

# MA294 Lecture

Timothy Kohl

Boston University

July 3, 2025

## Other basic facts about groups:

### Proposition

Let  $x, y, z, a, b$  be elements of a group  $(G, *)$  then

$$x * y = x * z \rightarrow y = z \text{ (left cancellation)}$$

$$a * x = b * x \rightarrow a = b \text{ (right cancellation)}$$

### Proof.

$$x * y = x * z$$

$$x^{-1} * x * y = x^{-1} * x * z \text{ (Note, we multiply both sides on the left.)}$$

$$e * y = e * z$$

$$y = z$$

A similar argument works for the other statement. □

These 'cancellation' rules imply the following.

## Proposition

*The Cayley table for a group  $(G, *)$  is a latin square.*

Why? If we look at a row of the Cayley table:

*		$y$	$\dots$	$z$
$x$		$x * y$		$x * z$

we cannot have  $x * y = x * z$  unless  $y = z$  by left cancellation so there are no repeats in a given row.

And for columns:

*		$x$	...	
$a$		$a * x$		
$b$		$b * x$		

we find that  $a * x = b * x$  only if  $a = b$  so there are no repeated elements in a column.

# The Order of a Group Element

## Definition

In a group  $(G, *)$  if  $a \in G$  and  $n \geq 1$  is an integer, then

$$a^n = \underbrace{a * a * \cdots * a}_{n\text{-times}}$$

That is  $a^1 = a$ ,  $a^2 = a * a$ ,  $a^3 = a * a * a$ , and similar to how one defines  $a^0$  for a *number*, we define  $a^0 = e$ , the identity of  $G$ .

And the use of the notation ' $a^{-1}$ ' for the inverse, fits in with this definition, since

$$a^{-1} * a = a^{-1} * a^1 = a^{(-1)+1} = a^0 = e$$

and similarly, we may define  $a^{-n}$  to be  $a^{-1} * a^{-1} * \cdots * a^{-1} = (a^{-1})^n$ . That is, exponents in groups, work like they do for numbers.

Notation Alert: If  $*$ ='+' like in  $\mathbb{Z}$  or  $\mathbb{Z}_m$  then instead of writing

$$a^n = a * a * \cdots a$$

we write

$$na = a + a + \cdots + a$$

so that, for example, if  $2 \in \mathbb{Z}_5$  we have  $3 \cdot 2 = 2 + 2 + 2 = 6 = 1$ .

An important, yet not so obvious point is that for any  $a \in G$  and any  $n$  the power  $a^n \in G$  by the closure property.

The simplest way to see this is by noting that

$$a^n = \underbrace{a * a * \cdots * a}_{(n-1)\text{-times}} * a$$

namely  $a^{n-1} * a$ .

So if we assume that  $a^{n-1} \in G$  then  $a^{n-1} * a \in G$  so  $a^n \in G$ .

And the same holds for negative powers.

Other examples:

In  $D_3$ , we have

$$r_{120}^0 = r_0$$

$$r_{120}^1 = r_{120}$$

$$r_{120}^2 = r_{120} \circ r_{120} = r_{240}$$

$$r_{120}^3 = r_{120}^2 \circ r_{120} = r_{240} \circ r_{120} = r_0 \text{ [Why?]}$$

$$r_{120}^4 = r_{120}^3 \circ r_{120} = r_0 \circ r_{120} = r_{120} \text{ [Note: We're back at } r_{120}\text{]}$$

$$r_{120}^{-1} = r_{240}$$

$$r_{120}^{-2} = r_{120}$$

$$r_{120}^{-3} = r_0$$



For the flips like  $f_1$ , the powers are a bit simpler

$$f_1^0 = r_0$$

$$f_1^1 = f_1$$

$$f_1^2 = r_0$$

$$f_1^3 = f_1$$

$$f_1^{-1} = f_1$$

And in  $\mathbb{Z}_6$  we have

$$0 \cdot 2 = 0$$

$$1 \cdot 2 = 2$$

$$2 \cdot 2 = 2 + 2 = 4$$

$$3 \cdot 2 = 2 + 2 + 2 = 0$$

$$4 \cdot 2 = 2 + 2 + 2 + 2 = 2$$

$$(-1) \cdot 2 = (-2) = 4$$

$$(-2) \cdot 2 = (-4) = 2$$

etc...

The discussion of powers of elements leads naturally to the concept of 'order' of an element.

### Definition

If  $x \in G$  where  $G$  is finite, then the order of  $x$  is the least positive integer  $m$  such that  $x^m = e$ , in which case we write  $|x| = m$ .

If  $G$  is infinite, then it's possible that  $x, x^2, x^3, \dots$  are all distinct (non-identity) elements of  $G$ , in which case we say that  $x$  has infinite order and we write  $|x| = \infty$ .

Note, if  $G$  is infinite, (as a set) it's still possible that it has elements of finite order, there are many possibilities.

Examples:

For  $2 \in \mathbb{Z}_6$  we have  $1 \cdot 2 = 2$ ,  $2 \cdot 2 = 4$  and  $3 \cdot 2 = 0$  and so  $|2| = 3$ .

In  $D_3$ ,  $|r_{120}| = 3$  since  $r_{120}^2 = r_{240}$  and  $r_{120}^3 = r_{360} = r_0$

In contrast,  $|f_1| = 2$  since  $f_1^2 = r_0$ .

For the element  $1 \in \mathbb{Z}$  we have the multiples  $1, 1+1=2, 1+1+1=3, \dots$  none of which *ever* equals 0, so 1 has infinite order.

Note, for any group  $G$ , the identity element  $e$  has order 1, and it is the unique element of order 1.

## Consequences of Order

If  $x \in G$  has order  $m$  then  $x^{2m} = (x^m)^2 = e^2 = e$ , and similarly  $x^{3m} = e$  etc.

### Theorem

If  $x \in G$  and  $|x| = m$  then  $x^t = e$  if and only if  $m|t$ .

### Proof.

Suppose  $x^t = e$ , where  $t$  is *not* a multiple of  $m$  then by the division algorithm  $t = qm + r$  where  $r \in \{1, \dots, m-1\}$  (i.e  $r \neq 0$ ) which means  $x^t = x^{qm+r} = x^{qm}x^r$ .

But  $x^{qm} = (x^m)^q = e$  so we have that  $x^t = x^r$  but then since  $x^t = e$  then  $x^r = e$ .

However, since  $r < m$  this contradicts the fact that  $|x| = m$ , which is the *least* positive power of  $x$  which is the identity.  $\square$

What can happen is that for some groups  $G$ , there is an  $x \in G$  such that  $G = \{e, x, x^2, \dots, x^{m-1}\}$  and one says that  $x$  *generates*  $G$ .

Also, we sometimes use the notation of '1' for the identity which is consistent with the usual view of raising a number to the zero-th power being 1, i.e.  $x^0 = 1$ , so that if  $G$  is generated by  $x$ , it consists of  $\{1, x, x^2, \dots, x^{m-1}\}$  if  $|x| = m$ .

If  $G$  is generated by  $x$  then we write  $G = \langle x \rangle$ , and we sometimes say  $G$  is a *cyclic* group since the powers of  $x$  'cycle' through these distinct powers, i.e.

$$1, x, x^2, \dots, x^{m-1}, x^m = 1, x^{m+1} = x, x^{m+2} = x^2, \dots \text{ etc.}$$

If  $G$  is infinite, then it's possible that for some element  $x$  one has that  $G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ .

How does this work?

Well, it simply means that each non-zero power of  $x$  is not the identity of  $G$ , so that  $G$  consists of

$$\{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = 1, x^1 = x, x^2, x^3, \dots\}$$

in which case we say that  $G$  is an infinite cyclic group.

The prime example of this is  $\mathbb{Z} = \langle 1 \rangle$  since every element of  $\mathbb{Z}$  is a multiple of 1.

In fact, we can use this idea to actually *define* an infinite group consisting of powers of  $x$ .

For  $x$  a 'variable' (symbol, whatever), one can define 'the' infinite cyclic group

$$C_{\infty} = \{x^n \mid n \in \mathbb{Z}\}$$

with the group operation being based on the rules of exponents, namely:

$$x^i * x^j = x^{i+j}$$

which is very naturally closed, and associative since

$$x^i * (x^j * x^k) = x^i * x^{j+k} = x^{i+j+k}$$

which is the same as  $(x^i * x^j) * x^k = x^{i+j} * x^k$ .



Moreover, it contains an identity element  $1 = x^0$  since clearly  $x^0 * x^i = x^i$  and  $x^i * x^0 = x^i$ , and similarly every element  $x^i$  has inverse  $x^{-i}$ .

If you've observed that the operations in  $C_\infty$  mirror those of the integers, you are correct, but the interesting contrast is that  $C_\infty$  is 'multiplicative' while  $\mathbb{Z}$  is an additive group.

# Group Isomorphisms

Observe that in parallel, in  $\mathbb{Z}$  one has  $m \cdot 1 + n \cdot 1 = (m + n) \cdot 1 = m + n$  and in  $C_\infty$  we have  $x^m \cdot x^n = x^{m+n}$ , i.e. the exponents in  $C_\infty$  add together just as the integers do in  $\mathbb{Z}$ .

## Definition

If  $(G_1, *_1)$  and  $(G_2, *_2)$  are groups, then a bijection  $\beta : G_1 \rightarrow G_2$  is an isomorphism if one has

$$\beta(g *_1 h) = \beta(g) *_2 \beta(h)$$

for all  $g, h \in G_1$ , and we call such a bijection  $\beta$  an isomorphism and write  $G_1 \cong G_2$  and say  $G_1$  and  $G_2$  are isomorphic. (iso=same, morph=form)

Recall that a bijection  $\beta : G_1 \rightarrow G_2$  is a function which is 1-1, namely that  $\beta(x) = \beta(y)$  implies  $x = y$  and onto, namely that for every  $z \in G_2$  there exists  $x \in G_1$  such that  $\beta(x) = z$ .

An isomorphism is therefore a bijection which 'respects' the group structures in both groups, so that, in some way, the groups  $G_1$  and  $G_2$  are equivalent (although not necessarily equal) as groups.

Our first example has already been explored but let's make it official.

$$(\mathbb{Z}, +) \cong (C_\infty, \cdot)$$

by virtue of the function  $\beta : \mathbb{Z} \rightarrow C_\infty$  given by  $\beta(m) = x^m$ .

We can verify that  $\beta$  is a bijection.

If  $\beta(m) = \beta(n)$  then  $x^m = x^n$  which means

$$x^m \cdot x^{-n} = x^n x^{-n}$$

$$\downarrow$$

$$x^{m-n} = x^0 = 1$$

$$\downarrow$$

$$m - n = 0$$

$$\downarrow$$

$$m = n$$

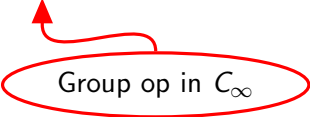
And that  $\beta : \mathbb{Z} \rightarrow C_\infty$  is onto is pretty obvious.

As to respecting the two group structures, observe that

$$\beta(m+n) = x^{m+n} = x^m \cdot x^n = \beta(m) \cdot \beta(n)$$



Group op in  $\mathbb{Z}$



Group op in  $C_\infty$

and so  $\beta$  is a group isomorphism.

And just as we defined  $C_\infty$  as an infinite group consisting of distinct powers  $\{x^i\}$  we can also define *the finite cyclic group of order (size)  $m$*  for any  $m > 1$ .

### Definition

Let  $C_m = \{1, x, \dots, x^{m-1}\}$  with group operation  $x^i \cdot x^j = x^{i+j \bmod m}$ , namely add the exponents mod  $m$ .

For example  $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$  where, for instance,  $x^3 \cdot x^4 = x^7 = x^1$  since  $7 \equiv 1 \pmod{6}$ , and where,  $x^{-i}$  is  $x^{m-i} = x^{6-i}$ , e.g.  $x^{-2} = x^4$ .

And the following is not unexpected.

### Theorem

*The map  $\beta : (\mathbb{Z}_m, +) \rightarrow (C_m, \cdot)$  given by  $\beta(i) = x^i$  is an isomorphism of groups, namely  $(\mathbb{Z}_m, +) \cong (C_m, \cdot)$ .*

Beyond cyclic groups, there are examples of groups that can be constructed by combining different groups together.

## Definition

Given groups  $(G_1, *_1)$  and  $(G_2, *_2)$  their direct product is the group defined on the set  $G_1 \times G_2 = \{(a, b) \mid a \in G_1 \text{ and } b \in G_2\}$  where the group operation is defined as follows:

$$(a, b) * (x, y) = (a *_1 x, b *_2 y)$$

namely the group operations in each coordinate are those of the individual  $G_i$ .



For example, the identity of  $G_1 \times G_2$  is  $(e_1, e_2)$  where  $e_i$  is the identity of  $G_i$  since  $(a, b) * (e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b)$ .

Also,  $(a, b)^{-1} = (a^{-1}, b^{-1})$  since

$$\begin{aligned}(a, b) * (a^{-1}, b^{-1}) &= (a * a^{-1}, b * b^{-1}) \\ &= (e_1, e_2)\end{aligned}$$

Note, if for a group  $G$  we define  $|G|$  to be the size of  $G$  as a set, then if  $|G_1|$  and  $|G_2|$  are finite then it's pretty clear that

$$|G_1 \times G_2| = |G_1| \cdot |G_2|$$

which means that we can create groups of different sizes from smaller groups by joining them in a direct product.

The nature of the direct product is not always so obvious, but at least we can work out the details if we know the structure of each 'component'.

Example: Let  $C_2 = \{1, x\}$  the cyclic group of order 2 and let  $C_3 = \{1, y, y^2\}$  be the cyclic group of order 3.

We use the symbol 'y' in  $C_3$  to prevent confusion with the 'x' in  $C_2$ .

So  $x^2 = 1$  and  $y^3 = 1$  and therefore

$$C_2 \times C_3 = \{(1, 1), (1, y), (1, y^2), (x, 1), (x, y), (x, y^2)\}$$

is a group with 6 elements.

So what is the nature of this group?

i.e. Is this group isomorphic to a group we *know*?

Again, the multiplication in  $C_2 \times C_3$  is 'coordinate-wise', for example  $(x, y)(1, y^2) = (x \cdot 1, y \cdot y^2) = (x, 1)$ , and  $(x, y)^{-1} = (x^{-1}, y^{-1}) = (x, y^2)$ .

CLAIM:  $C_2 \times C_3 \cong C_6$

How?

The key observation we want to make is that  $C_6$ , being cyclic, is generated by a single element of order 6, namely  $C_6 = \langle z \rangle = \{1, z, z^2, z^3, z^4, z^5\}$ , specifically every element is a power of a *single element*.

Define

$$\beta : C_6 = \{1, z, \dots, z^5\} \rightarrow C_2 \times C_3 = \{(1, 1), (1, y), (1, y^2), (x, 1), (x, y), (x, y^2)\}$$

by  $\beta(z) = (x, y)$ . (What does this mean?)

Defining  $\beta(z) = (x, y)$  implies that

$$\beta(z^2) = \beta(z \cdot z) = \beta(z)\beta(z) = (x, y)(x, y) = (x^2, y^2) = (1, y^2).$$

Keeping going in this direction we have

$$\beta(z^3) = \beta(z^2 \cdot z) = \beta(z^2) \cdot \beta(z) = (1, y^2)(x, y) = (x, y^3) = (x, 1).$$

Keeping going we get  $\beta(z^4) = \beta(z^3)\beta(z^1) = (x, 1)(x, y) = (1, y)$ , and  $\beta(z^5) = (x, y^2)$ .

That is,  $\beta(z) = (x, y)$  implies  $\beta(z^k) = (x, y)^k$ , and it follows that  $\beta$  is 1-1 and onto.

Given that  $2 \cdot 3 = 6$ , this example makes one wonder if  $C_m \times C_n \cong C_{mn}$ ?

The answer is, not generally, except in the following case.

### Theorem

$C_m \times C_n \cong C_{mn}$  if and only if  $\gcd(m, n) = 1$ .

### Proof.

(Sketch - The book has the full proof.)

If  $C_m = \langle x \rangle$  and  $C_n = \langle y \rangle$  where  $\gcd(m, n) = 1$  then one can prove that  $|(x, y)| = mn$ . (Exercise!)

As such, if  $C_{mn} = \langle z \rangle$  one can define  $\beta : C_{mn} \rightarrow C_m \times C_n$  by  $\beta(z) = (x, y)$  which is 1-1 and onto and preserves the group structure, because if  $\beta(z) = (x, y)$  then  $\beta(z^i) = (x, y)^i = (x^i, y^i)$ . □

For perspective, let's consider the group  $C_2 \times C_2$  which we can represent as  $\mathbb{Z}_2 \times \mathbb{Z}_2$  which is actually the usual way this group is examined.

As  $\mathbb{Z}_2 = \{0, 1\}$  then let  $V = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ .

This group is *not* isomorphic to  $\mathbb{Z}_4$ , in particular because

$$\mathbb{Z}_4 = \langle 1 \rangle = \{0, 1, 1 + 1, 1 + 1 + 1\}$$

while in contrast,  $V$  is not generated by a single element, since  $(1, 0) + (1, 0) = (0, 0)$ ,  $(0, 1) + (0, 1) = (0, 0)$ , and  $(1, 1) + (1, 1) = (0, 0)$ . That is, every element except the identity has order 2.

$V$  is called the Klein-4 group (Vierergruppe), although there are several 'versions' of this group, which are all isomorphic, but this one is fairly concrete.