Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Module 11: Groups
Fall 2021

This module corresponds to the following sections from your textbook:

40. Groups
41. Group Isomorphism
42. Subgroups
43. Fermat's Little Theorem

1 Groups

Informally, you are already familiar with operations. For example, the addition operation + takes a pair of numbers as input, and produces their sum as output. Now, we give the formal definition of an operation.

Definition 1 (Operation)**.** Let A be a set. An **operation** on A is a function that maps elements in $A \times A$ to elements in A.

Example 2. Consider the operations $\oplus$, $\otimes$, and $\ominus$, which are all functions from $\mathbb{Z}_n \times \mathbb{Z}_n$ to $\mathbb{Z}_n$, where $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

The operation $\oslash$ is a function from $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ to $\mathbb{Z}_p^*$, where p is a prime number and $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

A common symbol used to generically represent an operation is $*$.

Definition 3 (Properties of operations)**.** Let $*$ be an operation on a set A. The following are some important properties that the operation may have.

1. **Commutative property:** $*$ is commutative on A provided that $a * b = b * a$ for all $a, b \in A$.
2. **Closure property:** $*$ is closed on A provided that $a * b \in A$ for all $a, b \in A$.
3. **Associative property:** $*$ is associative on A provided that $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$.
4. **Identity element:** An element $e \in A$ is called an identity element for $*$ provided that $a * e = e * a = a$ for all $a \in A$.
5. **Inverses:** Suppose that $e \in A$ is the identity element. We call b an inverse of a provided that $a * b = b * a = e$.

Example 4. Consider the addition operation +, which is a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

The operation + satisfies the following properties in Definition 3:

- Commutative property: We have $a + b = b + a$ for all $a, b \in \mathbb{Z}$.
- Closure property: We have $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$.
- Associative property: We have $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.
- Identity element: We have $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$, so 0 is the identity element.

- Inverses: We have $a + (-a) = (-a) + a = 0$ for all $a \in \mathbb{Z}$, so $-a$ is the inverse of a.

Example 5. Consider the composition operation $\circ$ on the set S_n (the set of permutations all permutations on $\{1, 2, 3, \ldots, n\}$), which is a function from $S_n \times S_n$ to S_n.

The operation $\circ$ satisfies the following properties in Definition 3 (note that we are omitting the proofs):

- Closure property: If $\pi \in S_n$ and $\sigma \in S_n$, then $\pi \circ \sigma \in S_n$.
- Associative property: If $\pi \in S_n$ and $\sigma \in S_n$ and $\tau \in S_n$, then $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$.
- Identity element: There is a permutation ι such that $\pi \circ \iota = \iota \circ \pi = \pi$, for all $\pi \in S_n$.
- Inverses: If $\pi \in S_n$, then $\pi^{-1} \in S_n$ and $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$.

It does not satisfy the commutative property. In general, $\pi \circ \sigma \neq \sigma \circ \pi$ (but they can be equal in some special cases).

This leads us to the notion of a **group**. In the above two examples, $+$ on $\mathbb{Z}$ gives us a group, and $\circ$ on S_n gives us a group. More formally we define a group as follows.

Definition 6 (Group)**.** Let $*$ be an operation defined on a set G. We call the pair $(G, *)$ a group, provided:

1. The set G is closed under the operation $*$.
2. The operation $*$ is associative on G.
3. There is an identity element $e \in G$ for the operation $*$.
4. For every element $g \in G$, there is an inverse element for the operation $*$, commonly represented as g^{-1}.

Groups in which the operation is commutative have a special name.

Definition 7 (Abelian groups)**.** Let $(G, *)$ be a group. We call this group **Abelian** provided that $*$ is a commutative propert y on G.

Example 8. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are groups. They are all Abelian.

$(\mathbb{Q}, \times)$ is not a group, since $0 \in \mathbb{Q}$ does not have an inverse. Let $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then, $(\mathbb{Q}^*, \times)$ is an Abelian group.

Example 9. $(\mathbb{Z}_n, \oplus)$ and $(S_n, \circ)$ are groups.

$(\mathbb{Z}_n, \oplus)$ is Abelian, but $(S_n, \circ)$ is not.

Example 10. Consider the set $G = \{e, a, b, a * b\}$, where e is the identity element and all of the elements are their own inverse, so $e = a^2 = b^2 = (ab)^2$. So, $(G, *)$ is a group. This is called the **Klein four-group**, and has applications in algebra and graph theory.

We may represent the four elements as matrices, e.g.,

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad b = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad ab = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Verify, using matrix multiplication, that $(G, *)$ is an Abelian group.

Other representations are also possible (e.g., see p. 293 in the textbook and https://en.wikipedia.org/wiki/Klein_four-group).

Proposition 11 (Unique inverse)**.** *Let $(G, *)$ be a group. Every element of G has a unique inverse in G.*

Proof. By definition, every element in G has an inverse. Suppose, for the sake of contradiction, that $g \in G$ has two distinct inverses $h, k \in G$. So,

$$g * h = h * g = g * k = k * g = e,$$

where $e \in G$ is the identity element for $*$. By the associative property, we have

$$h * (g * k) = (h * g) * k.$$

Since, $g * k = e$, the LHS of the above equation simplifies to

$$h * (g * k) = h * e = h,$$

and since $h * g = e$, the RHS simplifies to

$$(h * g) * k = e * k = k.$$

So, we have $h = k$, which contradicts our supposition that h and k are distinct. Thus, every element of G has a unique inverse in G. □

Given a set G and an operation $*$, to prove that $(G, *)$ is a group requires showing that it fulfulls the four properties listed in Definition 6.

Definition 12 ($\mathbb{Z}_n^*$)**.** Let n be a positive integer. We define $\mathbb{Z}_n^*$ to be the integers in $\mathbb{Z}_n$ that are relatively prime with n. More formally,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

Example 13. Below is the multiplication table for $\mathbb{Z}_{10}$ that we have already seen in the previous chapter.

a \ b	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Recall that only the elements in $\mathbb{Z}_{10}$ that are relatively prime with n have an inverse (the products of inverses are highlighted in the table). If we remove all elements from $\mathbb{Z}_{10}$ that are not relatively prime with n, we get the following multiplication table for $\mathbb{Z}_{10}^*$.

a \ b	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Now, we can see that $(\mathbb{Z}_{10}^*, \otimes)$ is an Abelian group, since:

- For all $a, b \in \mathbb{Z}_{10}^*$, we have $a \otimes b \in \mathbb{Z}_{10}^*$.
- For all $a, b, c \in \mathbb{Z}_{10}^*$, we have $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.
- The element $1 \in \mathbb{Z}_{10}^*$ is an identity element, since we have $a \otimes 1 = 1 \otimes a = a$ for all $a \in \mathbb{Z}_{10}^*$.
- $1^{-1} = 1, 3^{-1} = 7, 7^{-1} = 3$, and $9^{-1} = 9$, so each element in $\mathbb{Z}_{10}^*$ has an inverse.
- For all $a, b \in \mathbb{Z}_{10}^*$, we have $a \otimes b = b \otimes a$.

Exercise

Draw the multiplication table for $\mathbb{Z}_{14}^*$, and find the inverse of each element. Compare your answer with Example 40.14 on p. 294.

Proposition 14. *Let n be a positive integer. Then, $(Z_n^*, \otimes)$ is a group.*

Proof. We prove that the closure property holds, i.e., that $a \otimes b \in \mathbb{Z}_n^*$ for all $a, b \in \mathbb{Z}_n^*$.

Since $a \in \mathbb{Z}_n^*$ is relatively prime with n, we can find integers x, y such that $ax + ny = 1$.

Similarly, since $b \in \mathbb{Z}_n^*$ is relatively prime with n, we can find integers w, z such that $bw + nz = 1$.

To show that $a \otimes b \in \mathbb{Z}_n^*$, we must show that $a \otimes b = (ab) \bmod n$ is relatively prime with n.

Multiplying our expressions above for a and b gives us $(ax + ny)(bx + nz) = 1$. If we can simplify the right-hand side of the equation into the form $(ab)X + nY = 1$, that would show that $\gcd(ab, n) = 1$ (and thus that ab and n are relatively prime). So we proceed as follows:

$$\begin{aligned} 1 &= (ax + ny)(bw + nz) \\ &= (ax)(bw) + (ax)(nz) + (ny)(bw) + (ny)(nz) \\ &= (ab)(wx) + n(axz + ybw + ynz) \\ &= (ab)X + nY \end{aligned}$$

Thus, we have shown that ab is relatively prime with n. So, $(Z_n^*, \otimes)$ satisfies the closure property.

Refer to the proof for Proposition 40.15 on p. 294 of the textbook to see that the remaining properties are also satisfied. □

The cardinality of $\mathbb{Z}_n^*$ is important enough that it has its own function.

Definition 15. Let $n \geq 2$ be an integer. Euler's totient is defined as

$$\varphi(n) = |\mathbb{Z}_n^*|.$$

Note that $\varphi(1)$ is defined to be 1.

2 Group Isomorphism

Sometimes, two seemingly distinct groups may be essentially the "same", or what we will more formally define as **isomorphic**. For example, below we provide the addition table for $(Z_4, \oplus)$ and the multiplication table for $(Z_5^*, \otimes)$.

a \ b	$\oplus$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

a \ b	$\otimes$	1	2	3	4
	1	1	2	3	4
	2	2	4	1	3
	3	3	1	4	2
	4	4	3	2	1

Notice that:

- In $(\mathbb{Z}_4, \oplus)$, 0 is the identity element. In $(\mathbb{Z}_5^*, \otimes)$, 1 is the identity element.
- $(\mathbb{Z}_4, \oplus)$ has a "special" element 1 that can be used to "generate" the remaining elements in $\mathbb{Z}_4$: $1 \oplus 1 = 2$, $1 \oplus 1 \oplus 1 = 3$, and $1 \oplus 1 \oplus 1 \oplus 1 = 0$. Similarly, $(\mathbb{Z}_5^*, \otimes)$ has a "special" element 2 that can be used to "generate" the remaining elements: $2 \otimes 2 = 4$, $2 \otimes 2 \otimes 2 = 3$, and $2 \otimes 2 \otimes 2 \otimes 2 = 1$.
- In $(\mathbb{Z}_4, \oplus)$, 2 is its own inverse. In $(\mathbb{Z}_5^*, \otimes)$, 4 is its own inverse.
- In $(\mathbb{Z}_4, \oplus)$, we can "generate" 3 using three copies of the "special" element: $1 \oplus 1 \oplus 1 = 3$. Similarly, in $(\mathbb{Z}_5^*, \otimes)$ we can "generate" 3 using three copies of the "special" element: $2 \otimes 2 \otimes 2 = 3$.

Now, we can define a bijection $f : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ that maps each element in $(\mathbb{Z}_4, \oplus)$ to an element in $(\mathbb{Z}_5^*, \otimes)$ that is its "twin", based on our observations above: $f(0) = 1$, $f(1) = 2$, $f(2) = 4$, and $f(3) = 3$.

Now, let us rearrange the rows and columns of the multiplication table, so that the "twin" elements are located in the same position in the table. We reproduce the two tables beside each other below:

a \ b	$\oplus$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

a \ b	$\otimes$	1	2	4	3
	1	1	2	4	3
	2	2	4	3	1
	4	4	3	1	2
	3	3	1	2	4

Notice above that in both tables, the elements in each row are "shifted" to the left with respect to the row above it, and the left-most element is relocated to the resulting "empty" space in the right-most position of the row. All that is different between the two tables is the name of the elements (which we could replace with, e.g., a, b, c, d and x, y, z, w) and the symbols $\oplus$ and $\otimes$ (which we could replace with $*$). Because these two groups are effectively the "same", we call them **isomorphic**. More formally, we define isomorphism as follows.

Definition 16 (Isomorphism of groups)**.** Let $(G, *)$ and $(H, \star)$ be groups. A function $f : G \to H$ is called a group isomorphism provided f is one-to-one and onto, and satisfies

$$f(g * h) = f(g) \star f(h) \text{ for all } g, h \in G.$$

When there is an isomorphism from G to H, we say G is isomorphic to H and write $G \cong H$.

The requirement $f(g * h) = f(g) \star f(h)$ above can be thought of informally as "assembling two items g and h and then shipping them should be the same as shipping g and h individually, to be assembled at the destination".

Exercise

Show that $(\mathbb{Z}_4, \oplus)$ is isomorphic to $(\mathbb{Z}_5^*, \otimes)$. We already provided the bijective function $f : \mathbb{Z}_4 \to \mathbb{Z}_5^*$. So, what is left is to show that $f(g*h) = f(g) \star f(h)$ for all $g, h \in G$. For example, $f(1 \oplus 2) = f(3) = 3$ and $f(1) \otimes f(2) = 2 \otimes 4 = 3$. Complete for the remaining elements.

As was mentioned previously, both $(\mathbb{Z}_4, \oplus)$ and $(\mathbb{Z}_5^*, \otimes)$ have a "special" element that can be used to "generate" any element in the group. We call this "special" element a **generator**. The generator element of $(\mathbb{Z}_4, \oplus)$ is 1, and the generator element of $(\mathbb{Z}_5^*, \otimes)$ is 2. Observe below how the generator element can be used to generate all the elements of its respective group:

$$\begin{aligned} 1 &= 1 \\ 1 \oplus 1 &= 2 \\ 1 \oplus 1 \oplus 1 &= 3 \\ 1 \oplus 1 \oplus 1 \oplus 1 &= 0 \end{aligned} \qquad \begin{aligned} 2 &= 2 \\ 2 \otimes 2 &= 4 \\ 2 \otimes 2 \otimes 2 &= 3 \\ 2 \otimes 2 \otimes 2 \otimes 2 &= 1. \end{aligned}$$

Exercise

$(\mathbb{Z}_4, \oplus)$ and $(\mathbb{Z}_5^*, \otimes)$ actually both have **two** generator elements (that shouldn't be surprising, considering that we have already established that they are isomorphic). The element 3 is a generator element in both $(\mathbb{Z}_4, \oplus)$ and $(\mathbb{Z}_5^*, \otimes)$. Show that this is the case, as was done above.

Note that not all groups have a generator element. For example, the Klein 4-group does not have a generator element—recall that in this group, every element g has the property that $g * g = e$ (where e is the identity element), so it is impossible for any of the elements to be a generator. Groups that have a generator element have a special name.

Definition 17 (Generator, cyclic group)**.** Let $(G, *)$ be a group. An element $g \in G$ is called a **generator** for G provided every element of G can be expressed in terms of g and g^{-1} using the operation $*$.

If a group conatins a generator, it is called **cyclic**.

The inverse element of g is only needed for groups with infinitely many elements.

Example 18. Consider the group $(\mathbb{Z}, +)$.

All positive integers can be expressed in terms of the element 1 and the operation $+$; e.g., $2 = 1 + 1$ and $3 = 1 + 1 + 1$.

To generate the negative integers we need to use the inverse element of 1, which is -1; e.g., $-2 = (-1) + (-1)$ and $-3 = (-1) + (-1) + (-1)$.

0 can be expressed as $1 + (-1)$.

So, $(\mathbb{Z}, +)$ is a cyclic group.

Example 19. An example of a non-cyclic group is the symmetric group S_3. Recall from Module 6:

$$\begin{aligned} S_3 &= \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\} \\ &= \{(1), (1,2)(3), (1,3)(2), (1)(2,3), (1,2,3), (1,3,2)\} \end{aligned}$$

Any permutation $\sigma \in S_3$ will have the property that either $\sigma = \iota$, or $\sigma \circ \sigma = \iota$, or $\sigma \circ \sigma \circ \sigma = \iota$, where $\iota \in S_3$ is the identity element. So, none of the elements in S_3 can be a generator.

Exercise

You may verify the claim we make in the above example.

Finally, note that any two finite cyclic groups of the same order (i.e., with the same number of elements) are isomorphic.

Theorem 20. *Let $(G, *)$ be a finite cyclic group. Then, $(G, *)$ is isomorphic to $(\mathbb{Z}_n, \oplus)$ where $n = |G|$.*

Proof. Omitted. See proof for Theorem 41.4 on p. 300 of the textbook. □

3 Subgroups

Consider the group $(\mathbb{Z}, +)$. We now define $(E, +)$, where $E = \{x \in \mathbb{Z} : 2 \mid x\}$ is the set of even integers. Notice that $(E, +)$ satisfies all four properties of a group. We call $(E, +)$ a **subgroup** of $(\mathbb{Z}, +)$.

Definition 21 (Subgroup)**.** Let $(G, *)$ be a group and let $H \subseteq G$. If $(H, *)$ is also a group, we call it a subgroup of $(G, *)$.

Example 22. We list all four subgroups of $(\mathbb{Z}_6, \oplus)$, all with the operation $\oplus$:

$$\{0\} \qquad \{0, 1, 2, 3, 4, 5\}$$
$$\{0, 3\} \qquad \{0, 2, 4\}$$

Let us first show that $(\{0, 3\}, \oplus)$ is a group:

- We do not have to check for associativity, since we know that $(\mathbb{Z}_6, \oplus)$ is associative, so any subgroup $(G, \oplus)$ where $G \in \mathbb{Z}_6$ is also associative.
- The set is closed on $\oplus$: $0 \oplus 0 = 0$, $0 \oplus 3 = 3$, and $3 \oplus 3 = 0$.
- The identity element 0 is in the set.
- Every element has an inverse: The inverse of 0 is itself (since $0 \oplus 0 = 0$), and the inverse of 3 is itself (since $3 \oplus 3 = 0$).

Exercise

Check, as done above, that $(\{0, 2, 4\}, \oplus)$ is also a group.

In summary, given a group $(G, *)$ and $(H, *)$ where $H \subseteq G$, to prove that $(H, *)$ is a subgroup of $(G, *)$:

- Prove that H is closed under $*$.
- Prove that the identity element $e \in G$ is also in H.
- Prove that the inverse of every element H is also in H.

But how do we know that there are no other subgroups of $(\mathbb{Z}_6, \oplus)$, besides the ones that we listed in Example 22? We could check all possible subsets of $\mathbb{Z}_6$, which is a bit tedious. For example, we can see that $(\{0, 1, 2, 3\}, \oplus)$ is not a group, because $2 \oplus 3 = 5$ and 5 is not in the set, so $(\{0, 1, 2, 3\}, \oplus)$ is not closed on $\oplus$.

In Example 22, the number of elements in each of the four subgroups are 1, 2, 3, and 6—note that these are divisors of 6. Lagrange's Theorem states that the cardinality of a subgroup must divide the cardinality of the group. So, in Example 22, this means that we don't need to look for a subgroup with cardinality 4 or 5.

Theorem 23 (Lagrange's Theorem)**.** *Let $(H, *)$ be a subgroup of a finite group $(G, *)$ and let $a = |H|$ and $b = |G|$. Then, $a \mid b$.*

Proof. Omitted. See the proof accompanying Theoerm 42.4 on p. 305 of the textbook. □

Exercise

Find all the subgroups of $(\mathbb{Z}_{10}, \oplus)$. Compare your answer with Example 42.2 on p. 303 of the textbook.

4 Fermat's Little Theorem

We close with two important theorems. We omit the proofs, which can be found in Section 43 of the textbook.

Theorem 24 (Fermat's Little Theorem)**.** *Let p be a prime and let a be an integer. Then,*

$$a^p \equiv a \pmod{p}.$$

For example, if $a = 5$ and $p = 23$, we have $5^{23} \equiv 23$. This is a very important result in mathematics, and is relied upon by RSA, which is one of the most widely-used public-key cryptosystems.

If a and p are relatively prime, we can restate Fermat's Little Theorem as

$$a^{p-1} \equiv 1 \pmod{p}.$$

Note that we do this by dividing both sides by a, which can only be done if a has an inverse (which exists only if a and p are relatively prime—refer to our discussion on modular division).

There is a more general version of Fermat's Little Theorem, which is called Euler's Theorem.

Theorem 25 (Euler's Theorem)**.** *Let n be a positive integer and let a be an integer relatively prime to n. Then,*

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ is Euler's totient.

Example 26. Let $n = 9$. Note that $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ and $\varphi(9) = |\mathbb{Z}_9^*| = 6$. So, Euler's Theorem tells us that any element in $\mathbb{Z}_9^*$ raised to the power 6 equals 1. In other words, $1^6 \equiv 2^6 \equiv 4^6 \equiv 5^6 \equiv 7^6 \equiv 7^6 \equiv 1$.

The contrapositive of Fermat's Little Theorem is as follows.

Theorem 27. *Let a and n be positive integers. If $a^n \not\equiv a \pmod{n}$, then n is not prime.*

This is useful for primality testing.

Example 28. Let us show that $n = 3007$ is not prime. One method would be to factor 3007. But for sufficiently large values of n, the computational cost would make factoring infeasible. So, we use Theorem 27:

$$2^{3007} \equiv 66 \not\equiv 2 \pmod{3007}.$$

So, 3007 is not prime.