INF 240 - Exercise problems - 1
Solutions

Nikolay Kaleyski

Exercise 1. *Suppose a group $(G, \cdot)$ has two identity elements e_1 and e_2. Since e_1 is an identity element, it must satisfy*

$$e_1 \cdot a = a$$

for any a from the group, including $a = e_2$; hence

$$e_1 \cdot e_2 = e_2.$$

On the other hand, since e_2 is an identity element, it must satisfy

$$a \cdot e_2 = a$$

for any a from the group, including $a = e_1$; hence

$$e_1 \cdot e_2 = e_1.$$

We thus have

$$e_1 \cdot e_2 = e_1 = e_2$$

and so e_1 and e_2 must actually be the same element.

Exercise 2. *Suppose both a and b are inverse to s in $(G, \cdot)$. Then we must have*

$$as = bs = sa = sb = e$$

where e is the identity element of G. Consider the equation

$$as = bs$$

and multiply both sides by a from the right to get

$$asa = bsa.$$

Since $sa = e$, the above becomes

$$ae = be,$$

i.e.

$$a = b$$

so that the two inverses are actually the same element.

Exercise 3. *Addition and multiplication modulo* 4 *are computed by simply evaluating the operation (addition or multiplication) as for ordinary integers, and then modulating, i.e. computing the remainder of division by* 4*. Note that modulation can be done at any point during the computation, and this can be used to simplify the computations.*

For example, $2+3 = 5 = 1 \mod 4$ *since* $5 = 1 \cdot 4 + 1$*. Similarly,* $3 \cdot 3 = 9 = 1 \mod 4$ *since* $9 = 2 \cdot 4 + 1$*.*

The addition table should then be

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 1: Addition table for $\mathbb{Z}_4$

and the multiplication table should be

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Table 2: Multiplication table for $\mathbb{Z}_4$

Exercise 4. *To show that* $(\mathbb{Z}_4, +_4)$ *is a group, we must show that the operation* $+$*, i.e. "addition modulo* 4*", satisfies the three axioms from the definition of a group:*

1. *it is associative;*
2. *it has a neutral element* e *such that* $a + e = e + a = a$ *for any* $a \in \mathbb{Z}_4$*;*
3. *every element* a *has an inverse* $i(a)$ *such that* $a + i(a) = i(a) + a = e$

The fact that addition modulo 4 is associative follows from the fact that it can be represented using ordinary addition of integers (without modulation), and that ordinary addition is associative, i.e. for any three integers $a, b, c \in \mathbb{Z}$*, we have*

$$a + (b + c) = (a + b) + c.$$

Since modulation can be applied at any point during the operation, we have

$$a +_4 (b +_4 c) = (a + (b + c)) \mod 4$$

and

$$(a +_4 b_4) + c_4 = ((a + b) + c) \mod 4.$$

But since $a + (b + c) = (a + b) + c$*, modulating both of these expressions by* 4 *yields the same result, and so also* $a +_4 (b +_4 c) = (a +_4 b) +_4 c$*. Thus, the operation is associative.*

It is easy to see that $0 \in \mathbb{Z}_4$ *is a neutral element, since* $0 +_4 a = a +_4 0 = a$ *for any* $a \in \mathbb{Z}_4$.

The inverse to any given $a \in \mathbb{Z}_4$ *is* $i(a) = 4 - a$, *since then* $a + i(a) = i(a) + a = a + 4 - a = 4 = 0 \mod 4$, *i.e. summing any* $a \in \mathbb{Z}$ *with* $(4 - a)$ *always yields the neutral element* 0.

To conclude, $(\mathbb{Z}_4, +_4)$ *is a group.*

Exercise 5. *Once again, the operation "multiplication modulo 4" is associative since it can be defined in terms of ordinary multiplication over the integers which is itself associative. The neutral element in this case is clearly* $1 \in \mathbb{Z}_4$, *since* $a \cdot_4 1 = 1 \cdot_4 a = a$ *for any* $a \in \mathbb{Z}_4$. *However, if we look at Table 2, we can see that* 0 *and* 2 *do not have inverses with respect to multiplication, since no matter what we multiply them by, we are never going to get the neutral element* 1. *Thus* $(\mathbb{Z}_4, \cdot_4)$ *is not a group.*

Exercise 6. *The operation "multiplication modulo 5" is associative and has* $1 \in \mathbb{Z}_5$ *as its neutral element. Whether* $(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$ *is a group or not therefore hinges on whether every non-zero element in* $\mathbb{Z}_5$, *viz.* $1, 2, 3, 4$, *has an inverse, i.e. whether for every* $a \in \mathbb{Z}_5 \setminus \{0\}$ *there is some* $i(a) \in \mathbb{Z}_5 \setminus \{0\}$ *such that* $ai(a) = i(a)a = 1$. *Since there are only 4 elements in the set, this can be done by trial and error. It is not difficult to see that* $1 \cdot 1 = 1 \mod 5$, $2 \cdot 3 = 1 \mod 5$, $3 \cdot 2 = 1 \mod 5$, *and* $4 \cdot 4 = 1 \mod 5$. *Thus,* $(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$ *is a group.*

Exercise 7. *As before, we simply have to check whether every element in* $\mathbb{Z}_6 \setminus \{0\}$ *has a multiplicative inverse modulo* 6*; and, again, this can be done by trial and error. We can see that* 3 *does not have an inverse, since* $3 \cdot 1 = 3 \mod 6$, $3 \cdot 2 = 0 \mod 6$, $3 \cdot 3 = 3 \mod 6$, $3 \cdot 4 = 0 \mod 6$, *and* $3 \cdot 5 = 3 \mod 6$. *Since not all elements have inverses,* $(\mathbb{Z}_6 \setminus \{0\}, \cdot_6)$ *cannot be a group.*

Exercise 8. *From the table, it is clear that* 0 *is a neutral element (since* $a \circ 0 = 0 \circ a = a$ *for any* a*), and that every element has an inverse (since the neutral element* 0 *can be found in every row and every column of the table). The only question which needs to be resolved is thus whether the group operation is associative. In this case, the operation is given by a look-up table (and not by an "elegant" formula like in the case of addition or multiplication modulo* n*), so the only possibility is to manually check all triples* a, b, c *and check whether* $a \circ (b \circ c) = (a \circ b) \circ c$. *It is easy to find a triple which does not satisfy associativity, however. For instance, we have*

$$2 \circ (3 \circ 2) = 2 \circ 2 = 3$$

but

$$(2 \circ 3) \circ 2 = 3 \circ 2 = 2.$$

Thus, the operation is not associative, and $(\mathbb{Z}_4, \circ)$ *is not a group.*

Exercise 9. *The element* 3 *does generate* $\mathbb{Z}_5 \setminus \{0\}$ *since we have*

$$\begin{aligned} 3 &= 3 \\ 3 \cdot 3 &= 4 \\ 3 \cdot 3 \cdot 3 &= 2 \\ 3 \cdot 3 \cdot 3 \cdot 3 &= 1 \end{aligned}$$

and so the powers of 3 *generate all elements; on the other hand, we have*

$$\begin{aligned} 4 &= 4 \\ 4 \cdot 4 &= 1 \end{aligned}$$

and so the powers of 4 *only generate two of the elements of* $\mathbb{Z}_5 \setminus \{0\}$*, i.e.* 4 *is not a generator of* $\mathbb{Z}_5 \setminus \{0\}$*.*

Exercise 10. *Clearly,* 0 *cannot generate* $\mathbb{Z}_{11}$*, since no matter how many times we add it to itself, we would always get* 0*.*

On the other hand, we have

$$\begin{aligned} 1 &= 1 \\ 1+1 &= 2 \\ 1+1+1 &= 3 \\ 1+1+1+1 &= 4 \\ 1+1+1+1 &= 5 \\ 1+1+1+1+1 &= 6 \\ 1+1+1+1+1+1 &= 7 \\ 1+1+1+1+1+1+1 &= 8 \\ 1+1+1+1+1+1+1+1 &= 9 \\ 1+1+1+1+1+1+1+1+1 &= 10 \\ 1+1+1+1+1+1+1+1+1+1 &= 0, \end{aligned}$$

and thus $g = 1$ *is the smallest generator of* $\mathbb{Z}_{11}$ *(with respect to addition. Recall that e.g.* $5g$ *is simply shorthand for* $g+g+g+g+g$*. Thus:*

$$5g + 3g = (g+g+g+g+g) + (g+g+g) = 8g = 8,$$

and

$$g + 8g = 9g = 9.$$

On the other hand, note that $11g = 0$*. Thus*

$$12g = 11g + g = 0 + g = g = 1.$$

Exercise 11. *As before,* 1 *cannot possibly generate* $\mathbb{Z}_{11} \setminus \{0\}$ *since multiplying* 1 *with itself always gives back* 1*, no matter how many times we do it. We thus try to check whether* 2 *could generate all elements of* $\mathbb{Z}_{11} \setminus \{0\}$*. We have*

$$
\begin{aligned}
2 &= 2 \\
2 \cdot 2 &= 4 \\
2 \cdot 2 \cdot 2 &= 8 \\
2 \cdot 2 \cdot 2 \cdot 2 &= 5 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 10 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 9 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 7 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 3 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 6 \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 &= 1,
\end{aligned}
$$

and so $g = 2$ does generate all elements of $\mathbb{Z}_{11} \setminus \{0\}$. We then have:

$$g^5 \cdot g^3 = (g \cdot g \cdot g \cdot g \cdot g) \cdot (g \cdot g \cdot g) = g^8 = 2^8 = 3$$

and

$$g \cdot g^8 = g^9 = 6.$$

Since $g^1 0 = 1$, we finally have

$$g^1 2 = g^1 0 \cdot g^2 = 1 \cdot g^2 = g^2 = 2^2 = 4.$$

Exercise 12.

```
for i in [1..100] do
    i, Modinv(i,101);
end for;
```