Chapter 4

The Group Zoo

"The universe is an enormous direct product of representations of symmetry groups." (Hermann Weyl, mathematician)

In the previous chapter, we introduced *groups* (together with subgroups, order of a group, order of an element, abelian and cyclic groups) and saw as examples the group of symmetries of the square and of the rectangle. The concept of group in mathematics is actually useful in a variety of areas beyond geometry and sets of geometric transformation. We shall next consider many sets endowed with binary operations yielding group structures. We start with possibly the most natural example, that of real numbers. Since both addition and multiplication are possible operations over the reals, we need to distinguish with respect to which we are considering a group structure.

Example 1. We have that $(\mathbb{R}, +)$ is a group.

- $\mathbb{R}$ is closed under addition, which is associative.
- $\forall x \in \mathbb{R}, x + 0 = 0 + x = x$, hence 0 is the identity element.
- $\forall x \in \mathbb{R}, \exists(-x) \in \mathbb{R}$, so that $x + (-x) = 0$.

Example 2. We have that $(\mathbb{R}^*, \cdot)$, where $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, forms a group:

- $\mathbb{R}^*$ is closed under multiplication, which is associative.
- $\forall x \in \mathbb{R}^*$, $x \cdot 1 = 1 \cdot x = x$, hence 1 is the identity element.
- $\forall x \in \mathbb{R}^*, \exists x^{-1} = \frac{1}{x}$, so that $x \cdot (\frac{1}{x}) = (\frac{1}{x}) \cdot x = 1$.

Both $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot)$ are abelian groups, of infinite order ($|\mathbb{R}| = \infty$, $|\mathbb{R}^*| = \infty$).

Recall the Definition of Group

Do you remember from last week?

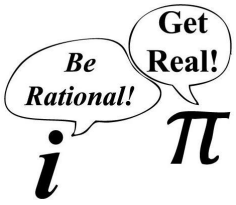
Check List:
✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

Have you thought of examples of groups you might know?

Real Numbers

- The real numbers $\mathbb{R}$ form a group, with respect to addition.

Check List:
✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse



- What about multiplication?
- The real numbers without the zero form a group for multiplication.
- What about the set of complex numbers? (left as exercise)

Consider the set of integers $\mathbb{Z}$.

Definition 10. We say that $a, b \in \mathbb{Z}$ are congruent modulo n if their difference is an integer multiple of n. We write

$$a \equiv b \bmod n \Leftrightarrow a - b = t \cdot n, \quad t \in \mathbb{Z}.$$

Example 3. Here are a few examples of computation.

- $7 \equiv 2 \bmod 5$ because $7 - 2 = 1 \cdot 5$,
- $-6 \equiv -1 \bmod 5$ because $-6 - (-1) = (-1) \cdot 5$,
- $-1 \equiv 4 \bmod 5$ because $-1 - 4 = (-1) \cdot 5$,
- $-6 \equiv 4 \bmod 5$ because $4 - (-6) = 2 \cdot 5$.

We are of course interested in finding a group structure on integers mod n. To do so, we first need to recall what are equivalence classes.

Proposition 3. *Congruence mod n is an **equivalence relation** over the integers, i.e., it is a relation that is reflexive, symmetric and transitive.*

Proof. We need to verify that congruence mod n is indeed reflexive, symmetric, and transitive as claimed.

Reflexive: it is true that $a \equiv a \bmod n$ since $a - a = 0 \cdot n$.

Symmetric: we show that if $a \equiv b \mod n$ then $b \equiv a \mod n$. Now $a \equiv b \bmod n \iff a - b = tn \iff b - a = (-t)n \iff b \equiv a \mod n$.

Transitive: we show that if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$. Now if $a - b = t_1 n$ and $b - c = t_2 n$, then $a - c = a - b + b - c = (t_1 + t_2)n$, showing that $a \equiv c \mod n$. □

Given an equivalence relation over a set, this relation always partitions it into equivalence classes. In particular, we get here:

Theorem 4. *Congruence $\bmod n$ partitions the integers $\mathbb{Z}$ into (disjoint) **equivalence classes**, where the equivalence class of $a \in \mathbb{Z}$ is given by*

$$\bar{a} = \{b \in \mathbb{Z},\ a \equiv b \mod n\}.$$

More Numbers : Integers mod n

For a positive integer n, two integers a and b are said to be **congruent modulo** n if their difference $a - b$ is an integer multiple of n:

$$a = b \bmod n.$$

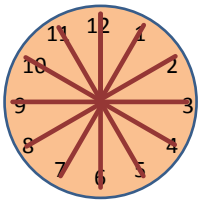
Example:

$7 = 2 \bmod 5$

since 7-2 is a multiple of 5.

We have $a = b \bmod n \Leftrightarrow a-b = 0 \bmod n \Leftrightarrow n \mid a-b \Leftrightarrow a-b = nq \Leftrightarrow a = nq + b$

Integers mod 12



- Integers mod 12 can be represented by {0,1,2,3,4,5,6,7,8,9,10,11}
- Suppose it is 1pm, add 12 hours, this gives 1 am.

Proof. Recall first that a "partition" refers to a disjoint union, thus we have to show that

$$\mathbb{Z} = \bigcup_{a\in\mathbb{Z}} \bar{a} = \bigcup_{a\in\mathbb{Z}} \{b \in \mathbb{Z},\ a \equiv b \mod n\}$$

where $\bar{a} \cap \bar{a'}$ is empty if $\bar{a} \neq \bar{a'}$. Since a runs through $\mathbb{Z}$, we already know that $\mathbb{Z} = \bigcup_{a\in\mathbb{Z}} \bar{a}$, thus the real work is to show that two equivalence classes are either the same or disjoint. Take

$$\bar{a} = \{b \in \mathbb{Z},\ a \equiv b \mod n\},\ \bar{a'} = \{b' \in \mathbb{Z},\ a' \equiv b' \mod n\}.$$

If the intersection $\bar{a} \cap \bar{a'}$ is empty, the two sets are disjoint. Let us thus assume that there is one element c which belongs to the intersection. Then

$$c \equiv a \mod n \text{ and } c \equiv a' \mod n \Rightarrow c = a + tn = a' + sn$$

for some integers s, t. But this shows that

$$a - a' = sn - tn = (s - t)n \Rightarrow a \equiv a' \mod n$$

and we concluce that the two equivalence classes are the same. □

Note that $a \equiv b \bmod n \iff a - b = t \cdot n \iff a = b + tn$, which means that both a and b have the same remainder when we divide them by n. Furthermore, since every integer $a \in \mathbb{Z}$ can be uniquely represented as $a = tn + r$ with $r \in \{0, 1, 2, \ldots, (n-1)\}$, we may choose r as the **representative** of a in its equivalence class under congruence mod n, which simply means that integers mod n will be written $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

Let us define now addition of integers mod n:

$$(a \mod n) + (b \mod n) \equiv (a + b) \mod n.$$

When we write $a \mod n$, we are chosing a as a representative of the equivalence class $\bar{a}$, and since the result of the addition involves a, we need to make sure that it will not change if we pick a' as a representative instead of a!

Proposition 4. *Suppose that $a' \equiv a$ mod n, and $b' \equiv b$ mod n, then $(a'$ mod $n) \pm (b'$ mod $n) \equiv (a \pm b)$ mod n.*

Proof. Since $a' \equiv a \bmod n$, and $b' \equiv b \bmod n$, we have by definition that

$$a' = a + qn,\ b' = b + rn,\ q, r \in \mathbb{Z}$$

hence

$$a' \pm b' = (a + qn) \pm (b + rn) = (a \pm b) + n(q \pm r) \equiv a \pm b \mod n.$$

□

Equivalence Relation

Being congruent mod n is an equivalence relation.

- It is reflexive: a = a mod n
- It is symmetric: if a=b mod n, then b=a mod n.
- It is transitive: if a=b mod n and b=c mod n, then a=c mod n

Thus if a = b mod n, they are in the same equivalence class.
We work with a representative of an equivalence class, it does not matter which (typically between 0 and n-1).

What it means: we identify all elements which are "the same" as one element, an equivalent class!

Addition modulo n

Let us define addition mod n:

(a mod n) + (b mod n) = (a+b) mod n

Problem: given a and n, there are many a' such that a = a' mod n, in fact, all the a' in the equivalence class of a.
Thus addition should work independently of the choice of a', that is, independently of the choice of the representative!

Take a' = a mod n, b'=b mod n, then it must be true that (a' mod n) + (b' mod n) = (a+b) mod n.
a' =a mod n ⇔ a' = a +qn for some q
b' =b mod n ⇔ b' = b+rn for some r
Thus (a+qn)+(b+rn) = (a+b) + n(q+r) = a+b mod n.

All this work was to be able to claim the following:

The integers mod n together with addition form a group G,

where by integers mod n we mean the n equivalence classes

$$G = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\},$$

also denoted by $\mathbb{Z}/n\mathbb{Z}$, and by addition, the binary law

$$\overline{a} + \overline{b} = (a + b) \mod n.$$

We indeed fullfil the definition of a group:

- Closure: since $(a + b) \mod n \in G$.
- Associativity.
- The identity element is $\overline{0}$, since $\overline{a} + \overline{0} = a \mod n = \overline{a}$.
- The inverse of a is $\overline{n-a}$, since $\overline{a} + \overline{n-a} = n \mod n = \overline{0}$.

We further have that G is commutative. Indeed $\overline{a_1} + \overline{a_2} = \overline{a_2} + \overline{a_1}$ (by commutativity of regular addition!).

Therefore G is an abelian group of order n. The group G of integers mod n has in fact more properties.

Proposition 5. *The group G of integers mod n together with addition is cyclic.*

Proof. We have that G has order $|G| = n$. Recall that for a group to be cyclic, we need an element of G of order n, that is an element $\bar{a}$ such that (in additive notation)

$$\bar{a} + \ldots \bar{a} = n\bar{a} = \bar{0}.$$

We take for $\bar{a}$ the element $\overline{1}$, which when repeatedly composed with itself will generate all the elements of the group as follows:

$$\begin{cases} \overline{1} + \overline{1} = \overline{2} \\ \overline{1} + \overline{1} + \overline{1} = \overline{3} \\ \vdots \\ \underbrace{\overline{1} + \overline{1} + \overline{1} + \cdots + \overline{1}}_{(n-1)\ times} = \overline{n-1} \\ \underbrace{\overline{1} + \overline{1} + \overline{1} + \cdots + \overline{1}}_{n\ times} = \overline{n} = \overline{0}. \end{cases}$$

□

Group Structure of Integers mod n

- The set of integers mod n forms an abelian group, with binary operation addition modulo n, and identity element 0 (that is, the equivalence class of 0).
- It has order n.
- It is an abelian group.
- Is it cyclic?

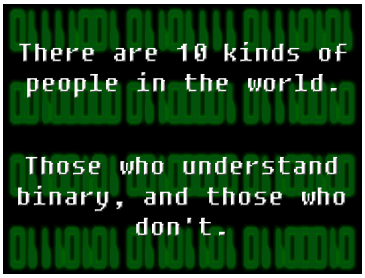
… and n is the smallest integer with that property!

Yes! 1 is of order n since 1+1…+1=n=0 mod n…

Integers mod 2

- The group of integers mod 2 = {0,1} (choice of representatives!)
- Bits are integer modulo 2!

	0	1
0	0	1
1	1	0



Example 4. The group $(\mathbb{Z}/2\mathbb{Z}, +)$ of integers mod 2 has Cayley table

	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

and forms a cyclic group of order 2 ($\mathbb{Z}/2\mathbb{Z} = \langle\overline{1}\rangle,\ \overline{1}^2 = \overline{1} + \overline{1} = \overline{0}$).

Example 5. The group $(\mathbb{Z}/3\mathbb{Z}, +)$ of integers mod 3 has Cayley table

	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

This is a cyclic group of order 3: $\mathbb{Z}/3\mathbb{Z} = \langle\overline{1}\rangle = \langle\overline{2}\rangle$.

Example 6. The Cayley table of the group $(\mathbb{Z}/4\mathbb{Z}, +)$ of integers mod 4 is

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

This is a cyclic group: $(\mathbb{Z}/4\mathbb{Z}, +) = \langle\overline{1}\rangle = \langle\overline{3}\rangle$. The subgroup $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}\}$ of $(\mathbb{Z}/4\mathbb{Z}, +)$ has a Cayley table quite similar to that of $(\mathbb{Z}/2\mathbb{Z}, +)$!

	$\overline{0}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{0}$

A "historical" use of integers modulo n is credited to the Roman emperor Julius Caesar (100 BC 44 BC), who apparently was communicating with his army generals using what is now called *Caesar's cipher*. A modern way of explaining his cipher is to present it as an encryption scheme e_K defined by

$$e_K(x) = x + K \mod 26,\ K = 3$$

where x is an integer between 0 and 25, corresponding to a letter in the alphabet (for example, 0↦A,...,25↦Z). This is a valid encryption scheme, because it has a decryption function d_K such that $d_K(e_K(x)) = x$ for every integer x mod 26.

Integers mod 4

- Integers mod 4 = { 0,1,2,3} (choice of representatives!)
- Order of the elements?

✓0 has order 1
✓1 has order 4
✓2 has order 2
✓3 has order 4

It is a cyclic group!

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Can you spot a subgroup?

- {0,2} is a subgroup of order 2. It is cyclic!

	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

After studying integers modulo n with respect to addition, we consider multiplication. First, we check that

$$(a \mod n) \cdot (b \mod n) \equiv (a \cdot b) \mod n$$

does not depend on the choice of a representative in $a \mod n$ and $b \mod n$.

Proposition 6. *Suppose that* $a' \equiv a \mod n$ *and* $b' \equiv b \mod n$, *then* $(a' \mod n) \cdot (b' \mod n) \equiv (a \cdot b) \mod n$.

Proof. We write $a' = a+qn$, $b' = b+rn$ and compute $a' \cdot b' = (a+qn)(b+rn) = ab + n(ar + qb + n)$ as needed! □

This operation obeys (1) closure, (2) associativity, and (3) there exists an identity element $\bar{1}$: $\overline{a} \cdot \bar{1} = \overline{a}$. But not every $\overline{a}$ has an inverse! For an inverse $\bar{a}^{-1}$ of $\bar{a}$ to exist, we need $aa^{-1} = 1 + zn$, where $z \in \mathbb{Z}$.

Example 7. If $n = 4$, 2 cannot have an inverse, because 2 multiplied by any integer is even, and thus cannot be equal to $1 + 4z$ which is odd.

To understand when an inverse exists, we will need the *Bézout's Identity*.

Theorem 5. *Let* a, b *be integers, with greatest common divisor* $\gcd(a, b) = d$. *Then there exist integers* m, n *such that*

$$am + bn = d.$$

Conversely, if $am' + bn' = d'$ *for some integers* m', n', *then* d *divides* d'.

Proof. Recall that the Euclidean Algorithm computes $\gcd(a, b)$! Suppose $b < a$. Then we divide a by b giving a quotient q_0 and remainder r_0:

$$a = bq_0 + r_0, \ r_0 < b. \tag{4.1}$$

Next we divide b by r_0: $b = r_0q_1+r_1$, $r_1 < r_0$, and r_0 by r_1: $r_0 = r_1q_2+r_2$, $r_2 < r_1$ and we see the pattern: since $r_{k+1} < r_k$, we divide r_k by r_{k+1}

$$r_k = r_{k+1}q_{k+2} + r_{k+2}, \ r_{k+2} < r_{k+1}. \tag{4.2}$$

Each step gives us a new nonnegative remainder, which is smaller than the previous one. At some point we will get a zero remainder: $r_N = r_{N+1}q_{N+2}+0$.

Caesar's Cipher

To send secrete messages to his generals, Caesar is said to have used the following cipher.

e_K: x → e_K(x)=x+K mod 26, K=3

Map A to 0,…,Z to 25 and decipher this message from Caesar: YHQL YLGL YLFL

It is a well-defined cipher because there is a function d_K such that $d_K(e_K(x))=x$ for every x integer mod 26.

Integers mod n and Multiplication?

Need to check well defined, like for addition!

Are integers mod n a group under multiplication?

- No! not every element is invertible.
- Example: 2 is not invertible mod 4

Etienne Bezout (1730 –1783)

Invertible elements mod n are those integers modulo n which are coprime to n.

Proof. Bezout's identity! There are integers x,y such that ax+ny=gcd(a,n), and if ax'+ny'=d then gcd(a,n)|d.

- If gcd(a,n) =1 → ax+ny =1 for some x,y → ax =1 mod n→ a invertible.
- If a invertible → ax=1 mod n for some x → ax+ny=1 for some y → gcd(a,n)|1 → gcd(a,n)=1

We now show inductively that $d = \gcd(a, b)$ is equal to r_{N+1}. The line (4.1) shows that $\gcd(a, b)$ divides r_0. Hence $\gcd(a, b) \mid \gcd(b, r_0)$. Suppose that $\gcd(a, b) \mid \gcd(r_{N-1}, r_N)$. Since $r_{N-1} = r_N q_{N+1} + r_{N+1}$, we have that $\gcd(r_{N-1}, r_N)$ divides both r_{N+1} and r_N thus it divides $\gcd(r_{N+1}, r_N)$. Thus $\gcd(a, b) | \gcd(r_{N-1}, r_N) | \gcd(r_N, r_{N+1}) = r_{N+1}$. On the other hand, backtracking, we see that r_{N+1} divides a, b: $r_{N+1} \mid r_N$ thus since $r_{N-1} = r_N q_{N+1} + r_{N+1}$, we have $r_{N+1} \mid r_{N-1}, \ldots$

To show Bézout's identity, we write $d = r_{N+1} = r_{N-1} - r_N q_{N+1}$, and substitute for each remainder its expression in terms of the previous remainders

$$r_{k+2} = r_k - r_{k+1} q_{k+2}$$

all the way back until the only terms involved are a, b. This gives that $d = r_{N+1} = am + bn$ for some $m, n \in \mathbb{Z}$, as desired.

Conversely, let d' be a positive integer. Suppose that $am' + bn' = d'$ for some integers m', n'. By definition of greatest common divisor, d divides a and b. Thus there exist integers a', b' with $a = da'$ and $b = db'$, and

$$da'm' + db'n' = d'.$$

Now d divides the two terms of the sum, thus it divides d'. □

We are ready to characterize integers mod n with a multiplicative inverse.

Corollary 1. *The integers mod n which have multiplicative inverses are those which are coprime to n, i.e. , $\{\bar{a}, \mid \gcd(a, n) = 1\}$.*

Proof. If $\gcd(a, n) = 1$, Bézout's identity tells us that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus $ax = 1 + (-y)n$ and $\overline{x}$ is the inverse of a.

Conversely, if there is an $\overline{x}$ such that $\overline{ax} = \bar{1}$ then $ax = 1 + yn \iff ax - yn = 1$ for some $y \in \mathbb{Z}$. By Bézout's identity, we have $\gcd(a, n) \mid 1$, showing that $\gcd(a, n) = 1$. □

The set $(\mathbb{Z}/n\mathbb{Z})^*$ of invertible elements mod n forms a group under multiplication.

Indeed (a) closure holds: $(\overline{a}\overline{b})^{-1} = (\overline{b}^{-1})(\overline{a}^{-1}) \in (\mathbb{Z}/n\mathbb{Z})^*$, (b) associativity holds, (c) the identity element is $\bar{1}$, (d) every element is invertible (we just proved it!).

What is the order of this group?

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \#\{a \in \{0, 1, 2, \ldots, (n-1)\} \mid \gcd(a, n) = 1\} = \varphi(n),$$

where $\varphi(n)$ is a famous function called the Euler totient, which by definition counts the number of positive integers coprime to n.

Group of Invertible modulo n

The set of invertible elements mod n form a group under multiplication.

- This group is closed: the product of two invertible elements is invertible.
- Multiplication is associative, the identity element is 1 (the equivalence class of 1).
- Every element has an inverse.

Its order is the Euler totient function $\varphi(n)$.
By definition it counts how many integers are coprime to n.

Roots of Unity

We call a complex number z an **nth root of unity** if $z^n = 1$.
Thus $z = e^{2i\pi/n}$ is an nth root of unity because $(e^{2i\pi/n})^n = 1$.
A nth root of unity is called **primitive** if n is the smallest positive integer such that $(e^{2i\pi/n})^n = 1$.

Example:
We have that i is a 4rth root of unity, because $i^4 = 1$.
Also -1 is a 4rth root of unity, because $(-1)^4 = 1$.
Now i is primitive, because $i^2 \neq 1$, $i^3 \neq 1$.
But (-1) is not primitive because $(-1)^2 = 1$.

Let us see one more example of a group. From the complex numbers, a very special discrete set is that of nth roots of unity, which by definition is

$$\omega^{(n)} = \{w \in \mathbb{C} \mid w^n = 1\} = \{e^{i\frac{2\pi}{n}k},\ k = 1, 2, \ldots, n\},$$

since $(e^{i\frac{2\pi}{n}k})^n = e^{i2\pi k} = 1$ for any $k \in \mathbb{Z}$. Note that the polynomial $X^n - 1 = 0$ has at most n roots, and we found already n of them, given by $e^{i\frac{2\pi}{n}k}$, $k = 1, \ldots, n$, thus there is no another nth root of unity.

The set $\omega^{(n)}$ of nth roots of unity forms a group under multiplication.

Indeed, (a) closure is satistifed: $e^{i\frac{2\pi}{n}k_1}e^{i\frac{2\pi}{n}k_2} = e^{i\frac{2\pi}{n}(k_1+k_2)} \in \omega^{(n)}$, (b) as is associativity. (c) The identity element is 1. Finally (d) every element in $\omega^{(n)}$ is invertible: $(e^{i\frac{2\pi}{n}k_1})^{-1} = e^{i\frac{2\pi}{n}(-k_1)}$.

We also have commutativity since $e^{i\frac{2\pi}{n}k_1}e^{i\frac{2\pi}{n}k_2} = e^{i\frac{2\pi}{n}(k_1+k_2)} = e^{i\frac{2\pi}{n}k_2}e^{i\frac{2\pi}{n}k_1}$.

An nth root of unity ω is said to be primitive if n is the smallest positive integer for which $\omega^n = 1$. But then, since $\omega^{(n)}$ has n elements, all the nth roots of unity are obtained as a power of ω! For example, take $\omega = e^{i\frac{2\pi}{n}}$ (you may want to think of another example of primitive nth root of unity!), then

$$\{\omega^k = e^{i\frac{2\pi}{n}k},\ k = 1, \ldots, n\} = \omega^{(n)}.$$

We just proved the following:

Proposition 7. *The group $(\omega^{(n)}, \cdot)$ of nth roots of unity is a cyclic group of order n generated by a primitive nth root of unity, e.g. $\omega = e^{i\frac{2\pi}{n}}$.*

Example 8. Consider $(\omega^{(3)}, \cdot) = (\{1, e^{i\frac{2\pi}{3}}, e^{i\frac{2\pi}{3}2}\}, \cdot)$. There are two primitive roots of unity. Set $\omega = e^{i\frac{2\pi}{3}}$. The Cayley table of $(\omega^{(3)}, \cdot)$ is

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

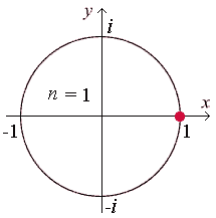
Example 9. Consider $(\omega^{(4)}, \cdot) = (\{1, i, -1, -i\}, \cdot)$, with Cayley table

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

So i is a primitive 4th root of unity since $i \neq 1, i^2 = -1, i^3 = -i, i^4 = 1$ and $\langle i \rangle = \omega^{(4)}$, but -1 is not a primitive root because $(-1)^2 = 1$.

Group Structure of Roots of Unity

- nth roots of unity form a group with respect to multiplication, the identity element is 1 (which is a root of unity!)
- It is an abelian group.
- It has order n.
- It is cyclic, generated by a primitive root!



4rth roots of unity

- i = 4rth primitive root of unity
- The group of 4rth roots of unity is {1, i^2=-1, i^3=-i }

	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-I	1	i
-i	-i	1	i	-1

So far we have seen many examples of groups: integers mod n with addition, invertible integers mod n with multiplication, nth roots of unity with multiplication, $\mathbb{R}$ with addition, $\mathbb{R}^*$ with multiplication, and all those groups we saw as symmetries (that of the square, of the rectangle, of triangles...) with composition. Among them, some were infinite, some were finite, some were cyclic, some not, some of the groups were abelian, some were not.

The time has come ("the Walrus said" ...) to sort things out a bit, and try to "quantify" the similarity or dissimilarity of the group structures we encountered in our "group zoo".

We start here to develop tools for analyzing and classifying group structure. Suppose we are given two groups $(G, \cdot)$ and $(H, *)$ with possibly different sets G, H and respective binary operation $\cdot$ and $*$.

Definition 11. A map $f : G \to H$ which obeys

$$\underbrace{f(\underbrace{g_l \cdot g_k}_{\text{in G}})}_{\text{in H}} = \underbrace{f(g_l) * f(g_k)}_{\text{in H}}, \text{ for all } g_k, g_l \in G$$

is called a group homomorphism.

Recall that a map $f : G \to H$ which takes elements of the set G and pairs them with elements of H is called

- injective or one-to-one, if no two different elements g_1, g_2 of G map to the same $h \in H$, i.e., $f(g_1) \neq f(g_2)$ if $g_1 \neq g_2$.
- surjective or onto if for all $h \in H$, there exists $g \in G$ so that $f(g) = h$.
- bijective if it is both injective and surjective.

Definition 12. If $f : G \to H$ is a group homomorphism and also a bijection, then it is called a group isomorphism. We then say that G and H are isomorphic, written $G \simeq H$.

Maybe it will be easier to remember this word by knowing its origin: iso $\equiv$ same, morphis $\equiv$ form or shape. Let us see a first example of group homomorphism.

Examples of Groups we saw

	law	Identity element	order	abelian
Integers mod n	+	0	n	yes
Invertible integers mod n	*	1	$\varphi(n)$	yes
nth roots of unity	*	1	n	yes
$\mathbb{R}$	+	0	infinite	yes
$\mathbb{R}$ \{0}	*	1	infinite	yes
Symmetries of square	○	Do-nothing	8	no
Symmetries of rectangle	○	Do-nothing	4	Yes
Symmetries of equilateral triangle	○	Do-nothing	6	no
Symmetries of isosceles triangle	○	Do-nothing	2	yes

Time to sort out things!

Let (G,·), (H,*) be two groups. A map f: G →H is called a **group homomorphism** if f(g·h)=f(g)*f(h).

A group homomorphism is a map that preserves the group structure.

A group homomorphism is called **a group isomorphism** if it is a bijection.

If there is a group isomorphism between two groups G and H, then G and H are said to be isomorphic. Two groups which are isomorphic are basically “the same”.

Example 10. Consider the group $(\mathbb{Z}/4\mathbb{Z}, +)$ of integers mod 4, as in Example 6, with Cayley table

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

and the group $(\omega^{(4)}, \cdot)$ of 4rth roots of unity whose Cayley table

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

was computed in Example 9. These two groups are isomorphic, which can be seen on the Cayley tables, because they are the same, up to a change of labels ($1 \leftrightarrow 0$,$i \leftrightarrow 1$,$-1 \leftrightarrow 2$,$-i \leftrightarrow 3$). Formally, we define a map

$$f : (\mathbb{Z}/4\mathbb{Z}, +) \to (\omega^{(4)}, \cdot),\ n \mapsto i^n.$$

It is a group homomorphism, since $f(n+m) = i^{m+n} = i^n i^m = f(n)f(m)$. It is also a bijection: if $f(n) = f(m)$, then $i^n = i^m$ and $n \equiv m \mod 4$, which shows injectivity. The surjectivity is clear (check that every element has a preimage, there are 4 of them to check!)

Example 11. Similarly, we can show that the group $(\mathbb{Z}/4\mathbb{Z}, +)$ is isomorphic to the group of rotations by an angle of $2\pi/4$, whose Cayley table is

	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^3	r^3	1	r	r^2

by considering the map

$$f : (\mathbb{Z}/4\mathbb{Z}, +) \to (\text{rotations of the square}, \circ),\ n \mapsto r^n.$$

It is a group homomorphism, since $f(n+m) = r^{m+n} = r^n r^m = f(n)f(m)$. It is also a bijection: if $f(n) = f(m)$, then $r^n = r^m$ and $n \equiv m \mod 4$, which shows injectivity. The surjectivity is clear as above.

4rth roots of unity vs Integers mod 4

	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-I	1	i
-i	-i	1	i	-1

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The two tables are the same, up to a change of labels: $1 \leftrightarrow 0, i \leftrightarrow 1, -1 \leftrightarrow 2, -i \leftrightarrow 3$

Let us define a map f: {integers mod 4} → {4rth root of unity}, n → i^n

- It is a group homomorphism: $f(n+m) = i^{m+n} = i^m i^n = f(n)f(m)$.
- It is a bijection: if $f(n)=f(m)$ then $i^n = i^m$ → $n=m \bmod 4$ shows injectivity. This is clearly surjective.

Integers mod 4 vs Rotation of 2π/4

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	1	*r*	r^2	r^3
1	*1*	*r*	r^2	r^3
r	*r*	r^2	r^3	*1*
r^2	r^2	r^3	*1*	*r*
r^3	r^3	*1*	*r*	r^2

The two tables are the same, up to a change of labels: $1 \leftrightarrow 0, r \leftrightarrow 1, r^2 \leftrightarrow 2, r^3 \leftrightarrow 3$

Let us define a map f: {integers mod 4} → {rotation of 2π/4}, n → r^n

- It is a group homomorphism: $f(n+m) = r^{m+n} = r^m r^n = f(n)f(m)$.
- It is a bijection: if $f(n)=f(m)$ then $r^n = r^m$ → $n=m \bmod 4$ shows injectivity. This is clearly surjective.

What happened in these two examples is that the three groups considered (the integers mod 4, the 4rth roots of unity, and the rotations of the square) are all cyclic of order 4. As we shall see next, all cyclic groups of a given order are in fact isomorphic. Hence, from a structural point they are the same. We shall call the equivalent (up to isomorphism) cyclic group of order n, or the infinite cyclic group, as respectively

the cyclic group C_n of order n if $n < \infty$, or the infinite cyclic group C_∞ otherwise.

Theorem 6. *Any infinite cyclic group is isomorphic to the additive group of integers $(\mathbb{Z}, +)$. Any cyclic group of order n is isomorphic to the additive group $(\mathbb{Z}/n\mathbb{Z}, +)$ of integers mod n.*

Before starting the proof, let us recall that $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Its order is $|\mathbb{Z}| = \infty$.

Proof. Let G be a cyclic group. Whether it is finite or not, a cyclic group is generated by one of its elements g, i.e., $\langle g \rangle = G$. Define the map

$$\begin{cases} f : \mathbb{Z} \to G, & k \mapsto f(k) = g^k \quad \text{if } |G| = \infty \\ f : \mathbb{Z}/n\mathbb{Z} \to G, & k \mapsto f(k) = g^k \quad \text{if } |G| = n < \infty. \end{cases}$$

Note that $f : \mathbb{Z}/n\mathbb{Z} \to G$ is *well-defined*, since it does not depend on the choice of k as a representative of the equivalence class of $k \mod n$. Indeed, if $k' \equiv k \mod n$, then $k' = k + sn$ for some integer s, and

$$f(k') = f(k + sn) = g^{k+sn} = g^k g^{sn} = g^k.$$

This map is bijective (one-to-one and onto) and

$$f(k + l) = g^{k+l} = g^k \cdot g^l = f(k) \cdot f(l),$$

hence it is a homomorphism that is bijective. It is then concluded that f is an isomorphism between the integers and any cyclic group. □

Example 12. With this theorem, to prove that the integers mod 4, the 4rth roots of unity, and the rotations of the square are isomorphic, it is enough to know that are all cyclic of order 4. Thus

$$C_4 \simeq (\mathbb{Z}/4\mathbb{Z}, +) \simeq (\omega^{(4)}, \cdot) \simeq (\text{rotations of the square}, \circ).$$

The Cyclic Group C_n

- We just saw 3 cyclic groups of order 4, all of them with same multiplication table. They are essentially the "same group", thus to analyze them, there is no need to distinguish them.

Theorem. An infinite cyclic group is isomorphic to the additive group of integers, while a cyclic group of order *n* is isomorphic to the additive group of integers modulo n.

This is also saying that there is exactly one cyclic group (up to isomorphism) whose order is *n*, denoted by C_n and there is exactly one infinite cyclic group.

Proof of Theorem

A cyclic group is generated by one element (multiplicative notation)

Part 1

- Let G be an infinite cyclic group, G=<x>, g of order infinite. Define the map f:{group of integers}→G, $f(n)=x^n$.
- This is a group homorphism: $f(m+n)= x^{n+m} = x^n x^m = f(m)f(n)$.
- This is a bijection, thus we have a group isomorphism.

Part 2

- Let G be a cyclic group of order n, G=<x>, with g of order n. Define the map f:{group of integers mod n}→G, $f(n)= x^n$.
- This is a group homorphism: $f(m+n)= x^{n+m} = x^n x^m = f(m)f(n)$.
- This is a bijection, thus we have a group isomorphism.

We can summarize the cyclic groups encountered so far:

group	C_n	order n
integers mod n $(+)$	C_n	order n
nth roots of unity $(\cdot)$	C_n	order n
rotations of regular polygons with n sides	C_n	order n
symmetries of isosceles triangles	C_2	order 2
$(\mathbb{Z}, +)$	C_∞	infinite order

Now that we know that cyclic groups are all just instances of the abstract cyclic group C_n for some $n \in \mathbb{N}$ or $n = \infty$, we can ask ourselves how much structure exists in C_n as a function of the properties of the number $n \in \mathbb{N}$. This is important, because every instance of C_n will naturally inherit the structure of C_n! We start with the subgroups of C_n.

Theorem 7. *Subgroups of a cyclic group are cyclic.*

Proof. Let $(G, \cdot)$ be a cyclic group, denoted multiplicatively, finite or infinite. By definition of cyclic, there exists an element $g \in G$ so that $G = \langle g \rangle$. Now let H be a subgroup of G. This means that H contains 1. If $H = \{1\}$, it is a cyclic group of order 1. If H contains more elements, then necessarily, they are all powers of g. Let m be the smallest positive power of g that belongs to H, i.e., $g^m \in H$ (and $g, g^2, \ldots, g^{m-1} \notin H$). We must have by closure that $\langle g^m \rangle$ is a subgroup of H. Assume for the sake of contradiction that there exists $g^t \in H, t > m$ and $g^t \notin \langle g^m \rangle$. Then by the Euclidean division algorithm,

$$t = mq + r, \ 0 < r < m - 1.$$

Therefore

$$g^t = g^{mq+r} = g^{mq} g^r \in H,$$

and since g^{mq} is invertible, we get

$$\underbrace{g^{-mq}}_{\in H} \underbrace{g^t}_{\in H} = g^r \Rightarrow g^r \in H.$$

But r is a positive integer smaller than m, which contradicts the minimality of m. This shows that g must belong to $\langle g^m \rangle$ (i.e., $r = 0$) and hence $\langle g^m \rangle$ will contain all elements of the subgroup H, which by definition is cyclic and generated by g. □

Cyclic Groups seen so far

Group	order	C_n
integers mod n	n	C_n
nth roots of unity	n	C_n
Symmetries of the isosceles triangle	2	C_2
Subgroup of rotations of 90 degrees of the square	4	C_4
Subgroup {0,2} of the integers mod 4	2	C_2

Subgroups of a Cyclic Group

Proposition

Subgroups of a cyclic group are cyclic.

A cyclic group is generated by one element (multiplicative notation)

Proof. G is a cyclic group, so G=<x>. Let H be a subgroup of G. If H={1}, then it is cyclic. Otherwise, it contains some powers of x. We denote by m the smallest power of x in H, and $\langle x^m \rangle \leq H$.

Let us assume that there is some other x^i in H, then by minimality of m, i>m, and we can compute the Euclidean division of i by m: $x^i = x^{mq+r}$, $0 \leq r < m$.

$\langle x^m \rangle$ subgroup of H

Thus x^r in H and by minimality of m, r=0, so that $x^i = x^{mq}$ and every element in H is in $\langle x^m \rangle$.

We next study the order of elements in a cyclic group.

Theorem 8. *In the cyclic group C_n, the order of an element g^k where $\langle g\rangle = C_n$ is given by $|g^k| = n/\gcd(n,k)$.*

Proof. Recall first that g has order n. Let r be the order of g^k. By definition, this means that $(g^k)^r = 1$, and r is the smallest r that satisfies this. Now we need to prove that $r = n/\gcd(n,k)$, which is equivalent to show that (1) $r|\frac{n}{\gcd(n,k)}$ and (2) $\frac{n}{\gcd(n,k)}|r$.

Step 1. We know that $g^{kr} = 1$ and that g has order n. By definition of order, $kr \geq n$. Suppose that $kr > n$, then we apply the Euclidean division algorithm, to find that

$$kr = nq + s,\ 0 \leq s < n \Rightarrow g^{kr} = g^{nq}g^s = g^s \in G$$

and s must be zero by minimality of n. This shows that $\boxed{n \mid rk}$.

Step 2. Using

$$\gcd(n,k)|n \text{ and } \gcd(n,k)|k,$$

with $n|kr$, we get $\boxed{\frac{n}{\gcd(n,k)}|\frac{k}{\gcd(n,k)}r.}$

Step 3. But $\gcd(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}) = 1$ from which we obtain $\boxed{\frac{n}{gcd(n,k)}|r}$ which conclude the proof of (2)! We are now left with (1), namely show that r must divide $n/\gcd(n,k)$.

Step 4. Note that

$$(g^k)^{n/\gcd(n,k)} = (g^n)^{k/\gcd(n,k)} = 1.$$

Now we know that r is the smallest integer that satisfies $(g^k)^r = 1$ thus $n/\gcd(n,k) \geq r$, and using again the Euclidean division algorithm as we did in Step 1, we must have that

$$\frac{n}{\gcd(n,k)} = qr + s \Rightarrow (g^k)^{\frac{n}{\gcd(n,k)}} = (g^k)^{qr+s}, \quad 0 \leq s < r.$$

This would imply

$$1 = 1 \cdot g^s \Rightarrow s = 0.$$

Hence $\boxed{r|\frac{n}{gcd(n,k)}.}$ □

Example 13. The order of 1 is $|1| = |g^n| = \frac{n}{\gcd(n,n)} = 1$, and the order of g is $|g| = \frac{n}{\gcd(n,1)} = n$.

Order of Elements in a Cyclic Group

Proposition. Let G be a cyclic group of order n, generated by g. Then the order of g^k is $|g^k|=n/\gcd(n,k)$.

Order is the smallest positive integer r such that $(g^k)^r$ is 1

Before we start the proof, let us check this statement makes sense!

Recall that G is cyclic generated by g means that $G=\{1, g, g^2,\ldots, g^{n-1}\}$, and $g^n=1$.

- ✓ If k =n, then $g^k = g^n =1$ and n/gcd(n,k)=n/n=1 thus |1|=1.
- ✓ If k=1, then $g^k =g$ and n/gcd(n,k)=n thus |g|=n.

Proof of the Proposition

- Given g^k, we have to check that its order r is n/gcd(k,n). This is equivalent to show that r| n/gcd(k,n) and n/gcd(k,n) | r.
- Step 1 : g^k has order r means $g^{kr} = 1$, which implies n | kr.

n is the smallest integer such that $g^n =1$, thus if $g^{kr} =1$, kr>n and by Euclidean division, $kr =nq+s$, $0 \le s<n$. But then $1=g^{kr}= g^{nq+s} = g^s$ showing that s=0 my minimality of n.

- Step 2: gcd(k,n) |k and gcd(k,n)|n thus n/gcd(k,n) | (k/ gcd(k,n))r.
- Step 3 : n/gcd(k,n) and k/gcd(k,n) are coprime thus n/gcd(k,n)|r.
- Step 4: only left to show that r | n/gcd(k,n). But $(g^k)^{n/\gcd(k,n)}=1$ thus r | n/gcd(k,n) [if you understood Step 1, this is the same argument!]

Combining the fact that a cyclic group of order n has cyclic subgroups generated by its elements $\{g^k\}$, and the fact that the orders of these elements are $|g^k| = n/\gcd(n,k)$, we can prove one more result regarding the order of subgroups in a cyclic group.

Theorem 9. *The order of a (cyclic) subgroup of a group C_n divides the order of the group.*

Proof. We have seen in Theorem 7 that if $G = \langle g \rangle$ and H is a subgroup of G, then

$$H = \langle g^m \rangle$$

for some m. We have also seen in Theorem 8 that $|g^m|$ is $n/\gcd(n,m)$, hence $|H| = |g^m| = \frac{n}{\gcd(n,m)}$. Now by definition,

$$\frac{n}{\gcd(n,m)} | n.$$

□

The beauty of these results is that they apply to every instance of the cyclic group C_n. One may work with the integers mod n, with the nth roots of unity, or with the group of rotations of a regular polygon with n sides, it is true for all of them that

- all their subgroups are cyclic as well,
- the order of any of their elements is given by Theorem 8,
- and the size of every of their subgroups divides the order of the group.

If we think of the type of searches we did in the first chapters, where we were looking for subgroups in the Cayley tables, it is now facilitated for cyclic groups, since we can rule out the existence of subgroups which do not divide the order of the group!

Order of Subgroups in a Cyclic Group

- We have seen: every subgroup of a cyclic group is cyclic, and if G is cyclic of order n generated by g, then g^k has order n/gcd(k,n).
- What can we deduce on the order of subgroups of G?

•Let H be a subgroup of G. Then H is cyclic by the first result.
•Since H is cyclic, it is generated by one element, which has to be some power of g, say g^k.
•Thus the order of H is the order of its generator, that is n/gcd(n,k).

In particular, the order of a subgroup divides the order of the group!

Examples

Thus these results apply to all the cyclic groups we have seen:

- nth roots of unity
- integer mod n
- rotations of 2π/n

Example 14. Let us see how to use Theorem 8, for example with 4rth roots of unity. We know that $-1 = i^2$, thus $n = 4$, $k = 2$, and the order of -1 is

$$\frac{n}{\gcd(n,k)} = \frac{4}{2} = 2,$$

as we know!

Example 15. Let us see how to use Theorem 8, this time with the integers mod 4. Let us be careful here that the notation is additive, with identity element 0. Recall that the integers mod 4 are generated by 1. Now assume that we would like to know the order of 3 mod 4. We know that $k = 3$ and $n = 4$, thus

$$\frac{n}{\gcd(n,k)} = \frac{4}{1} = 4,$$

and indeed

$$3{+}3 = 6 \equiv 2 \mod 4,\ 3{+}3{+}3 = 9 \equiv 1 \mod 4,\ 3{+}3{+}3{+}3 = 12 \equiv 0 \mod 12.$$

This might not look very impressive because these examples are small and can be handled by hand, but these general results hold no matter how big C_n is!

Let us summarize briefly what happened in this chapter. In the first half, we showed that we already know in fact more groups than we thought! The list includes the integers modulo n with addition, the invertible integers modulo n with multiplication, the roots of unity, etc

We then decided to start to classify a bit all these groups, thanks to the notion of group isomorphism, a formal way to decide when two groups are essentially the same! We then showed that there is only one cyclic group C_n, of which the integers mod n, the nth roots of unity,..., are particular instances. We then took a closer look at C_n, and studied its subgroups, the order of its elements, and the order of its subgroups.

4rth root of unity

- We saw that i is a primitive root, thus it generates the cyclic group of 4rth roots of unity.
- To determine the order of -1, we notice that $-1= i^2$.
- Now we only need to compute n/gcd(n,k)=4/gcd(4,2)=2.

Integers mod 4

- What is the order of 3 mod4 ?
- We recall that the integers mod 4 are generated by 1.
- Thus 3=k, n=4, and we compute n/gcd(k,n)=4/gcd(3,4)=4.

Exercises for Chapter 4

Exercise 16. We consider the set $\mathbb{C}$ of complex numbers.

1. Is $\mathbb{C}$ a group with respect to addition?
2. Is $\mathbb{C}$ a group with respect to multiplication?
3. In the case where $\mathbb{C}$ is a group, what is its order?
4. Can you spot some of its subgroups?

Exercise 17. Alice and Bob have decided to use Caesar's cipher, however they think it is too easy to break. Thus they propose to use an affine cipher instead, that is

$$e_K(x) = k_1 x + k_2 \mod 26,\ K = (k_1, k_2).$$

Alice chooses $K = (7, 13)$, while Bob opts for $K = (13, 7)$. Which cipher do you think will be the best? Or are they both equally good?

Exercise 18. Show that the map $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot),\ x \mapsto \exp(x)$ is a group homomorphism.

Exercise 19. Show that a group homomorphism between two groups G and H always maps the identity element 1_G to the identity element 1_H.

Exercise 20. In this exercise, we study a bit the invertible integers modulo n.

1. Take $n = 5$, and compute the group of invertible integers modulo 5. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the groups we have already classified?)
2. Take $n = 8$, and compute the group of invertible integers modulo 8. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the groups we have already classified?)

Exercise 21. Let f be a group homomorphism $f : G \to H$ where G and H are two groups. Show that

$$f(g^{-1}) = f(g)^{-1}.$$