\mathbb{C}, +) \to (\mathbb{C}^*, \times)$) ;*
4. *$\ln : \left(\mathbb{R}_+^*, \times\right) \to (\mathbb{R}, +)$;*
5. *$p : G \times G' \mapsto G$; $(x, x') \mapsto x$ et $q : G \times G' \mapsto G'$; $(x, x') \mapsto x'$;*
6. *$\mathcal{V}_a : \mathcal{F}(X, G) \to G$; $f \mapsto f(a)$ où $a \in X$ ("valeur en a"), ...*

Remarque 1 *Si f est un morphisme de groupes de G dans G' on a nécessairement $f(1_G) = 1_{G'}$ d'où $f(x^n) = (f(x))^n$ pour tous $x \in G$ et $n \in \mathbb{Z}$.*

La composée de deux morphismes de groupes est un morphisme de groupes :

Proposition 1 *Soient trois groupes G, G' et G''. Si f (*resp. *g) est un morphisme de G dans G' (*resp. *de G' dans G''), alors $g \circ f$ est un morphisme de G dans G''.*

Définition 4 *Un morphisme de groupes $f : G \to G'$ est*

- *un* endomorphisme *si $G = G'$;*
- *un* isomorphisme *si f est bijectif de G sur G' ;*
- *un* automorphisme *si $G = G'$ et f est bijectif de G sur G.*

Dans les derniers cas, la réciproque de f est automatiquement un morphisme :

Proposition 2 *Si f est un isomorphisme de groupes de G sur G', alors $f^{-1} : G' \to G$ est un (iso)morphisme de groupes de G' sur G.*

L'injectivité d'un morphisme de $f : G \to G'$ groupes peut (et doit) être étudiée à l'aide de la définition suivante :

Définition 5 *le* noyau *de f est*

$$\ker f = f^{-1}\left(\{1_{G'}\}\right) = \{x \in G \mid f(x) = 1_{G'}\} \ ([2])$$

On peut alors énoncer

Proposition 3 *Soit $f : G \to G'$ un morphisme de groupes. Il y a équivalence entre*

1. *f est injectif et*
2. *$\ker f = \{1_G\}$.*

D'une manière plus générale, les morphismes respectent bien la notion de sous-groupe :

Proposition 4 *Soit $f : G \to G'$ un morphisme de groupes. Alors*

1. *$\mathrm{Im}\, f$ est un sg de G' ;*
2. *$\ker f$ est un sg de G.*

2 Anneaux

Définition 6 *Un* anneau *est un triplet $(A, +, \times)$ où $(A, +)$ est un groupe abélien (le neutre étant noté 0_A) et $\times$ une l.c.i. sur A telle que*

(A1) *$\times$ est associative ;*

(A2) *$\times$ admet un élément neutre dans A noté 1_A ;*

(A3) *$\times$ est distributive à droite et à gauche par rapport à $+$.*

On impose en outre que $0_A \neq 1_A$ ([3]) : il y a donc au moins deux éléments dans tout anneau. Notons que l'addition d'un anneau est toujours commutative. Lorsque c'est de plus le cas de la multiplication, on parle d'*anneau commutatif*. Même dans le cas contraire, il peut arriver que deux éléments x, $y \in A$ vérifient $xy = yx$: on dit que x et y *commutent*.

Exemple 4

1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$;*
2. *$A = \{0_A, 1_A\}$ muni des lois $+$ et $\times$ définies par*

$+$	0_A	1_A
0_A	0_A	1_A
1_A	1_A	0_A

et

$\times$	0_A	1_A
0_A	0_A	0_A
1_A	0_A	1_A

3. *Les structures d'anneau canoniques sur $A \times A'$ et $\mathcal{F}(X, A)$ sont définies de la même manière que pour les groupes.*
4. *$(\mathcal{P}(E), \triangle, \cap)$;*
5. *$(\mathrm{End}(G), +, \circ)$ si G est un groupe abélien.*

[2] Attention à la notation "f^{-1}", qui *ne signifie pas* que f soit bijective.

[3] Selon le programme. En fait, il est possible d'envisager des anneaux avec $0_A = 1_A$ (p. ex. $A = \{0_A\}$), voire sans l'axiome (A2) (anneau "non unitaire").

2.1 Règles de calcul

Les relations suivantes sont valides quels que soient les éléments de l'anneau considéré. Elles généralisent la propriété de distributivité.

- $\left(\sum_{i=1}^{n} x_i\right) \times y = \sum_{i=1}^{n} x_i y$;
  $x \times \left(\sum_{j=1}^{p} y_j\right) = \sum_{j=1}^{p} x y_j$;
- $\left(\sum_{i=1}^{n} x_i\right) \times \left(\sum_{j=1}^{p} y_j\right) = \sum_{\substack{1\leq i\leq n \\ 1\leq j\leq p}} x_i y_j$;
- $\prod_{k=1}^{p} \sum_{i_k=1}^{n_k} x_{k,i_k} = \sum_{\substack{1\leq i_1\leq n_1 \\ \dots \\ 1\leq i_p\leq n_p}} x_{1,i_1} \dots x_{p,i_p}$

Théorème 2 (Newton) *Si x, y sont deux éléments* qui commutent *($xy = yx$) dans l'anneau A et si $n \in \mathbb{N}$:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Théorème 3 *Si x, y sont deux éléments* qui commutent *($xy = yx$) dans l'anneau A et si $n \in \mathbb{N}$:*

$$x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^{n-k-1} y^k.$$

À partir de cette formule, on peut retrouver la somme des termes des éléments d'une suite géométrique : posons $x = 1_A$. On en déduit $1_A - y^n = (1_A - y) \sum_{k=0}^{n-1} y^k$ d'où lorsque $1_A - y$ est inversible :

$$\sum_{k=0}^{n-1} y^k = (1_A - y)^{-1} (1_A - y^n) \ \ (= (1_A - y^n)(1_A - y)^{-1}).$$

2.2 Eléments inversibles

Un élément x de l'anneau A est *inversible* s'il est symétrisable pour $\times$, càd s'il existe $y \in A$ tel que $xy = yx = 1_A$. y est alors unique, c'est l'inverse de x noté x^{-1}. C'est toujours le cas de 1_A (*resp.* -1_A), avec $(1_A)^{-1} = 1_A$ (*resp.* $(-1_A)^{-1} = -1_A$). Nécessairement un tel élément inversible x est non nul.

Notation 3 *L'ensemble des éléments inversibles de l'anneau A est noté $\mathcal{U}(A)$ ou A^*.*

Exemple 5

1. *$\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Idem pour $\mathbb{R}$ et $\mathbb{C}$.*
2. *Attention, $\mathcal{U}(\mathbb{Z}) = \mathbb{Z}^* = \{-1, 1\} \neq \mathbb{Z} \setminus \{0\}$.*

Proposition 5 *$(\mathcal{U}(A), \times)$ est un groupe (le* groupe multiplicatif *de A).*

2.3 Diviseurs de zéro

$(A, +, \times)$ est un anneau ; $a \in A$.

Définition 7 *a est un* diviseur de zéro *dans A si $a \neq 0_A$ et s'il existe $b \in A$, $b \neq 0_A$, tel que $ab = 0_A$ ou $ba = 0_A$.*

L'élément b est donc aussi un diviseur de zéro. Il s'agit des éléments qui *ne sont pas* simplifiables pour la multiplication.

Exemple 6 *Dans $A = \mathbb{Z}^2$, $a = (1, 0)$ et $b = (0, 1)$ sont des diviseurs de zéro.*

Définition 8 *L'anneau A est* intègre *s'il est commutatif et sans diviseur de zéro.*

Cette définition permet de donner un sens à la notion de divisibilité : $a \neq 0_A$ divise $b \neq 0_A$ s'il existe $c \in A$ tel que $ac = b$ $(= ca)$. L'intégrité de A garantit l'unicité de c : quotient exact de b par a. Un anneau intègre est ainsi un anneau dans lequel on peut faire de l'arithmétique.

Exemple 7 *L'anneau $\mathbb{Z}$ est intègre.*

2.4 Sous-anneaux

Quel est le plus petit ensemble de propriétés que doit vérifier une partie B d'un anneau $(A, +, \times)$ pour devenir un anneau à part entière (une fois muni des restrictions des lois + et $\times$) ?

Définition 9 *B est un* sous-anneau *(sa) de A si*

(SA1) $1_A \in B$;

(SA2) $\forall x \in B, \forall y \in B, x - y \in B$;

(SA3) $\forall x \in B, \forall y \in B, xy \in B$.

(SA1) et (SA2) assurent que B est un sg de $(A, +)$, alors que selon (SA3) $\times$ est une l.c.i. sur B admettant un élément neutre dans B (SA1). Ainsi, $(B, +, \times)$ est un anneau (inclus dans A) ([4]).

Exemple 8

1. *A est un sous-anneau de A ;*
2. *$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset (\mathbb{C}, +, \times)$;*
3. *Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ (comparer avec th. 1).*

2.5 Morphismes d'anneaux

Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux[5]. Soit f une application de A dans A'.

Définition 10 *f est un* morphisme d'anneaux *de A dans A' si*

1. $\forall x \in A, \forall y \in A, f(x+y) = f(x) + f(y)$;
2. $\forall x \in A, \forall y \in A, f(xy) = f(x) f(y)$;
3. $f(1_A) = 1_{A'}$.

[4] Contrairement au cas des groupes, la notion de *sous-anneau* ne coïncide pas avec celle d'*anneau inclus*.

Il peut exister une partie B d'un anneau A (avec $1_A \notin B$) et un élément b de B, $b \neq 1_A$, vérifiant $xb = bx = x$ pour tout $x \in \boldsymbol{B}$ −mais évidemment pas pour tout $x \in A$. B serait alors un anneau inclus dans A, mais pas un sous-anneau de A.

La construction d'un tel contre-exemple sort du cadre de ce programme.

[5] Les lois sont notées identiquement ; il n'y aura jamais ambiguïté.

f est donc en particulier un morphisme de groupes du groupe $(A,+)$ dans le groupe $(A',+)$. À ce titre (rem. 1), $f(0_A) = 0_{A'}$. Par contre, la condition 3. n'est pas automatique (elle empêche, par exemple, f d'être l'application nulle).

Exemple 9

1. $\mathrm{Id}_A : A \to A$;
2. $\mathcal{V}_a : \mathcal{F}(X,A) \to A$; $f \mapsto f(a)$;
3. $f : \mathbb{Z} \to A$; $n \mapsto n.1_A$ *où* A *est un anneau ;*
4. A *étant l'anneau de l'exemple 4.2,*

$$\begin{array}{rccc} f: & (\mathcal{P}(E), \triangle, \cap) & \to & (\mathcal{F}(E,A), +, \times) \\ & X & \mapsto & \chi_X \end{array}$$

   χ_X *étant l'application caractéristique de* X *;*

5. $\lim : CV(\mathbb{R}) \to \mathbb{R}$; $(u_n) \mapsto \lim(u_n)$;
6. *Le seul morphisme d'anneau de* $\mathbb{Z}$ *dans* $\mathbb{Z}$ *est* $\mathrm{Id}_{\mathbb{Z}}$*, ...*

On a les notions d'endo—, iso— et automorphisme d'anneaux, et on peut parler de noyau d'un morphisme d'anneaux. À ce sujet, on peut énoncer pour les morphismes d'anneaux les propriétés analogues aux propositions 1, 2 et 3.

Mais *attention !* le noyau d'un morphisme d'anneaux $f : A \to A'$ n'est *jamais* un sous-anneau de A (puisqu'il ne contient pas 1_A). On peut seulement énoncer

Proposition 6 *Soit* $f : A \to A'$ *un morphisme d'anneaux.*

1. *Si* B *est un sous-anneau de* A*,* $f\langle B\rangle$ *est un sous-anneau de* A' *;*
2. *Si* B' *est un sous-anneau de* A'*,* $f^{-1}\langle B'\rangle$ *est un sous-anneau de* A*.*

En outre, un morphisme d'anneaux $f : A \to A'$ envoie[6] $\mathcal{U}(A)$ dans $\mathcal{U}(A')$:

Proposition 7 *Soit* $f : A \to A'$ *un morphisme d'anneaux et soit* $x \in A$*.*

1. $f(nx) = nf(x)$ *pour tout* $n \in \mathbb{Z}$ *;*
2. $f(x^n) = (f(x))^n$ *pour tout* $n \in \mathbb{N}$ *;*
3. $x \in \mathcal{U}(A) \Rightarrow f(x) \in \mathcal{U}(A')$*, auquel cas 2. est valide pour tout* $n \in \mathbb{Z}$*.*

3 Corps

Définition 11 *Un* corps *est un anneau* $(K,+,\times)$ *dans lequel tout élément non nul est inversible (symétrisable pour la loi* $\times$*).*

[6] non surjectivement en général

Cela signifie que l'ensemble $K^* = \mathcal{U}(K)$ des éléments inversibles de K coïncide avec $K \setminus \{0_K\}$ (il est donc le plus grand possible), ou encore que : tout élément non nul de K est simplifiable pour $\times$. Rappelons que K^* est un groupe pour $\times$.

Comme un anneau, un corps est dit *commutatif* si sa multiplication est commutative. Les corps non commutatifs sont très rares[7].

Pour un exemple, voir le corps $\mathbb{H}$ des *quaternions* (W. R. Hamilton) construit en exercice.

Exemple 10

1. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$;
2. *L'anneau* A *de l'exemple 4.2 est un corps.*

Un corps commutatif est notamment un anneau intègre, mais dans ce cas la relation de divisibilité est triviale (puisque tout élément non nul divise tout autre).

3.1 Sous-corps

Soit $(K,+,\times)$ un corps et soit $L \subset K$.

Définition 12 L *est un* sous-corps *(sc) de* K *si*

(SC1) $1_K \in L$;

(SC2) $\forall x \in L,\ \forall y \in L,\ x - y \in L$;

(SC3) $\forall x \in L,\ \forall y \in L \setminus \{0_K\},\ xy^{-1} \in L$.

(SC1) se combine avec (SC2) pour faire de L un sg de $(K,+)$ et avec (SC3) pour faire de $L \setminus \{0_K\}$ un sg de $(K^*,\times)$. Ainsi L, muni des restrictions des lois $+$ et $\times$, est un corps (avec $0_L = 0_K$ et $1_L = 1_K$).

Exemple 11

1. $\mathbb{Q} \subset \mathbb{R} \subset (\mathbb{C},+,\times)$;
2. *Le seul sous-corps de* $\mathbb{Q}$ *est* $\mathbb{Q}$*.*

3.2 Morphismes de corps

Soient K et K' deux corps.

Définition 13 *Un* morphisme de corps *de* K *dans* K' *est un morphisme d'anneaux de l'anneau* K *dans l'anneau* K'*.*

On a donc les mêmes conditions et remarques que pour les anneaux, mais la présence d'une structure de corps au départ et à l'arrivée ajoute quelques résultats.

Exemple 12

1. $\mathrm{Id}_K : K \to K$;
2. *Le seul endomorphisme de corps de* $\mathbb{Q}$ *est* $\mathrm{Id}_{\mathbb{Q}}$;
3. *La conjugaison* $\mathbb{C} \to \mathbb{C}$; $z \mapsto \bar{z}$*.*

Un morphisme de corps est toujours injectif compte tenu de cette dernière propriété :

Proposition 8 *Soit* $f : K \to K'$ *un morphisme de corps. Pour tout* $x \in K^*$*,* $f(x) \in K'^*$ *et* $f(x^n) = (f(x))^n$ *pour tout* $n \in \mathbb{Z}$*. En particulier,* $\ker f = \{0_K\}$*.*

[7] On montre (Wedderburn 1905) qu'il s'agit nécessairement de corps *infinis*.