MA2C03 - DISCRETE MATHEMATICS - TUTORIAL NOTES

Brian Tyrrell

14 & 15/11/2016

1 Cayley tables

This week the majority of our time was spent answering questions regarding the assignment. However we did have the time to go through the proof that $(\mathbb{Z}_3, \oplus_3, 0)$ is an abelian group.

To prove $(\mathbb{Z}_3, \oplus_3, 0)$ is an abelian group we need to show five properties;

(1) **Closure** of $\oplus_3$.

(2) **Associativity** of $\oplus_3$.

(3) Existence of an **identity** element.

(4) Every element has an **inverse**.

(5) **Commutativity** of $\oplus_3$.

Proof.

(1) Choose $x, y \in \mathbb{Z}_3$. By definition of $\oplus_3$,

$$x \oplus_3 y = (x + y) \text{mod } 3$$

Thus $x \oplus_3 y \in \mathbb{Z}_3$ by definition.

(2) Associativity of $\oplus_3$ follows from the associativity of $+$ on $\mathbb{Z}$.

(3) The element 0 is the identity; we need to show

$$\forall x \in \mathbb{Z} \qquad x \oplus_3 0 = 0 \oplus_3 x = x$$

This follows as for all $x \in \mathbb{Z}_3$,

$$x \oplus_3 0 = (x + 0)\text{mod } 3 = x \text{ mod } 3 = x = (0 + x)\text{mod } 3 = 0 \oplus_3 x$$

(4) We show the existence of inverses by constructing a *cayley table* (a table showing $\oplus_3$ acting on every pair of elements);

$\oplus_3$	0	1	2
0	**0**	1	2
1	1	2	**0**
2	2	**0**	1

We highlight the identity element (0 in this case) and we immediately can deduce the inverse of elements;

- $0 \oplus_3 0 = 0 \Rightarrow 0^{-1} = 0$
- $1 \oplus_3 2 = 0 \Rightarrow 2^{-1} = 1$
- $2 \oplus_3 1 = 0 \Rightarrow 1^{-1} = 2$

Thus every element in the structure has an inverse.

(5) Finally

$$\forall x, y \in \mathbb{Z}_3,\ x \oplus_3 y = (x+y) \text{mod } 3 = (y+x) \text{mod } 3 = y \oplus_3 x$$

using the commutativity of $+$ in $\mathbb{Z}$. Thus $\oplus_3$ is commutative.

We conclude $(\mathbb{Z}_3, \oplus_3, 0)$ is an abelian group, as required. ■

Remark. (4) is a useful way to prove if elements have inverses, and find them if they do.