Tutorat mathématique : TD1

Université François Rabelais

Département informatique de Blois

Algèbre

*
* *

Problème 1

On définit sur l'ensemble $\mathbb{N}$ la loi de composition $\star$ telle que :

$$\forall (a,b) \in \mathbb{N}^2, a \star b = a + b - ab$$

1. Est-ce que la loi $\star$ est une loi de composition interne ?

   - Commutativité : $\forall a, b \in E, (a \star b) = (b \star a)$

     C'est évident ici par symétrie de la loi $\star$.
   - Associativité : $\forall a, b, c \in E, (a \star b) \star c = a \star (b \star c)$

     $(a \star b) \star c = (a + b - ab) \star c = a + b - ab + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc$

     $a \star (b \star c) = a \star (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = a + b + c - ab - ac - bc + abc$

     La loi $\star$ est associative.
   - Unifère : $\exists! e \in E, \forall x \in E | x \star e = e \star x = x$

     $0 \star a = 0 + a - 0 \times a = a$

     La loi $\star$ possède l'élément neutre.

   La loi $\star$ est bien une loi de composition interne.

2. Est-ce que $(\mathbb{R}, \star)$ est-un groupe abélien ? Si non, quelle(s) propriété(s) lui manque(nt) t-il ?

   $$(E, \star) \text{ est un groupe} \Leftrightarrow \begin{cases} E \text{ est stable pour } \star \\ \star \text{ est associative} \\ (E, \star) \text{ possède l'élément neutre} \\ \text{Tout élément de } E \text{ possède un symétrique} \end{cases}$$

   Si $\star$ est commutative $(E, \star)$ est un groupe *abélien*.

   - Éléments symétrisables : $\forall x \in E, \exists! x^{-1} \in E | x \star x^{-1} = x^{-1} \star x = e$

     $a \star a^{-1} = a + a^{-1} - aa^{-1} \Leftrightarrow 0 = a + a^{-1} - aa^{-1}$

     $\Leftrightarrow -a = a^{-1}(1 - a)$

     $\Leftrightarrow a^{-1} = -\frac{a}{(1-a)}$

     $(\mathbb{R}, \star)$ n'est pas un groupe car 1 n'a pas de symétrique : $1 \star a = 1 - a - a = 1$.

Cependant $(\mathbb{R}\backslash\{1\}, \star)$ est bien un groupe abélien.

En fait 1 joue le même rôle pour $(\mathbb{R}, \star)$ que 0 pour $(\mathbb{R}, \times)$. Il est l'élément absorbant de $(\mathbb{R}, \star)$.

- Absorbance : $\exists! \aleph \in E, \forall x \in E | x \star \aleph = \aleph \star x = \aleph$

3. Calculer $\underbrace{a \star a \star ... \star a}_{n \text{ fois}} = a^{\star n}$.

Il semblerait que $1 - x^{\star n} = (1-x)^n$.

Démontrons que la propriété $P(n) : \forall n \in \mathbb{N}, 1 - x^{\star n} = (1-x)^n$ est vraie.

- Initialisation (pour $n = 0$)

  $0 \star 0 = x^{\star 0} = 0$

  $1 - x^{\star 0} = (1-x)^0$

  Donc $P(0)$ est vraie.

- Hérédité

  On suppose qu'il existe un entier n tel que $P(n)$ est vraie.

  On veut montrer que la propriété est vraie au rang $n+1$, c'est à dire, montrer que :

  $$1 - x^{\star(n+1)} = (1-x)^{n+1}$$

  On utilise l'hypothèse de récurrence :

  $$\begin{aligned} 1 - \underbrace{x \star x \star .. \star x}_{n+1 \text{ fois}} &= 1 - x \star x^{\star n} \\ &= 1 - x \star (1 - (1-x)^n) \\ &= 1 - (x + 1 - (1-x)^n - x(1 - (1-x)^n)) \\ &= -x + x + (1-x)^n (1-x)) \\ &= (1-x)^{n+1} \end{aligned}$$

  $P(n+1)$ est vraie.

- Conclusion

  La propriété est initialisée à 0 et héréditaire. Dès lors, d'après le principe de récurrence $P(n) : \forall n \in \mathbb{N}, 1 - x^{\star n} = (1-x)^n$ est vraie.

Problème 2

Soit la loi de composition interne $\star$ définie sur $E = \{a, b, c, d\}$ telle que :

$\star$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	b	c	d	d
d	a	c	b	d

1. La loi $\star$ est-elle commutative ? Associative ? Pour quels éléments l'écriture $x \star x \star x$ a t-elle

un sens ?

La loi $\star$ n'est pas commutative. On donne un contre-exemple : $(a \star c) = d \neq b = (c \star a)$.

La loi $\star$ n'est pas associative. On exhibe un contre-exemple :

$(a \star a) \star c = c \star c = d$

$a \star (a \star c) = a \star d = b$

Donc $a \star (a \star c) \neq (a \star a) \star c$.

On a 4 éléments, soit 8 cas à tester. C'est fini raisonnable, on peut calculer tous les cas.

- Pour a :
  $(a \star a) \star a = c \star a = b$
  $a \star (a \star a) = a \star c = d$
- Pour b :
  $(b \star b) \star b = b \star b = b$
  $b \star (b \star b) = b \star b = b$
- Pour c :
  $(c \star c) \star c = d \star c = b$
  $c \star (c \star c) = c \star d = d$
- Pour d :
  $(d \star d) \star d = d \star d = d$
  $d \star (d \star d) = d \star d = d$

L'écriture $x \star x \star x$ n'a de sens que pour b et d.

2. $(E, \star)$ possède-t-elle l'élément neutre ? Un élément neutre à gauche ? Un élément neutre à droite ?

$(E, \star)$ ne possède pas l'élément neutre, ni aucun élément neutre à droite. Mais b est neutre à gauche.

3. L'ensemble $A = \{a, b, c\}$ est-il stable ?

A n'est pas stable car $c \star c = d \notin A$. Mais le sous ensemble $B = \{b, c, d\}$ est stable.

Problème 3

Soit un ensemble Ω tel que $\text{card}(\Omega) = n$.
Combien de lois de composition interne différentes peut-on créer sur Ω ? Parmi toutes ces lois, combien sont commutatives ? Combien possèdent l'élément neutre ?

1. Combien de lois de composition interne différentes peut-on créer sur E ?

On a n^2 cases pour chaque table représentant une loi de composition interne sur E.

Pour chaque case on a n choix d'éléments. Dès lors, on a au total n^{n^2} lois de composition interne différentes sur E.

2. Parmi toutes ces lois de composition interne différentes, combien sont commutatives ?

On sait qu'une loi de composition interne est commutative si et seulement si sa table de Cayley est symétrique. Dès lors on doit fixer sa diagonale supérieure (ou inférieure). Il nous reste alors $\frac{n(n+1)}{2}$ cases où les valeurs sont à choisir.

Dès lors, on a au total $n^{\frac{n(n+1)}{2}}$ lois de composition interne différentes sur E.

3. Parmi toutes ces lois de composition interne différentes, combien ont un élément neutre ?

La présence de l'élément neutre suppose de fixer la colonne est la ligne de l'élément correspondant. On a donc $n^2 - 2n - 1 = (n-1)^2$ cases où les valeurs sont à choisir. De plus, on a n choix pour l'élément neutre.

Dès lors, on a au total $n \times n^{(n-1)^2} = n^{n^2-2n+2}$ lois de composition interne différentes sur E.

Problème 4

Soit une loi $\star$ associative sur un ensemble E. Un élément $x \in E$ est dit *idempotent* si et seulement si $x \star x = x$.

1. Montrer que si x et y sont idempotents et commutent, alors $x \star y$ est idempotent.

Comme la loi est commutative, associative et que x et y sont idempotents et commutent, on a :

$$\begin{aligned}(x \star y) \star (x \star y) &= (y \star x) \star (x \star y) \\ &= y \star (x \star x) \star y \\ &= y \star x \star y \\ &= x \star (y \star y) \\ &= x \star y\end{aligned}$$

2. Montrer que si x est idempotent et inversible, alors x^{-1} est idempotent.

$$\begin{aligned}x \star x = x &\Leftrightarrow (x \star x)^{-1} = x^{-1} \\ &\Leftrightarrow x^{-1} \star x^{-1} = x^{-1}\end{aligned}$$

Problème 5

On définit le groupe des n-entiers relatifs comme suit :

$$\forall n \in \mathbb{N}, n\mathbb{Z} = \{n \times k | k \in \mathbb{Z}\}$$

1. Déterminer $0\mathbb{Z}$ et $1\mathbb{Z}$.

$0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$

2. Montrer que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$

Soit $n \in \mathbb{N}$.

- $0 = n \times 0$ donc $0 \in n\mathbb{Z}$

- $\forall (k_1, k_2) \in \mathbb{Z}^2, nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}$
- $\forall k \in \mathbb{Z}, n(-k) \in n\mathbb{Z}$

3. Montrer que $A = 3\mathbb{Z} \cup 4\mathbb{Z}$ n'est pas stable pour l'addition.

3 et 4 appartiennent à A seulement $3+4 = 7$ n'appartient pas à A. $(3, 4) \in A^2$ et $3+4 = 7 \notin A$. Dès lors A n'est pas stable pour $+$.

4. Montrer que l'application f telle que $f : \begin{cases} \mathbb{Z} & \to \mathbb{Z} \\ k & \mapsto 6k \end{cases}$ est un endomorphisme de $(\mathbb{Z}, +)$.

$\forall (k_1, k_2) \in \mathbb{Z}^2, f(k_1 + k_2) = 6(k_1 + k_2) = 6k_1 + 6k_2 = f(k_1) + f(k_2)$

Donc f est bien un endomorphisme de $(\mathbb{Z}, +)$

5. Déterminer $\ker(f)$ et $\mathrm{Im}(f)$. Qu'en déduisez-vous ?

$\ker(f) = \{k \in \mathbb{Z} | f(k) = 0\}$

Or $f(k) = 0 \Leftrightarrow 6k = 0$

$\Leftrightarrow k = 0$

$\ker(f) = \{0\}$ Donc f est injective.

$\mathrm{Im}(f) = \{f(k) | k \in \mathbb{Z}\}$

$= \{6k | k \in \mathbb{Z}\}$

$= 6\mathbb{Z}$

$\mathrm{Im}(f) = 6\mathbb{Z} \neq \mathbb{Z}$. Donc f n'est pas surjective.

Problème 6

On se place ici dans l'algèbre $\mathcal{L}$ de la logique propositionnelle.
On considère qu'un système [d'opérateurs] S est *complet* quand toute formule $\varphi \in \mathcal{L}$ peut-être représentée à l'aide de S. On considère que $S = \{\neg, \vee, \wedge\}$ est un système complet.

1. Combien d'opérateurs d'arité 2 peut-on définir au total ?

Les opérateurs d'arité 2 de la logique sont définis sur l'ensemble $\{0, 1\}$ dès lors, on a $2^{2^2} = 16$ opérateurs.

2. Trouver un système à 8 opérateurs d'arité 2 qui n'est pas complet.

Il nous suffit de fixer un élément de la table de Cayley des opérateurs définissables. Soient tous les opérateurs $\diamondsuit$ que l'on peut définir, alors, si l'on fixe $\diamondsuit(1, 1) = 1$, on peut bien définir $2^3 = 8$ opérateurs différents. Cependant, on montre facilement par récurrence que si I est l'interprétation telle que pour toute variable logique p on ait $I(p) = 1$ et φ, une formule résultante, alors, on peut montrer que $I(\varphi) = 1$. En particulier, l'opérateur de négation $\neg$ ne peut pas être définie.

3. On considère les deux opérateurs $\uparrow$ et $\downarrow$ respectivement *Nand* et *Nor* dont on donne la table de vérité suivante :

p	q	$p \uparrow q$	$p \downarrow q$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

(a) Ces opérateurs sont-ils associatifs ? Commutatifs ? Montrer que $\{\uparrow\}$ et $\{\downarrow\}$ sont des systèmes complets ?

Les deux opérateurs sont commutatifs et associatifs.

Pour montrer que ces systèmes sont complets, on les ramène à S. Soient p et q des variables logiques telles que $p, q \in \{0, 1\}$.

De plus, on remarque que $p \uparrow q = \neg(p \wedge q)$ et $p \downarrow q = \neg(p \vee q)$

- Pour $\{\uparrow\}$.
  - $\neg p = \neg(p \wedge p)$
    $= p \uparrow p$
  - $p \wedge q = \neg\neg(p \wedge q)$
    $= \neg\,(p \uparrow q)$
    $= (p \uparrow q) \uparrow (p \uparrow q)$
  - $p \vee q = \neg(\neg p \wedge \neg q)$
    $= \neg p \uparrow \neg q$
    $= (p \uparrow p) \uparrow (q \uparrow q)$
- Pour $\{\downarrow\}$.
  On utilise la même méthodologie.

(b) Montrer que les seuls opérateurs qui forment à eux seuls un système complets sont $\uparrow$ et $\downarrow$.

On suppose qu'il existe un autre opérateur $\updownarrow$ dont la table de vérité est :

p	q	$p \updownarrow q$
0	0	?
0	1	?
1	0	?
1	1	?

Si la valeur de la dernière ligne est 1 alors toute formule construite en utilisant le seul connecteur $\updownarrow$ doit prendre la valeur 1 si les variables propositionnelles composant cette formule prennent la valeur 1. Donc, aucune combinaison ne peut exprimer la négation d'un énoncé φ. La valeur de cette dernière ligne du tableau doit être 0. De la même façon la valeur de la première ligne doit être 1. Alors nous avons :

p	q	$p \updownarrow q$
0	0	1
0	1	?
1	0	?
1	1	0

Plusieurs cas sont alors possibles. Si les valeurs de la 2ème et 3ème ligne sont 0, alors l'opérateur $\updownarrow$ est identique à $\uparrow$. De même, s'il elles sont égales à 1, alors celui-ci est pareil à $\downarrow$.

Reste deux possibilités :

- Si la 2ème ligne est à 1 et la 3ème à 0.
  Dans ce cas $p \updownarrow q = \neg p$.
- Si la 2ème ligne est à 0 et la 3ème à 1.
  Dans ce cas $p \updownarrow q = \neg q$.

Dans les deux cas, on sait que le connecteur $\neg$ ne forme pas à lui seul un système complet, il ne peut exprimer que la négation et l'identité.

L'hypothèse de départ est absurde. Il n'existe pas d'autres opérateur binaire formant un système complet.

Problème 7

1. Soit l'application φ telle que $\varphi : \begin{cases} \mathbb{C}^* & \to \mathbb{R}^* \\ z & \mapsto |z| \end{cases}$

   (a) Montrer que φ définie un morphisme de groupes de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}^*, \times)$.

   Soit $z, z' \in \mathbb{C}$, alors
   $\varphi(zz') = |zz'|$
   $= |z||z'|$
   $= \varphi(z) \times \varphi(z')$
   On a effectivement un morphisme de groupes de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}^*, \times)$.

   (b) Calculer $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$. En donner une interprétation géométrique.

   On note $z = x + iy$ tel que $(x, y) \in \mathbb{R}^2$.

   - $\ker(\varphi) = \{z \in \mathbb{C}^* | \varphi(z) = 1\}$
     $\varphi(z) = 1 \Leftrightarrow |z| = 1$
     $\Leftrightarrow |z|^2 = 1$
     $\Leftrightarrow x^2 + y^2 = 1$
     On a donc $\ker(\varphi)$ qui représente le cercle de rayon 1 soit le cercle trigonométrique.
   - $\mathrm{Im}(\varphi) = \{\varphi(\mathbb{C}^*)\}$
     $= \mathbb{R}_+^*$
     Le module représente une distance. Celle de l'origine au point z.

2. Soit l'application ψ telle que $\psi : \begin{cases} \mathbb{R} & \to \mathbb{U} \\ \theta & \mapsto e^{i\theta} \end{cases}$. On rappelle que $\mathbb{U} = \{z \in \mathbb{C}^* | |z| = 1\}$

(a) Montrer que ψ définie un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{U}, \times)$.

Soit $\theta, \theta' \in \mathbb{R}$, alors

$$\begin{aligned}\psi(\theta + \theta') &= e^{i(\theta+\theta')} \\ &= e^{i\theta+i\theta'} \\ &= e^{i\theta} \times e^{i\theta'} \\ &= \psi(\theta) \times \psi(\theta')\end{aligned}$$

On a effectivement un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{U}, \times)$.

(b) ψ est-elle injective ? Surjective ? Bijective ?

On utilise les propriétés du noyau et de l'image.

- ψ est injective $\Leftrightarrow \ker(\psi) = \{0\}$. Le noyau est réduite à l'élément neutre de $(\mathbb{R}, +)$. D'après la définition du noyau, on a :
  $$\begin{aligned}\psi(\theta) = 1 &\Leftrightarrow e^{i\theta} = 1 \\ &\Leftrightarrow \theta = 0[2\pi] \\ &\Leftrightarrow \theta \in 2\pi\mathbb{Z}\end{aligned}$$
  $\ker(\psi) \neq \{0\}$. Ainsi ψ n'est pas injective. On remarque cependant que si l'on fait la restriction sur $[0, 2\pi[$. Alors, ψ est bien injective.

- ψ est surjective $\Leftrightarrow \mathrm{Im}(\psi) = \mathbb{U}$. L'image coïncide avec l'ensemble d'arrivée.
  $\forall \theta \in \mathbb{R}, e^{i\theta} = \cos(\theta) + i\sin(\theta)$
  Ainsi $\left|e^{i\theta}\right| = \sqrt{\cos^2(\theta) + \sin^2(\theta)} = 1$.
  Donc ψ est surjective. Elle n'est pas bijective car elle n'est pas injective.