Structures algébriques : groupes, anneaux et corps

Table des matières

1 Groupes

1.1 Lois de composition interne

DEFINITION 1
Soit E un ensemble. Une *loi de composition interne* (LCI) sur E est une application T de $E \times E$ dans E, notée généralement de façon infixe : on écrit $x\,T\,y$ plutôt que $T(x,y)$, lorsque $(x,y) \in E \times E$.

EXEMPLES 1
- *La somme sur* $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *(mais pas sur* $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$*).*
- *Le produit sur* $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$*...*
- *La différence sur* $\mathbb{R}$ *ou* $\mathbb{Z}$ *(mais pas sur* $\mathbb{N}$*).*
- *La composition des applications sur* F^F *(applications de* F *dans* F*).*
- *La loi* $\oplus$ *définie sur* $\mathbb{R}^2$ *par* $(x_1,y_1) \oplus (x_2,y_2) = (x_1+x_2, y_1+y_2)$.
- *La loi* $\otimes$ *définie sur* $\mathbb{R}^2$ *par* $(x_1,y_1) \otimes (x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ *(vous la reconnaissez ?)*
- *Les lois* $\cup$, $\cap$ *et* Δ *(réunion, intersection et différence symétrique) définies sur* $\mathcal{P}(F)$.

DEFINITION 2
- Une LCI T sur E sera dite *associative* lorsque :
$$\forall x,y,z \in E^3, \qquad (x\,T\,y)\,T\,z = x\,T\,(y\,T\,z).$$
- Une LCI T sur E sera dite *commutative* lorsque :
$$\forall x,y \in E^2, \qquad x\,T\,y = y\,T\,x.$$
- Si T est une LCI associative sur E, $e \in E$ est un *neutre* pour T lorsque :
$$\forall x \in E, \qquad x\,T\,e = e\,T\,x = x.$$

PROPOSITION 1 *Si* T *est une LCI associative sur* E *qui admet un neutre, alors ce neutre est unique. On peut alors parler DU neutre de* T.

PREUVE : On suppose e_1 et e_2 neutres pour T, et on considère $e_1\,T\,e_2$... ■

EXEMPLES 2
- *La somme et le produit sur* $\mathbb{C}$ *(**donc sur ses sous-ensembles**) est associative et commutative, et admettent pour neutres respectifs* 0 *et* 1.
- *La différence n'est ni associative ni commutative sur* $\mathbb{R}$.
- *La loi* $\circ$ *(composition des fonctions de* F *dans* F*) est associative, mais n'est pas commutative (sauf si* F *est un singleton, auquel cas...). Elle admet un neutre, qui est l'application* Id_F.
- *Les lois* $\cup$, $\cap$ *et* Δ *sur* $\mathcal{P}(F)$ *sont associatives et commutatives. Elles admettent pour neutres respectifs* $\emptyset$, F, *et* $\emptyset$.
- $\oplus$ *et* $\otimes$ *sont associatives et commutatives sur* $\mathbb{R}^2$.
- *Vue comme LCI sur* $\mathbb{N}^*$, $+$ *n'admet pas d'élément neutre.*

EXERCICE 1 *Montrer que les lois* $\oplus$ *et* $\oplus$ *sur* $\mathbb{R}^2$ *(cf exemples 1) admettent chacune un neutre.*

DEFINITION 3
Si T est une LCI associative sur E qui admet un neutre e et $x \in E$, on dit que x admet un *symétrique pour* T s'il existe $y \in E$ tel que $x\,T\,y = y\,T\,x = e$.

PROPOSITION 2 *Dans la définition précédente, si* y *existe, il est unique. On peut alors parler DU symétrique de* x *pour* T. *On le note généralement* x^{-1}.

PREUVE : Partir de $y_1\,T(x\,T\,y_2) = (y_1\,T\,x)T\,y_2$... ■

Remarques 1
- On peut avoir $x\,T\,y = e_G$ sans avoir $y\,T\,x = e_G$. On prendra par exemple $E = \mathbb{N}^{\mathbb{N}}$, T la loi $\circ$ de composition des fonctions, $y : n \mapsto n+1$ et $x : n \mapsto \text{Max}(n-1, 0)$.
- Les lois notées . sont souvent "oubliées" dans l'écriture : $x.y$ devient xy.
- Grâce à l'associativité, on s'autorise à noter $x\,T\,y\,T\,z$ la valeur commune de $(x\,T\,y)\,T\,z$ et $x\,T\,(y\,T\,z)$.
- Lorsque la loi est additive $+$, le symétrique est noté $-x$ et est appelé "opposé". Lorsque la loi est multiplicative ., le symétrique est appelé "inverse". On n'utilisera JAMAIS la notation $\frac{1}{x}$ (sauf pour les complexes-réels-entiers), puisqu'alors la notation $\frac{y}{x}$ serait ambigüe dans le cas d'une loi multiplicative non commutative (ce qui sera la rêgle en algèbre linéaire) : a priori, $y \cdot \frac{1}{x}$ et $\frac{1}{x} \cdot y$ peuvent être distincts...

Exercice 2 *Si x et y admettent un symétrique pour une loi $*$, montrer que $x * y$ admet également un symétrique.*

1.2 Groupes

Definition 4
Un *groupe* est un ensemble non vide muni d'une loi de composition interne $(G, *)$ tels que :
- $*$ est associative ;
- $*$ admet un neutre e_G ;
- tout élément de G est symétrisable (admet un symétrique) pour $*$.

Si $*$ est commutative, on dit que $(G, *)$ est commutatif, ou encore *abélien*.

Exemples 3
On fournit d'abord des exemples de groupes : dans les deux premiers cas et le dernier, il s'agit de groupes abéliens. Les deux autres (comme la plupart des groupes fonctionnels) sont non commutatifs.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *munis de la somme.*
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$, $\mathbb{U}_n$ *munis du produit.*
- *L'ensemble des homothéties et translations du plan, muni de la loi* $\circ$.
- *L'ensemble des permutations (bijections) de* $[\![1, n]\!]$ *muni de la loi* $\circ$.
- *L'ensemble* $\mathcal{P}(E)$ *muni de la différence symétrique* Δ.

Exemples 4
Pour diverses raisons (à déterminer), les couples suivants ne sont pas des groupes :
- $(\mathbb{N}, +)$, $(\mathbb{R}, .)$.
- $(\mathbb{U}, +)$.
- $(E^E, \circ)$.
- $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

Exercice 3 *Montrer que* $(\mathbb{R}^2, \oplus)$ *et* $(\mathbb{R}^2 \setminus \{(0,0)\}, \otimes)$ *sont des groupes commutatifs.*

1.3 Sous-groupes

Definition 5
Un *sous-groupe* d'un groupe $(G, *)$ est une partie *non vide* H de G telle que :
- $*$ induit sur H une loi de composition interne.
- Muni de cette loi, H est un groupe.

On note alors : $H < G$.

Remarques 2
- *En pratique*, pour montrer qu'une partie non vide H de G en constitue un sous-groupe, il suffit de vérifier :
  - $e_G \in H$;

- H est stable par $*$;
- pour tout $x \in H$, le symétrique x, a priori dans G, est en fait dans H.

- L'intérêt principal de la remarque précédente tient dans le fait que dans bien des cas, on peut montrer que $(H, *)$ est un groupe en montrant grâce au critère précédent que c'est un *sous-groupe d'un groupe connu*. Il est alors inutile de montrer l'associativité, la commutativité et même l'existence d'un neutre : il n'y a que des VERIFICATIONS à faire.

EXEMPLES 5

- *Pour la loi $+$, on a la "tour de groupe" (inclusions successives de sous-groupes/groupes) suivante :*

$$\{0\} < 1515\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$$

- *Pour la multiplication usuelle :*

$$\{1\} < \mathbb{U}_n < \mathbb{U} < \mathbb{C}^*$$

mais aussi :

$$\{1\} < \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$$

- *Si G est un groupe, $\{e_G\}$ et G en constituent des sous-groupes (dits* triviaux*)*

EXERCICE 4 *Soient H_1 et H_2 deux sous-groupes de $(G, .)$. Montrer que $H_1 \cap H_2$ est également un sous-groupe de G.*

On verra en TD que ça se passe moins bien pour la *réunion* de deux sous-groupes.

EXERCICE 5 *On définit l'ensemble :*

$$\mathbb{Z}[\sqrt{2}] = \left\{k + l\sqrt{2} \mid k, l \in \mathbb{Z}\right\}.$$

Montrer que $(\mathbb{Z}[\sqrt{2}], +)$ constitue un groupe ($+$ est l'addition usuelle des réels).

1.4 Morphismes de groupes

DEFINITION 6

- Soient $(G, *)$ et (H, T) deux groupes. Une application de G dans H est un "*morphisme de groupes*" lorsque :

$$\forall x, y \in G, \qquad f(x * y) = f(x)\, T\, f(y).$$

- Si $G = H$ et $* = T$, on parle d'*endomorphisme*.
- Si f est bijective, on parle d'*isomorphisme*.
- Si f est un endomorphisme bijectif, on parle d'*automorphisme*.

EXEMPLES 6

- *$x \mapsto 2^x$ réalise un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, .)$;*
- *$x \mapsto 2x$ réalise un automorphisme de $(\mathbb{R}, +)$;*
- *$x \mapsto 3 \ln x$ réalise un isomorphisme de $(\mathbb{R}_+^*, .)$ sur $(\mathbb{R}, +)$;*
- *$z \mapsto |z|$ réalise un morphisme de $(\mathbb{C}^*, .)$ dans $(\mathbb{R}^*, .)$.*
- *Si G est un groupe* **abélien**, *$x \mapsto x^2$ et $x \mapsto x^{-1}$ réalisent des endomorphismes de G.*
- *$\theta \mapsto e^{i\theta}$ réalise un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, .)$, et même sur $(\mathbb{U}, .)$.*

EXERCICE 6 *Si f est un morphisme de $(G, *)$ dans $(H, \circ)$ et g un morphisme de $(H, \circ)$ dans (K, T), montrer que $g \circ f$ réalise un morphisme de $(G, *)$ dans (K, T).*

EXERCICE 7 *Montrer que si f est un isomorphisme de $(G, *)$ sur $(H, \circ)$, alors son application réciproque f^{-1} réalise un isomorphisme de $(H, \circ)$ sur $(G, *)$.*

PROPOSITION 3 *Quelques propriétés élémentaires des morphismes de groupes : f est ici un morphisme de $(G,*)$ dans (H,T).*

- $f(e_G) = e_H$.
- *Si f est un isomorphisme, alors son application réciproque réalise un isomorphisme de (H,T) sur $(G,*)$.*
- *Si $G_1 < G$, alors $f(G_1) < H$.*
- *Si $H_1 < H$, alors $f^{-1}(H_1) < G$.*

PREUVE : Elémentaire, donc à savoir faire seul ! ■

DFINITION 7
Soit f un morphisme de G dans H.

- Le *noyau* de f, noté Ker f est l'ensemble des antécédents par f de e_H :

$$\text{Ker } f = \{x \in G;\quad f(x) = e_H\} = f^{-1}(e_H)$$

  (attention, f n'est pas supposée bijective ; il n'est donc pas question de la bijection réciproque de f).
- L'*image* de f, noté Im f est $f(G)$ (ensemble des images par f des éléments de G).

D'après les deux derniers points de la proposition 3, le noyau et l'image de f sont des sous-groupes respectifs de G et H.

EXERCICE 8 *Montrer que $(\mathbb{U},.)$ est un groupe, en le voyant successivement comme image et noyau d'un morphisme de groupe.*

Bien entendu, et c'est une trivialité, un morphisme de G dans H est surjectif si et seulement si son image est égale à H. Ce résultat est d'ailleurs sans intérèt ... Le résultat suivant est bien plus intéressant, puisqu'il réduit énormément le travail, pour montrer qu'un morphisme est injectif.

PROPOSITION 4 *Soit f un morphisme de $(G,*)$ dans (H,T). Alors f est injectif si et seulement si son noyau est réduit à $\{e_G\}$.*

PREUVE : Elémentaire, donc à savoir faire seul... ■

EXERCICE 9 *L'application $\varphi : \mathbb{R}^2 \to \mathbb{R}^2, (x,y) \mapsto (2x-y, 3x+2y)$ est-elle injective ?*

2 Anneaux

2.1 Structure d'anneau

DFINITION 8
Un *anneau* est un ensemble muni de deux LCI $(A,+,.)$ tels que :

- $(A,+)$ est un groupe *commutatif* de neutre noté 0_A.
- La loi . est une LCI sur A associative et *distibutive* à gauche et à droite par rapport à + :

$$\forall x,y,z \in A, \qquad x.(y+z) = x.y + x.z \quad \text{et} \quad (x+y).z = x.z + y.z$$

- La loi . admet un neutre différent de 0_A, noté $\mathbf{1}_A$.

Si la loi . est commutative, l'anneau est dit commutatif ou abélien.

EXERCICE 10 *Si $x \in A$, montrer que $0_A.x = 0_A$ (considérer $0_A.x + 0_A.x$).*

EXEMPLES 7

- $(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$ *et* $(\mathbb{C},+,.)$ *sont des anneaux bien connus.*
- $(\mathcal{P}(E),\Delta,\cap)$ *est un anneau plus anecdotique.*
- $(\mathbb{R}^2,\oplus,\otimes)$ *est un anneau... connu sous une autre identité !*

- *L'ensemble des suites réelles, muni de l'addition et du produit des suites, est un anneau. Même chose pour l'ensemble des fonctions de I dans $\mathbb{R}$. On déterminera précisément les neutres de ces anneaux.*

Remarques 3
- Il est nécessaire d'imposer la distributivité à droite et à gauche. Par exemple, $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ n'est pas un anneau : on a bien $(f+g)\circ h = f\circ h + g\circ h$ pour tout f, g, h, mais pas nécessairement $f\circ(g+h) = f\circ g + f\circ h$.
- Lorsqu'on travaille dans un anneau, de nombreux calculs se passent "comme dans $\mathbb{R}$". Cela dit, il faut faire attention par exemple à ne pas diviser. Le meilleur moyen pour ne pas dire d'ânerie consiste en fait à "faire comme dans $\mathbb{Z}$".

2.2 Sous-anneaux

Definition 9
Soit $(A, +, .)$ un anneau. Une partie non vide A_1 de A est un *sous-anneau* de A lorsque :
- $\mathbf{1}_A \in A_1$;
- les lois $+$ et $.$ induisent des LCI sur A_1, et, muni de ces lois, $(A_1, +, .)$ est un anneau.

Remarque 4 Contrairement aux sous-groupes, on ne peut pas se passer de la condition $\mathbf{1}_A \in A_1$, qui ne découle pas des autres conditions[1]. On verra en exercice un contre-exemple.

Comme pour les sous-groupes, il est assez moyennement intéressant de montrer à nouveau les associativités et même la distributivité. Fort heureusement, on a le résultat (quasi-évident) suivant :

Proposition 5 *Une partie A_1 de A est un sous-anneau si et seulement si*
- *$(A_1, +)$ est un sous-groupe de $(A, +)$;*
- *$\mathbf{1}_A \in A_1$;*
- *$.$ induit une LCI sur A_1.*

Exemples 8
- *Bien entendu, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ qui est un sous-anneau de...*
- *L'ensemble des fonctions dérivables sur I constitue un sous-anneau des fonctions continues sur I, qui constitue lui-même un sous-anneau de l'ensemble des fonctions de I dans $\mathbb{R}$.*
- *L'ensemble des suites réelles stationnaires est un sous-anneau de $(\mathbb{R}^{\mathbb{N}}, +, .)$, qui est un sous-anneau de $(\mathbb{C}^{\mathbb{N}}, +, .)$*

Exercice 11 *Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.*

Exercice 12 *Montrer que si A_1 et A_2 sont deux sous-anneaux d'un anneau A, alors $A_1 \cap A_2$ est également un sous-anneau de A.*

2.3 Morphismes d'anneaux

Definition 10
Soient $(A, +, .)$ et $(B, +, .)$ deux anneaux (on note de la même façon les lois de A et B...). Un *morphisme d'anneaux* de A vers B est une application de A vers B telle que :
- $f(\mathbf{1}_A) = \mathbf{1}_B$;
- pour tout $x, y \in A$, $f(x+y) = f(x) + f(y)$ et $f(x.y) = f(x).f(y)$.

Exemples 9
- *$z \mapsto \overline{z}$ réalise un automorphisme d'anneaux de $\mathbb{C}$.*
- *$f \mapsto f(\pi)$ réalise un morphisme d'anneaux de $\mathbb{R}^{\mathbb{R}}$ sur[2] $\mathbb{R}$.*

[1] on se rappelle que dans le cas d'un sous-groupe H de G, la relation $e_G \in H$ est une conséquence de la définition
[2] comme pour les fonctions, on dit "de E *sur* F" plutôt que "de E *dans* F", lorsque le morphisme est surjectif

- $u \mapsto u_{1515}$ *réalise un morphisme d'anneaux surjectif (pourquoi ?) de* $\mathbb{C}^{\mathbb{N}}$ *sur* $\mathbb{C}$.

Remarques 5
- La relation $f(\mathbf{1}_A) = \mathbf{1}_B$ ne découle pas des autres relations[3] ; on ne peut donc pas s'en passer dans la définition.
- A fortiori, un morphisme d'anneaux est un morphisme de groupe (pour la première loi). A ce titre, on peut parler de son image et de son noyau. Malheureusement, si l'image est un sous-anneau de l'anneau d'arrivée (le montrer), le noyau n'est pas nécessairement un sous-anneau de l'anneau de départ, ce qui limite l'intéret des morphismes d'anneaux. Cependant, on garde l'équivalence entre l'injectivité de f et le fait que $\operatorname{Ker} f = \{0_A\}$.

Exercice 13 *Montrer que la composée de deux morphismes d'anneaux est un morphisme d'anneaux.*

Exercice 14 *Montrer que si f est un isomorphisme d'anneaux, alors son application réciproque également.*

2.4 Divisibilité

Dfinition 11
Soit $(A, +, .)$ un anneau *commutatif*.
- On dit que $x \in A$ est *inversible* s'il admet un symétrique pour la loi .
- On dit que a *divise* b s'il existe $c \in A$ tel que $b = ca$. On note $a|b$.
- On dit que a est un *diviseur de* 0 s'il existe $b \neq 0$ tel que $ab = 0$.
- Un anneau est dit *intègre* s'il ne contient pas de diviseur de 0 autre que 0 lui-même.

Les faits suivants sont faciles à montrer :

Proposition 6 *Dans un anneau commutatif $(A, +, .)$:*
- 0_A *n'est jamais inversible.*
- *Si x est inversible, alors ce n'est pas un diviseur de* 0.
- *Si $x_1, x_2, y \in A$ intègre, avec $y \neq 0$ et $x_1 y = x_2 y$, alors $x_1 = x_2$. On dit qu'*"on peut simplifier" *(ce qui ne veut pas dire* diviser*) par $y \neq 0$.*

Exemples 10
- $\mathbb{Z}$ *est intègre, et ses éléments inversibles sont* 1 *et* -1.
- $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$ *sont des anneaux intègres dont tous les éléments non nuls sont inversibles.*
- *L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre : toute application f qui s'annulle est diviseur de* 0 *(le montrer). Les éléments inversibles sont les fonctions qui ne s'annullent pas.*

Exercice 15 *Montrer que $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ est un sous-anneau intègre de $\mathbb{C}$, dont les inversibles sont* 1, i, -1 *et* $-i$.

2.5 Calculs dans les anneaux

- On rappelle la formule du *binôme de Newton*, qui s'étend de $\mathbb{Z}$ aux anneaux commutatifs, mais aussi (et cela sert effectivement[4]) dans un anneau quelconque, *avec deux éléments qui commutent* :

  Proposition 7 *Soient $a, b \in A$, avec $ab = ba$, et $n \in \mathbb{N}^*$. Alors :*

$$(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_n^k a^k b^{n-k}.$$

  Preuve : Récurrence sur $\mathbb{N}$ et formule du triangle de Pascal. ■

[3] contrairement aux morphismes de groupes, pour lesquels la relation $\varphi(e_G) = e_H$ est une conséquence de la définition
[4] en particulier dans les anneaux de matrices

- Si $x, y \in A$ commutent et $n \in \mathbb{N}^*$, alors $x - y | x^n - y^n$, et plus précisément :

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

BIEN ENTENDU, pour les deux derniers résultats, l'hypothèse essentielle $xy = yx$ ne sera jamais oubliée...

- Cas particulier de ce qui précède : si $1 - x$ est inversible (ce qui n'est pas EQUIVALENT à $x \neq 1$), on peut calculer $\sum_{k=0}^{n-1} x^k$ grâce à la formule :

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

$\mathbf{1}_A$ *commute en effet avec tous les éléments de l'anneau.*

- On verra en TD de Maple l'algorithme d'*exponentiation rapide*, qui permet de calculer a^n en $O(\ln n)$ multiplications. L'idée apparaît dans l'exemple suivant :

$$a^{53} = a.(a^2)^{26} = a.(a^4)^{13} = a.a^4.(a^8)^6 = a.a^4.(a^{16})^3 = a.a^4.a^{16}.a^{32}.$$

Il suffit donc de calculer les a^{2^k}, et d'en tenir compte dans le résultat final lorsque la puissance en cours est impaire (si $(a^4)^{13}$ apparaît en cours de calcul, alors a^4 interviendra dans le résultat). Au vu de cet exemple, on peut formaliser l'algorithme d'exponentiation rapide de la façon suivante :

```
Fonction Expo_rapide(x,n)
Debut
  Res<-1;  # Contiendra à la fin le résultat
  Puis<-x; # Contiendra les puissances successives de x
  N<-n;    # Puissance à laquelle Puis doit encore être évalué
  Tant_que N>0
    Si N est impair Alors Res<-Res*Puis Fsi;
    Puis<-Puis^2;
    N<-N/2 # en fait, le quotient dans la division euclidienne
    Fin_Tant_que;
  RETOURNER(Res)
Fin
```

Mise en oeuvre en TD Maple... où on verra une seconde version récursive plus rapide à écrire, mais qui semble un peu magique !

Pour prouver la validité de cet algorithme, on peut noter (là encore au vu de l'exemple) PUIS prouver que la quantité `Res*Puis^N` reste égale à x^n en cours d'exécution[5]. Quand on veut frimer, on parle d'*invariant de boucle.*

3 Corps

3.1 Structure de corps

DEFINITION 12

- Un *corps* est un anneau commutatif dans lequel tout élément non nul est inversible.
- Si $(\mathbb{K}, +, .)$ est un corps, un *sous-corps* de $\mathbb{K}$ est un sous-anneau $\mathbb{K}_1$ de $\mathbb{K}$ tel que pour tout élément non nul x de $\mathbb{K}_1$, on a $x^{-1} \in \mathbb{K}_1$; $(\mathbb{K}_1, +, .)$ est alors un corps.

[5] au début et à la fin de chaque tour de boucle

REMARQUE 6 Si on enlève l'hypothèse de commutativité, on obtient ce que les anglo-saxons appellent "*division ring*", traduit piteusement par "*anneau à division*". En taupe, dans les temps anciens, le terme de *corps* désignait d'ailleurs ces anneaux à divisions.

En anglais, les corps se nomment "*fields*". Pourquoi ? mystère...

3.2 Exemples

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{Z}$ (2 n'est pas inversible).
- On verra plus tard le *corps des fractions rationnelles* (quotients de polynômes).
- $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i]$ sont des sous-corps respectifs de $\mathbb{R}$ et $\mathbb{C}$.
- Si on reprend les lois $\oplus$ et $\otimes$ des exemples 1, $(\mathbb{R}^2, \oplus, \otimes)$ est un corps... qui ressemble fortement à $\mathbb{C}$.

3.3 Pour la suite

Il n'existe en Spé (hors MP/MP*) que $2,5$ corps : $\mathbb{R}$, $\mathbb{C}$, et (accessoirement...) $\mathbb{Q}$.

Bien entendu, si on passe l'X (et si on n'a pas trop de chance...), il ne faudra rien ignorer des corps finis $\mathbb{F}_q$, mais c'est une autre histoire !