Opérations, lois, structures en informatique

INFO1 - Semaines 43 & 45

Guillaume CONNAN

IUT de Nantes - Dpt d'informatique

Dernière mise à jour : 24 octobre 2013 à 14:47

Sommaire

Sommaire

Définition 1 (Loi de composition interne (LCI))

Une loi de composition interne définie sur un ensemble E est une fonction totale (ou application) de $E \otimes E$ dans E. On dit alors que E est un **magma**.

Définition 2 (Stabilité)

Un ensemble E est stable par une opération $\star$ si, et seulement si :

$$\Big(\forall \langle x,y\rangle\Big)\Big(\big(\langle x,y\rangle \in E\otimes E\big) \to \big(x\star y \in E\big)\Big)$$

Définition 3 (Loi de composition externe (LCE))

Une loi de composition externe définie sur un ensemble E et à opérateurs dans un ensemble K est une fonction totale (ou application) de $K \otimes E$ dans E.

Définition 4 (Morphisme)

Soit $\langle E, \star \rangle$ et $\langle F, \dagger \rangle$ deux magmas et φ une fonction totale de E dans F.
On dit que φ est un morphisme de E dans F si, et seulement si :

$$(\forall x)(\forall y)\big(\varphi(x \star y) = \varphi(x) \dagger \varphi(y)\big)$$

Définition 5 (Isomorphisme)

Soit $\langle E, \star \rangle$ et $\langle F, \dagger \rangle$ deux magmas et φ une fonction totale de E dans F. On dit que φ est un morphisme de E dans F si, et seulement si, c'est un morphisme BIJECTIF de E dans F.

Définition 6 (Commutativité)

Une LCI $\star$ sur E est commutative si, et seulement si

$$(\forall x)(\forall y)(x \star y = y \star x)$$

Définition 7 (Associativité)

Une LCI $\star$ sur E est associative si, et seulement si

$$(\forall x)(\forall y)(\forall z)(x \star (y \star z) = (x \star y) \star z)$$

Un magma muni d'une loi associative est appelé... un magma associatif.

Définition 8 (Élément neutre)

Un élément neutre e d'une LCI $\star$ sur E est un élément $e_\star$ qui vérifie :

$$(\forall x)(x \star e_\star = e_\star \star x = x)$$

Un magma associatif admettant un élément neutre est un **monoïde** (ou un magma associatif **unifère**).

Pouvez-vous démontrer que si l'élément neutre existe, il est unique ?

Définition 8 (Élément neutre)

Un élément neutre e d'une LCI $\star$ sur E est un élément $e_\star$ qui vérifie :

$$(\forall x)(x \star e_\star = e_\star \star x = x)$$

Un magma associatif admettant un élément neutre est un **monoïde** (ou un magma associatif **unifère**).

Pouvez-vous démontrer que si l'élément neutre existe, il est unique ?

Définition 8 (Élément neutre)

Un élément neutre e d'une LCI $\star$ sur E est un élément $e_\star$ qui vérifie :

$$(\forall x)(x \star e_\star = e_\star \star x = x)$$

Un magma associatif admettant un élément neutre est un **monoïde** (ou un magma associatif **unifère**).

Pouvez-vous démontrer que si l'élément neutre existe, il est unique ?

Définition 9 (Élément symétrisable)

Soit x un élément de E. Il est inversible (ou symétrisable) par $\star$ si, et seulement si,

$$(\exists y)(x \star y = y \star x = e_\star)$$

Pouvez-vous démontrer que si x admet un symétrique, alors ce symétrique est unique ?

Définition 9 (Élément symétrisable)

Soit x un élément de E. Il est inversible (ou symétrisable) par $\star$ si, et seulement si,

$$(\exists y)(x \star y = y \star x = e_\star)$$

Pouvez-vous démontrer que si x admet un symétrique, alors ce symétrique est unique ?

Définition 9 (Élément symétrisable)

Soit x un élément de E. Il est inversible (ou symétrisable) par $\star$ si, et seulement si,

$$(\exists y)(x \star y = y \star x = e_\star)$$

Pouvez-vous démontrer que si x admet un symétrique, alors ce symétrique est unique ?

Définition 10 (Régularité)

Un élément a de E est dit **régulier à gauche** (ou **simplifiable à gauche**) si, et seulement si :

$$(\forall x)(\forall y)((a \star x = a \star y) \rightarrow (x = y))$$

On a une définition similaire de la régularité à droite.
Un élément à la fois régulier à gauche et à droite est dit **régulier**.
Une loi telle que tout élément soit régulier est dite régulière.

Un élément inversible est régulier (vérifiez-le). Un élément régulier est-il inversible ?

Définition 10 (Régularité)

Un élément a de E est dit **régulier à gauche** (ou **simplifiable à gauche**) si, et seulement si :

$$(\forall x)(\forall y)((a \star x = a \star y) \rightarrow (x = y))$$

On a une définition similaire de la régularité à droite.
Un élément à la fois régulier à gauche et à droite est dit **régulier**.
Une loi telle que tout élément soit régulier est dite régulière.

Un élément inversible est régulier (vérifiez-le). Un élément régulier est-il inversible ?

Définition 10 (Régularité)

Un élément a de E est dit **régulier à gauche** (ou **simplifiable à gauche**) si, et seulement si :

$$(\forall x)(\forall y)((a \star x = a \star y) \rightarrow (x = y))$$

On a une définition similaire de la régularité à droite.
Un élément à la fois régulier à gauche et à droite est dit **régulier**.
Une loi telle que tout élément soit régulier est dite régulière.

Un élément inversible est régulier (vérifiez-le). Un élément régulier est-il inversible ?

Définition 11 (Distributivité)

On dit que la loi $\star$ définie sur E est distributive sur $\dagger$ définie sur E si, et seulement si :

$$\Big(\forall x\Big)\Big(\forall y\Big)\Big(\forall z\Big)\Big(\big(x\star(y\dagger z)=(x\star y)\dagger(x\star z)\big)\wedge\big((y\dagger z)\star x=(y\star x)\dagger(z\star x)\big)\Big)$$

Définition 12 (Élément absorbant)

Un élément absorbant d'une LCI $\star$ sur E est un élément $a_\star$ qui vérifie :

$$(\forall x)(x \star a_\star = a_\star \star x = a_\star)$$

Montrez que si un tel élément existe, il est unique.

Définition 12 (Élément absorbant)

Un élément absorbant d'une LCI $\star$ sur E est un élément $a_\star$ qui vérifie :

$$(\forall x)(x \star a_\star = a_\star \star x = a_\star)$$

Montrez que si un tel élément existe, il est unique.

Définition 12 (Élément absorbant)

Un élément absorbant d'une LCI $\star$ sur E est un élément $a_\star$ qui vérifie :

$$(\forall x)(x \star a_\star = a_\star \star x = a_\star)$$

Montrez que si un tel élément existe, il est unique.

Définition 13 (Élément involutif)

Soit $\star$ une loi sur un ensemble E admettant un élément neutre $e_\star$.
Alors x est **involutif** si, et seulement si, $x \star x = e_\star$.

Définition 13 (Élément involutif)

Soit $\star$ une loi sur un ensemble E admettant un élément neutre $e_\star$.
Alors x est **involutif** si, et seulement si, $x \star x = e_\star$.

Définition 14 (Élément idempotent)

Soit $\star$ une loi sur un ensemble E.
Alors x est **idempotent** si, et seulement si, $x \star x = x$.

Définition 13 (Élément involutif)

Soit $\star$ une loi sur un ensemble E admettant un élément neutre $e_\star$.
Alors x est **involutif** si, et seulement si, $x \star x = e_\star$.

Définition 14 (Élément idempotent)

Soit $\star$ une loi sur un ensemble E.
Alors x est **idempotent** si, et seulement si, $x \star x = x$.

Sommaire

É.Galois (1811-1832)

Définition 15 (Groupe)

Un groupe est un monoïde tel que tout élément est inversible.

Définition 16 (Sous-groupe)

$\langle H, \star \rangle$ est un sous-groupe de $\langle G, \star \rangle$ si, et seulement si, H est une partie de G et $\langle H, \star \rangle$ est un groupe.

Définition 15 (Groupe)

Un groupe est un monoïde tel que tout élément est inversible.

Définition 16 (Sous-groupe)

$\langle H, \star \rangle$ est un sous-groupe de $\langle G, \star \rangle$ si, et seulement si, H est une partie de G et $\langle H, \star \rangle$ est un groupe.

Définition 15 (Groupe)

Un groupe est un monoïde tel que tout élément est inversible.

Définition 16 (Sous-groupe)

$\langle H, \star \rangle$ est un sous-groupe de $\langle G, \star \rangle$ si, et seulement si, H est une partie de G et $\langle H, \star \rangle$ est un groupe.

Sommaire

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 17 (Anneau)

Soit A un ensemble muni de deux lois $\boxdot$ et $\boxplus$.
On dit que $\langle A, \boxplus, \boxdot \rangle$ est un anneau si, et seulement si :

- $\langle A, \boxplus \rangle$ est un groupe commutatif ;
- $\boxdot$ est associative ;
- $\boxdot$ est distributive sur $\boxplus$.

Si $\boxdot$ est commutative, alors l'anneau est dit *commutatif*.
Si $\boxdot$ admet un élément neutre, l'anneau est dit *unitaire*.
Les éléments d'un anneau unitaire qui admettent un symétrique par $\boxdot$ sont dits *inversibles*. On note A^* l'ensemble des éléments inversibles de A.

Définition 18 (Corps)

Soit $\mathbb{K}$ un ensemble muni de deux LCI $\boxplus$ et $\boxdot$. Le triplet $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ possède une structure de **corps** si, et seulement si,

- $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ a une structure d'anneau unitaire ;
- $\langle \mathbb{K} \setminus \{e_{\boxplus}\}, \boxdot \rangle$ a une structure de groupe.

Combien d'éléments a au minimum un corps ?

Définition 18 (Corps)

Soit $\mathbb{K}$ un ensemble muni de deux LCI $\boxplus$ et $\boxdot$. Le triplet $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ possède une structure de **corps** si, et seulement si,

- $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ a une structure d'anneau unitaire ;
- $\langle \mathbb{K} \setminus \{e_{\boxplus}\}, \boxdot \rangle$ a une structure de groupe.

Combien d'éléments a au minimum un corps ?

Définition 18 (Corps)

Soit $\mathbb{K}$ un ensemble muni de deux LCI $\boxplus$ et $\boxdot$. Le triplet $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ possède une structure de **corps** si, et seulement si,

- $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ a une structure d'anneau unitaire ;
- $\langle \mathbb{K} \setminus \{e_{\boxplus}\}, \boxdot \rangle$ a une structure de groupe.

Combien d'éléments a au minimum un corps ?

Définition 18 (Corps)

Soit $\mathbb{K}$ un ensemble muni de deux LCI $\boxplus$ et $\boxdot$. Le triplet $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ possède une structure de **corps** si, et seulement si,

- $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ a une structure d'anneau unitaire ;
- $\langle \mathbb{K} \setminus \{e_{\boxplus}\}, \boxdot \rangle$ a une structure de groupe.

Combien d'éléments a au minimum un corps ?

Définition 18 (Corps)

Soit $\mathbb{K}$ un ensemble muni de deux LCI $\boxplus$ et $\boxdot$. Le triplet $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ possède une structure de **corps** si, et seulement si,

- $\langle \mathbb{K}, \boxplus, \boxdot \rangle$ a une structure d'anneau unitaire ;
- $\langle \mathbb{K} \setminus \{e_{\boxplus}\}, \boxdot \rangle$ a une structure de groupe.

Combien d'éléments a au minimum un corps ?

```
class  (Eq a, Show a) => Num a  where
    (+), (-), (*)  :: a -> a -> a
    negate         :: a -> a
    abs, signum    :: a -> a
    fromInteger    :: Integer -> a
```

À quelle structure algébrique peut-on associer la classe Num ?

```haskell
class  (Eq a, Show a) => Num a  where
    (+), (-), (*)  :: a -> a -> a
    negate         :: a -> a
    abs, signum    :: a -> a
    fromInteger    :: Integer -> a
```

À quelle structure algébrique peut-on associer la classe Num ?

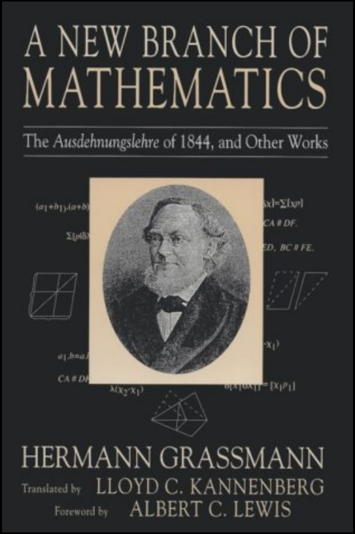
```haskell
class  (Num a) => Fractional a  where
    (/)          :: a -> a -> a
    recip        :: a -> a
    fromRational :: Rational -> a
```

À quelle structure algébrique peut-on associer la classe `Frational` ?

```
class  (Num a) => Fractional a  where
    (/)          :: a -> a -> a
    recip        :: a -> a
    fromRational :: Rational -> a
```

À quelle structure algébrique peut-on associer la classe `Frational` ?

Sommaire



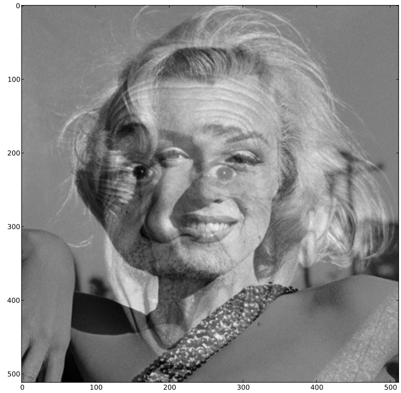
Hermann Graßmann (1809-1877)

Stefan Banach (1892-1945)

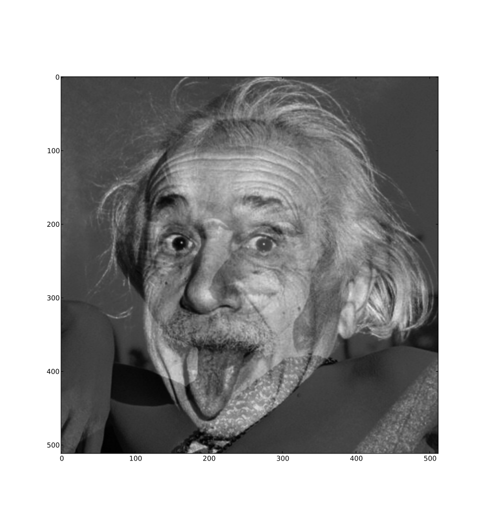
$3 \times \text{Marylin} + \text{Albert}$

$3 \times \text{Marylin} + \text{Albert}$

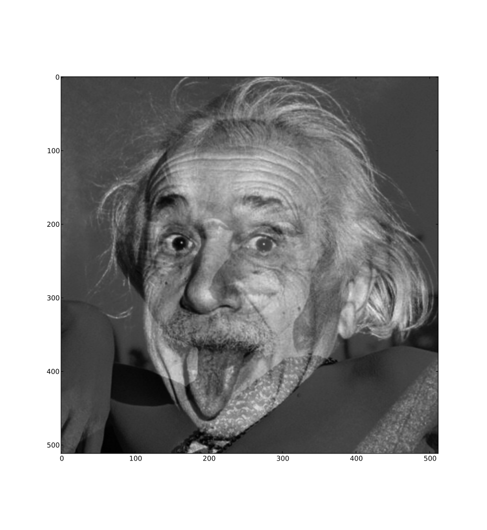
Marylin + Albert



Marylin + Albert



Marylin + 3 × Albert



Marylin + 3 × Albert

Définition 19 ($\mathbb{K}$-espace vectoriel)

Un $\mathbb{K}$-espace vectoriel V sur un corps commutatif $\langle \mathbb{K}, \oplus, \odot \rangle$ est un groupe abélien $\langle V, \dagger \rangle$ muni d'une loi de composition *externe* $\cdot$ de $\mathbb{K} \otimes V$ dans V vérifiant les quatre axiomes suivant, λ et μ désignant des scalaires quelconques, $\boldsymbol{u}$ et $\boldsymbol{v}$ des vecteurs quelconques et $1_\odot$ l'élément neutre de la loi $\odot$ sur $\mathbb{K}$:

$$(\lambda \oplus \mu) \cdot \boldsymbol{u} = \lambda \cdot \boldsymbol{u} \dagger \mu \cdot \boldsymbol{u} \qquad \text{(distributivité vectorielle) ;}$$

$$\lambda \cdot (\boldsymbol{u} \dagger \boldsymbol{v}) = \lambda \cdot \boldsymbol{u} \dagger \lambda \cdot \boldsymbol{v} \qquad \text{(distributivité scalaire) ;}$$

$$(\lambda \odot \mu) \cdot \boldsymbol{u} = \lambda \cdot (\mu \cdot \boldsymbol{u}) \qquad \text{(associativité) ;}$$

$$1_\odot \cdot \boldsymbol{u} = \boldsymbol{u} \qquad \text{(axiome d'identité)}$$

On dit que le corps $\mathbb{K}$ *opère* sur le groupe $\langle V, \dagger \rangle$.

```
imshow(3 * marilyn + einstein, cmap = cm.gray)
```

Définition 19 ($\mathbb{K}$-espace vectoriel)

Un $\mathbb{K}$-espace vectoriel V sur un corps commutatif $\langle\mathbb{K},\oplus,\odot\rangle$ est un groupe abélien $\langle V,\dagger\rangle$ muni d'une loi de composition *externe* $\cdot$ de $\mathbb{K}\otimes V$ dans V vérifiant les quatre axiomes suivant, λ et μ désignant des scalaires quelconques, $\boldsymbol{u}$ et $\boldsymbol{v}$ des vecteurs quelconques et $1_\odot$ l'élément neutre de la loi $\odot$ sur $\mathbb{K}$:

$$(\lambda\oplus\mu)\cdot\boldsymbol{u}=\lambda\cdot\boldsymbol{u}\dagger\mu\cdot\boldsymbol{u} \qquad \text{(distributivité vectorielle) ;}$$

$$\lambda\cdot(\boldsymbol{u}\dagger\boldsymbol{v})=\lambda\cdot\boldsymbol{u}\dagger\lambda\cdot\boldsymbol{v} \qquad \text{(distributivité scalaire) ;}$$

$$(\lambda\odot\mu)\cdot\boldsymbol{u}=\lambda\cdot(\mu\cdot\boldsymbol{u}) \qquad \text{(associativité) ;}$$

$$1_\odot\cdot\boldsymbol{u}=\boldsymbol{u} \qquad \text{(axiome d'identité)}$$

On dit que le corps $\mathbb{K}$ *opère* sur le groupe $\langle V,\dagger\rangle$.

```
imshow(3 * marilyn + einstein, cmap = cm.gray)
```

$$\langle b_1, b_2, b_3\rangle \dagger \langle b_1', b_2', b_3'\rangle = \langle b_1 \oplus b_1', b_2 \oplus b_2', b_3 \oplus b_3'\rangle$$

$$(\cdot) : \begin{array}{rcl} \mathbb{F}_2 \otimes T & \to & T \\ \langle \lambda, \langle b_1, b_2, b_3\rangle\rangle & \mapsto & \langle \lambda \odot b_1, \lambda \odot b_2, \lambda \odot b_3\rangle \end{array}$$

$$\langle b_1, b_2, b_3\rangle \dagger \langle b_1', b_2', b_3'\rangle = \langle b_1 \oplus b_1', b_2 \oplus b_2', b_3 \oplus b_3'\rangle$$

$$(\cdot) : \begin{array}{rcl} \mathbb{F}_2 \otimes T & \longrightarrow & T \\ \big\langle \lambda, \langle b_1, b_2, b_3\rangle\big\rangle & \longmapsto & \langle \lambda \odot b_1, \lambda \odot b_2, \lambda \odot b_3\rangle \end{array}$$

```haskell
data BoolInt = O | I deriving(Show,Read,Eq)

type BitChaine = [BoolInt]

bPlus :: BoolInt -> BoolInt -> BoolInt
bPlus    b1         b2
  |b1 == b2                    = O
  |otherwise                   = I

bFois :: BoolInt -> BoolInt -> BoolInt
bFois    I          I          =  I
bFois    _          _          =  O

cPlus :: BitChaine -> BitChaine -> BitChaine
cPlus    c1           c2           =  zipWith bPlus c1 c2

prodExt :: BoolInt -> BitChaine -> BitChaine
prodExt    b          c            =  map (\x -> bFois b x) c
```

```
*Main> bPlus O I
I
*Main> cPlus [O,O,I] [I,O,I]
[I,O,O]
*Main> prodExt I [O,O,I]
[O,O,I]
*Main> prodExt O [O,O,I]
[O,O,O]
```

```
lesBits = [O,I]

lesTrios = [[x,y,z] | x <- lesBits, y <- lesBits, z <- lesBits]

and [prodExt (bPlus b1 b2) t == cPlus (prodExt b1 t) (prodExt b2 t)
    | b1 <- lesBits, b2 <- lesBits, t <- lesTrios ]
```

Définition 20 (Combinaison linéaire de vecteurs)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ un corps opérant sur le groupe $\langle V, \dagger \rangle$ pour former un espace vectoriel de produit externe $\bullet$.

Soit $\langle \boldsymbol{u_0}, \boldsymbol{u_1}, \cdots, \boldsymbol{u_p} \rangle$ une famille de vecteurs de V.

Un vecteur $\boldsymbol{v}$ de V est une combinaison linéaire de la famille des $\langle \boldsymbol{u_i} \rangle_{0 \leqslant i \leqslant p}$ si, et seulement si, il existe une famille $\langle \lambda_0, \lambda_1, \cdots, \lambda_p \rangle$ de scalaires de $\mathbb{K}$ vérifiant :

$$\boldsymbol{v} = \dagger_{i=0}^{i=p} \lambda_i \bullet \boldsymbol{u_i} = \lambda_0 \bullet \boldsymbol{u_0} \dagger \lambda_1 \bullet \boldsymbol{u_1} \dagger \cdots \dagger \lambda_p \bullet \boldsymbol{u_p}$$

L'ensemble de ces combinaisons linéaires est noté :

$$\mathcal{V}\mathrm{ect}\{\boldsymbol{u_0}, \boldsymbol{u_1}, \cdots, \boldsymbol{u_p}\}$$

```
u = [O,I,I]
v = [I,O,I]
vect = [cPlus (prodExt b1 u) (prodExt b2 v) | b1 <- lesBits, b2 <-
    lesBits]
```

```
*Main> vect
[[O,O,O],[I,O,I],[O,I,I],[I,I,O]]
```

```
u = [O,I,I]
v = [I,O,I]
vect = [cPlus (prodExt b1 u) (prodExt b2 v) | b1 <- lesBits, b2 <-
    lesBits]
```

```
*Main> vect
[[O,O,O],[I,O,I],[O,I,I],[I,I,O]]
```

Définition 21 (Sev)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ un corps opérant sur le groupe $\langle V, \dagger \rangle$ pour former un espace vectoriel de produit externe $\bullet$.
Soit W un sous-ensemble de V.
Si, muni des mêmes opérations que V, W a une structure de $\mathbb{K}$-espace vectoriel, alors on dit que W est un **sous-espace vectoriel** de V.

Théorème 22 (Caractérisation (1) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ *un corps opérant sur le groupe* $\langle V, \dagger \rangle$ *pour former un espace vectoriel de produit externe* $\bullet$.
Soit W *un sous-ensemble de* V.
W *est un sous-espace vectoriel (sev) de* V *si, et seulement si :*

- $W \neq \emptyset$
- $(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \boldsymbol{u}, \boldsymbol{v} \rangle \in W^2 \rightarrow \boldsymbol{u} \dagger \boldsymbol{v} \in W)$
- $(\forall \lambda)(\forall \boldsymbol{u})(\langle \lambda, \boldsymbol{u} \rangle \in \mathbb{K} \otimes W \rightarrow \lambda \bullet \boldsymbol{u} \in W)$

Théorème 22 (Caractérisation (1) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ un corps opérant sur le groupe $\langle V, \dagger \rangle$ pour former un espace vectoriel de produit externe $\bullet$.
Soit W un sous-ensemble de V.
W est un sous-espace vectoriel (sev) de V si, et seulement si :

- $W \neq \emptyset$
- $(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \boldsymbol{u}, \boldsymbol{v} \rangle \in W^2 \rightarrow \boldsymbol{u} \dagger \boldsymbol{v} \in W)$
- $(\forall \lambda)(\forall \boldsymbol{u})(\langle \lambda, \boldsymbol{u} \rangle \in \mathbb{K} \otimes W \rightarrow \lambda \bullet \boldsymbol{u} \in W)$

Théorème 22 (Caractérisation (1) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ *un corps opérant sur le groupe* $\langle V, \dagger \rangle$ *pour former un espace vectoriel de produit externe* $\bullet$.
Soit W *un sous-ensemble de* V.
W *est un sous-espace vectoriel (sev) de* V *si, et seulement si :*

- $W \neq \emptyset$
- $(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \boldsymbol{u}, \boldsymbol{v} \rangle \in W^2 \rightarrow \boldsymbol{u} \dagger \boldsymbol{v} \in W)$
- $(\forall \lambda)(\forall \boldsymbol{u})(\langle \lambda, \boldsymbol{u} \rangle \in \mathbb{K} \otimes W \rightarrow \lambda \bullet \boldsymbol{u} \in W)$

Théorème 22 (Caractérisation (1) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ *un corps opérant sur le groupe* $\langle V, \dagger \rangle$ *pour former un espace vectoriel de produit externe* $\bullet$*.*
Soit W *un sous-ensemble de* V*.*
W *est un sous-espace vectoriel (sev) de* V *si, et seulement si :*

- $W \neq \emptyset$
- $(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \boldsymbol{u}, \boldsymbol{v} \rangle \in W^2 \to \boldsymbol{u} \dagger \boldsymbol{v} \in W)$
- $(\forall \lambda)(\forall \boldsymbol{u})(\langle \lambda, \boldsymbol{u} \rangle \in \mathbb{K} \otimes W \to \lambda \bullet \boldsymbol{u} \in W)$

Théorème 23 (Caractérisation (2) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ *un corps opérant sur le groupe* $\langle V, \dagger \rangle$ *pour former un espace vectoriel de produit externe* $\bullet$.
Soit W *un sous-ensemble de* V.
W *est un sous-espace vectoriel (sev) de* V *si, et seulement si :*

- $\mathbf{0} \in W$
- $(\forall \lambda)(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \lambda, \boldsymbol{u}, \boldsymbol{v} \rangle \in \mathbb{K} \otimes W \otimes W \rightarrow \boldsymbol{u} \dagger \lambda \bullet \boldsymbol{v} \in W)$

Théorème 23 (Caractérisation (2) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ *un corps opérant sur le groupe* $\langle V, \dagger \rangle$ *pour former un espace vectoriel de produit externe* $\bullet$.
Soit W *un sous-ensemble de* V.
W *est un sous-espace vectoriel (sev) de* V *si, et seulement si :*

- $\mathbf{0} \in W$
- $(\forall \lambda)(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \lambda, \boldsymbol{u}, \boldsymbol{v} \rangle \in \mathbb{K} \otimes W \otimes W \to \boldsymbol{u} \dagger \lambda \bullet \boldsymbol{v} \in W)$

Théorème 23 (Caractérisation (2) des sous-espaces vectoriels)

Soit $\langle \mathbb{K}, \oplus, \odot \rangle$ un corps opérant sur le groupe $\langle V, \dagger \rangle$ pour former un espace vectoriel de produit externe $\bullet$.
Soit W un sous-ensemble de V.
W est un sous-espace vectoriel (sev) de V si, et seulement si :

- $\mathbf{0} \in W$
- $(\forall \lambda)(\forall \boldsymbol{u})(\forall \boldsymbol{v})(\langle \lambda, \boldsymbol{u}, \boldsymbol{v} \rangle \in \mathbb{K} \otimes W \otimes W \rightarrow \boldsymbol{u} \dagger \lambda \bullet \boldsymbol{v} \in W)$