Mathematics for Machine Learning - Questions and Solutions

Edwin Fennell

Note - I'm not going to write out the questions here since they are very, very inefficiently posed and no way am I going to TeX all of that.

2.1 a. In order to show that this constitutes a group, we need to show four things:

- Closure - if $a, b \in \mathbb{R}$ then clearly $ab + a + b \in \mathbb{R}$. Now, suppose that $ab + a + b = -1$. This rearranges to

  $$a(b+1) = -(b+1)$$

  or

  $$(a+1)(b+1) = 0$$

  Therefore if neither a nor b is equal to -1, $a * b$ also cannot be equal to -1, and therefore * is a valid group operation on $\mathbb{R}\backslash\{-1\}$.

- Identity - our identity is 0 since for any $a \in \mathbb{R}\backslash\{-1\}$ we have

  $$a * 0 = a \cdot 0 + 0 + a = a$$

- Inverse - given a fixed $a \in \mathbb{R}\backslash\{-1\}$ we want to solve for x in the following:

  $$a * x = ax + x + a = 0$$

  we rearrange to get

  $$x = \frac{-a}{a+1}$$

  Therefore all elements in $\mathbb{R}\backslash\{-1\}$ have inverses under *

- Associativity - we consider the respective values of $(a * b) * c$ and $a * (b * c)$ for arbitrary $a, b, c \in \mathbb{R}\backslash\{-1\}$:

  $$(a * b) * c = (a * b)c + a * b + c = abc + ac + bc + ab + a + b + c$$

  $$(a * (b * c) = a(b * c) + b * c + a = abc + ac + bc + ab + a + b + c$$

  and so we have associativity.

Now we need to show that the resulting group is Abelian, but this is clear from the definition of * being completely symmetric in its two operands.

$\square$

b. Conveniently, from our proof of associativity we know immediately that

$$3 * x * x = 3x^2 + 3x + 3x + x^2 + x + x + 3 = 4x^2 + 8x + 3$$

Therefore we need to solve $4x^2 + 8x + 3 = 15$, or rather

$$4x^2 + 8x - 12 = 4(x^2 + 2x - 3) = 4(x + 3)(x - 1) + 0$$

From this we see that the solutions are exactly $x = 1, x = -3$

2.2 a. We need to show the four group axioms:

- Closure - By definiton of $\oplus$ the result of its application is a congruence class mod n. (Well-posedness is another matter but that isn't asked for here).
- Identity - the identity is $\bar{0}$ since
$$\forall a \in \mathbb{Z}, \bar{a} \oplus \bar{0} = \overline{(a + 0)} = \bar{a}$$
- Inverses - the inverse of $\bar{a}$ for any $a \in \mathbb{Z}$ is $\overline{-a}$:
$$\forall a \in \mathbb{Z}, \bar{a} \oplus \overline{-a} = \overline{(a - a)} = \bar{0}$$
- Associativity - we have
$$\forall a, b, c \in \mathbb{Z}, (\bar{a} \oplus \bar{b}) \oplus \bar{c} = \overline{(a + b)} \oplus \bar{c} = \overline{a + b + c}$$
and also
$$\forall a, b, c \in \mathbb{Z}, \bar{a} \oplus (\bar{b} \oplus \bar{c}) = \bar{a} \oplus \overline{(b + c)} = \overline{a + b + c}$$
and so we have associativity. Assuming that the operator $\oplus$ is well-defined, this more or less comes down to "addition is associative".

Therefore $(\mathbb{Z}_n, \oplus)$ is indeed a group.

b. I'm not going to write out the multiplication table for $\mathbb{Z}_5 \backslash \{\bar{0}\}$. I will show that this is a group when I prove the general case in part d of this question. Assuming that it is a group, it is clearly Abelian from the symmetric nature of $\otimes$.

c. Again, I'll use the result from part d. 8 is composite so this is not a group.

d. Suppose that n is composite. Then $\exists$ a,b s.t. $1 < a, b < n$ and $a \cdot b = n$. Therefore we have

$$\bar{a} \otimes \bar{b} = \bar{n} = \bar{0}$$

Therefore $\mathbb{Z}_n \backslash \{\bar{0}\}$ is not a group since it fails the requirement of closure.

Now, if n is instead prime, then $\mathbb{Z}_n \backslash \{\bar{0}\}$ is a group - we will show this by verifying the group axioms.

- Closure - suppose that $a, b \in \mathbb{Z}\backslash\{\overline{0}\}$. Now, suppose that

$$ab \equiv 0 \mod n$$

Then $ab = kn$ for some $k \in \mathbb{Z}$. Since n is prime, a and n are coprime, and therefore by Bezout's theorem, $\exists u, v \in \mathbb{Z}$ s.t.

$$ua + vn = 1$$

Therefore

$$b = b \cdot 1 = b(ua + vn) = ab \cdot u + bvn = (uk + bv)n$$

and so we find that b is a multiple of n. This is a contradiction since $b \in \mathbb{Z}\backslash\{\overline{0}\}$. Therefore $ab \not\equiv 0 \mod n$ and we have

$$\overline{a}, \overline{b} \neq \overline{0} \implies \overline{ab} \neq \overline{0}$$

and so we have closure

- Identity - the identity is trivially $\overline{1}$
- Inverse - for any $\overline{a} \neq \overline{0}$ we have that a and n are coprime. By Bezout's theorem we know that $\exists u, v \in \mathbb{Z}$ s.t.

$$ua + vn = 1$$

Therefore

$$\overline{a} \otimes \overline{u} = \overline{au} = \overline{(1 - vn)} = \overline{1}$$

and so we have constructed an inverse for $\overline{a}$

- Associativity - exactly the same proof as in part a. Essentially "multiplication is associative".

Therefore $(\mathbb{Z}_n, \otimes)$ is indeed a group.