Tutorat mathématiques : TD2

Université François Rabelais

`Département informatique de Blois`

Algèbre

*
* *

Problème 1

On dit qu'un anneau A est un *anneau de Boole* si :

$$\forall x \in A, x^2 = x$$

1. Démontrer que pour tout $x \in A, x = -x$.

   Par définition $(x+1)^2 = x+1 \Leftrightarrow x^2 + 1 + 2x = x + 1$
   $\Leftrightarrow x = -x$

2. Montrer que A est commutatif.

   Soit $(x, y) \in A^2$, alors : $(x+y)^2 = (x+y) \Leftrightarrow x^2 + y^2 + xy + yx = x + y$
   $\Leftrightarrow xy = -yx$
   $\Leftrightarrow xy = yx$

3. On note $\mathbb{B} = \mathbb{Z}/2\mathbb{Z}$.

   (a) Dresser la table de Cayley de $\mathbb{B}$ pour $+$ et $\times$ et montrer que $(\mathbb{B}, +, \times)$ est un anneau de Boole. Est-ce un corps ?

   Soient les tables de Cayley suivantes :

$+$	0	1
0	0	1
1	1	0

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

   On a bien $x^2 = x$ et $x = -x$. On peut affirmer que $\mathbb{B}$ est un anneau de Boole. De plus $\mathbb{B}$ ne possède pas de diviseur de 0. C'est un corps (aussi parce que 2 est un nombre premier).

   (b) Soient les opérations "ou exclusif" notée $\oplus$ et "conjonction" notée $\wedge$ du calcul propositionnel. Montrer que $(\mathbb{B}, \oplus, \wedge)$ est un corps.

On remarque que la table de vérité du $\oplus$ est identique à celle de $+$ sur $\mathbb{B}$. De même pour $\wedge$ par rapport à $\times$. En considérant la fonction d'interprétation $I : \mathcal{L} \to \{0, 1\}$, on en déduit par récurrence que $I(P \oplus Q) = I(P) + I(Q)$ et que $I(P \wedge Q) = I(P) \times I(Q)$ pour toutes formules P et Q.
On déduit aussi, par exemple, que $\oplus$ est associatif.

$$I((P \oplus Q) \oplus R) = (I(P) + I(Q)) + I(R) = I(P) + (I(Q) + I(R)) = I(P \oplus (Q \oplus R))$$

On montre les autres axiomes de la même manière, du fait que $(\mathbb{B}, +, \times)$ est un anneau de Boole (et même algèbre de Boole). Ainsi, comme on a montré que $(\mathbb{B}, +, \times)$ est un corps, on en déduit que $(\mathbb{B}, \oplus, \wedge)$ est aussi un corps.

Problème 2

On appelle *caractéristique* d'un anneau fini le plus petit entier n tel que :

$$n \times 1_A = 0_A$$

où 1_A est l'élément neutre de la multiplication sur A et 0_A l'élément neutre pour l'addition sur A.

1. Montrer que pour tout $x \in A, nx = 0_A$.

   On a $nx = n(1_A \times x)$
   $= (n \times 1_A) \times x$
   $= 0_A \times x$
   $= 0_A$

2. Montrer que si A est intègre, alors n est un nombre premier.

   On raisonne par contraposée. On souhaite montrer que

   $$\text{Si } A \text{ est intègre} \Rightarrow n \text{ est premier}$$

   On va démontrer que

   $$\text{Si } n \text{ n'est pas premier} \Rightarrow A \text{ n'est pas intègre}$$

   On suppose que $n = p \times q$ avec $1 < p < q < n$. Posons que $x = p \times 1_A$ et $y = q \times 1_A$.
   On sait que x et y sont différents de 0_A puisque que $p < q < n$. Pourtant :
   $x \times y = p \times 1_A \times q \times 1_A$
   $= (p \times q)1_A$
   $= n \times 1_A$
   $= 0_A$

Ainsi, si n n'est pas premier, alors A n'est pas intègre. Par contraposée, on retrouve l'énoncé initial qu'il fallait démontrer.

Problème 3

Soit $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

1. On rappelle que $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ est un anneau. Que peut-on en déduire pour $(\mathbb{Z}/5\mathbb{Z}, +)$?

   On en déduit que $(\mathbb{Z}/5\mathbb{Z}, +)$ est un groupe abélien.

2. Définir $\overline{2}$.

   $\overline{2} = \{2 + 5k | k \in \mathbb{Z}\}$.

3. Dresser la table de Cayley de $(\mathbb{Z}/5\mathbb{Z}, \times)$.

   On a la table de Cayley suivante :

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

4. En justifiant, préciser si $(\mathbb{Z}/5\mathbb{Z}, \times)$ est :

   (a) Un anneau commutatif.

   La table de Cayley ci-dessus est symétrique. Donc $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ est bien un anneau commutatif.

   (b) Un anneau intègre.

   D'après la table de Cayley de $\times$ ci-dessus, Si $a \neq \overline{0}$ et $b \neq \overline{0}$ alors $a \times b \neq \overline{0}$. On n'a aucun diviseur de $\overline{0}$, donc la $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ est bien un anneau intègre.

   (c) Un corps.

   $\overline{1}^{-1} = \overline{1} \quad \overline{2}^{-1} = \overline{3} \quad \overline{3}^{-1} = \overline{2} \quad \overline{4}^{-1} = \overline{1}$

   Ainsi, $\forall a \in \mathbb{Z}/5\mathbb{Z} | a \neq \overline{0}$ est inversible, donc $\mathbb{Z}/5\mathbb{Z}$ est un corps.

   Plus simplement, on sait que tout anneau intègre est un corps.

5. En détaillant les calculs. Développer puis simplifier $(x - \overline{2018})^3$ pour tout $x \in \mathbb{Z}/5\mathbb{Z}$.

   On a $2018 = 3[5]$, donc et $-\overline{3} = \overline{2}$

   Donc $\forall x \in \mathbb{Z}/5\mathbb{Z}, (x - \overline{2018})^3 = (x + \overline{2})^3$.

   Puisque $\mathbb{Z}/5\mathbb{Z}$ est un anneau commutatif, on peut utiliser la formule du binôme de Newton.

Il vient que :

$(x+\overline{2})^3 = x^3 + x^2 + \overline{2}x + \overline{3}$

Problème 4

Soit $\mathbb{F}$, un corps fini commutatif. Calculer le produit de tous les éléments de $\mathbb{F}^*$.

$$\prod_{x \in \mathbb{F}^*} x$$

On sait que dans un corps, tout élément non nul possède un inverse. De plus, comme $\mathbb{F}$ est commutatif, on peut regrouper chaque élément avec son inverse $xx^{-1} = 1$.
Ainsi, il reste uniquement les éléments tels que $x = x^{-1}$. Soit

$$\prod_{x \in \mathbb{F}^*} x = \prod_{x = x^{-1}} x$$

De plus $x = x^{-1} \Leftrightarrow x^2 = 1$. Il vient que

$$\prod_{x \in \mathbb{F}^*} x = \prod_{x^2 = 1} x$$

Or, dans un corps, l'équation $x^2 = 1$ a pour solution que 1 et -1 (opposé de 1). Et donc $1 \times -1 = -1$.

$$\prod_{x \in \mathbb{F}^*} x = -1$$

Problème 5

Résoudre les équations suivantes :

1. $x^2 + x + \overline{7} = \overline{0}$ pour $x \in \mathbb{Z}/13\mathbb{Z}$.

   $x^2 + x + \overline{7} = \overline{0}$. On remarque que $\overline{14} = \overline{1}$.

   $$\begin{aligned} x^2 + \overline{14}x + \overline{7} = \overline{0} &\Leftrightarrow (x+\overline{7})^2 - \overline{42} = \overline{0} \\ &\Leftrightarrow (x+\overline{7})^2 - \overline{3} = \overline{0} \\ &\Leftrightarrow (x+\overline{7})^2 - \overline{4}^2 = \overline{0} \end{aligned}$$

   On sait comme 13 est premier que $\mathbb{Z}/13\mathbb{Z}$ est un anneau intègre sans diviseur de zéro. On peut factoriser.

   $$\begin{aligned} &\Leftrightarrow (x+\overline{7}+\overline{4})(x+\overline{7}-\overline{4}) = \overline{0} \\ &\Leftrightarrow (x+\overline{11})(x+\overline{3}) = \overline{0} \end{aligned}$$

   Ainsi, on a les solutions $\mathscr{S} = \{\overline{2}, \overline{10}\}$.

2. $x^2 - \overline{4}x + \overline{3} = \overline{0}$ pour $x \in \mathbb{Z}/12\mathbb{Z}$.

   On va chercher à mettre le polynôme sous forme canonique. En particulier, la méthode de résolution classique ne fonctionne par ici.

   $x^2 - \overline{4}x + \overline{3} = \overline{0} \Leftrightarrow (x-\overline{2})^2 - \overline{1} = \overline{0}$

Cependant $\mathbb{Z}/12\mathbb{Z}$ n'est pas un anneau intègre car 12 n'est pas premier et il existe alors des diviseurs de zéro. Il vaut donc mieux chercher à résoudre $(x-\overline{2})^2 = \overline{1}$, soit $t^2 = \overline{1}$.

On a alors $(x-\overline{2}) \in \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Il vient alors que l'ensemble des solutions est $\mathscr{S} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$

Problème 6

Soit $(A, +, \times)$ un anneau intègre.
Démontrer les propriétés (i) et (ii).

$$\forall a \in A^*, \forall (x,y) \in A^2, \begin{cases} ax = ay \Rightarrow x = y & (i) \\ xa = ya \Rightarrow x = y & (ii) \end{cases}$$

Autrement dit, tout élément non nul d'un anneau intègre est simplifiable à gauche (i) et à droite (ii) pour la multiplication.

Soient $a \in A^*$ et $(x,y) \in A^2$.
$ax = ay \Leftrightarrow ax - ay = 0_A$
$\Leftrightarrow a(x-y) = 0_A$
Puisque A est intègre et $a \neq 0_A$, alors nécessairement $x - y = 0_A$ et donc $x = y$.
La proposition (ii) se montre de manière similaire.