INF 240 - Exercise problems - 1

Nikolay Kaleyski

1 Groups

Recall that a set S together with a binary operation $* : S \times S \to S$ is called a **group** if the operation $*$ satisfies the following properties:

1. *Associativity*: the order in which we apply the operation to elements does not matter, i.e. for any $s_1, s_2, s_3 \in S$, we have

$$(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3);$$

2. *Identity element*: there is a so-called identity element $e \in S$ which does not affect the other elements when applied to them with the operation, i.e. for any $s_1 \in S$, we have

$$s_1 * e = e * s_1 = s_1.$$

3. *Inverse element*: every element $s_1 \in S$ has a so-called inverse element $s_1^{-1} \in S$, so that applying the group operation to any element and its inverse gives the identity element e, i.e. $s_1 * s_1^{-1} = s_1^{-1} * s_1 = e$.

Note that the definition only specifies that (at least one) identity element and, for any element $s \in S$, (at least one) inverse element to s exists, but it does not claim that e.g. there is only one identity element. In fact, both the identity element and the inverse corresponding to a given element s are uniquely determined, which can be proved easily from the axioms of the group.

Exercise 1. *Show that a group has precisely one identity element.*

Exercise 2. *Show that for any element s in a group, there is precisely one inverse to s.*

1.1 Modular arithmetic

The set G_n represents all possible remainders of division by n, for some positive integer n. For example, $G_4 = \{0, 1, 2, 3\}$, since when dividing a number by 4, there are four possible remainder, viz. 0, 1, 2, and 3. To denote that the remainder of dividing a by b is m, we write $a \mod b = m$; thus, for example, $7 \mod 5 = 2$. The ordinary addition and multiplication operations can be extended to G_n: for instance, to multiply two numbers in G_4, we first multiply them as ordinary integers, and then compute the remainder of dividing the result by 4. So, $2 \cdot 3 = 2$ since $2 \cdot 3 = 6$ in $\mathbb{Z}$, and $6 \mod 4 = 2$.

More formally, we define $a \mod b = n$ if there exists an integer q and a non-negative integer $0 \leq r < b$ such that $a = bq + r$. In the above example, we had

$6 = 1 \cdot 4 + 2$, so that in this case we have $b = 1$ and $r = 2$. This definition makes it easier to see how modular arithmetic can be applied to negative numbers (note that integers a and q do not have to be non-negative!) For example, $-6 \mod 4 = 2$ since we can write $-6 = -2 \cdot 4 + 2$; here $q = -2$ and $r = 2$.

Exercise 3. *Create addition and multiplication tables modulo* 4 *by filling in Tables 1 and 2 below.*

$+$	0	1	2	3
0				
1				
2				
3				

Table 1: Addition table for G_4

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

Table 2: Multiplication table for G_4

Exercise 4. *Show that* G_4 *with addition modulo* 4*, which we can denote by* $(G_4, +)$*, is a group by verifying each of the three axioms from the definition, i.e. show that every triple* $s_1, s_2, s_3 \in G_4$ *satisfies associativity, find an identity element* e *and verify that for every element* $s \in G_4$ *(including* e *itself) it holds that* $e + z = z + e = z$*, and, for every* $s \in G_4$*, find its inverse.*

Exercise 5. *Decide whether* G_4 *with multiplication modulo* 4*, i.e. the structure* $(G_4, \cdot)$ *is a group.*

Exercise 6. *Although, say,* $(G_5, \cdot)$ *is not be a group due to* 0 *not having an inverse, it may still be a group if we consider only its non-zero elements. Consider* $G_5 \setminus \{0\} = \{1, 2, 3, 4\}$ *and show that it is a group.*

Exercise 7. *Similarly, decide whether* $(G_6, \cdot)$ *is a group.*

In Exercise 3, we computed Table 1, which is essentially a look-up table for the group operation of $(G_4, +)$. Consider, again, the set $G_4 = \{0, 1, 2, 3\}$. Instead of specifying the group operation in some "systematic" manner (such as by taking ordinary addition and reducing the result modulo 4), we can specify the operation by directly providing a look-up table. This allows us to define a lot more operations that may not have an "elegant" representation and, as long as one of these operations satisfies the three axioms from the definition, the resulting structure will be a group.

Exercise 8. *Consider the operation* $\circ$ *defined on* $\{0, 1, 2, 3\}$ *by Table 3. Check whether it satisfies each of the three axioms from the definition of a group, and decide whether it is a group.*

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	0	3
2	2	0	3	3
3	3	2	2	0

Table 3: Look-up table for an operation over G_4

1.2 Cyclic groups

A group is called **cyclic** if all of its elements can be generated by repeatedly applying the group operation to one of its elements. For example, consider the group $(G_5 \setminus \{0\}, \cdot)$. We can compute

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

and it is evident that all elements of $G_5 \setminus \{0\} = \{1, 2, 3, 4\}$ can be expressed as powers of 2. If this is the case, we say that 2 is a **generator** of $(G_5 \setminus \{0\}, \cdot)$, or that it **generates** it. It is also clear that even if a group is cyclic, not all of its elements can be generators, since e.g. any power of 1 is equal to 1, and we cannot generate any other element by taking powers of 1.

In general, this means if g is a generator of a group $(S, *)$, then all elements of S can be expressed as the set $< g >= \{e = g^0, g = g^1, g^2, g^3, \ldots, \}$ for all possible powers of g. However, g can be raised to the power of any natural number, which means we would have to consider an infinite number of powers. However, if the group S is of size n, it is enough to consider only the first n powers of g, i.e. $\{e = g^0, g = g^1, g^2, \ldots, g^{n-1}\}$. To see this, it is enough to show that these first n powers correspond to different elements of the group. Suppose that $g^i = g^j$ for some $0 \leq i < j < n$; then we have $g^j \cdot g^{-i} = e$, i.e. $g^{j-i} = e$, and $0 \leq j - i < n$; so the $(j-i)$-th power of g (which is among the first n powers) is the identity element, and from then on, the elements will keep repeating: $g^{j-i+1} = g$, $g^{j-1+2} = g^2$, etc. In this way, it is impossible for g to generate all n elements of S, which contradicts the fact that g generates S.

This explains how we can handle powers of g higher than $n-1$: if $i \geq n$, then i can be written as $i = nq + r$ for $r < n$. Then $g^i = g^{nq+r} = g^{nq} \cdot g^r = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r$. For example, if g generates a group of size $n = 15$, then $g^{25} = g^{25-15} = g^{10}$.

In the same way, we can handle negative powers of g: since e.g. $-40 = -3 \cdot 15 + 5$, then $g^{-40} = (g^{15})^{-3} \cdot g^5 = g^5$.

Exercise 9. *Check whether the remaining elements of* $G_5 \setminus \{0\}$*, viz.* 3 *and* 4*, are also generators of* $(G_5 \setminus \{0\}, \cdot)$*.*

The principle of cyclicity is the same in the case of additive groups, e.g. $(G_4, +)$, except that the "powers" of an element are actually multiples. More precisely, in the multiplicative case, applying the group operation, say, five times to an element a gives

$$a \cdot a \cdot a \cdot a \cdot = a^5,$$

whereas in the additive case we get

$$a + a + a + a + a = 5a.$$

NB: Note that the notations a^5 and $5a$ are simply shorthand for multiple application of the group operation. There is only one operation in a group, viz. the group operation.

Exercise 10. *Consider the group $(G_{11}, +)$. Find the smallest number g which generates it. Compute:*

- $5g + 3g$;
- $g + 8g$;
- $12g$;
- $-3g$;
- $-5g + 8g$.

Exercise 11. *Similarly, consider the group $(G_{11} \setminus \{0\}, \cdot)$. Find the smallest number g which generates it. Compute:*

- $g^5 \cdot g^3$;
- $g \cdot g^8$;
- g^{12};
- g^{-3};
- $g^{-5} \cdot g^8$.

2 Introduction to *Magma*

Magma is a computer algebra systems which can, among other things, be used to with groups, finite fields, Boolean functions, and other mathematical objects studied in the course of INF240. More information can be found at `http://magma.maths.usyd.edu.au`. Although *Magma* is proprietary software, a free online calculator is available on their website at `http://magma.maths.usyd.edu.au/calc` which can be used to run simple programs.

In this section, we will briefly look at how to perform modular arithmetic arithmetic with *Magma*.

Computing the remainder of dividing a by b, i.e. $a \mod b$, is done simply by typing e.g.

```
11 mod 5;
```

which will output 1 since $11 = 2 \cdot 5 + 1$. Thus, addition and multiplication over G_n can be implemented by simply writing e.g.

```
(a + b) mod n;
```

or

```
(a * b) mod n;
```

for some a, b, and n.

Suppose we want to compute the inverse of 15 in $G_{101} \setminus \{0\}$, i.e. we want to find an element i between 0 and 100 such that $(15 \cdot i) \mod 101 = 1$. One possibility is to use a *for* loop and check all possibilities:

```
for i in [1..100] do
        if (i*15) mod 101 eq 1 then
                print(i);
        end if;
end for;
```

The above code will print all integers i between 1 and 100 satisfying $i \cdot 15 \mod 101 = 1$. There is a more compact way to do this in *Magma*, which imitates mathematical set notation:

```
{ i : i in [1..100] | (15*i) mod 101 eq 1 };
```

This will compute the set of all integers between 1 and 100 such that $i \cdot 15 \mod 101 = 1$.

Nonetheless, this is still unnecessarily long, since *Magma* already has a built in command for computing the multiplicative inverse of an integer:

```
Modinv(15,101);
```

If it happens that no inverse exists, *Magma* will show an error.

Exercise 12. *We know that all elements of* $G_{101} \setminus \{0\}$ *are invertible. Use Magma to construct a look-up table of inverses, so that every row of the table contains an integer between 1 and 100 along with its inverse modulo* 101.