Chapter 5

More Group Structures

> *"The theory of groups is a branch of mathematics in which one does something to something and then compares the results with the result of doing the same thing to something else, or something else to the same thing. Group theory lets you see the similarities between different things, or the ways in which things can't be different, by expressing the fundamental symmetries."(J. Newman, Mathematics and the Imagination.)*

In the 4 previous chapters, we saw many examples of groups, coming from planar isometries and from numbers. In Chapter 4, we started to classify a bit some of our examples, using the notion of group isomorphism. The goal of this chapter is to continue this classification in a more systematic way!

What happened in Examples 10 and 11 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 $|\mathbb{Z}| = \infty$.

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.

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

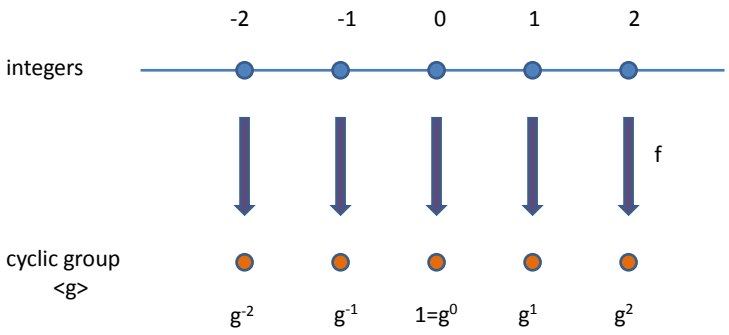
$$C_4 \simeq (\mathbb{Z}/4\mathbb{Z}, +) \simeq (\omega^{(4)}, \cdot) \simeq (\text{rotations of the square}, \circ).$$

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.

Idea of the Proof



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

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. □

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 $\boxed{n \mid rk}$.

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 $\langle x^m \rangle$.

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 $|g|=n$.

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 $|g| = \frac{n}{\gcd(n,1)} = n$.

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,

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

□

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, $kr = nq+s$, $0 \leq s < n$. 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!]

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!

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!

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!

Examples

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

- nth roots of unity
- integer mod n
- rotations of $2\pi/n$

4rth root of unity/ Integers mod 4

- 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.

- 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.

We will now start thinking the other way round! So far, we saw many examples, and among them, we identified several instances of the cyclic group C_n (integers mod n with addition, nth roots of unity with multiplication, rotations of regular polygons with n sides...). We also saw that C_n exists for every positive integer n. Surely, there are more groups than cyclic groups, because we know that the group of symmetries of the equilateral triangle seen in the exercises (let us call it D_3 where 3 refers to the 3 sides of the triangle) and the group of symmetries of the square (let us call it D_4, where 4 again refers to the 4 sides of the square) are not cyclic, since they are not abelian! (and we proved that a cyclic group is always abelian...) The "D" in D_3 and D_4 comes from the term "dihedral".

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	
2	C_2	
3	C_3	
4	C_4	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4

The next natural question is: what are possible other groups out there? To answer this question, we will need more tools.

Definition 13. Let $(G, \cdot)$ be a group and let H be a subgroup of G. We call the set

$$gH = \{gh | h \in H\}$$

a left coset of H.

We have that gH is the set of elements of G that we see when we multiply (i.e., combine using the group operation $\cdot$) the specific element $g \in G$ with all the elements of H. Similarly, a right coset of H is given by

$$Hg = \{hg | h \in H\}.$$

If the group is not abelian, there is a need to distinguish right and left cosets, since they might not be the same set!

Classification so far

Find more groups: either we look for some other examples, or for some more structure!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	
3	C_3	
4	C_4	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4
infinite	$\mathbb{R}$	

More Structure: Cosets

Let G be a group, and H a subgroup of G.

The set gH={gh, h in H} is called a **left coset** of H.

The set Hg={hg, h in H} is called a **right coset** of H.

The operation used is the binary operation of the group!

For example: take G to be the dihedral group D_4, and $H=\langle r\rangle=\{1,r,r^2,r^3\}$. Then $\langle r\rangle m=\{m,rm,r^2m,r^3m\}$ is a right coset of H.

It might help to think of a coset as a "translation of a subgroup H" by some element g of the group.

Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The coset $1 + H$ is $1 + H = \{1, 3\}$.

Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The coset Hm is $Hm = \{m, rm, r^2m, r^3m\}$.

Let us see a few properties of cosets.

Lemma 2. *Let G be a group, and H be a subgroup.*

1. *For every $g \in G$, $g \in gH$ and $g \in Hg$.*
2. *We have $gH = H$ if and only if $g \in H$.*

Proof. 1. Since H is a subgroup, $1 \in H$, hence $g \cdot 1 \in gH$ that is $g \in gH$. Similarly $1 \cdot g \in Hg$ showing that $g \in Hg$.

2. Suppose first that $g \in H$. Then gH consists of elements of H, each of them multiplied by some element g of H. Since H is a subgroup, $gh \in H$ and $gH \subset H$. To show that $H \subseteq gH$, note that

$$g^{-1}h \in H \Rightarrow g(g^{-1}h) \in gH \Rightarrow h \in gH$$

for every $h \in H$!
Conversely, if $gH = H$, then $gh \in H$ for every h, and $g \cdot 1 \in H$.

□

The next lemma tells us when two cosets are the same set!

Lemma 3. *Let G be a group with subgroup H. Then*

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H,\ g_1, g_2 \in G.$$

Proof. If $g_1H = g_2H$, then $\{g_1h | h \in H\} = \{g_2h | h \in H\}$ and there exists an $h \in H$ such that $g_1h = g_2 \cdot 1$, which shows that $h = g_1^{-1}g_2 \in H$.

Conversely, if $g_1^{-1}g_2 \in H$, then $g_1^{-1}g_2 = h \in H$ and $g_2 = g_1h$ which shows that $g_2H = g_1hH = g_1H$, where the last equality follows from the above lemma. □

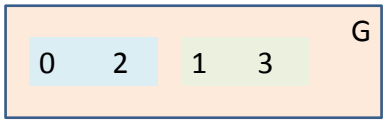
How to Visualize Cosets?

Write a left coset using the additive notation of the binary operation of the group, that is

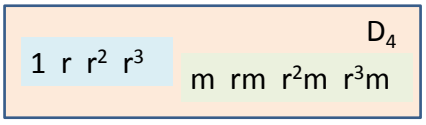
$g+H=\{g+h, h \text{ in } H\}$.

Then a coset of H can be seen as a translation of H!

G= {0,1,2,3} integers modulo 4
H={0,2} is a subgroup of G.
The coset 1+H = {1,3}.



$D_4 = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}$
$H=<r>=\{1,r,r^2,r^3\}$ subgroup of G.
The coset $<r>m=\{m,rm,r^2m,r^3m\}$



Same Cosets?

Again G= {0,1,2,3} integers modulo 4, with subgroup H={0,2}.

All cosets of H: 0+H={0,2}, 1+H = {1,3},2+H={0,2},3+H={3,1} .

Some cosets are the same! When does it happen?

Lemma. We have $g_1H=g_2H$ if and only if $g_1^{-1}g_2$ is in H.

Proof. If $g_1H=g_2H$ then $g_1 \cdot 1 = g_2h$ that is $h^{-1} = g_1^{-1}g_2$ which shows that $g_1^{-1}g_2$ is in H.

H is a subgroup!

Conversely, if $g_1^{-1}g_2$ is in H, then $g_1^{-1}g_2 = h$ for some h in H, and $g_2 = g_1h$ which shows that $g_2H = g_1hH = g_1H$.

We next show that cosets of a given subgroup H of G have the property of partitioning the group G. This means that G can be written as a disjoint union of cosets! That

$$G = \bigcup gH$$

comes from the fact that g runs through every element of G (and $g \in gH$), thus the union of all cosets gH will be the group G. To claim that we have a partition, we need to argue that this is a disjoint union, namely that cosets are either identical or disjoint.

Proposition 8. *Let G be a group with subgroup H, and let g_1, g_2 be two elements of G. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.*

Proof. If the intersection of g_1H and g_2G is empty, we are done. So suppose there exists an element g both in g_1H and in g_2H. Then

$$g = g_1h = g_2h'$$

thus

$$g_1hH = g_2h'H \Rightarrow g_1H = g_2H,$$

using Lemma 2. □

Example 18. We continue Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The cosets of H are $1 + H = \{1, 3\}$ and $0 + H = \{0, 2\}$. We have

$$G = (1 + H) \cup (0 + H).$$

Example 19. . We continue Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The cosets of H are $Hm = \{m, rm, r^2m, r^3m\}$ and $H = \{1, r, r^2, r^3\}$. We have

$$D_4 = Hm \cup H.$$

We need a last property of cosets before proving a fundamental theorem of group theory!

Cosets partition the Group!

Let G be a group, with subgroup H, and take *all the cosets gH* of H.

Since g takes every value in G, and H contains 1, the union of all cosets is the whole group: $G = \bigcup gH$.

We now prove that two cosets g_1H and g_2H are either identical or disjoint!

Suppose there exists an element g both in g_1H and in g_2H, then $g = g_1h = g_2h'$. Thus $g_1hH = g_1H = g_2h'$ $H = g_2H$.

Cosets partition the Group: Examples

G= {0,1,2,3} integers modulo 4

H={0,2} is a subgroup of G.

The coset 1+H = {1,3}.

G

0 2 1 3

G = {0,2} U {1, 3} = H U (1+H)

$D_4 = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}$

H=<r>={1,r,r^2,r^3} subgroup of G.

The coset <r>m={m,rm,r^2m,r^3m}

D_4

1 r r^2 r^3

m rm r^2m r^3m

$D_4 = \{1,r,r^2,r^3\} \cup \{m\ rm\ r^2m\ r^3m\}$
$= \langle r \rangle \cup \langle r \rangle m$

Proposition 9. *Let G be a group with subgroup H. Then*

$$|H| = |gH|,\ g \in G.$$

In words, cosets of H all have the same cardinality.

Proof. To prove that the two sets H and gH have the same number of elements, we define a bijective map (one-to-one correspondence) between their elements. Consider the map:

$$\lambda_g : H \to gH, h \mapsto \lambda_g(h) = gh.$$

This map is injective (one to one): indeed

$$\lambda_g(h_1) = \lambda_g(h_2) \Rightarrow gh_1 = gh_2$$

and since g is invertible, we conclude that $h_1 = h_2$.

This map is surjective (onto): indeed, every element in gH is of the form gh, and has preimage h. □

Example 20. We continue Example 22. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. We have

$$\begin{aligned} |1 + H| &= |\{1, 3\}| = 2 \\ |H| &= |\{0, 2\}|. \end{aligned}$$

Example 21. We continue Example 23. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. We have

$$\begin{aligned} |Hm| &= |\{m, rm, r^2m, r^3m\}| = 4, \\ |H| &= |\{1, r, r^2, r^3\}|. \end{aligned}$$

We are finally ready for Lagrange Theorem!

Cardinality of a Coset

We have $|gH|=|H|$ (the cardinality of a coset of H is the cardinality of H).

The two sets gH and H are in bijection.
Indeed, consider the map $\lambda_g: H \to gH$, that sends h to gh.

- for every gh in gH, there exists a preimage, given by h.
- if two elements h and h' are mapped to the same element, then gh=gh', and it must be that h=h'.

Both steps rely on g being invertible!

Cardinality of a Coset: Examples

G= {0,1,2,3} integers modulo 4
H={0,2} is a subgroup of G.

G
0 2 1 3

| H |= |1+H| =2

$D_4 = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}$
$H = \langle r \rangle = \{1, r, r^2, r^3\}$ subgroup of G.

D_4
1 r r^2 r^3
m rm r^2m r^3m

$|\langle r \rangle| = |\langle r \rangle m|$

Theorem 10. *Let G be a group and H be a subgroup of G. Then*

$$|G| = [G : H]|H|$$

where $[G : H]$ is the number of distinct left (or right) cosets of H in G. If $|G|$ is finite, then

$$[G : H] = \frac{|G|}{|H|}$$

and $|H|$ divides $|G|$.

Note that this also shows that the number of distinct left or right cosets is the same. It is called the index of H in G.

Proof. We know that the cosets of H partition G, that is

$$G = \bigcup_{k=1}^{r} g_k H,$$

where $r = [G : H]$ is the number of distinct cosets of H.

We have also seen that $|gH| = |H|$ in Proposition 9, i.e., all the cosets have the same cardinality as H. Therefore

$$|G| = \sum_{k=1}^{r} |g_k H| = r|H| = [G : H]|H|.$$

□

Example 22. We finish Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The cosets of H are $1 + H = \{1, 3\}$ and $0 + H = \{0, 2\}$. Then $[G : H] = 2$ and

$$|G| = [G : H]|H| = 2|H| = 4.$$

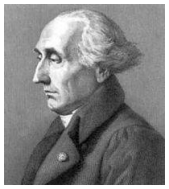
Example 23. . We also finish Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The cosets of H are $Hm = \{m, rm, r^2m, r^3m\}$ and $H = \{1, r, r^2, r^3\}$. Then $[G : H] = 2$ and

$$|D_4| = [G : H]|H| = 2|H| = 8.$$

Lagrange Theorem

The number of cosets of H in G is called **the index of H in G** , denoted by **[G:H]**.

Lagrange Theorem. Let G be a group, then $|G| = [G:H]\,|H|$. If $|G|<\infty$, then $|G|/|H| = [G:H]$ that is **the order of a subgroup divides the order of the group**.



Joseph Louis Lagrange (1736 – 1813)

Proof. The cosets of H partition G, thus $|G| = \Sigma\,|gH|$. Since $|gH|=|H|$, we have $|G| = \Sigma\,|H|$, and thus $|G|=|H|\cdot$(number of terms in the sum)$= |H|\,[G:H]$.

Lagrange Theorem: Examples

G= {0,1,2,3} integers modulo 4
H={0,2} is a subgroup of G.

G
0 2 1 3

$|G|=4= [G:H]|H|=2\cdot 2$

$D_4 = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}$
$H=\langle r\rangle=\{1,r,r^2,r^3\}$ subgroup of G.

D_4
$1\ r\ r^2\ r^3$
$m\ rm\ r^2m\ r^3m$

$|D_4|=8 = [G:H]|H|=2\cdot 4$

Lagrange Theorem has many consequences.

Corollary 2. *Let G be a finite group. For any $g \in G$, the order $|g|$ of g divides the order of the group $|G|$.*

Proof. Consider the subgroup of G generated by g:

$$\langle g \rangle = \{g, g^2, \cdots, g^{|g|} = 1\}.$$

The order of this subgroup is $|g|$. Hence by Lagrange Theorem, we have

$$|g| \text{ divides } |G|.$$

□

This for example explains why the group of symmetries of the square contains only elements of order 1,2, and 4!

Corollary 3. *A group of prime order is cyclic.*

Proof. Let G be a group of order p, for a prime p. This means elements of G can only have order 1 or p. If g is not the identity element, then g has order p, which shows that G is cyclic. □

Let us now go back to our original question about finding new groups. What we just learnt is that if the order is a prime, then there is only the cyclic group C_p. Thus (boldface means that the classification is over for this order):

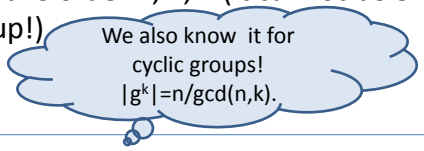
order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	**x**
2	C_2	**x**
3	C_3	**x**
4	C_4	
5	C_5	**x**
6	C_6	D_3
7	C_7	**x**
8	C_8	D_4

Corollary 1of Lagrange Theorem

Corollary. Let G be a finite group. The order of an element of G divides the order of the group.

Proof. Let g be an element of G. Then H=<g> is a subgroup of G, with order the order of g (by definition of cyclic group!). Since the order of H divides |G|, the order of g divides |G|.

Example. D_4 ={1, r,r^2,r^3,m,rm,r^2m,r^3m}.
Since |D_4 |=8, elements of D_4 have order 1, 2, 4 (it cannot be 8 because this is not a cyclic group!)



Corollary 2 of Lagrange Theorem

Corollary. If |G| is a prime number, then G is a cyclic group.

Proof. If |G| is a prime number p, then we know that the order of an element must divide p, and thus it must be either 1 or p, by definition of prime number. Thus every element g which is not the identity has order p, and G=<g>.

Example. If |G|=3, then G must be the cyclic group C_3.

Since we cannot find any new group of order 2 or 3, let us look at order 4.

We can use a corollary of Lagrange Theorem that tells us that in a group of order 4, elements can have only order 1, 2 or 4.

- If there exists an element of order 4, then we find the cyclic group C_4.
- If there exists no element of order 4, then all elements have order 2 apart the identity. Thus we have a group $G = \{1, g_1, g_2, g_3\}$. Let us try to get the Cayley table of this group. For that, we need to know whether $g_1 g_2$ is the same thing as $g_2 g_1$...But $g_1 g_2$ is an element of G by closure, thus it has order 2 as well:

  $$(g_1 g_2)^2 = g_1 g_2 g_1 g_2 = 1 \Rightarrow g_1 g_2 = g_2^{-1} g_1^{-1}.$$

  But now, because every element has order 2

  $$g_1^2 = 1 \Rightarrow g_1^{-1} = g_1, \ g_2^2 = 1 \Rightarrow g_2^{-1} = g_2$$

  and we find that

  $$g_1 g_2 = g_2 g_1.$$

  Furthermore, $g_1 g_2$ is an element of G, which cannot be 1, g_1 or g_2, thus it has to be g_3.

Let us write the Cayley table of the group of order 4 which is not cyclic.

	1	g_1	g_2	$g_1 g_2$
1	1	g_1	g_2	$g_1 g_2$
g_1	g_1	1	$g_1 g_2$	g_2
g_2	g_2	$g_1 g_2$	1	g_1
$g_1 g_2$	$g_1 g_2$	g_2	g_1	1

We recognize the table of the symmetries of the rectangle! This group is also called *the Klein group*.

Classification so far

Find more groups: either we look for some other examples, or for some more structure: nothing new for prime orders!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	x
4	C_4	
5	C_5	x
6	C_6	D_3
7	C_7	x
8	C_8	D_4
infinite	$\mathbb{R}$	

Order 4

- By Lagrange Theorem, a group of order 4 has elements with order 1,2 or 4.
- If there exists an element of order 4, this is C_4!
- If not, all elements different than the identity are of order 2…

Take g_1, g_2 in G={1, g_1, g_2, g_3} thus g_1g_2 is in G and $(g_1g_2)(g_1g_2)=1$! This implies $g_1g_2=g_2^{-1}g_1^{-1}=g_2g_1$ and g_1 commute with g_2 !

	1	g_1	g_2	$g_3=g_1g_2$
1	1	g_1	g_2	g_3
g_1	g_1	1	g_3	g_2
g_2	g_2	g_3	1	g_1
$g_3=g_1g_2$	g_3	g_2	g_1	1

This is the Klein Group!

We can update our table of small groups:

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	**x**
2	C_2	**x**
3	C_3	**x**
4	C_4, Klein group	**x**
5	C_5	**x**
6	C_6	D_3
7	C_7	**x**
8	C_8	D_4

Good news: we have progressed in our list of small groups, but we still have not found a group which is not a group of symmetries (up to isomorphism!). We will get back to this question in the next chapter. For now, let us see a few more applications of Lagrange Theorem.

Corollary 4. *Let G be a finite group. Then*

$$g^{|G|} = 1$$

for every $g \in G$.

Proof. We have from Lagrange Theorem that $|g| \mid |G|$, thus $|G| = m|g|$ for some integer m and hence:

$$g^{|G|} = (g^{|g|})^m = 1^m = 1.$$

□

Classification so far

Find more groups: either we look for some other examples, or for some more structure: nothing new for order 4!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	x
4	C_4, Klein group	x
5	C_5	x
6	C_6	D_3
7	C_7	x
8	C_8	D_4
infinite	$\mathbb{R}$	

Corollary 3 of Lagrange Theorem

Corollary. If $|G|$ is finite, then $g^{|G|}=1$.

Proof. We know that the order of an element must divide $|G|$, thus the order of g, say $|g|=k$, must divide $|G|$, that is $|G|=km$ for some m. Then $g^{|G|} = g^{km} = (g^k)^m=1$.

Example. If $G=D_4$, then $r^8=1$ (in fact $r^4=1$) and $m^8=1$ (in fact $m^2=1$).

We continue and prove a result from number theory, known as Euler Theorem.

Theorem 11. *Let a and n be two integers. Then*

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

if $\gcd(a, n) = 1$.

Proof. If $\gcd(a, n) = 1$, then a is invertible modulo n, and we know that the order of the group of integers mod n under multiplication is $\varphi(n)$. By the previous result

$$a^{|G|} = a^{\varphi(n)} \equiv 1 \mod n.$$

□

Finally, another nice theorem from number theory is obtained, called **Fermat little theorem**.

Corollary 5. *For every integer a and every prime p, we have $a^p \equiv a \mod p$.*

Proof. Just replace n by a prime p in Euler Theorem, and recall that $\varphi(p) = p - 1$ by definition of $\varphi(p)$. □

The key result of this chapter is really Lagrange Theorem! Thanks to this result and its corollaries, we have learnt a lot about the structure of a group: (1) that the order of a subgroup always divides the order of the group, (2) that the order of an element always divides the order of the group. We also obtained some partial classification of groups of small orders: we showed that for every order we have a cyclic group, and that all the groups we have seen so far are isomorphic to groups of symmetries!

The group structure of integers modulo n, and that of invertible elements modulo n are important in practice in the areas of coding theory and cryptography. A famous example coming from cryptography is the cryptosystem called RSA.

Corollary 4 of Lagrange Theorem

Euler Theorem. We have that $a^{\varphi(n)} = 1 \bmod n$ if gcd(a,n)=1.

Proof. Take G the group of invertible elements mod n. We know that its order is $\varphi(n)$, because a is invertible mod n if and only if gcd(a,n)=1. We also know that $a^{|G|} = 1$ by the previous corollary!

Leonhard Euler
(1707 – 1783)

Corollary 5 of Lagrange Theorem

Little Fermat Theorem. We have $a^{p-1} = 1 \bmod p$ for $a \neq 0$.

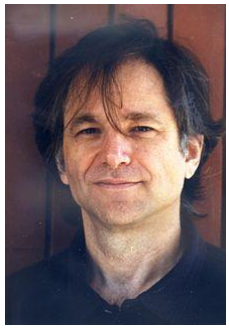
Proof. Take n=p a prime in Euler Theorem.

Pierre de Fermat
(1601 –1665)

Application of Euler Theorem: RSA

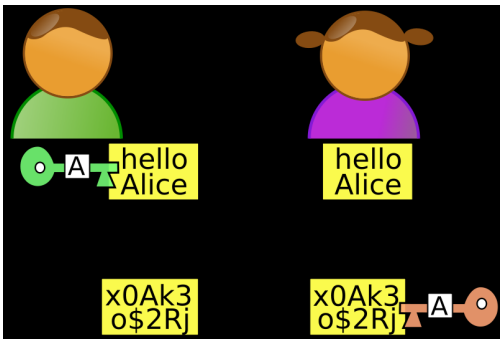
RSA is an encryption scheme discovered by River, Shamir and Adleman (in 1978).



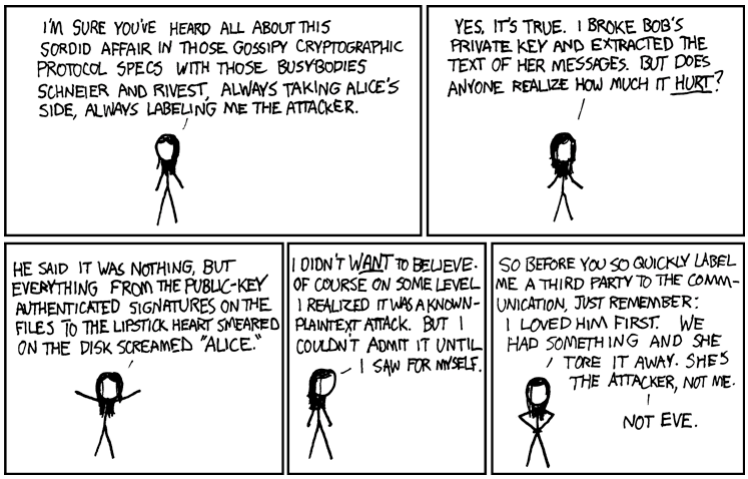


Alice and Bob Story

Alice and Bob want to exchange confidential data in the presence of an eavesdropper Eve.



Alice and Bob story by xkcd



RSA Protocol (I)

- Select two distinct large primes p and q ("large" means 100 digits ☺).
- Compute n=pq.
- The Euler totient function of n is $\varphi(n)$ = (p-1)(q-1).

This function counts the integers coprime to n.

- Pick an odd integer e such that e is coprime to $\varphi(n)$.
- Find d such that ed = 1 modulo $\varphi(n)$.

e exists because it is coprime to the Euler totient function!

Publish e and n as public keys, keep d private.

RSA Protocol (II)

- Alice: public key = (n,e), d is private.
- Bob sends m to Alice via the following encryption: $c = m^e \bmod n$.
- Alice decrypts: $m = c^d \bmod n$.

Why can Alice decrypt?

Step 1 $c^d \bmod n = (m^e)^d \bmod n$.

Step 2 We have $ed = 1 + k\varphi(n)$.

Step 3 Now $(m^e)^d \bmod n = m^{1+k\varphi(n)} = m \bmod n$ when m is coprime to n.

Exercises for Chapter 5

Exercise 29. Let G be a group and let H be a subgroup of G. Let gH be a coset of H. When is gH a subgroup of G?

Exercise 30. As a corollary of Lagrange Theorem, we saw that the order of an element of a group G divides $|G|$. Now assume that d is an arbitrary divisor of $|G|$. Is there an element g in G with order d?

Exercise 31. Take as group G any group of order 50. Does it contain an element of order 7?

Exercise 32. Take as group G the Klein group of symmetries of the rectangle. Choose a subgroup H of G, write G as a partition of cosets of H, and check that the statement of Lagrange Theorem holds.

Exercise 33. This exercise looks at Lagrange Theorem in the case of an infinite group. Take as group $G = \mathbb{R}$ and as subgroup $H = \mathbb{Z}$. Compute the cosets of H and check that the cosets of H indeed partition G. Also check that the statement of Lagrange Theorem holds.