Algèbre générale de PCSI

I - Vocabulaire relatif aux ensembles et aux applications

1) Parties d'un ensemble

On suppose connues "intuitivement" la notion d'*ensemble* et la *relation d'appartenance* : on écrit $x \in E$ le fait que "x est un *élément* de E".
Étant donnés deux ensembles E et F, on dit que E est une *partie* de F, ou encore que E est *inclus* dans F, si et seulement si tout élément de E est un élément de F (formellement : $\forall x \quad (x \in E \Rightarrow x \in F)$ ou encore : $\forall x \in E \quad x \in F$). On note si c'est le cas $E \subset F$.
Pour tout ensemble E, on note $\mathcal{P}(E)$ l'ensemble des parties de E.
Étant données deux parties A, B d'un ensemble E, on définit :

- leur *intersection* $A \cap B = \{x \in E \,/\, x \in A \quad \text{et} \quad x \in B\}$
  (lire "l'ensemble des x éléments de E **tels que** x appartient à A et x appartient à B").
- leur *réunion* $A \cup B = \{x \in E \,/\, x \in A \quad \text{ou} \quad x \in B\}$ (**ou inclusif** : $A \cap B \subset A \cup B$!)
- leur *différence* $A \backslash B = \{x \in E \,/\, x \in A \quad \text{et} \quad x \notin B\}$
- leur *différence symétrique* $A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \setminus (A \cap B)$ (associée au **ou exclusif**).

NB : lorsque $A \subset E$, $E \backslash A$ est appelé ***le*** *complémentaire de A dans E*, noté aussi $\complement_E^A$ ou $\overline{A}$ s'il n'y a pas d'ambiguïté sur E (notamment en probabilités).

Attention ! Pour être développée en toute rigueur, la théorie des ensembles suppose une construction axiomatique précise. En effet, on ne peut attribuer le statut d'ensemble à n'importe quelle "collection" d'objets (cf. le *paradoxe de Russell* : si E était "l'ensemble de tous les ensembles", considérer $A = \{X \in E \,/\, X \notin X\}$ conduirait à une contradiction, puisqu'on ne pourrait avoir, ni $A \in A$, ni $A \notin A$).

2) Produits d'ensembles

On suppose également connues intuitivement les notions de *couple* et plus généralement de *p-uplet* (ou *p-liste*) (liste ordonnée de p objets non nécessairement distincts, notée $(x_1, \ldots, x_p)$). Les couples sont les 2-uplets de la forme (x, y), **à ne pas confondre** avec la *paire* $\{x, y\}$, ensemble à 2 éléments, cette dernière notation supposant que $x \neq y$. Les 3-uplets sont appelés *triplets*, les 4-uplets *quadruplets*, ...

Étant donnés deux ensembles E, F, on définit leur *produit (cartésien)* $E \times F$ comme l'ensemble des couples (x, y), x décrivant E et y décrivant F.
On définit de même le produit $E_1 \times \cdots \times E_p = \prod_{k=1}^{p} E_k$ de p ensembles comme l'ensemble des p-uplets $(x_1, \ldots, x_p)$, x_k décrivant E_k pour tout k.
Lorsque les E_k sont tous égaux à un même ensemble E, ce produit est noté E^p.

3) Applications

Formellement, étant donnés deux ensembles E, F, une *application de E dans* (ou *vers*) F est un triplet de la forme (E, F, Γ), où E est *l'ensemble de départ*, F *l'ensemble d'arrivée* et Γ *le graphe*, étant par définition une partie de $E \times F$ vérifiant la condition suivante : pour tout x de E, il existe un unique y de F tel que $(x, y) \in \Gamma$.

En pratique, une telle application étant notée f, on note — pour tout x de E — $f(x)$ l'unique élément de F associé à x en vertu de la condition précédente, de sorte que le graphe de f s'écrit $\Gamma = \{(x, y) \in E \times F \,/\, y = f(x)\}$ ou encore sous forme *paramétrique* :
$\Gamma = \{(x, f(x)),\ x \in E\}$ (lire "l'ensemble des couples $(x, f(x))$, x **décrivant** E").

On écrit $f : \begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x) \end{array}$ l'application f de E dans F qui à x associe $f(x)$.
Lorsque $y = f(x)$, on dit que :

- y est ***l'image de*** x ***par*** f (elle est unique) ;
- x est ***un*** *antécédent de* y *par* f (y peut admettre plusieurs antécédents).

Exemples : l'application de E dans E, qui à tout x associe x lui-même, est *l'identité de* E (ou *application identique*), notée Id_E ou id_E ;
étant donnée une partie A de E, l'application de E dans $\{0,1\}$ qui à x associe 1 si $x \in A$, 0 sinon, est *la fonction indicatrice de* A, notée $\mathbb{1}_A$.

L'ensemble des applications de E dans F est noté $\mathcal{F}(E,F)$, ou parfois F^E.

Étant donné trois ensembles E, F, G et deux applications $f \in \mathcal{F}(E,F)$, $g \in \mathcal{F}(F,G)$ (l'ensemble d'arrivée de f **est égal** à l'ensemble de départ de g), on définit leur *composée*

$$g \circ f : \begin{array}{ccc} E & \to & G \\ x & \mapsto & g \circ f(x) = g\big(f(x)\big) \end{array} .$$

Si $f \in \mathcal{F}(E,F)$ et $A \in \mathcal{P}(E)$, l'application de A dans F, qui à x associe $f(x)$, est appelée ***la*** *restriction de* f *à* A, notée $f_{|A}$.
Pour $g \in \mathcal{F}(A,F)$, on dit que f est ***un*** *prolongement de* g *à* E si et seulement si $f_{|A} = g$.

4) Injections, surjections, bijections

Soient E, F deux ensembles et f une application de E dans F. On dit que f est :

- une *injection* (ou *application injective*) si et seulement si tout élément de F admet **au plus** un antécédent par f, ce qui peut se traduire par la propriété suivante : pour tout $(x,x') \in E^2$,
$$f(x) = f(x') \Rightarrow x = x' \quad \text{ou encore } (\textit{contraposée}) \quad x \neq x' \Rightarrow f(x) \neq f(x') \ ;$$
- une *surjection* (ou *application surjective*) si et seulement si tout élément de F admet **au moins** un antécédent par f ($\forall y \in F \quad \exists x \in E \quad y = f(x)$) ;
- une *bijection* (ou *application bijective*) si et seulement si f est à la fois injective et surjective, c'est-à-dire si et seulement si tout élément de F admet **un unique** antécédent par f.

Théorème et définition : $f \in \mathcal{F}(E,F)$ est bijective si et seulement s'il existe $g \in \mathcal{F}(F,E)$ telle que
$$g \circ f = \mathrm{Id}_E \quad \textbf{et} \quad f \circ g = \mathrm{Id}_F.$$
Si c'est le cas, g est unique, bijective, appelée *la bijection réciproque de* f, notée f^{-1}. C'est l'application de F dans E qui, à tout élément y de F, associe son unique antécédent par f, $x = f^{-1}(y)$ (notation **exclusivement réservée** au cas où f est bijective).

Attention ! On peut avoir $g \circ f = \mathrm{Id}_E$ alors que ni f ni g n'est bijective
(par exemple, $E = F = G = \mathbb{N}$, $f : x \mapsto x+1$, $g : y \mapsto 0$ si $y = 0$, $y-1$ si $y > 0$).

Propriétés : soient E, F, G trois ensembles, $f \in \mathcal{F}(E,F)$ et $g \in \mathcal{F}(F,G)$.

a) Si f et g sont injectives (*resp.* surjectives, bijectives), alors $g \circ f$ l'est aussi.

b) Lorsque f et g sont bijectives, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

c) $g \circ f$ injective $\Rightarrow$ f injective ; $\quad g \circ f$ surjective $\Rightarrow$ g surjective.

5) Image directe, image réciproque d'une partie par une application

Soient E, F deux ensembles et f une application de E dans F.

- Pour toute partie A de E, on définit *l'image directe de* A *par* f, notée $f(A)$, la partie de F définie par :
$$f(A) = \{y \in F \ / \ \exists x \in A \quad y = f(x)\} = \{f(x),\ x \in A\}.$$

Attention ! $x \in A \Rightarrow f(x) \in f(A)$ mais la réciproque peut être fausse si f n'est pas injective.

Exemple : $f(E)$ est une partie de F, appelée *ensemble image de* f.
f est surjective si et seulement si $f(E) = F$.

- Pour toute partie B de F, on définit *l'image réciproque de* B *par* f, notée $f^{-1}(B)$, la partie de E définie par
$$f^{-1}(B) = \{x \in E \ / \ f(x) \in B\}$$

Attention ! Cette notation est en usage même si f n'est pas bijective, on peut toujours écrire $f^{-1}(B)$ avec B **partie de** F ; par contre, l'expression $f^{-1}(y)$ pour y **élément de** E est réservée au cas où f est bijective !!

6) Équations

Soient E, F deux ensembles, f une application de E dans F et b un élément de F.
"*Résoudre l'équation* $f(x) = b$ (*d'inconnue* $x \in E$)", c'est déterminer $\{x \in E \ / \ f(x) = b\}$, appelé *ensemble des solutions de l'équation.* Cet ensemble n'est autre que $f^{-1}(\{b\})$.

- L'ensemble des solutions est non vide si et seulement si $b \in f(E)$.
- Si f est surjective, l'ensemble des solutions est non vide, quel que soit b.
- Si f est injective, l'ensemble des solutions est, soit vide (si $b \notin f(E)$), soit un singleton (si $b \in f(E)$).
- Si f est bijective, l'ensemble des solutions est le singleton $\left\{f^{-1}(b)\right\}$, quel que soit b.

7) Familles

Soient I, E deux ensembles et x une application de I dans E. Dans certains contextes, on choisit de noter — pour i dans I — x_i l'élément de E, image de i par x. x est alors notée $(x_i)_{i\in I}$ (*famille d'éléments de* E *indexée par* I). L'ensemble des familles d'éléments de E indexées par I est noté E^I.

- Lorsque I, partie de $\mathbb{N}$, est de la forme $[n_0, +\infty[$, on parle de *suite d'éléments de* E, notée $(x_n)_{n\geq n_0}$.
- Lorsque I est un ensemble fini, on parle de *système d'éléments de* E (ou de *famille finie*).
- Lorsque $I = [\![1, p]\!]$, on identifie souvent la famille $(x_i)_{i\in[\![1,p]\!]}$ et le p-uplet $(x_1, \ldots, x_p)$, ainsi que l'ensemble E^I et le produit cartésien E^p.

Attention ! Ne pas confondre famille $(x_i)_{i\in I}$ et ensemble image $\{x_i,\ i \in I\}$, qui est une partie de E. Par exemple, pour une suite constante, l'ensemble I est infini tandis que l'ensemble image est un singleton.

8) Relations d'équivalence, relations d'ordre

Soit E un ensemble ; formellement, une *relation binaire sur* E est un couple $\mathcal{R} = (E, \Gamma)$ où Γ est une partie de $E \times E$, appelée *le graphe de la relation* $\mathcal{R}$. En pratique, x, y étant dans E, on écrit $x\mathcal{R}y$ et l'on dit que x *est en relation avec* y si et seulement si $(x, y) \in \Gamma$.
Si $\mathcal{R}$ est une relation binaire sur E, on dit que :

- la relation $\mathcal{R}$ est *réflexive* si et seulement si : $\forall x \in E \quad x\mathcal{R}x$
- la relation $\mathcal{R}$ est *transitive* si et seulement si : $\forall (x, y, z) \in E^3 \quad \big(x\mathcal{R}y \quad \text{et} \quad y\mathcal{R}z\big) \Rightarrow x\mathcal{R}z$
- la relation $\mathcal{R}$ est *symétrique* si et seulement si : $\forall (x, y) \in E^2 \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- la relation $\mathcal{R}$ est *antisymétrique* si et seulement si : $\forall (x, y) \in E^2 \quad (x\mathcal{R}y \quad \text{et} \quad y\mathcal{R}x) \Rightarrow y = x$
- $\mathcal{R}$ est une *relation d'équivalence sur* E si et seulement si $\mathcal{R}$ est réflexive, transitive et symétrique
- $\mathcal{R}$ est une *relation d'ordre sur* E si et seulement si $\mathcal{R}$ est réflexive, transitive et antisymétrique ; si $\mathcal{R}$ est une relation d'ordre sur E, deux éléments x, y de E sont dits *comparables* si et seulement si $x\mathcal{R}y$ ou $y\mathcal{R}x$. Lorsque deux éléments quelconques sont comparables, on dit que l'ordre est *total*, sinon qu'il est *partiel*.

Exemples : 1) sur $\mathbb{N}$, la relation $\leq$ ("inférieur ou égal à") est une relation d'ordre total, la relation $|$ ("divise") est une relation d'ordre partiel (2 et 3 ne sont pas comparables)

2) dans $\mathcal{P}(E)$, la relation $\subset$ ("inclus dans") est une relation d'ordre, partiel dès que E possède au moins deux éléments !

3) dans n'importe quel ensemble E, la relation d'égalité est à la fois une relation d'ordre et une relation d'équivalence (**Attention !** "antisymétrique" n'est pas le contraire de "symétrique")

4) dans $E = \mathbb{Z} \times \mathbb{Z}^*$, la relation définie par

$$(a,b)\,\mathcal{R}\,(c,d) \Leftrightarrow ad = bc$$

est une relation d'équivalence

5) étant donné $\theta \in \mathbb{R}^*$, la relation (*congruence modulo* θ) définie dans $\mathbb{R}$ par

$$x \equiv y \Leftrightarrow \frac{y-x}{\theta} \in \mathbb{Z}$$

est une relation d'équivalence

6) dans l'ensemble des droites d'un plan affine, la relation "est parallèle à" est une relation d'équivalence.

Classes d'équivalence

Soient E un ensemble non vide et $\mathcal{R}$ une relation d'équivalence sur E.
Pour tout élément a de E, *la classe d'équivalence de* a est l'ensemble des éléments de E en relation avec a :

$$cl(a) = \{x \in E \ / \ x\mathcal{R}a\}.$$

On vérifie facilement que :

- deux éléments ont la même classe d'équivalence si et seulement s'ils sont en relation
- deux classes d'équivalence sont soit égales, soit disjointes
- les classes d'équivalence forment *une partition* de E (*i.e.* un ensemble de parties de E, non vides, disjointes deux à deux et dont la réunion est E).

Applications au dénombrement : dans le cas où E est un ensemble fini, son cardinal est la somme des cardinaux des classes d'équivalences. Si ces dernières ont toutes même cardinal, le cardinal de E est le produit de ce cardinal commun par le nombre de classes d'équivalence (*principe des bergers*).

Concrètement, une relation d'équivalence sur E permet de regrouper ("classer") les éléments de E par paquets ayant un "point commun" (le fait d'être en relation...).
Revoir les exemples 4), 5) et 6) ci-dessus !

9) Lois de composition interne

Soit E un ensemble ; on appelle *loi de composition interne sur* E toute application de $E \times E$ dans E.
Si $*$ est une loi de composition interne sur E, l'élément de E associé à un couple (x,y) est en général noté $x * y$ (notation *infixe*, au lieu de $*(x,y)$, notation *préfixe*).

On dit que :

- la loi $*$ est *associative* si et seulement si : $\forall (x,y,z) \in E^3 \quad (x*y)*z = x*(y*z)$;
- la loi $*$ est *commutative* si et seulement si : $\forall (x,y) \in E^2 \quad x*y = y*x$;
- la loi $*$ admet un élément neutre si et seulement si : $\exists e \in E \quad \forall x \in E \quad x*e = e*x = x$.
  Si c'est le cas, un tel élément e est unique, appelé *l'élément neutre de la loi* $*$.

Lorsque $*$ admet un élément neutre e, on dit qu'un élément x de E *admet un symétrique* pour la loi $*$ si et seulement si : $\exists x' \in E \quad x*x' = x'*x = e$.
Si c'est le cas, un tel élément x' est unique, appelé *le symétrique de* x pour la loi $*$, souvent noté x^{-1}.

II - Structure de groupe

1) Définition

On appelle *groupe* tout couple $(G, \cdot)$ où $\cdot$ est une loi de composition interne sur G, associative, possédant un élément neutre (noté e) et telle que tout élément x de G admette un symétrique pour $\cdot$, noté x^{-1}.
On dit qu'un groupe $(G, \cdot)$ est *abélien* (ou *commutatif*) si et seulement si la loi $\cdot$ est en outre commutative.

NB : lorsque la loi est appelée *multiplication*, l'élément neutre est souvent noté 1 et le symétrique est appelé *inverse* ; un groupe abélien est souvent noté $(G, +)$, l'élément neutre étant noté 0 et le symétrique de x noté $-x$ et appelé *opposé* de x (notation *additive*).

Exemple : $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$ sont des groupes abéliens.

Notations : on définit les *itérés* d'un élément x d'un groupe en posant :

- dans $(G, \cdot)$: $x^0 = e$, $\forall n \in \mathbb{N} \quad x^{n+1} = x^n \cdot x$ et $x^{-n} = (x^n)^{-1}$;
  on vérifie alors : $\forall (p, q) \in \mathbb{Z}^2 \quad x^{p+q} = x^p \cdot x^q$ et $(x^p)^q = x^{pq}$;
- dans $(G, +)$: $0.x = 0$, $\forall n \in \mathbb{N} \quad (n+1).x = n.x + x$ et $(-n).x = -(n.x)$;
  on vérifie alors : $\forall (p, q) \in \mathbb{Z}^2 \quad (p+q).x = p.x + q.x$ et $q.(p.x) = (pq).x$.

Attention ! $(x \cdot y)^2 = x \cdot y \cdot x \cdot y$ n'est pas toujours égal à $x^2 \cdot y^2$; toutefois, si x et y *commutent* (c'est-à-dire si $x \cdot y = y \cdot x$) alors on vérifie : $\forall p \in \mathbb{Z} \quad (x \cdot y)^p = x^p \cdot y^p$.

Propriété : soit $(G, \cdot)$ un groupe ; $\forall (x, y) \in G^2 \quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

NB : s'il n'y a pas ambiguïté sur le choix de la loi de composition interne, on parle du "groupe G".

2) Sous-groupes

$(G, \cdot)$ désigne un groupe, e son élément neutre.

a) Définition

Soit H une partie de G. On dit que H est un *sous-groupe* de $(G, \cdot)$ si et seulement si la restriction de la loi $\cdot$ à $H \times H$ induit sur H une structure de groupe.

b) Caractérisations

Une partie H de G est un sous-groupe de $(G, \cdot)$ si et seulement si H est non vide, stable par $\cdot$ et par passage au symétrique, c'est-à-dire

$$\big(\forall (x, y) \in H^2 \quad x \cdot y \in H\big) \quad \text{et} \quad \big(\forall x \in H \quad x^{-1} \in H\big).$$

Exemples : 1) Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.
2) L'ensemble $\mathbb{U}$ des complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$; pour $n \geq 2$, l'ensemble des racines n-ièmes de 1 dans $\mathbb{C}$ est un sous-groupe de cardinal n de $(\mathbb{U}, \times)$.

III - Structure d'anneau *(complément hors programme)*

1) Définition

On appelle *anneau* tout triplet $(A, +, \times)$, où $+$ et $\times$ sont deux lois de composition interne sur A telles que :

1) $(A, +)$ est un groupe abélien
(en *notation additive :* l'élément neutre de $+$ est noté 0, $-x$ est *l'opposé* de x) ;

2) $\times$ est associative, admet un élément neutre (souvent noté 1) ;

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

Un anneau $(A, +, \times)$ est dit *commutatif* si et seulement si $\times$ est en outre commutative.

Notations : le produit $x \times y$ de deux éléments est souvent noté $x.y$, voire xy ; on dispose des itérés d'un élément x de A pour $+$ (les $n.x$, $n \in \mathbb{Z}$) et pour $\times$ (les *puissances* x^n, $n \in \mathbb{N}$).

Si x est *inversible* pour $\times$ (c'est-à-dire s'il existe x' élément de A tel que $xx' = x'x = 1$), on dispose en outre des *puissances négatives*, l'inverse x' de x est noté x^{-1} ou encore $\dfrac{1}{x}$ si l'anneau est commutatif.

2) Règles de calcul dans un anneau

1) $\forall x \in A \quad 0 \times x = x \times 0 = 0$, $-x = (-1) \times x = x \times (-1)$.

2) $\forall (x, y) \in A^2 \quad -(x \times y) = (-x) \times y = x \times (-y)$, $(-x) \times (-y) = x \times y$.

3) Propriétés classiques des itérés...

4) *Formule du binôme de Newton :* si x et y *commutent* (*i.e.* si $xy = yx$),

$$\forall n \in \mathbb{N} \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} . x^{n-k} y^k$$

5) Si x et y commutent,

$$\forall n \in \mathbb{N}^* \quad x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^{n-1-k} y^k$$

Attention ! On peut *a priori* avoir $x \times y = 0$ avec x et y tous les deux non nuls.

3) Anneaux intègres

Dans ce paragraphe, $(A, +, \times)$ désigne un anneau commutatif.

Définition : A est dit *intègre* si et seulement si

$$\forall (x, y) \in A^2 \quad xy = 0 \Rightarrow (x = 0 \text{ ou } y = 0)$$

4) Exemples

1) $(\mathbb{Z}, +, \times)$, $(\mathbb{K}[X], +, \times)$ sont des anneaux commutatifs intègres.

2) $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau commutatif non intègre.

3) $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau non commutatif, non intègre (pour $n \geq 2$).

IV - Structure de corps

1) Définition

On appelle *corps* (commutatif) tout anneau commutatif, non réduit à $\{0\}$, dont tous les éléments non nuls sont inversibles.

2) Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont les "corps de nombres" classiques.

Pour tout corps $\mathbb{K}$, on construit l'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ et le corps $\mathbb{K}(X)$ des fractions rationnelles à coefficients dans $\mathbb{K}$ (hors programme en PSI, construit à partir de $\mathbb{K}[X]$ de la même façon que $\mathbb{Q}$ est construit à partir de $\mathbb{Z}$).

Remarque culturelle : il existe aussi des corps finis. Par exemple, pour p nombre premier, l'ensemble des p classes de congruence des entiers relatifs modulo p peut être muni d'une structure de corps.