

# **PMATH 347: Groups and Rings**

University of Waterloo  
William Slofstra  
Spring 2021

Marco Yang

Last updated: June 8, 2021

# Contents

## 1 Groups

1	<b>Binary operations and definition of a group</b> .....	2
	Binary operations	
	Associative operations	
	Commutative (abelian) operations	
	Identities	
	Inverses	
	Properties of inverses	
	Inverses and solving equations	
	Left and right cancellation property	
	Groups	
	A non-abelian example	
	Additive notation	
	Multiplication table	
	Order of elements	
2	<b>Dihedral and permutation groups</b> .....	18
	Dihedral groups	
	Special elements of $D_{2n}$	
	Putting rotation and reflection together	
	What's group theory about?	
	Permutation groups	
	Permutations	
	Fixed points and support sets	
	Commuting elements	
	Cycles	

## 2 Subgroups and homomorphisms

3	<b>Subgroups</b> .....	29
	Subgroups	
	Speeding up the subgroup check	
	Finite subgroups	

	Subgroups generated by a set	
	Lattice of subgroups	
<b>4</b>	<b>Cyclic groups</b> .....	<b>37</b>
	Generators and cyclic groups	
	Order of cyclic groups	
	Examples in closer detail	
	Generators of $\mathbb{Z}/n\mathbb{Z}$	
	Order of elements in $\mathbb{Z}/n\mathbb{Z}$	
	Subgroups of $\mathbb{Z} \bmod n\mathbb{Z}$	
	Proofs later	
<b>5</b>	<b>Homomorphisms</b> .....	<b>45</b>
	Homomorphisms	
	Making new homomorphisms from old	
	Images of homomorphisms	
	Properties of images	
	Pulling back subgroups	
	The kernel of a homomorphism	
	Application: subgroups of cyclic groups	
	Review on bijections	
	Isomorphisms	
	Isomorphism as a relation	
	Isomorphisms of cyclic groups	
	Multiplicative notation for cyclic groups	

### **3 Cosets, Lagrange's Theorem, and Products**

<b>6</b>	<b>Cosets and Lagrange's Theorem</b> .....	<b>61</b>
	Affine spaces	
	Cosets in the dihedral group	
	Sets of cosets	
	Cosets of a kernel	
	Indexes and Lagrange's theorem	
	Consequences of Lagrange's theorem	
	Beginning to prove Lagrange's theorem	
	Partitions	
	Proof of Lagrange's theorem	
	Equivalence relations	
	Equivalence classes	
<b>7</b>	<b>Normal subgroups</b> .....	<b>75</b>
	When is a left coset a right coset?	
	Conjugation and set multiplication	
	Equivalent characterizations of normal subgroups	
	Warning: normal subgroups are not transitive	
	Normalizers	

	Centres	
<b>8</b>	<b>Product groups</b> .....	<b>82</b>
	Getting more groups	
	Two subgroups of a product	
	Homomorphisms between products	
	Groups of small order (revised)	
	How do we know if a group is a product?	
	Unique factorizations	
	Internal (direct) products	
	A weaker condition	

## **4 Quotients and the Isomorphism Theorems**

<b>9</b>	<b>Quotient groups</b> .....	<b>93</b>
	Left cosets and functions	
	Quotient groups	
	Normal subgroups are kernels	
	Examples of quotient groups	
<b>10</b>	<b>First isomorphism and correspondence theorems</b> .....	<b>99</b>
	Homomorphisms from quotients	
	Comparison to universal property of products	
	Proving the universal property of quotients	
	The first isomorphism theorem	
	Images and pullbacks	
	Subgroup correspondence for isomorphisms	
	Set operation identities	
	Set operation identities for surjections	
	The set of pullbacks in $\text{Sub}(G)$	
	Correspondence theorem for quotient groups	
	Identifying $q(K)$	
<b>11</b>	<b>Second and third isomorphism theorems</b> .....	<b>111</b>
	Third isomorphism theorem	
	What if $K$ isn't normal?	
	Revisiting products	
	Second isomorphism theorem	

## **Week 1: Groups**

# 1: Binary operations and definition of a group

## Binary operations

### Definition — binary operation

A **binary operation** on a set  $X$  is a function  $b: X \times X \rightarrow X$ .

Notation:

- We can use any letter ( $b, m$ ) or symbol ( $+$ ,  $\cdot$ ).
- We can use function notation (typically for symbols)

$$b: X \times X \rightarrow X : (x, y) \mapsto b(x, y)$$

or inline notation (typically for letters)

$$+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (x, y) \mapsto x + y.$$

- Some symbols:  $a + b$ ,  $a \times b$ ,  $a \cdot b$ ,  $a \circ b$ ,  $a \oplus b$ ,  $a \otimes b$ ,  $a \odot b$ ,  $a \diamond b$ ,  $a * b$ ,  $a \bullet b$ ,  $a \boxplus b$ ,  $a \boxtimes b$ .
- If not ambiguous, can drop the symbol:

$$X \times X \rightarrow X : (a, b) \mapsto ab.$$

### Example

- Addition  $+$  is a binary operation on  $\mathbb{N}$ , but subtraction  $-$  is not since  $a - b$  is not necessarily in  $\mathbb{N}$ .
- Subtraction is a binary operation on  $\mathbb{Z}$ , *i.e.*, it defines a function  $-: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ .
- If  $(V, +, \cdot)$  is a vector space over a field  $\mathbb{K}$ , then  $+$  is a binary operation on  $V$ , but  $\cdot$  is not since  $\cdot$  is a function  $\mathbb{K} \times V \rightarrow V$ .

### Definition — $k$ -ary operation

A  **$k$ -ary operation** on a set  $X$  is a function

$$\underbrace{X \times X \times \cdots \times X}_{k \text{ times}} \rightarrow X.$$

A 1-ary operation is called a **unary operation**.

**Example**

- Negation  $\mathbb{Z} \rightarrow \mathbb{Z} : x \mapsto -x$  is a unary operation.
- Taking the multiplicative inverse  $x \mapsto 1/x$  is not a unary operation on  $\mathbb{Q}$ , since  $1/0$  is not defined, but it is a unary operation on

$$\mathbb{Q}^\times := \{a \in \mathbb{Q} : a \neq 0\}.$$

## Associative operations

### Definition — associative

A binary operation  $\boxtimes: X \times X \rightarrow X$  is **associative** if

$$a \boxtimes (b \boxtimes c) = (a \boxtimes b) \boxtimes c$$

for all  $a, b, c \in X$ .

Many operations mentioned so far are associative:

- Addition and multiplication for  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , polynomials, and functions;
- Vector addition, matrix addition and multiplication;
- Modular addition and multiplication on  $\mathbb{Z}/n\mathbb{Z}$ ;
- Function composition (homework).

Subtraction and division are not associative:

$$10 - (5 - 1) = 6 \neq 4 = (10 - 5) - 1.$$

Subtraction is adding negative numbers; similarly for division. So we aren't as interested in subtraction and division, thus we can focus on associative operations.

A **bracketing** of a sequence  $a_1, \dots, a_n \in X$  is a way of inserting brackets into  $a_1 \boxtimes \dots \boxtimes a_n$  so that the expression can be evaluated (with binary steps).

### Example

Bracketings of  $a_1, \dots, a_4$  are:

- $a_1 \boxtimes (a_2 \boxtimes (a_3 \boxtimes a_4))$
- $a_1 \boxtimes ((a_2 \boxtimes a_3) \boxtimes a_4)$
- $(a_1 \boxtimes a_2) \boxtimes (a_3 \boxtimes a_4)$
- $(a_1 \boxtimes (a_2 \boxtimes a_3)) \boxtimes a_4$
- $((a_1 \boxtimes a_2) \boxtimes a_3) \boxtimes a_4$

### Proposition

A binary operation  $\boxtimes: X \times X \rightarrow X$  is associative if and only if for all finite sequences  $a_1, \dots, a_n \in X$  with  $n \geq 1$ , every bracketing of  $a_1, \dots, a_n$  evaluates to the same element of  $X$ .



Meaning if  $\boxtimes$  is associative, then the notation  $a_1 \boxtimes \cdots \boxtimes a_n$  is unambiguous.

*Proof.*

( $\Leftarrow$ ) The two bracketings  $a \boxtimes (b \boxtimes c)$  and  $(a \boxtimes b) \boxtimes c$  of  $a, b, c$  evaluate to the same element of  $X$  for all sequences of length 3. So  $\boxtimes$  is associative by definition.

( $\Rightarrow$ ) By induction. Base cases are  $n = 1, 2, 3$ . For  $n = 1, 2$ , there is only one bracketing. For  $n = 3$ , follows from the definition of associativity.

Suppose the proposition is true for all sequences of length  $1 \leq k < n$ .

Let  $w$  be a bracketing of  $a_1, \dots, a_n$ . Then  $w = w_1 \boxtimes w_2$  where  $w_1$  is a bracketing of  $a_1, \dots, a_k$  and  $w_2$  is a bracketing of  $a_{k+1}, \dots, a_n$  for some  $k < n$ . By induction,

$$\begin{aligned} w_1 &= (\cdots ((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \\ w_2 &= (a_{k+1} \boxtimes \cdots (a_{n-2} \boxtimes (a_{n-1} \boxtimes a_n)) \cdots) \end{aligned}$$

So by repeatedly applying associativity,

$$\begin{aligned} w &= (\cdots ((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \boxtimes (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots) \\ &= (\cdots (a_1 \boxtimes a_2) \cdots \boxtimes a_{k-1}) \boxtimes (a_k \boxtimes (a_{k+1} \boxtimes \cdots \boxtimes a_n) \cdots) \\ &= \cdots \\ &= (a_1 \boxtimes (a_2 \boxtimes \cdots (a_{n-1} \boxtimes a_n)) \cdots) \end{aligned}$$

□

## Commutative (abelian) operations

### Definition — commutative (abelian)

A binary operation  $\boxtimes: X \times X \rightarrow X$  is **commutative** or **abelian** if  $a \boxtimes b = b \boxtimes a$  for all  $a, b \in X$ .

Many familiar operations are commutative:

- Addition and multiplication on  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$
- Vector and matrix addition
- Modular addition and multiplication on  $\mathbb{Z}/n\mathbb{Z}$

The following operations are **not** commutative:

- Subtraction and division:  $3 - 1 \neq 1 - 3$
- Function composition
- Matrix multiplication

Note:

1. Subtraction and division are not commutative or associative
2. Function composition and matrix multiplication are not commutative, but are associative

We won't study operations like (1), but we are interested in those like (2).

The first half of this course is group theory: single associative operation, not necessarily commutative.

The second half of this course is ring theory: two associative operations, focus on the both commutative case.

## Identities

### Definition — identity

Let  $\boxtimes$  be a binary operation on a set  $X$ . An element  $e \in X$  is an **identity** for  $\boxtimes$  if

$$e \boxtimes x = x \boxtimes e = x$$

for all  $x \in X$ .

### Example

- The zero element 0 of  $\mathbb{Z}$  is an identity for  $+$ , since  $0 + x = x + 0 = x$  for all  $x \in \mathbb{Z}$ .
- $1 \in \mathbb{Q}$  is an identity for  $\cdot$ , since  $1 \cdot x = x \cdot 1 = x$  for all  $x \in \mathbb{Q}$ .
- $0 \in \mathbb{Q}$  is not an identity for  $\cdot$ , since  $0 \cdot x = 0 \neq x$  for all  $x \in \mathbb{Q}$ .

### Lemma

If  $e, e' \in X$  are both identities for  $\boxtimes$ , then  $e = e'$ .

### Proof.

$$e = e \boxtimes e' = e'.$$

□

## Inverses

### Definition — inverse

Let  $\boxtimes$  be a binary operation on  $X$  with an identity element  $e$ . An element  $y$  is a **left inverse** for  $x$  (with respect to  $\boxtimes$ ) if  $y \boxtimes x = e$ , a **right inverse** if  $x \boxtimes y = e$ , and an **inverse** if  $x \boxtimes y = y \boxtimes x = e$ .

### Example

- $-n$  is an inverse for  $n \in \mathbb{Z}$  with respect to  $+$ , since  $n + (-n) = (-n) + n = 0$ .
- $n \in \mathbb{Z}$  does not have an inverse with respect to  $\cdot$  unless  $n = \pm 1$ .
- If  $x \in \mathbb{Q}$  is non-zero, then  $1/x$  is an inverse of  $x$  with respect to  $\cdot$ . The element  $0$  does not have an inverse, since there is no element  $y$  with  $0 \cdot y = 1$ .

### Lemma

Let  $\boxtimes$  be an associative binary operation with an identity  $e$ . If  $y_L$  and  $y_R$  are left and right inverses of  $x$  respectively, then  $y_L = y_R$ .

### Proof.

$$y_L = y_L \boxtimes e = y_L \boxtimes (x \boxtimes y_R) = (y_L \boxtimes x) \boxtimes y_R = e \boxtimes y_R = y_R.$$

□

Corollaries:

- If  $x$  has both a left and a right inverse, then  $x$  has an inverse.
- Inverses are unique: if  $y$  and  $y'$  are both inverses of  $x$ , then  $y = y'$ .

An element  $a$  is **invertible** if it has an inverse, in which case the inverse is denoted by  $a^{-1}$ .

### Exercise

Show it is possible to have a left (resp. right) inverse, but not be invertible. Also show left and right inverses are not necessarily unique (unless an element has both).

## Properties of inverses

### Lemma

1. If  $\boxtimes$  has an identity  $e$ , then  $e$  is invertible, and  $e^{-1} = e$ .
2. If  $a$  is invertible, then so is  $a^{-1}$ , and  $(a^{-1})^{-1} = a$ .
3. If  $\boxtimes$  is associative, and  $a$  and  $b$  are invertible, then so is  $a \boxtimes b$ , and  $(a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$ .

### *Proof.*

1.  $e \boxtimes e = e$ .
2.  $a \boxtimes a^{-1} = a^{-1} \boxtimes a = e$ , so  $a$  is an inverse to  $a^{-1}$ .
3.  $(a \boxtimes b) \boxtimes (b^{-1} \boxtimes a^{-1}) = a \boxtimes (b \boxtimes b^{-1}) \boxtimes a^{-1} = a \boxtimes e \boxtimes a^{-1} = a \boxtimes a^{-1} = e$ , and similarly  $(b^{-1} \boxtimes a^{-1}) \boxtimes (a \boxtimes b) = e$ .

□

## Inverses and solving equations

### Proposition

Let  $\boxtimes$  be an associative binary operation on  $X$  with an identity  $e$ , and let  $x$  and  $y$  be variables taking values in  $X$ .

An element  $a \in X$  is invertible if and only if the equations  $a \boxtimes x = b$  and  $y \boxtimes a = b$  have unique solutions for all  $b \in X$ .

### Proof.

( $\Leftarrow$ ) A solution to  $a \boxtimes x = e$  is a right inverse of  $a$ , and a solution to  $y \boxtimes a = b$  is a left inverse. Since both solutions exist,  $a$  has an inverse.

( $\Rightarrow$ ) Suppose  $a$  is invertible. Then

$$a \boxtimes (a^{-1} \boxtimes b) = (a \boxtimes a^{-1}) \boxtimes b = e \boxtimes b = b$$

so  $a^{-1} \boxtimes b$  is a solution to  $a \boxtimes x = b$ .

If  $x_0$  is a solution to  $a \boxtimes x = b$ , then

$$a^{-1} \boxtimes b = a^{-1} \boxtimes (a \boxtimes x_0) = (a^{-1} \boxtimes a) \boxtimes x_0 = e \boxtimes x_0 = x_0$$

so  $a^{-1} \boxtimes b$  is the unique solution to  $a \boxtimes x = b$ .

Similarly,  $b \boxtimes a^{-1}$  is the unique solution to  $y \boxtimes a = b$ .

□

## Left and right cancellation property

### Proposition

Let  $\boxtimes$  be an associative binary operation and let  $a \in X$ . Then:

1. If  $a$  has a left inverse and  $a \boxtimes u = a \boxtimes v$ , then  $u = v$ .
2. If  $a$  has a right inverse and  $u \boxtimes a = v \boxtimes a$ , then  $u = v$ .

### *Proof.*

1.  $u = a_L \boxtimes a \boxtimes u = a_L \boxtimes a \boxtimes v = v$ .
2. Similar.

□

(1) and (2) also hold for  $n \in \mathbb{Z}$  with respect to  $\cdot$  if  $n \neq 0$ , even though  $n$  is not invertible for  $n \neq \pm 1$ .

## Groups

### Definition — group

A **group** is a pair  $(G, \boxtimes)$  where

1.  $G$  is a set, and
2.  $\boxtimes$  is an associative binary operation on  $G$  such that
  - (a)  $\boxtimes$  has an identity  $e$ , and
  - (b) every element  $g \in G$  is invertible with respect to  $\boxtimes$ .

A group is **abelian** (or **commutative**) if  $\boxtimes$  is abelian.

A group is **finite** if  $G$  is a finite set. The **order** of  $G$  is the number of elements in  $G$  if  $G$  is finite, or  $+\infty$  if  $G$  is infinite.

The order of  $G$  is denoted by  $|G|$ .

Terminology:

- Usually we refer to  $(G, \boxtimes)$  simply as  $G$ , and just assume the operation is given. (Note: we still need to clearly specify the operation for each group we work with.)
- It's cumbersome to write  $\boxtimes$ , so usually we use one of the following options:
  - Use  $\cdot$  as the standard symbol:  $g \cdot h$  is the product of  $g, h \in G$ .
  - Drop the symbol entirely:  $gh$  is the product of  $g, h \in G$ .
- The identity of  $G$  is denoted by  $e$  (or  $e_G$  for clarity). Also used are  $1$  and  $1_G$ .
- $g^{-1}$  is defined for all  $g \in G$ . The function  $G \rightarrow G : g \mapsto g^{-1}$  can be regarded as a unary operation on  $G$ .
- Consider  $\iota : G \rightarrow G : g \mapsto g^{-1}$ . Since  $(g^{-1})^{-1} = g$ ,  $\iota \circ \iota = \text{Id}_G$ , the identity map  $G \rightarrow G$ . In particular,  $\iota$  is a bijection (injective and surjective).
- If  $g \in G$ , then

$$g^n := \underbrace{g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} := (g^{-1})^n = (g^n)^{-1}$$

where  $g^0 := e$ . Exercise: if  $m, n \in \mathbb{Z}$ , then  $(g^n)^m = g^{mn}$ .

- If  $g, h \in G$ , then

$$(gh)^n = gh \cdots gh,$$

which is not necessarily the same as  $g^n h^n$  if  $G$  is not abelian.



**Example**

- $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  are all (abelian) groups under operation  $+$ . The identity is 0 and the inverse of  $n$  is  $-n$ . These groups have infinite order.
- $\mathbb{Z}/n\mathbb{Z}$  is also a group under  $+$  (and also abelian). The identity is  $0 = [0]$  and the inverse of  $[m]$  is  $-[m] = [-m]$ . This group is finite with order  $|\mathbb{Z}/n\mathbb{Z}| = n$ .
- If  $(V, +, \cdot)$  is a vector space, then  $(V, +)$  is a group. The identity is 0 and the inverse of  $v$  is  $-v$ .
- $\mathbb{Z}$  is not a group with respect to  $\cdot$ , since most elements do not have an inverse.
- $\mathbb{Q}$  is also not a group with respect to  $\cdot$ , since 0 does not have an inverse.
- $\mathbb{Q}^\times$  is a group with respect to  $\cdot$ .
- Every group has to contain at least one element, the identity. So the simplest possible group is 1 with operation  $1 \cdot 1 = 1$ . This is the **trivial group**.

## A non-abelian example

All the previous examples are abelian.

Let  $\text{GL}_n(\mathbb{K})$  denote the invertible  $n \times n$  matrices over a field  $\mathbb{K}$ .

### Proposition

$\text{GL}_n(\mathbb{K})$  is a group under matrix multiplication (called the **general linear group**).  
For  $n \geq 2$ ,  $\text{GL}_n(\mathbb{K})$  is non-abelian.

### *Proof.*

If  $A$  and  $B$  are invertible matrices, then  $AB$  is also invertible, so matrix multiplication is an associative binary operation on  $\text{GL}_n(\mathbb{K})$ . The identity matrix is an identity and every element has an inverse by definition, so  $\text{GL}_n(\mathbb{K})$  is a group.

Exercise: find matrices  $A, B$  such that  $AB \neq BA$ . □

## Additive notation

Standard notation for a group operation is  $gh$ . This is called **multiplicative notation**.

For groups like  $(\mathbb{Z}, +)$ , it is confusing to write  $mn$  instead of  $m + n$  since  $mn$  already has another meaning.

For abelian groups  $G$ , we can also use **additive notation**. In additive notation, we write the group operation as  $g + h$ . The identity is denoted by 0 or  $0_G$ . Inverses are denoted by  $-g$ .

Writing  $g^n$  in additive notation gives

$$\underbrace{g + \cdots + g}_{n \text{ times}}$$

so instead of  $g^n$  we use  $ng$ . Similarly  $g^{-n}$  is  $-ng$ .

Multiplicative notation	Additive notation
$g \cdot h$ or $gh$	$g + h$
$e_G$ or $1_G$	$0_G$
$g^{-1}$	$-g$
$g^n$	$ng$

For non-abelian groups we always use multiplicative notation. For abelian groups, we can choose either. Note the conventions may conflict, so we should be clear about which we choose.

For a group like  $(\mathbb{Z}, +)$ , we could use  $mn$ , but it is clearer to use  $m + n$ .

For a group like  $(\mathbb{Q}^\times, \cdot)$ , we could use  $x + y$ , but it is clearer to use  $x \cdot y$  or  $xy$ .

## Multiplication table

### Definition — multiplication table

The **multiplication table** of a group  $G$  is a table with rows and columns indexed by the elements of  $G$ . The cell for row  $g$  and column  $h$  contains the product  $gh$ .

The multiplication table contains the complete information of the group (even for infinite groups).

### Example

For  $\mathbb{Z}/2\mathbb{Z}$ :

	0	1
0	0	1
1	1	0

## Order of elements

### Definition — order of a group element

If  $G$  is a group, then the order of  $g \in G$  is

$$|g| := \min\{k \geq 1 : g^k = e_G\} \cup \{+\infty\}.$$

Easy properties:

- $|g| = 1$  if and only if  $g = e_G$ .
- If  $g^n = 1$ , then  $g^{n-1}g = gg^{n-1} = g^n = 1$ , so  $g^{n-1} = g^{-1}$ . In particular, if  $|g| = n < \infty$ , then  $g^{-1} = g^{n-1}$ .

### Example

We use additive notation for  $\mathbb{Z}/n\mathbb{Z}$ , so  $g^n$  is written as  $ng$  and  $e = 0$ . For this group,  $k1 = 0$  if and only if  $n \mid k$ , so  $|1| = n$ .

### Lemma

$g^n = e$  if and only if  $g^{-n} = e$ , so in particular,  $|g| = |g^{-1}|$ .

### Proof.

We have  $g^{-n} = (g^n)^{-1}$ . Since  $g \mapsto g^{-1}$  is a bijection,  $g^n = e$  if and only if  $(g^n)^{-1} = e^{-1} = e$ .

But  $g^{-n} = (g^{-1})^n$  also, so  $\{k \geq 1 : g^k = e\} = \{k \geq 1 : (g^{-1})^k = e\}$  which implies  $|g| = |g^{-1}|$ .  $\square$

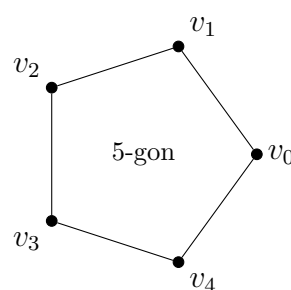
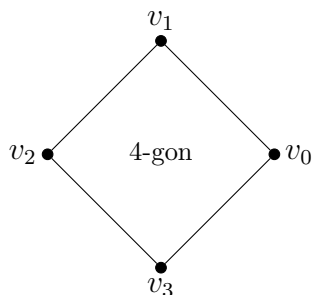
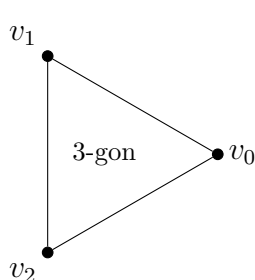
## 2: Dihedral and permutation groups

### Dihedral groups

#### Definition — $n$ -gon

A regular polygon  $P_n$  with  $n \geq 3$  vertices is called an  **$n$ -gon**.

Specifically: set  $v_k = (\cos(2\pi k/n), \sin(2\pi k/n)) = e^{2\pi i k/n}$  and get an  $n$ -gon by drawing a line segment from  $v_k$  to  $v_{k+1}$  for all  $0 \leq k \leq n$  (where  $v_n := v_0$ ).



#### Definition — symmetry, dihedral group

A **symmetry** of the  $n$ -gon  $P_n$  is an invertible linear transformation  $T \in \text{GL}_2(\mathbb{R})$  such that  $T(P_n) = P_n$ .

The set of symmetries of  $P_n$  is called the **dihedral group** and is denoted by  $D_{2n}$  (or  $D_n$ ).

(Think of matrices and linear transformations interchangeably. Matrix multiplication = composition of transformations.)

#### Proposition

$D_{2n}$  is a group under composition.

Proof later (key point:  $S, T \in D_{2n} \implies ST \in D_{2n}$ ).

**Lemma**

Say  $v_i$  and  $v_j$  are adjacent in  $P_n$  if they are connected by a line segment.

1. If  $T \in D_{2n}$ , then  $(T(v_0), T(v_1))$  are adjacent.
2. If  $S, T \in D_{2n}$  and  $S(v_i) = T(v_i)$  for  $i = 0, 1$ , then  $S = T$ .

*Proof.*

1.  $v_0, v_1$  are adjacent and  $T$  is linear (lines map to lines).
2.  $v_0, v_1$  are linearly independent (and form a basis in  $\mathbb{R}^2$ ).

□

**Corollary**

$$|D_{2n}| \leq 2n.$$

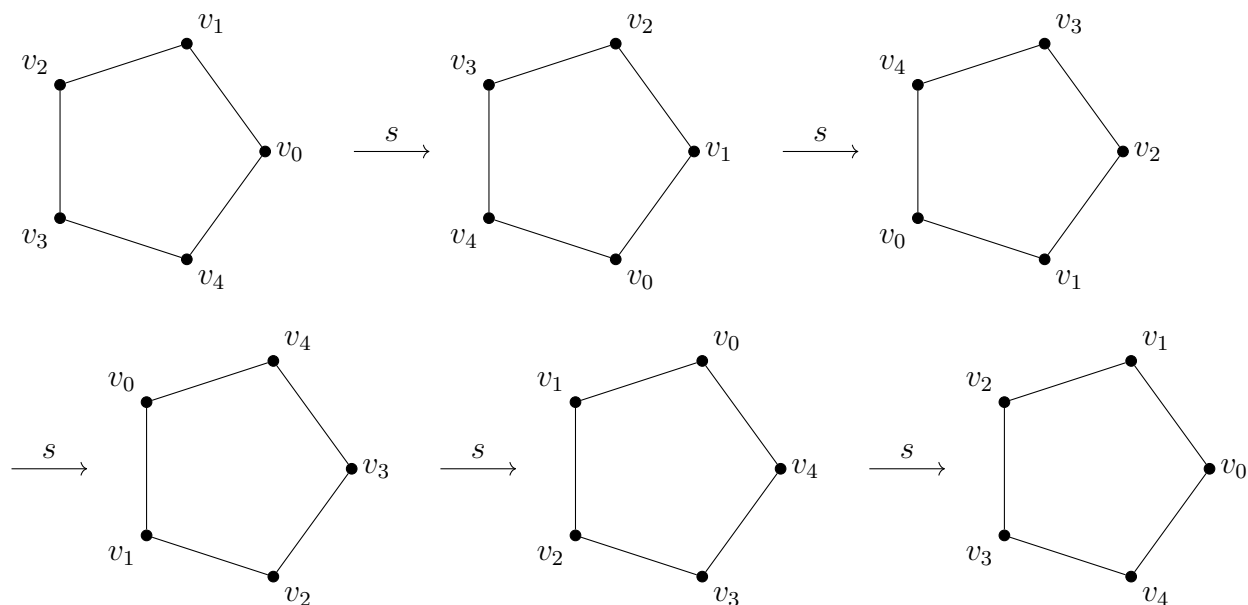
*Proof.*

Let  $A$  be the set of adjacent  $(v_i, v_j)$ , so  $|A| = 2n$ . By lemma,  $D_{2n} \rightarrow A : T \mapsto (T(v_0), T(v_1))$  is well-defined and injective. □

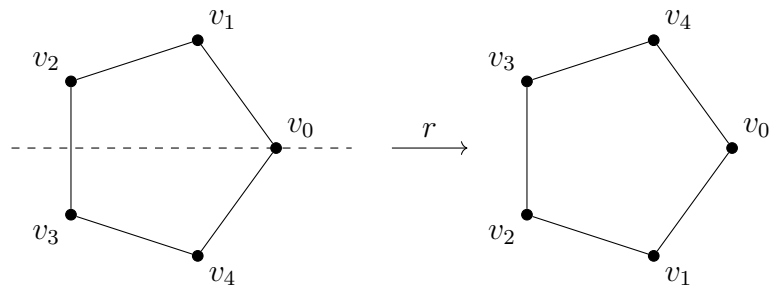
Intuitively, we can ask: for every pair of adjacent vertices  $(v_i, v_j)$ , is there an element  $T \in D_{2n}$  with  $T(v_0) = v_i$  and  $T(v_1) = v_j$ ? If yes, then  $|D_{2n}| = 2n$ .

### Special elements of $D_{2n}$

Let  $s \in D_{2n}$  be rotation by  $2\pi/n$  radians, so  $|s| = n$  (that is,  $s^n = e$  and  $s^k \neq e$  for  $1 \leq k < n$ ).



Let  $r$  be reflection through the  $x$ -axis.



$|r| = 2$ , that is,  $r^2 = e$  and  $r \neq e$ .

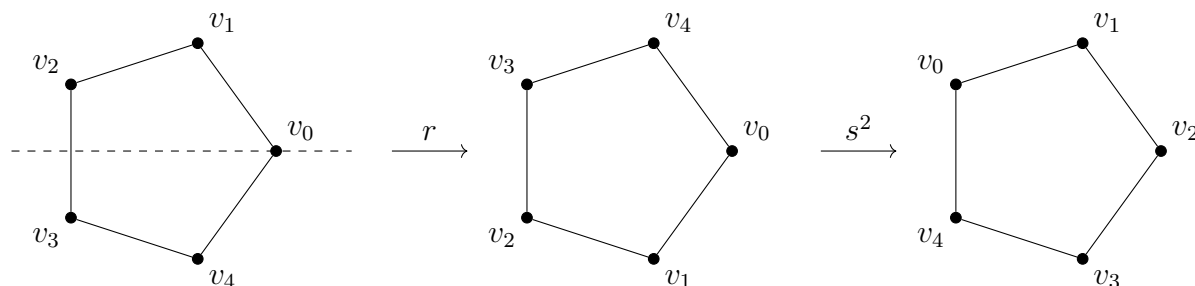
We have  $r(v_0) = v_0$  and  $r(v_1)$  is now the vertex before  $v_0$  rather than the vertex after.



## Putting rotation and reflection together

$s^i$  for  $0 \leq i < n$  sends  $v_0 \mapsto v_i$  and  $v_1 \mapsto v_{i+1}$ . (Say  $v_n = v_0$  and  $s^0 = e$ .)

$s^i r$  for  $0 \leq i < n$  sends  $v_0 \mapsto v_i$  and  $v_1 \mapsto v_{i-1}$ . (Say  $v_{-1} = v_{n-1}$ .)



### Proposition

$D_{2n} = \{s^i r^j : 0 \leq i < n, 0 \leq j < 2\}$ , so  $|D_{2n}| = 2n$ .

So what is  $rs$ ?

$rs(v_0) = r(v_1) = v_{n-1}$  and  $rs(v_1) = r(v_2) = v_{n-2}$ .

So  $rs = s^{n-1}r = s^{-1}r$ .

### Corollary

$D_{2n}$  is a finite non-abelian group.

In summary:

- $D_{2n} = \{s^i r^j : 0 \leq i < n, 0 \leq j < 2\}$
- $|D_{2n}| = 2n$
- $s^n = e, r^2 = e, rs = s^{-1}r$
- $D_{2n}$  is a finite non-abelian group.

Exercise: show these relations are enough to completely determine  $D_{2n}$ .

**What's group theory about?**

Basic answer: sets with one binary operation.

Better answer: group theory is the study of symmetry.

If we resize or rotate  $P_n$ , then the symmetries remain the same.

Kleinian view of geometry:

- $D_{2n}$  captures what it means to be a regular  $n$ -gon.
- More generally, geometry is about the study of symmetries.

## Permutation groups

If  $X$  is a set, let  $\text{Fun}(X, X)$  be the set of functions  $X \rightarrow X$ . Then

$$\circ: \text{Fun}(X, X) \times \text{Fun}(X, X) \rightarrow \text{Fun}(X, X) : (f, g) \mapsto f \circ g$$

is an associative operation with an identity  $\text{Id}_X$ .

Let  $S_X = \{f \in \text{Fun}(X, X) : f \text{ is a bijection}\}$ .

### Proposition

$S_X$  is a group under  $\circ$ .

*Proof.*

Homework. □

### Definition — symmetric group

Let  $n \geq 1$ . The **symmetric group** (or **permutation group**)  $S_n$  is the group  $S_X$  with  $X = \{1, \dots, n\}$ .

Elements of  $S_n$  are bijections  $\pi: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ .

What makes such a  $\pi$  a bijection? Every element of  $\{1, \dots, n\}$  must appear in the list  $\pi(1), \dots, \pi(n)$  and no element can appear twice.

We have  $n$  choices for  $\pi(1)$ ,  $n - 1$  choices for  $\pi(2)$ , ..., 1 choice for  $\pi(n)$ . Thus  $|S_n| = n(n - 1) \cdots 1 = n!$ .

Note  $|S_1| = 1! = 1$ , so  $S_1$  is the trivial group.

## Permutations

Elements of  $S_n$  are called **permutations**. We have several ways of representing permutations:

1. Two-line representation:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}$$

2. One-line representation:  $\pi = 651423$ .

3. Disjoint cycle representation: write down the **cycles** of  $\pi$ . Here  $\pi(1) = 6$ ,  $\pi(6) = 3$ , and  $\pi(3) = 1$ , so  $(163)$  is a cycle of  $\pi$ .

$\pi = (163)(25)(4) = (163)(25)$ . We typically drop cycles of length 1, and write cycles containing the smallest unused element first.

The identity is empty in disjoint cycle notation, so we just use  $e$ .

Multiplication can be done in two-line or disjoint cycle notation:

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25) \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix} = (126)(345) \\ \pi\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix} = (15)(234) \end{aligned}$$

One-line notation is hard, so we don't use it here.

Inversion can also be done in two-line or disjoint cycle notation:

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25) \\ \pi^{-1} &= \begin{pmatrix} 6 & 5 & 1 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (136)(25) \end{aligned}$$

If  $\pi(i) = j$ , then  $\pi^{-1}(j) = i$ , so cycles of  $\pi^{-1}$  are cycles of  $\pi$  in reverse order.

## Fixed points and support sets

### Definition — fixed point, support set

The **fixed points** of a permutation  $\pi \in S_n$  are the numbers  $1 \leq i \leq n$  such that  $\pi(i) = i$ .

The **support set** of  $\pi \in S_n$  is

$$\text{supp}(\pi) = \{1 \leq i \leq n : \pi(i) \neq i\}.$$

$\pi$  and  $\sigma$  are **disjoint** if  $\text{supp}(\pi) \cap \text{supp}(\sigma) = \emptyset$ .

### Example

$$\text{supp}((163)(25)) = \{1, 2, 3, 5, 6\}.$$

Some notes:

- In general,  $\text{supp}(\pi)$  are exactly the numbers that appear in the disjoint cycle representation of  $\pi$  (when length-1 cycles are omitted).
- $\text{supp}(\pi) = \emptyset$  if and only if  $\pi = e$ .
- $\text{supp}(\pi^{-1}) = \text{supp}(\pi)$ .
- If  $i \in \text{supp}(\pi)$ , then  $\pi(i) \in \text{supp}(\pi)$ .

## Commuting elements

### Definition — commute

Two elements  $g, h$  in a group  $G$  **commute** if  $gh = hg$ .

### Lemma

If  $\pi, \sigma \in S_n$  are disjoint, then  $\pi\sigma = \sigma\pi$ .

#### *Proof.*

Suppose  $1 \leq i \leq n$ .

If  $i \in \text{supp}(\pi)$ , then  $\pi(i) \in \text{supp}(\pi)$ . Since  $\pi, \sigma$  are disjoint, we have  $i, \pi(i) \notin \text{supp}(\sigma)$ . So  $\pi(\sigma(i)) = \pi(i) = \sigma(\pi(i))$ .

By symmetry,  $\pi(\sigma(i)) = \sigma(\pi(i))$  if  $i \in \text{supp}(\sigma)$ .

If  $i \notin \text{supp}(\pi) \cup \text{supp}(\sigma)$ , then  $\pi(\sigma(i)) = i = \sigma(\pi(i))$ .

Then  $\pi(\sigma(i)) = \sigma(\pi(i))$  for all  $i$ , so  $\pi\sigma = \sigma\pi$ . □

## Cycles

### Definition — cycle

A  **$k$ -cycle** is an element of  $S_n$  with disjoint cycle notation  $(i_1 i_2 \cdots i_k)$ .

Suppose the cycles of  $\pi \in S_n$  are  $c_1, \dots, c_k$ . We can regard  $c_i$  as an element of  $S_n$  and  $\pi = c_1 \cdot c_2 \cdots c_k$  as a product in  $S_n$ . Since  $c_i$  and  $c_j$  are disjoint,  $c_i c_j = c_j c_i$ . Thus the order of cycles in disjoint cycle representation doesn't matter.

### Example

$$\pi = (163)(25) = (25) \cdot (163).$$

Additionally, we have  $\pi^{-1} = c_k^{-1} \cdots c_1^{-1} = c_1^{-1} \cdots c_k^{-1}$ .

### Example

If  $c$  and  $c'$  are non-disjoint cycles, then they don't necessarily commute:  $(12)(23) = (123)$  while  $(23)(12) = (123)^{-1} = (132) \neq (12)(23)$ .

If  $\pi$  is a permutation, then  $\pi$  commutes with  $\pi^i$  for all  $i$ , so  $\pi$  and  $\pi^i$  commute. However,  $\pi$  and  $\pi^i$  don't have disjoint support sets.

## **Week 2: Subgroups and homomorphisms**



## 3: Subgroups

### Subgroups

#### Definition — subgroup

Let  $(G, \cdot)$  be a group. A subset  $H \subseteq G$  is a **subgroup** of  $G$  if

1. for all  $g, h \in H$ ,  $g \cdot h \in H$  ( $H$  is **closed under products**),
2. for all  $g \in H$ ,  $g^{-1} \in H$  ( $H$  is **closed under inverses**), and
3.  $e_G \in H$ .

Notation:  $H \leq G$ .

#### Example

- $\mathbb{Z} \leq \mathbb{Q}^+ := (\mathbb{Q}, +)$ .
- $\mathbb{Q}_{>0} := \{x \in \mathbb{Q} : x > 0\} \leq \mathbb{Q}^\times$ .

Check: if  $x, y \in \mathbb{Q}$  and  $x, y > 0$ , then  $xy > 0 \implies xy \in \mathbb{Q}_{>0}$ . Also, if  $x > 0$ , then  $1/x > 0 \implies 1/x \in \mathbb{Q}_{>0}$ .

#### Example

Let  $G = D_{2n}$  and  $s$  be rotation.

$H = \{e = s^0, s, s^2, \dots, s^{n-1}\}$  is a subgroup of  $D_{2n}$ .

#### Proof.

Claim:  $s^i \in H$  for all  $i \in \mathbb{Z}$ .

Proof: let  $i = nk + r$  with  $0 \leq r < n$ . Then  $s^i = s^{nk+r} = (s^n)^k s^r = s^r$  since  $s^n = e$ .

Checking subgroup properties:

- If  $s^i, s^j \in H$ , then  $s^{i+j} \in H$ .
- If  $s^i \in H$ , then  $s^{-i} \in H$ .
- $e \in H$ .

□

$H$  is the smallest subgroup containing  $s$  (since subgroups are closed under products).

Notation for  $H$  is  $\langle s \rangle$ .

**Example**

Let  $G = \mathbb{Z} = (\mathbb{Z}, +)$ .

If  $m \in \mathbb{Z}$ , then  $m\mathbb{Z} := \{km : k \in \mathbb{Z}\} = \{n \in \mathbb{Z} : m \mid n\}$  is a subgroup of  $\mathbb{Z}$ .

In particular,  $0\mathbb{Z} = \{0\}$  is a subgroup of  $\mathbb{Z}$  called the **trivial subgroup**.

**Definition — trivial subgroup, proper subgroup**

If  $G$  is a group, then  $\{e\}$  is a subgroup called the **trivial subgroup**.

Also,  $G$  is a subgroup of  $G$ . A subgroup  $H$  is **proper** if  $H \neq G$ . Notation:  $H < G$ .

$H$  is a proper non-trivial subgroup if  $\{e\} \neq H < G$ .

**Example**

Some non-subgroups:

- $\mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} : x \geq 0\}$  is not a subgroup of  $\mathbb{Q}^+$ .  
If  $x, y \in \mathbb{Q}_{\geq 0}$ , then  $x + y \in \mathbb{Q}_{\geq 0}$ . Also,  $0 \in \mathbb{Q}_{\geq 0}$ .  
But if  $x \in \mathbb{Q}_{\geq 0}$ , then  $-x \notin \mathbb{Q}_{\geq 0}$  unless  $x = 0$ .
- $\mathbb{Q}^\times$  is not a subgroup of  $(\mathbb{Q}, \cdot)$  because  $(\mathbb{Q}, \cdot)$  is not a group.

**Proposition**

If  $H$  is a subgroup of  $(G, \boxtimes)$ , then  $(H, \boxtimes|_{H \times H})$  is a group, such that

1. the identity of  $H$  is  $e_H = e_G$ , and
2. the inverse of  $g \in H$  is the same as the inverse of  $g$  in  $G$ .

**Proof.**

First, we show  $\boxtimes|_{H \times H}$  is a binary operation on  $H$ . Note  $\boxtimes$  is a function  $G \times G \rightarrow G$ , so  $\boxtimes|_{H \times H}$  is a function  $H \times H \rightarrow G$ . But if  $g, h \in H$ , then  $g \boxtimes h \in H$ . Thus  $\boxtimes|_{H \times H}$  is a function  $H \times H \rightarrow H$ .

From now on, denote this function by  $\tilde{\boxtimes}$ .

Since  $\boxtimes$  is associative,  $\tilde{\boxtimes}$  is associative.

Note  $e_H = e_G$  is the identity for  $\tilde{\boxtimes}$ .

If  $g \in H$ , then  $g^{-1}$  with respect to  $\tilde{\boxtimes}$  is in  $H$ .

Since  $g \tilde{\boxtimes} g^{-1} = g^{-1} \tilde{\boxtimes} g = e_G = e_H$ ,  $g^{-1}$  is the inverse of  $g$  with respect to  $\tilde{\boxtimes}$ .

So  $(H, \tilde{\boxtimes})$  is a group. □

We call  $\tilde{\boxtimes}$  the **operation induced by  $\boxtimes$**  on  $H$ . Usually we just refer to  $\tilde{\boxtimes}$  as  $\boxtimes$ .

**Example**

- $\mathbb{Z}$  is a subgroup of  $\mathbb{Q}$  with operation  $+$ .
- If  $H$  is a subgroup of  $(G, \cdot)$ , then  $H$  is a group with operation  $\cdot$ .

## Speeding up the subgroup check

### Proposition

$H$  is a subgroup of  $G$  if and only if

1.  $H$  is non-empty, and
2.  $gh^{-1} \in H$  for all  $g, h \in H$ .

### Proof.

( $\implies$ ) If  $H$  is a subgroup of  $G$ , then  $e_G \in H$ , so  $H \neq \emptyset$ . Also if  $g, h \in H$ , then  $h^{-1} \in H$  and  $gh^{-1} \in H$ .

( $\impliedby$ ) By (1), there is some  $x \in H$ . By (2),  $xx^{-1} = e_G \in H$ .

Also by (2),  $e_G \cdot x^{-1} = x^{-1} \in H$  (so  $H$  is closed under inverses).

Now if  $x, y \in H$ , then  $y^{-1} \in H$ , so  $xy = x(y^{-1})^{-1} \in H$  (so  $H$  is closed under products).

□

### Example

Let  $(V, +, \cdot)$  be a vector space.

If  $W$  is a subspace of  $V$ , then  $W$  is a subgroup of  $(V, +)$ .

Check:

- $0 \in W$  so  $W$  is non-empty.
- If  $v, w \in W$ , then  $v + (-w) = v - w \in W$ .

$W$  is a subgroup by the proposition.

## Finite subgroups

### Proposition

Suppose  $H$  is a finite subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if

1.  $H$  is non-empty, and
2.  $gh \in H$  for all  $g, h \in H$ .

### *Proof.*

The forward direction is trivial.

Suppose  $g \in H$ . By induction, we can show  $g^n \in H$  for all  $n \in \mathbb{N}$ .

Since  $H$  is finite, the sequence  $g, g^2, g^3, \dots \in H$  must eventually repeat.

So  $g^i = g^j$  for some  $1 \leq i < j \implies g^n = e$  for  $n = j - i$ .

If  $n = 1$ , then  $g^n = g = e$  so  $g^{-1} = e \in H$ . If  $n > 1$ , then  $g^{n-1} = g^{-1} \in H$ . □

## Subgroups generated by a set

### Proposition

Suppose  $\mathcal{F}$  is a non-empty set of subgroups of  $G$ . Then

$$K := \bigcap_{H \in \mathcal{F}} H$$

is a subgroup of  $G$ .

### Proof.

Note  $e_G \in H$  for all  $H \in \mathcal{F}$ , so  $e_G \in K$  and thus  $K$  is non-empty.

Now consider  $x, y \in K$ . Then  $x, y \in H$  for all  $H \in \mathcal{F}$ , so  $y^{-1} \in H$  for all  $H \in \mathcal{F}$ , so  $xy^{-1} \in H$  for all  $H \in \mathcal{F}$ , so  $xy^{-1} \in K$ .

By proposition,  $K$  is a subgroup of  $G$ . □

### Definition — subgroup generated by a set

Let  $S$  be a subset of a group  $G$ .

The **subgroup generated by  $S$  in  $G$**  is

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H.$$

Notes:

- The intersection is non-empty because  $S \subseteq G \leq G$ .
- If  $S \subseteq K \leq G$ , then  $\langle S \rangle \subseteq K$ . So say that  $\langle S \rangle$  is the smallest subgroup of  $G$  containing  $S$ .
- $\langle \emptyset \rangle = \langle e \rangle = \{e\}$ , the trivial subgroup.
- If  $S = \{s_1, s_2, \dots\}$ , we often write  $\langle S \rangle = \langle s_1, s_2, \dots \rangle$ .

### Example

Consider  $D_{2n}$  and its rotation generator  $s$ .

Let  $K = \{e = s^0, s^1, s^2, \dots, s^{n-1}\}$ . As previously checked,  $K$  is a subgroup of  $D_{2n}$ .

Since  $s \in K$ ,  $\langle s \rangle \in K$ .

On the other hand, we can show by induction that  $s^i \in \langle s \rangle$  for all  $i \in \mathbb{Z}$ . So  $K \subseteq \langle s \rangle \implies \langle s \rangle = K$ .

Note that  $\langle s \rangle$  is constructed by taking all products of  $s$  with itself. Can we generalize this example?

If  $S \subset G$ , let  $S^{-1} = \{s^{-1} : s \in S\}$ .

### Proposition

If  $S \subset G$ , let

$$K = \{e\} \cup \{s_1 \cdots s_k : k \geq 1, s_1, \dots, s_k \in S \cup S^{-1}\}.$$

Then  $\langle S \rangle = K$ .

### Proof.

Claim 1:  $S \subseteq K \subseteq \langle S \rangle$ .

Proof: We know  $e \in \langle S \rangle$ . Prove by induction that  $s_1 \cdots s_k \in \langle S \rangle$  for all  $k \geq 1$  and  $s_1, \dots, s_k \in S \cup S^{-1}$ .

Claim 2:  $K$  is a subgroup.

Proof:  $e \in K$  by construction. Consider  $x, y \in K$ . Then

$$\begin{aligned} x &= s_1 \cdots s_k, \quad k \geq 0, \quad s_1, \dots, s_k \in S \cup S^{-1} \\ y &= t_1 \cdots t_\ell, \quad \ell \geq 0, \quad t_1, \dots, t_\ell \in S \cup S^{-1}. \end{aligned}$$

So  $xy = s_1 \cdots s_k t_1 \cdots t_\ell \in K$ , and  $x^{-1} = s_k^{-1} \cdots s_1^{-1} \in K$  since  $s_k^{-1}, \dots, s_1^{-1} \in S \cup S^{-1}$ .

So  $K$  is a subgroup.

Proof of proposition:  $S \subseteq K$  and  $\langle S \rangle$  is the smallest subgroup containing  $S$ , so  $\langle S \rangle \subseteq K$ .

Thus  $\langle S \rangle = K$ . □

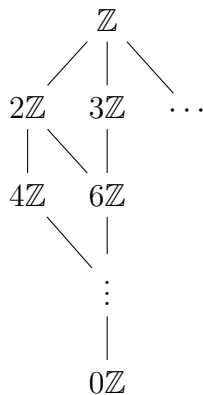
## Lattice of subgroups

Subgroups of  $G$  are ordered by set inclusion  $\subseteq$ .

If  $H_1, H_2 \leq G$  and  $H_1 \subseteq H_2$ , then  $H_1 \leq H_2$ , so we also write this order as  $\leq$ . (Exercise.)

The set of subgroups of  $G$  with order  $\leq$  is called the **lattice of subgroups of  $G$** .

The first subgroup below  $H_1, H_2 \leq G$  in the lattice is  $H_1 \cup H_2$ . The first subgroup above  $H_1, H_2 \leq G$  in the lattice is  $\langle H_1 \cup H_2 \rangle$ .





## 4: Cyclic groups

### Generators and cyclic groups

#### Definition — generate, cyclic

A subset  $S$  of a group  $G$  **generates**  $G$  if  $\langle S \rangle = G$ .

A group  $G$  is **cyclic** if  $G = \langle a \rangle$  for some  $a \in G$ .

#### Example

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$  (generators are not unique)
- $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle = \langle [-1] \rangle$
- $\mathbb{Q}^+$  is not cyclic (homework)
- If  $G$  is a group, then  $\langle a \rangle$  is a cyclic group for any  $a \in G$  (called the **cyclic subgroup generated by  $a$** ).

#### Lemma

1. If  $a \in G$ , then  $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ .
2. If  $|a| = n$ , then  $\langle a \rangle = \{a^i : 0 \leq i < n\}$ .

#### Proof.

1. Follows from previous proposition about  $\langle S \rangle$ .
2. See argument for  $\langle s \rangle$  in  $D_{2n}$ .

□

Questions:

- In (2), can  $|\langle a \rangle|$  be smaller than  $n$ ?
- Does  $|\langle a \rangle|$  determine  $|a|$ ?

## Order of cyclic groups

### Proposition

If  $G = \langle a \rangle$ , then  $|G| = |a|$ .

### *Proof.*

We've already seen that  $|G| \leq |a|$ .

Suppose  $|G| = n < \infty$ .

The sequence  $a^0, a^1, a^2, \dots, a^n \in G$  must have repetition. So there are  $0 \leq i < j \leq n$  with  $a^i = a^j$ , which means  $a^{j-i} = e$  and hence  $|a| \leq n$ .

So  $|a| \leq |G|$ , thus  $|a| = |G|$ . □

## Examples in closer detail

### Example

For  $G = \mathbb{Z}$ :

- Infinite cyclic group.
- Generators:  $+1$  and  $-1$ .
- Order of  $m \in \mathbb{Z}$  is

$$|m| = \begin{cases} \infty & m \neq 0 \\ 1 & m = 0 \end{cases}.$$

- Cyclic subgroups are  $\langle m \rangle = m\mathbb{Z} = \{km : k \in \mathbb{Z}\}$ . (Note difference in  $\langle a \rangle$  between additive and multiplicative notation.)

Homework: all subgroups of  $\mathbb{Z}$  are cyclic.

### Example

Can we analyze  $\mathbb{Z}/n\mathbb{Z}$  in the same way?

(Note: at this point we may drop the brackets. For example, in  $\mathbb{Z}/5\mathbb{Z}$ ,  $3 = 8$ .)

Questions:

- What are the generators of  $\mathbb{Z}/n\mathbb{Z}$ ?
- What are the orders of elements of  $\mathbb{Z}/n\mathbb{Z}$ ?
- What are the subgroups?

## Generators of $\mathbb{Z}/n\mathbb{Z}$

### Lemma

Suppose  $G = \langle S \rangle$ . Then  $G = \langle T \rangle$  if and only if  $S \subseteq \langle T \rangle$ .

So  $\mathbb{Z}/n\mathbb{Z} = \langle [a] \rangle$  if and only if  $[1] \in \langle [a] \rangle$  (since  $[1]$  is a generator). Note then

$$\begin{aligned}
 [1] \in \langle [a] \rangle &\iff xa = 1 \pmod{n} && \text{for some } x \in \mathbb{Z} \\
 &\iff xa - 1 = yn && \text{for some } x, y \in \mathbb{Z} \\
 &\iff xa + yn = 1 && \text{for some } x, y \in \mathbb{Z} \\
 &\iff \gcd(a, n) = 1
 \end{aligned}$$

so  $\langle [a] \rangle = \mathbb{Z}/n\mathbb{Z}$  if and only if  $\gcd(a, n) = 1$ .

## Order of elements in $\mathbb{Z}/n\mathbb{Z}$

### Lemma

If  $G$  is a group,  $g \in G$ , and  $g^n = e$ , then  $|g| \mid n$ .

### Proof.

Homework. □

If  $a \in \mathbb{Z}$ , then  $n[a] = 0$ , so  $|[a]| \mid n$ .

### Lemma

Suppose  $a \mid n$ . Then  $|[a]| = \frac{n}{a}$ .

### Proof.

If  $n = ka$ , then  $\ell[a] \neq 0$  for  $1 \leq \ell < k$  and  $k[a] = [ka] = 0$ , so  $|[a]| = k$ . □

### Lemma

Suppose  $a \in \mathbb{Z}$  and let  $b = \gcd(a, n)$ . Then  $\langle [a] \rangle = \langle [b] \rangle$ .

### Proof.

Since  $b \mid a$ , there is  $k$  such that  $a = kb$ . Thus  $[a] \in \langle [b] \rangle$ , so  $\langle [a] \rangle \subseteq \langle [b] \rangle$ .

By properties of gcd, there are  $x, y \in \mathbb{Z}$  such that  $xa + yn = b$ .

So  $[b] = x[a] + y[n] = x[a]$ , which implies  $[b] \in \langle [a] \rangle$  and thus  $\langle [b] \rangle \subseteq \langle [a] \rangle$ .

Hence  $\langle [a] \rangle = \langle [b] \rangle$ . □

### Proposition

Suppose  $a \in \mathbb{Z}$ . Then

$$|[a]| = \frac{n}{\gcd(a, n)}.$$

*Proof.*

Let  $b = \gcd(a, n)$ . Then  $\langle [a] \rangle = \langle [b] \rangle$ . So

$$|[a]| = |\langle [a] \rangle| = |\langle [b] \rangle| = |[b]|.$$

But  $b \mid n$ , so by lemma  $[b] = \frac{n}{b}$ .

□

## Subgroups of $\mathbb{Z}/n\mathbb{Z}$

### Corollary

Let  $n \geq 1$ .

- The order  $d$  of any cyclic subgroup of  $\mathbb{Z}/n\mathbb{Z}$  divides  $n$ .
- For every  $d \mid n$ , there is a unique cyclic subgroup of  $\mathbb{Z}/n\mathbb{Z}$  of order  $d$ . It is generated by  $[a]$ , where  $a = \frac{n}{d}$ .

### Proof.

If  $|\langle [a] \rangle| = d$ , then  $d = |[a]| \mid n$  by lemma.

Also,  $d = \frac{n}{\gcd(a, n)}$ , and by lemma,  $\langle [a] \rangle = \langle [\frac{n}{d}] \rangle$ .

Conversely, if  $d \mid n$  and  $a = \frac{n}{d}$ , then  $|\langle [a] \rangle| = d$ . □

### Example

Cyclic subgroups of  $\mathbb{Z}/6\mathbb{Z}$ :

- $\langle 6 \rangle = \{0\}$ .
- $\langle 3 \rangle = \{0, 3\}$ .
- $\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$ .
- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}/6\mathbb{Z} = \langle 5 \rangle$ .

Cyclic subgroups of  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  prime:

- $\langle p \rangle = \langle 0 \rangle$ .
- $\langle 1 \rangle = \mathbb{Z}/p\mathbb{Z}$ .

**Proofs later**

- Every subgroup of a cyclic group is cyclic. (So the previous corollary is a complete list of subgroups of  $\mathbb{Z}/n\mathbb{Z}$ .)
- Every cyclic group is isomorphic to one of  $\mathbb{Z}/n\mathbb{Z}$  for  $n \geq 1$ , or  $\mathbb{Z}$ .



## 5: Homomorphisms

### Homomorphisms

#### Definition — homomorphism (morphism)

Let  $G$  and  $H$  be groups. A function  $\phi: G \rightarrow H$  is a **homomorphism** (or **morphism**) if

$$\phi(g \cdot h) = \phi(g) \cdot \phi(h)$$

for all  $g, h \in G$ .

A homomorphism preserves the group operation from  $G$  to  $H$ .

#### Example

- For  $\mathbb{K}$  a field,  $\mathbb{K}^\times = \{a \in \mathbb{K} : a \neq 0\}$  is a group with operation  $\cdot$ .  
Then  $\text{GL}_n \mathbb{K} \rightarrow \mathbb{K}^\times : A \mapsto \det(A)$  is a homomorphism because  $\det(AB) = \det(A) \det(B)$  for all  $A, B$ .
- Let  $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\} \leq \mathbb{R}^\times$ . Then  $\mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0} : x \mapsto \sqrt{x}$  is a homomorphism since  $\sqrt{xy} = \sqrt{x}\sqrt{y}$ .
- Additive notation:  $\phi: (G, +) \rightarrow (H, +)$  is a homomorphism if  $\phi(x+y) = \phi(x) + \phi(y)$  for all  $x, y \in G$ .  
 $\phi: \mathbb{Z} \rightarrow \mathbb{Z} : k \mapsto mk$  is a homomorphism for any  $m \in \mathbb{Z}$  since  $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$  for all  $x, y \in \mathbb{Z}$ .
- If  $V, W$  are vector spaces and  $T: V \rightarrow W$  is a linear transformation, then  $T$  is a homomorphism from  $(V, +)$  to  $(W, +)$  since  $T(v + w) = T(v) + T(w)$  for all  $v, w \in V$ .
- Mixed notation:  $\mathbb{R}^+ \rightarrow \mathbb{R}^\times : x \mapsto e^x$  is a homomorphism since  $e^{x+y} = e^x \cdot e^y$  for all  $x, y \in \mathbb{R}^+$ .
- $\mathbb{R}^+ \rightarrow \mathbb{R}^+ : x \mapsto e^x$  is not a homomorphism because  $e^{x+y} \neq e^x + e^y$  in general (take  $x = y = 0$ ).

**Lemma**

Suppose  $\phi: G \rightarrow H$  is a homomorphism. Then:

1.  $\phi(e_G) = e_H$ .
2.  $\phi(g^{-1}) = \phi(g)^{-1}$  for all  $g \in G$ .
3.  $\phi(g^n) = \phi(g)^n$  for all  $n \in \mathbb{Z}$ .
4.  $|\phi(g)| \mid |g|$  for all  $g \in G$  (say  $n \mid \infty$  for all  $n \in \mathbb{N}$ ).

*Proof.*

1.  $\phi(e_G) = \phi(e_G^2) = \phi(e_G) \cdot \phi(e_G)$ , so  $e_H = \phi(e_G)^{-1} \cdot \phi(e_G) = \phi(e_G)^{-1} \cdot \phi(e_G) \cdot \phi(e_G) = \phi(e_G)$ .
2.  $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$  and similarly  $\phi(g^{-1})\phi(g) = e_H$ , so  $\phi(g^{-1})$  is the unique inverse of  $\phi(g)$ .
3. Use induction for  $n \geq 0$ , additionally with part (b) for  $n < 0$ .
4. If  $|g| = n < \infty$ , then  $g^n = e_G$  so  $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$ . Homework: prove  $|\phi(g)| \mid n$ .

□

## Making new homomorphisms from old

### Lemma

If  $H \leq G$  and  $H$  is considered as a group with the induced operation from  $G$ , then  $i: H \rightarrow G : x \mapsto x$  is a homomorphism.

*Proof.*

$$i(g \cdot h) = g \cdot h = i(g) \cdot i(h).$$

□

### Lemma

If  $\phi: G \rightarrow M$  and  $\psi: H \rightarrow K$  are homomorphisms, then  $\psi \circ \phi$  is a homomorphism.

*Proof.*

$$(\psi \circ \phi)(g \cdot h) = \psi(\phi(g) \cdot \phi(h)) = \psi(\phi(g)) \cdot \psi(\phi(h)).$$

□

### Corollary

If  $\phi: G \rightarrow H$  is a homomorphism and  $K \leq G$ , then the **restriction**  $\phi|_K$  is a homomorphism.

*Proof.*

$$\phi|_K = \phi \circ i, \text{ where } i: K \rightarrow G \text{ is the inclusion } x \mapsto x.$$

□

## Images of homomorphisms

If  $f: X \rightarrow Y$  is a function and  $S \subseteq X$ , then say  $f(S) := \{f(x) : x \in S\}$ .

### Proposition

If  $\phi: G \rightarrow H$  is a homomorphism and  $K \leq G$ , then  $\phi(K) \leq H$ .

That is, homomorphisms send subgroups of the domain to subgroups of the codomain.

### Proof.

Since  $K$  is non-empty,  $\phi(K)$  is non-empty.

If  $x, y \in \phi(K)$ , then  $x = \phi(x_0)$  and  $y = \phi(y_0)$  for some  $x_0, y_0 \in K$ .

So  $xy^{-1} = \phi(x_0)\phi(y_0)^{-1} = \phi(x_0)\phi(y_0^{-1}) = \phi(x_0y_0^{-1}) \in \phi(K)$ , since  $x_0y_0^{-1} \in K$ . □

### Definition — image

If  $\phi: G \rightarrow H$  is a homomorphism, the **image** of  $\phi$  is the subgroup  $\text{Im } \phi = \phi(G) \leq H$ .

### Example

- Let  $\phi: \mathbb{R}^+ \rightarrow \mathbb{R}^\times : x \mapsto e^x$ .  
 $e^x > 0$  for all  $x \in \mathbb{R}$ , so  $\text{Im } \phi \subseteq \mathbb{R}_{>0}$ .  
 If  $y \in \mathbb{R}_{>0}$ , then  $y = \phi(\log y)$ , so  $\text{Im } \phi = \mathbb{R}_{>0}$ .
- If  $K \leq G$  and  $i: K \rightarrow G$  is inclusion, then  $\text{Im } i = K$ .
- For  $\phi: \mathbb{Z} \rightarrow \mathbb{Z} : k \mapsto mk$  for some  $m \in \mathbb{Z}$ ,  $\phi(\mathbb{Z}) = m\mathbb{Z}$ .

## Properties of images

### Lemma

If  $\phi: G \rightarrow H$  is a homomorphism with  $\text{Im } \phi \leq K \leq H$ , then the function  $\tilde{\phi}: G \rightarrow K: x \mapsto \phi(x)$  is also a homomorphism with  $\text{Im } \tilde{\phi} = \text{Im } \phi \leq K$ .

*Proof.*

$$\begin{aligned}\tilde{\phi}(x \cdot y) &= \phi(x \cdot y) \\ &= \phi(x) \cdot \phi(y) && \text{in } H \\ &= \tilde{\phi}(x) \cdot \tilde{\phi}(y) && \text{in } K.\end{aligned}$$

Also  $\tilde{\phi}(G) = \phi(G)$ , regarded as a subset of  $K$ . □

We usually just refer to  $\tilde{\phi}$  as  $\phi$ .

### Lemma

A homomorphism  $\phi: G \rightarrow H$  is surjective if and only if  $\text{Im } \phi = H$ .

*Proof.*

Obvious from definition. □

### Corollary

$\phi$  induces a surjective homomorphism  $\tilde{\phi}: G \rightarrow K$ , where  $K = \text{Im } \phi$ .

### Proposition

Let  $\phi: G \rightarrow H$  be a homomorphism. If  $S \subseteq G$ , then  $\phi(\langle S \rangle) = \langle \phi(S) \rangle$ .

*Proof.*

First,  $\phi(S^{-1}) = \{\phi(s^{-1}) : s \in S\} = \{\phi(s)^{-1} : s \in S\} = \phi(S)^{-1}$ . Thus

$$\begin{aligned}\phi(\langle S \rangle) &= \phi(\{s_1 \cdots s_k : k \geq 0, s_1, \dots, s_k \in S \cup S^{-1}\}) \\ &= \{\phi(s_1) \cdots \phi(s_k) : k \geq 0, s_1, \dots, s_k \in S \cup S^{-1}\} \\ &= \{t_1 \cdots t_k : k \geq 0, t_1, \dots, t_k \in \phi(S) \cup \phi(S)^{-1}\} \\ &= \langle \phi(S) \rangle.\end{aligned}$$

□

## Pulling back subgroups

If  $f: X \rightarrow Y$  is a function and  $S \subseteq Y$ , then say  $f^{-1}(S) := \{x \in X : f(x) \in S\}$ .

### Proposition

If  $\phi: G \rightarrow H$  is a homomorphism and  $K \leq H$ , then  $\phi^{-1}(K) \leq G$ .

That is, we can also get a subgroup of the domain from a subgroup of the codomain.

Note: the forward and backward processes are not necessarily inverses, so we don't have a bijection (just yet).

### *Proof.*

$\phi(e_G) = e_H \in K$ , so  $e_G \in \phi^{-1}(K)$ .

If  $x, y \in \phi^{-1}(K)$ , then  $\phi(x), \phi(y) \in K$  so  $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in K$  and hence  $xy^{-1} \in \phi^{-1}(K)$ .  $\square$

## The kernel of a homomorphism

### Definition — kernel

If  $\phi: G \rightarrow H$  is a homomorphism, then the **kernel** of  $\phi$  is the subgroup  $\ker \phi := \phi^{-1}(\{e_H\}) = \{g \in G : \phi(g) = e_H\} \leq G$ .

### Example

- For  $\det: \mathrm{GL}_n(\mathbb{K}) \rightarrow \mathbb{K}^\times$ , we have  $\ker \det = \{A \in \mathrm{GL}_n(\mathbb{K}) : \det(A) = 1\}$ .  
This subgroup of  $\mathrm{GL}_n(\mathbb{K})$  is called the **special linear group**, denoted by  $\mathrm{SL}_n(\mathbb{K})$ .
- If  $\phi: \mathbb{Z} \rightarrow \mathbb{Z} : k \mapsto mk$ , then  $\phi(k) = 0$  if and only if  $mk = 0$ , so

$$\ker \phi = \begin{cases} \{0\} & m \neq 0 \\ \mathbb{Z} & m = 0 \end{cases}.$$

- If  $\phi: \mathbb{R}^+ \rightarrow \mathbb{R}^\times : x \mapsto e^x$ , then  $e^x = 1$  if and only if  $x = 0$ , so  $\ker \phi = \{0\}$ .

### Proposition

A homomorphism  $\phi: G \rightarrow H$  is injective if and only if  $\ker \phi = \{e_G\}$ .

### Proof.

( $\implies$ ) If  $\phi$  is injective, then  $\phi(x) = e_H = \phi(e_G)$  if and only if  $x = e_G$ , so  $\ker \phi = \{e_G\}$ .

( $\impliedby$ ) Suppose  $\ker \phi = \{e_G\}$  and  $\phi(x) = \phi(y)$ .

Then  $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_H$ , so  $xy^{-1} \in \ker \phi$ .

But then  $xy^{-1} = e_G$ , so  $x = y$ . That is,  $\phi$  is injective.

□



## Application: subgroups of cyclic groups

### Proposition

If  $H$  is a subgroup of a cyclic group  $G$ , then  $H$  is cyclic.

### Proof.

We need the following facts:

1. All subgroups of  $\mathbb{Z}$  are of the form  $m\mathbb{Z} = \langle m \rangle$ , hence cyclic. (Homework.)
2.  $G$  is cyclic if and only if there is a surjective homomorphism  $\mathbb{Z} \rightarrow G$ . (Homework.)
3. If  $f: X \rightarrow Y$  is a surjective function and  $S \subseteq Y$ , then  $f(f^{-1}(S)) = S$ . (Exercise.)

Since  $G$  is cyclic, by (2) there is a surjective homomorphism  $\phi: \mathbb{Z} \rightarrow G$ .

By (1), since all subgroups of  $\mathbb{Z}$  are cyclic, there is  $m \in \mathbb{Z}$  such that  $\phi^{-1}(H) = \langle m \rangle$ .

So let  $\psi: \mathbb{Z} \rightarrow \mathbb{Z}$  be the homomorphism with  $\psi(k) = mk$ .

Then  $\phi \circ \psi: \mathbb{Z} \rightarrow G$  is a homomorphism. We see that

$$(\phi \circ \psi)(\mathbb{Z}) = \phi(m\mathbb{Z}) = \phi(\phi^{-1}(H)) = H$$

by (3).

We can restrict the codomain of  $\phi \circ \psi$  to get a surjective homomorphism  $\mathbb{Z} \rightarrow H$ . Hence  $H$  is cyclic by (2).  $\square$

## Review on bijections

### Definition — bijection

Let  $f: X \rightarrow Y$  be a function. Then  $f$  is:

- **injective** if for all  $x_1, x_2 \in X$ ,  $f(x_1) = f(x_2)$  implies that  $x_1 = x_2$ ;
- **surjective** if for all  $y \in Y$ , there exists  $x \in X$  with  $f(x) = y$ ; and
- **bijective** if  $f$  is both injective and surjective.

### Proposition

$f: X \rightarrow Y$  is a bijection if and only if there is a function  $g: Y \rightarrow X$  such that  $f \circ g = 1_Y$  and  $g \circ f = 1_X$ .

If  $g$  exists, then it is unique, and we denote it by  $f^{-1}$ .

## Isomorphisms

### Definition — isomorphism

A homomorphism  $\phi: G \rightarrow H$  is an **isomorphism** if  $\phi$  is a bijection.

### Lemma

$\phi: G \rightarrow H$  is an isomorphism if and only if  $\ker \phi = \{e_G\}$  and  $\text{Im } \phi = H$ .

### Example

- $\mathbb{R}^+ \rightarrow \mathbb{R}_{>0} : x \mapsto e^x$  is an isomorphism.
- If  $\phi: G \rightarrow H$  is injective, then  $\phi$  induces an isomorphism  $G \rightarrow \text{Im } \phi$ .
- $\mathbb{Z} \rightarrow m\mathbb{Z} : k \mapsto mk$  is an isomorphism.

### Proposition

Suppose  $\phi: G \rightarrow H$  is an isomorphism. Then  $\phi^{-1}: H \rightarrow G$  is also an isomorphism.

#### Proof.

$\phi^{-1}$  is also a bijection, so we just need to show that it is a homomorphism.

Let  $g, h \in H$ . Then  $\phi(\phi^{-1}(g) \cdot \phi^{-1}(h)) = \phi(\phi^{-1}(g)) \cdot \phi(\phi^{-1}(h)) = g \cdot h$ .

So  $\phi^{-1}(g) \cdot \phi^{-1}(h) = \phi^{-1}(g \cdot h)$ . Hence  $\phi^{-1}$  is a homomorphism.  $\square$

### Corollary

A homomorphism  $\phi: G \rightarrow H$  is an isomorphism if and only if there is a homomorphism  $\psi: H \rightarrow G$  such that

1.  $\psi \circ \phi = 1_G$ , and
2.  $\phi \circ \psi = 1_H$ .

This shows isomorphisms are to homomorphisms as bijections are to functions.

*Proof.*

( $\Leftarrow$ ) If  $\psi$  exists, then  $\phi$  is a bijection.

( $\Rightarrow$ ) If  $\phi$  is an isomorphism, then we can take  $\psi = \phi^{-1}$ .

□

### Definition — isomorphic

We say that groups  $G$  and  $H$  are **isomorphic** if there is an isomorphism  $\phi: G \rightarrow H$ .

Notation:  $G \cong H$ .

Key facts:

- If  $G \cong H$ , then  $H \cong G$  (symmetry).

Proof: If  $\phi: G \rightarrow H$  is an isomorphism, then  $\phi^{-1}: H \rightarrow G$  is an isomorphism.

- If  $G \cong H$  and  $H \cong K$ , then  $G \cong K$  (transitivity).

Proof: If  $\phi: G \rightarrow H$  is an isomorphism and  $\psi: H \rightarrow K$  is an isomorphism, then  $\psi \circ \phi$  is an isomorphism.

- $G \cong G$  (reflexivity).

Proof:  $1_G: G \rightarrow G$  is an isomorphism.

**Isomorphism as a relation**

Idea: if  $G \cong H$ , then  $G$  and  $H$  are identical *as groups*.

If  $\phi: G \rightarrow H$  is an isomorphism, then:

- $|G| = |H|$ ;
- $G$  is abelian if and only if  $H$  is abelian;
- $|g| = |\phi(g)|$  for all  $g \in G$ ;
- $K \subseteq G$  is a subgroup of  $G$  if and only if  $\phi(K)$  is a subgroup of  $H$ .

## Isomorphisms of cyclic groups

### Proposition

If  $G$  and  $H$  are cyclic groups, then  $G \cong H$  if and only if  $|G| = |H|$ .

### Proof.

The forward implication is obvious.

Suppose  $G = \langle a \rangle$  and  $H = \langle b \rangle$  where  $|G| = |H|$ .

Claim:  $a^i = a^j$  for  $i < j$  if and only if  $|a| \mid j - i$ .

Proof: if  $a^i = a^j$  then  $a^{j-i} = e$ , apply the homework to finish. Conversely, if  $|a| \mid j - i$ , then  $j - i = k|a|$ . So  $a^{j-i} = a^{k|a|} = e$  and hence  $a^j = a^i$ .

(Note: if  $|a| = \infty$ , then  $a^i \neq a^j$  for all  $i \neq j \in \mathbb{Z}$ .)

Now define  $\phi: G \rightarrow H : a^i \mapsto b^i$ .

Notice  $|a| = |G| = |H| = |b|$ . Then  $a^i = a^j$  implies  $|a| \mid j - i$  implies  $|b| \mid j - i$  implies  $b^i = b^j$ , so  $\phi$  is well-defined.

We see  $\phi(a^i \cdot a^j) = \phi(a^{i+j}) = b^{i+j} = b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j)$  for all  $a^i, a^j \in G$ , so  $\phi$  is a homomorphism.

Similarly to above,  $\psi: H \rightarrow G : b^i \mapsto a^i$  is well-defined and clearly an inverse to  $\phi$ .

Thus  $\phi$  is an isomorphism. □

### Corollary

Suppose  $G$  is a cyclic group.

- If  $|G| = \infty$ , then  $G \cong \mathbb{Z}$ .
- If  $|G| = n < \infty$ , then  $G \cong \mathbb{Z}/n\mathbb{Z}$ .

### Corollary

Cyclic groups are abelian.

### Exercise

Prove the previous corollary without the corollary before it.

## Multiplicative notation for cyclic groups

Sometimes it is convenient to use the multiplicative form of cyclic groups.

### Definition

Let  $a$  be a formal indeterminate. Let

- $C_\infty = \{a^i : i \in \mathbb{Z}\}$  with  $a^i \cdot a^j = a^{i+j}$ ; and
- $C_n = \{a^i : i \in \mathbb{Z}/n\mathbb{Z}\}$  with  $a^i \cdot a^j = a^{i+j}$ .

Of course, we have:

- $C_\infty \cong \mathbb{Z}$  via  $a^i \mapsto i$ .
- $C_n \cong \mathbb{Z}/n\mathbb{Z}$  via  $a^i \mapsto i$ .

## **Week 3: Cosets, Lagrange's Theorem, and Products**



## 6: Cosets and Lagrange's Theorem

### Affine spaces

Linear subspaces motivate the definition of subgroups. Let  $T: V \rightarrow W$  be a linear transformation (so  $T$  is a homomorphism  $(V, +) \rightarrow (W, +)$ ). We get  $\ker T = \{x \in V : T(x) = 0\}$  which are the “solutions to  $Tx = 0$ ”. What are the solutions to  $Tx = b$ ?

Note  $Tx = b$  has a solution if and only if  $b \in \operatorname{Im} T$ . If  $b \in \operatorname{Im} T$  and  $Tx = b$  has solution  $x_0$ , then all other solutions are of the form  $x_0 + x_1$  for  $x_1 \in \ker T$ . We conclude the space of solutions has form  $x_0 + \ker T$ . We call this an **affine subspace** (like a linear subspace, but may not contain 0).

#### Definition — coset

If  $S \subseteq G$  and  $g \in G$ , we let

$$gS = \{gh : h \in S\} \quad \text{and} \quad Sg = \{hg : h \in S\}.$$

If  $H \leq G$ , then  $gH$  is called a **left coset** of  $H$  in  $G$  and  $Hg$  is called a **right coset** of  $H$  in  $G$ .

For abelian groups,  $gH = Hg$ . In additive notation, a coset of  $H$  in  $(G, +)$  is  $g + H$ .

#### Example

- If  $U$  is a subspace of vector space  $(V, +, \cdot)$ , cosets of  $U$  are affine subspaces  $v + U$  for  $v \in V$ .
- Given  $m \in \mathbb{Z}$ , cosets of  $m\mathbb{Z}$  are sets

$$a + m\mathbb{Z} = \{a + km : k \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

## Cosets in the dihedral group

Recall  $D_{2n} = \{s^i r^j : 0 \leq i < n, j \in \{0, 1\}\}$ .

Say  $H = \langle s \rangle = \{e = s^0, s^1, \dots, s^{n-1}\}$ .

The right cosets of  $H$  are:

- $He = H$
- $Hr = \{r, sr, \dots, s^{n-1}r\}$
- $Hs^i = \{s^i, s^{i+1}, \dots, s^{n-1}, e, s^1, \dots, s^{i-1}\} = H$
- $Hs^i r = \{s^i r, s^{i+1}r, \dots, s^{n-1}r, r, sr, \dots, sr, \dots, s^{i-1}r\} = H$

Notice  $D_{2n} = H \sqcup Hr$  where  $\sqcup$  is disjoint union.

Exercise 1: use  $rs = s^{-1}r$  to show  $s^i r = r s^{-i}$  for all  $i \in \mathbb{Z}$ .

Exercise 2: if  $S \subseteq G$  and  $g, h \in G$ , then  $ghS = g(hS)$ .

The left cosets of  $H$  are:

- $eH = H$
- $s^i H = H$
- $s^i r H = r s^{-i} H = rH$

Notice

$$\begin{aligned} rH &= \{r, rs, rs^2, \dots, rs^{n-1}\} \\ &= \{r, s^{-1}r, s^{-2}r, \dots, s^{-n+1}r\} \\ &= \{r, s^{n-1}r, s^{n-2}r, \dots, sr\} \\ &= Hr \end{aligned}$$

so in this case, the left and right cosets are equal.

What about  $K = \langle r \rangle = \{e, r\}$ ?

Left cosets:  $rK = \{r, e\} = K$  and  $s^i K = \{s^i, s^i r\} = s^i r K$ . We see the left cosets are  $s^i K$  for  $0 \leq i < n$ , and

$$D_{2n} = \bigsqcup_{i=0}^{n-1} s^i K.$$

Right cosets:  $Kr = \{r, e\} = K$  and  $Ks^i = \{s^i, rs^i\} = \{s^i, s^{-1}r\}$  and  $Ks^i r = \{s^i r, s^{-1}\} = Ks^{-1}$ . We see the right cosets are  $Ks^i$  for  $0 \leq i < n$ , and

$$D_{2n} = \bigsqcup_{i=0}^{n-1} Ks^i.$$

In this case, the left and right cosets are not equal.

## Sets of cosets

### Definition — set of cosets

If  $H \leq G$ , let

$$G/H = \{gH : g \in G\} = \{S \subseteq G : S = gH \text{ for some } g \in G\}$$

be the **set of left cosets** of  $H$  in  $G$ , and

$$H \backslash G = \{Hg : g \in G\} = \{S \subseteq G : S = Hg \text{ for some } g \in G\}$$

be the **set of right cosets** of  $H$  in  $G$ .

We are very interested in trying to understand  $G/H$  and  $H \backslash G$ .

### Example

- $D_{2n}/\langle s \rangle = \{\langle s \rangle, r\langle s \rangle\}$ .
- $D_{2n}/\langle r \rangle = \{s^i \langle r \rangle, 0 \leq i < n\}$ .

### Example

Consider  $n\mathbb{Z} \leq \mathbb{Z}$ . Then

$$a + n\mathbb{Z} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} =: [a]$$

so

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &= \{a + n\mathbb{Z} : a \in \mathbb{Z}\} \\ &= \{a + n\mathbb{Z} : 0 \leq a < n\} \\ &= \{[a] : 0 \leq a < n\}. \end{aligned}$$

A big question for later: for which  $H \leq G$  is  $G/H$  a group?

## Cosets of a kernel

Suppose  $\phi: G \rightarrow K$  is a homomorphism and let  $H = \ker \phi$ . (Note  $\phi(x) = b$  has a solution  $x$  for  $b \in K$  if and only if  $b \in \text{Im } \phi$ .)

### Lemma

Suppose  $\phi(x_0) = b$ . The set of solutions  $\phi^{-1}(\{b\})$  to  $\phi(x) = b$  is  $x_0H = Hx_0$ .

#### Proof.

Suppose  $\phi(x_1) = b$ . Then  $\phi(x_0^{-1}x_1) = b^{-1}b = e$ , so  $x_0^{-1}x_1 \in H$  and thus  $x_1 = x_0(x_0^{-1}x_1) \in x_0H$ .

Conversely, if  $x_1 = x_0h$  for  $h \in H$ , then  $\phi(x_1) = \phi(x_0)\phi(h) = b$ , so every element of  $x_0H$  is a solution.

A similar argument using right cosets shows the set of solutions is also  $Hx_0$ .  $\square$

In this case, the left cosets are the right cosets.

### Proposition

If  $\phi: G \rightarrow K$  is a homomorphism, then there is a bijection between  $G/\ker \phi$  and  $\text{Im } \phi$ .

#### Proof.

$g \cdot \ker \phi$  is the set of solutions to  $\phi(x) = b$  where  $b = \phi(g)$ .

As a result,  $\phi(g \cdot \ker \phi) = \{b\}$  and  $b \in \text{Im } \phi$ .

In the other direction,  $g \ker \phi = \phi^{-1}(\{b\})$ .  $\square$

### Example

Suppose  $G = \mathbb{Z}$  and  $K = \mathbb{Z}/n\mathbb{Z}$ .

From tutorial, there is a homomorphism  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]$ . We get  $\ker \phi = n\mathbb{Z}$  and  $\text{Im } \phi = \mathbb{Z}/n\mathbb{Z}$ .

Then  $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \leq a < n\} = \{a + n\mathbb{Z} : 0 \leq a < n\}$ , so  $a + n\mathbb{Z}$  is the set of solutions of  $[x] \equiv [a]$  in  $\mathbb{Z}/n\mathbb{Z}$ .

## Indexes and Lagrange's theorem

Given  $H \leq G$ , how many left cosets does  $H$  have?

### Definition — index

The **index** of  $H$  in  $G$  is

$$[G : H] = \begin{cases} |G/H| & G/H \text{ is finite} \\ \infty & G/H \text{ is infinite} \end{cases}.$$

### Theorem — Lagrange's theorem

If  $H \leq G$ , then  $|G| = [G : H] \cdot |H|$ .

Why use left cosets in the definition?

### Proposition

The function  $\phi: G/H \rightarrow H \backslash G : S \mapsto S^{-1}$  is a bijection.

#### *Proof.*

Suppose  $S \in G/H$ , so  $S = gH$  for some  $g \in G$ . Then

$$\begin{aligned} S^{-1} &= \{(gh)^{-1} : h \in H\} \\ &= \{h^{-1}g^{-1} : h \in H\} \\ &= \{hg^{-1} : h \in H\} \\ &= Hg^{-1} \end{aligned}$$

because  $H \rightarrow H : h \mapsto h^{-1}$  is a bijection. So  $\phi$  is well-defined, and a similar argument shows  $\psi: H \backslash G \rightarrow G/H : S \mapsto S^{-1}$  is well-defined.

Finally,  $\psi$  is an inverse to  $\phi$ . □

### Corollary

If  $H \leq G$  then

$$[G : H] = \begin{cases} |H \backslash G| & H \backslash G \text{ is finite} \\ \infty & H \backslash G \text{ is infinite} \end{cases}.$$

Results from Lagrange's theorem: if  $H \leq G$ , then  $|H|$  divides  $|G|$ , and if  $G$  is finite, then  $[G : H] = \frac{|G|}{|H|}$ .

**Example**

- $G = D_{2n}$ ,  $H = \langle s \rangle$ . Here,  $|D_{2n}| = 2n$ ,  $|H| = n$ , so  $[G : H] = 2$ .
- $G = D_{2n}$ ,  $H = \langle r \rangle$ . Here,  $|D_{2n}| = 2n$ ,  $|H| = 2$ , so  $[G : H] = n$ .
- $G = \mathbb{Z}$ ,  $H = m\mathbb{Z}$ . Here,  $|G| = |H| = \infty$ , but  $[G : H] = |\mathbb{Z}/m\mathbb{Z}| = m$ . So  $|G| = [G : H]|H|$ , but we don't learn anything about  $[G : H]$  from Lagrange's theorem.

## Consequences of Lagrange's theorem

### Corollary

If  $x \in G$ , then  $|x|$  divides  $|G|$ .

#### Proof.

$|x| = |\langle x \rangle|$  and  $|\langle x \rangle|$  divides  $|G|$ . □

### Proposition

If  $|G|$  is prime, then  $G$  is cyclic.

#### Proof.

Let  $x \in G$  and  $x \neq e$ . Then  $|x| \neq 1$ , and  $|x| \mid |G|$ , so  $|x| = |G|$ . Then since  $|\langle x \rangle| = |x| = |G|$ , we have  $G = \langle x \rangle$  (since  $G$  is finite). □

We can thus list out groups of small orders (up to isomorphism)...

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$ , ??
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$ , $D_6 = S_3$ , ??
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$ , $D_8$ , ??
9	$\mathbb{Z}/9\mathbb{Z}$ , ??

### Corollary

If  $\phi: G \rightarrow K$  is a homomorphism, then  $|\text{Im } \phi| = [G : \ker \phi]$ , and hence divides  $|G|$ .

#### Proof.

There is a bijection  $G/\ker \phi \rightarrow \text{Im } \phi$ , so  $|\text{Im } \phi| = [G : \ker \phi]$  by definition. Lagrange's theorem then implies  $|\text{Im } \phi|$  divides  $|G|$  (and  $|K|$ ). □

**Exercise**

If  $G, K$  are groups, then  $\phi: G \rightarrow K : g \mapsto e_K$  is a homomorphism (called the **trivial homomorphism**). Show  $\phi: G \rightarrow K$  is the trivial homomorphism if and only if  $\text{Im } \phi = \{e\}$  (the trivial subgroup).

As a result, if  $G$  and  $K$  have coprime order, then the only homomorphism  $\phi: G \rightarrow K$  is the trivial homomorphism.



## Beginning to prove Lagrange's theorem

Recall

$$\begin{aligned} D_{2n} &= \{s^i r^j : 0 \leq i < n, j \in \{0, 1\}\} \\ &= \langle s \rangle \sqcup r \langle s \rangle \\ &= \bigsqcup_{i=0}^{n-1} s^i \langle r \rangle. \end{aligned}$$

Here, the cosets of  $H$  are disjoint, so we can divide  $G$  into  $[G : H]$  sets of size  $|H|$ .

Does this work in general?

### Proposition

Let  $H \leq G$  and suppose  $g, k \in G$ . Then the following are equivalent:

1.  $g^{-1}k \in H$
2.  $k \in gH$
3.  $gH = kH$
4.  $gH \cap kH \neq \emptyset$

Example:  $H = hH$  if and only if  $h \in H$  (using (3) and (1)).

### Proof.

(1)  $\implies$  (2): If  $g^{-1}k = h \in H$ , then  $k = gh \in gH$ .

(2)  $\implies$  (3): Suppose  $k = gh$  for some  $h \in H$ . If  $h' \in H$ , then  $kh' = g(hh') \in gH$  since  $hh' \in H$ . So  $kH \subseteq gH$ . Also  $g = kh^{-1} \in kH$ , so similarly  $gH \subseteq kH$ .

(3)  $\implies$  (4): If  $gH = kH$ , then  $gH \cap kH = gH \neq \emptyset$  (since  $g \in gH$ ).

(4)  $\implies$  (1): Suppose  $x \in gH \cap kH$ . Then  $x = gh_1 = kh_2$  for  $h_1, h_2 \in H$ . So  $g^{-1}k = h_1h_2^{-1} \in H$ .  $\square$

## Partitions

### Definition — partition

Let  $X$  be a set. A **partition** of  $X$  is a subset  $\mathcal{Q}$  of  $2^X$  such that

$$(a) \bigcup_{S \in \mathcal{Q}} S = X \quad \text{and} \quad (b) S \cap T = \emptyset \text{ for all } S \neq T \in \mathcal{Q}.$$

Equivalently,  $\mathcal{Q}$  is a partition if  $X = \bigsqcup_{S \in \mathcal{Q}} S$  or every element of  $X$  is contained in exactly one element of  $\mathcal{Q}$ .

We can show cosets partition  $G$ :

### Corollary

If  $H \leq G$ , then  $G/H$  is a partition of  $G$ .

#### *Proof.*

$g \in gH$ , so every element of  $G$  belongs to some element of  $G/H$ . Then  $\bigcup_{S \in G/H} S = G$ .

Suppose  $S \neq T$  are in  $G/H$ . If  $S \cap T \neq \emptyset$ , then  $S = T$  by (3) and (4) of the proposition. So  $S \cap T = \emptyset$ .  $\square$

We can also show cosets have the same size:

### Lemma

If  $S \subseteq G$  and  $g \in G$ , then  $S \rightarrow gS : h \mapsto gh$  is a bijection.

#### *Proof.*

Inverse is  $gS \rightarrow S : h \mapsto g^{-1}h$ .  $\square$

As a consequence, if  $H$  is finite and  $g \in G$ , then  $|gH| = |H|$ .

## Proof of Lagrange's theorem

*Proof (Lagrange's theorem).*

If  $|H| = \infty$  then  $|G| = \infty$ .

Since cosets are disjoint, if  $[G : H] = \infty$  then  $|G| = \infty$ .

Now suppose  $|H|$  and  $[G : H]$  are finite. By lemma,  $|gH| = |H|$  for all  $g \in G$ . Since  $G/H$  is a partition of  $G$ ,  $G$  is a disjoint union of  $[G : H]$  subsets all of size  $|H|$ .

So  $|G| = [G : H]|H|$ . □

## Equivalence relations

### Definition — relation

A **relation**  $\sim$  on a set  $X$  is a subset of  $X \times X$ .

Notation:  $a \sim b$  if  $(a, b) \in \sim$ .

### Example

- $=$  on  $X$
- $\leq, <, >, \geq$  on  $\mathbb{N}$  (or any ordered set)
- $\subseteq$  on  $2^X$

### Definition — equivalence relation

A relation  $\sim$  on  $X$  is an **equivalence relation** if

- $x \sim x$  for all  $x \in X$  (reflexivity)
- $x \sim y \implies y \sim x$  for all  $x, y \in X$  (symmetry)
- $x \sim y$  and  $y \sim z \implies x \sim z$  for all  $x, y, z \in X$  (transitivity).

### Example

- $=$  on  $X$
- $\equiv_m$  (congruence mod  $m$ ) on  $\mathbb{Z}$
- not  $\leq, <, >, \geq$  on  $\mathbb{N}, \mathbb{R}$ , etc.
- isomorphism  $\cong$  on the *proper class* of groups

## Equivalence classes

### Definition — equivalence class

If  $\sim$  is an equivalence relation on  $X$ , the **equivalence class** of  $x \in X$  is  $[x] = [x]_{\sim} := \{y \in X : x \sim y\}$ .

### Proposition

Let  $\sim$  be an equivalence relation on  $X$ . If  $x, y \in X$  then the following are equivalent:

1.  $x \sim y$
2.  $y \in [x]$
3.  $[x] = [y]$
4.  $[x] \cap [y] \neq \emptyset$

#### *Proof.*

(1)  $\implies$  (2): By definition.

(2)  $\implies$  (3): If  $z \in [y]$ , then  $x \sim y \sim z \implies z \in [x]$ , so  $[y] \subseteq [x]$ . Also  $x \sim y \implies y \sim x \implies [x] \subseteq [y]$ .

(3)  $\implies$  (4):  $[x] \cap [y] = [x] \supseteq \{x\} \neq \emptyset$ .

(4)  $\implies$  (1): If  $z \in [x] \cap [y]$ , then  $x \sim z \sim y \implies x \sim y$ . □

Equivalence relations yield partitions:

### Corollary

If  $\sim$  is an equivalence relation on  $X$ , then  $\{[x]_{\sim} : x \in X\}$  is a partition of  $X$ .

Partitions yield equivalence relations:

### Corollary

If  $\mathcal{Q}$  is a partition of  $X$ , then there is an equivalence relation  $\sim$  on  $X$  such that  $\{[x]_{\sim} : x \in X\} = \mathcal{Q}$ .

**Proof.**

Every element  $x \in X$  is contained in a unique set  $S_x \in \mathcal{Q}$ . Define  $\sim$  by saying  $x \sim y \iff S_x = S_y$ .  $\square$

Let's apply this to cosets:

**Proposition**

If  $H \leq G$ , define a relation  $\sim_H$  on  $G$  by  $g \sim_H k$  if  $g^{-1}k \in H$ . Then  $\sim_H$  is an equivalence relation, and the equivalence class of  $g \in G$  is  $[g] = gH$ .

For example,  $h \sim e$  if and only if  $h \in H$ .

## 7: Normal subgroups

### When is a left coset a right coset?

From before:

#### Proposition

Let  $H \leq G$  and suppose  $g, k \in G$ . Then the following are equivalent:

1.  $g^{-1}k \in H$
2.  $k \in gH$
3.  $gH = kH$
4.  $gH \cap kH \neq \emptyset$

By symmetry:

#### Proposition

Let  $H \leq G$  and suppose  $g, k \in G$ . Then the following are equivalent:

1.  $k^{-1}g \in H$
2.  $k \in Hg$
3.  $Hg = Hk$
4.  $Hg \cap Hk \neq \emptyset$

Caution:  $g^{-1}k \in H$  does not necessarily imply  $kg^{-1} \in H$ .

#### Lemma

If  $H \leq G$  and  $Hg = hH$  for  $g, h \in G$ , then  $gH = Hg$ .

*Proof.*

$g \in Hg = hH$ , so  $gH = hH$ . □

#### Definition — normal subgroup

A subgroup  $N \leq G$  is a **normal subgroup** if  $gN = Ng$  for all  $g \in G$ .

Notation:  $N \trianglelefteq G$ .

## Conjugation and set multiplication

### Definition — conjugate

If  $g, h \in G$ , then **conjugate** of  $h$  by  $g$  is  $ghg^{-1}$ .

Conjugates come up in change of basis and diagonalization in linear algebra.

Note  $gSg^{-1} = \{ghg^{-1} : h \in S\}$ . We also get  $gN = Ng$  if and only if  $gNg^{-1} = N$ .

Also,  $S \subseteq T$  if and only if  $gS \subseteq gT$  if and only if  $Sg \subseteq Tg$ .



## Equivalent characterizations of normal subgroups

### Proposition

Let  $N \leq G$ . Then the following are equivalent:

- |  |                                  |
|--|----------------------------------|
| 1. $N \trianglelefteq G$ ( $gN = Ng$ for all $g \in G$ ) | 4. $G/N = N \setminus G$         |
| 2. $gNg^{-1} = N$ for all $g \in G$                      | 5. $G/N \subseteq N \setminus G$ |
| 3. $gNg^{-1} \subseteq N$ for all $g \in G$              | 6. $N \setminus G \subseteq G/N$ |

### Proof.

We've already done  $(1) \iff (2)$ .

Clearly  $(2) \implies (3)$ .

For  $(3) \implies (2)$ , suppose  $gNg^{-1} \subseteq N$  for all  $g \in G$ . Given  $g \in G$ , we know  $g^{-1}Ng \subseteq N$ , so  $N \subseteq gNg^{-1}$ . Hence  $N = gNg^{-1}$ .

Clearly  $(1) \implies (4) \implies (5)$  and  $(6)$ .

For  $(5) \implies (1)$ , suppose  $G/N \subseteq N \setminus G$ . If  $g \in G$ , then  $gN = Nh$  for some  $h \in G$ . By lemma,  $gN = Ng$ .

$(6) \implies (1)$  is similar. □

### Example

- $\langle s \rangle \leq D_{2n}$ : we already saw  $G/\langle s \rangle = \langle s \rangle \setminus G$ . So  $\langle s \rangle \trianglelefteq D_{2n}$ . We can also check  $s^i \langle s \rangle s^{-i} = \langle s \rangle$  and  $r \langle s \rangle r^{-1} = \langle s \rangle$  (since  $rs^i r^{-1} = s^{-i}$ ).
- $\langle r \rangle \leq D_{2n}$ :  $G/\langle r \rangle \neq \langle r \rangle \setminus G$ , so  $\langle r \rangle$  is not normal. Indeed,  $srs^{-1} = s^2r \notin \langle r \rangle$  for  $n \geq 3$ .
- If  $G$  is abelian, then all subgroups are normal.
- If  $\phi: G \rightarrow K$  is a homomorphism, then  $\ker \phi$  is normal.

Previous proof:  $G/\ker \phi$  is the set of solution sets to equations  $\phi(x) = b$  where  $b \in \text{Im } \phi$ , which is  $\ker \phi \setminus G$ .

Alternative: if  $x \in \ker \phi$  and  $g \in G$ , then we have  $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e$ , so  $gxg^{-1} \in \ker \phi \implies g(\ker \phi)g^{-1} \subseteq \ker \phi$ .

**Warning: normal subgroups are not transitive**

The subgroup relation  $\leq$  is transitive: if  $H \leq G$  and  $K \leq H$ , then  $K \leq G$ . (Usually we just say  $K \leq H \leq G \implies K \leq G$ .)

The normal subgroup relation  $\trianglelefteq$  is not transitive: consider  $H = \langle r, s^2 \rangle \leq D_8$ . Then  $rs^2 = s^{4-2}r = s^2r \implies rs^2r^{-1} = s^2$ . Exercise: check  $H \trianglelefteq D_8$ . From the homework,  $H$  is abelian so  $\langle r \rangle \trianglelefteq H$ . But  $\langle r \rangle \not\trianglelefteq D_8$ .

## Normalizers

### Definition — normalizer

Let  $S \subseteq G$ . Then  $N_G(S) := \{g \in G : gSg^{-1} = S\}$  is called the **normalizer** of  $S$  in  $G$ .

### Lemma

$$N_G(S) \leq G.$$

*Proof.*

$$eSe = S, \text{ so } e \in N_G(S).$$

$$\text{If } g, h \in N_G(S), \text{ then } ghS(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S \text{ so } gh \in N_G(S).$$

$$\text{If } g \in N_G(S), \text{ then } g^{-1}Sg = g^{-1}(gSg^{-1})g = eSe = S, \text{ so } g^{-1} \in N_G(S). \quad \square$$

### Lemma

Suppose  $H \leq G$ . Then  $H \trianglelefteq G$  if and only if  $N_G(H) = G$ .

### Corollary

If  $G = \langle S \rangle$  and  $H \leq G$ , then  $H \trianglelefteq G$  if and only if  $gHg^{-1} = H$  for all  $g \in S$ .

*Proof.*

$H \trianglelefteq G$  if and only if  $N_G(H) = G$  if and only if  $S \subseteq N_G(H)$  (the normalizer is a subgroup of  $G$ , so it is equal to  $G$  iff it contains the generators of  $G$ ).  $\square$

Warning: it is possible to have  $gHg^{-1} \subseteq H$  and  $g \notin N_G(H)$ .

### Lemma

If  $|g| < \infty$  and  $gHg^{-1} \subseteq H$ , then  $g \in N_G(H)$ .

*Proof.*

Induction: if  $gHg^{-1} \subseteq H$ , then  $g^iHg^{-i} \subseteq H$  for all  $i \geq 0$ .

If  $|g| = n < \infty$ , then  $g^{-1}Hg = g^{n-1}Hg^{-(n-1)} \subseteq H$ . Hence  $H \subseteq gHg^{-1}$ , so  $gHg^{-1} = H$ .  $\square$

### Corollary

Suppose  $G = \langle S \rangle$  is finite and  $H \leq G$ . If  $gHg^{-1} \subseteq H$  for all  $g \in S$ , then  $H \trianglelefteq G$ .

## Centres

### Definition — centre

If  $G$  is a group, the **centre** of  $G$  is  $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$ .

That is,  $Z(G)$  is the set of elements in  $G$  which commute with all elements in  $G$ .

### Example

$$Z(\mathrm{GL}_n \mathbb{C}) = \{\lambda I_n : \lambda \neq 0\}.$$

### Proposition

$$Z(G) \trianglelefteq G.$$

*Proof (exercise).*

$eh = he$  for all  $h \in G$ , so  $e \in Z(G)$ .

If  $g, h \in Z(G)$  and  $k \in G$ , then  $ghk = gkh = kgh$  so  $gh \in Z(G)$ .

If  $g \in Z(G)$  and  $k \in G$ , then  $gk = kg \implies k = g^{-1}kg \implies kg^{-1} = g^{-1}k$  so  $g^{-1} \in Z(G)$ .

Thus  $Z(G) \leq G$ .

By definition, we clearly have  $kZ(G) = Z(G)k$  for all  $k \in G$ , so  $Z(G) \trianglelefteq G$ . □

## 8: Product groups

### Getting more groups

#### Proposition

Suppose  $(G_1, \cdot_1)$  and  $(G_2, \cdot_2)$  are groups. Then  $G_1 \times G_2$  is a group under operation

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2)$$

for  $g_i, h_i \in G_i$  where  $i = 1, 2$ .

#### *Proof (homework).*

Since  $G_1$  and  $G_2$  are groups, they are closed under  $\cdot_1$  and  $\cdot_2$  respectively, so  $\cdot$  is clearly a binary operation on  $G_1 \times G_2$  by construction. Furthermore,  $\cdot_1$  and  $\cdot_2$  are associative, so  $\cdot$  is clearly associative by construction.

Letting  $e_1 = e_{G_1}$  and  $e_2 = e_{G_2}$ , we see

$$(e_1, e_2) \cdot (g_1, g_2) = (g_1, g_2) = (g_1, g_2) \cdot (e_1, e_2)$$

for all  $g_1 \in G_1$  and  $g_2 \in G_2$ , so  $(e_1, e_2)$  is an identity in  $G_1 \times G_2$ .

For  $(g_1, g_2) \in G_1 \times G_2$ , we know  $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$  and

$$(g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) = (e_1, e_2) = (g_1^{-1}, g_2^{-1}) \cdot (g_1, g_2)$$

so  $(g_1, g_2)$  has an inverse in  $G_1 \times G_2$ , namely  $(g_1^{-1}, g_2^{-1})$ . □

#### Definition — product group

If  $G_1, G_2$  are groups, the group  $G_1 \times G_2$  with the operation from the above proposition is called the **product** of  $G_1$  and  $G_2$ .

#### Example: Klein 4-group

Obviously  $|G_1 \times G_2| = |G_1| \cdot |G_2|$ , so the group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  has order 4. We call this the **Klein 4-group**.

The group's multiplication table is

	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(1, 0)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(1, 1)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

so all elements have order 2 and thus the group is not cyclic.

The identity is  $(0, 0)$ . In general,  $e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$ .

## Two subgroups of a product

### Proposition

Suppose  $G = H \times K$ . Let  $\tilde{H} = \{(h, e_K) : h \in H\}$  and  $\tilde{K} = \{(e_H, k) : k \in K\}$ . Then

1.  $\tilde{H}, \tilde{K} \leq G$ .
2.  $H \rightarrow \tilde{H} : h \mapsto (h, e)$  and  $K \rightarrow \tilde{K} : k \mapsto (e, k)$  are isomorphisms.

*Proof (homework).*

□

So we can think of  $H$  and  $K$  as subgroups of  $H \times K$ . Note  $H \times K$  can have many other subgroups as well.

Compactly, we can write  $\tilde{H} = H \times \{e\} \leq H \times K$  and  $\tilde{K} = \{e\} \times K \leq H \times K$ .

These subgroups commute.

### Lemma

If  $h \in \tilde{H}$  and  $k \in \tilde{K}$ , then  $hk = kh$ .

*Proof (homework).*

For clarity, say  $\tilde{h} = (h, e) \in \tilde{H}$  and  $\tilde{k} = (e, k) \in \tilde{K}$ . Then

$$\tilde{h}\tilde{k} = (h, e) \cdot (e, k) = (h, k) = (e, k) \cdot (h, e) = \tilde{k}\tilde{h}.$$

□

### Corollary

If  $\phi: H \times K \rightarrow G$  is a homomorphism, then  $\phi(h)\phi(k) = \phi(k)\phi(h)$  for all  $h \in \tilde{H}$  and  $k \in \tilde{K}$ .

This is a simple result, but we can actually prove a version equivalent to the converse as well.



## Homomorphisms between products

### Lemma

If  $\alpha: H \rightarrow G$  and  $\beta: K \rightarrow G$  are homomorphisms such that  $\alpha(h)\beta(k) = \beta(k)\alpha(h)$  for all  $h \in H$  and  $k \in K$ , then  $\gamma: H \times K \rightarrow G: (h, k) \mapsto \alpha(h)\beta(k)$  is a homomorphism.

### Proof.

For all  $x, z \in H$  and  $y, w \in K$ :

$$\begin{aligned}\gamma((x, y) \cdot (z, w)) &= \gamma((xz, yw)) \\ &= \alpha(xz)\beta(yw) \\ &= \alpha(x)\alpha(z)\beta(y)\beta(w) \\ &= \alpha(x)\beta(y)\alpha(z)\beta(w) \\ &= \gamma(x, y)\gamma(z, w).\end{aligned}$$

□

Notation: the homomorphism  $\gamma$  is called  $\alpha \cdot \beta$  (not entirely standard).

### Corollary

If  $\alpha: H \rightarrow H'$  and  $\beta: K \rightarrow K'$  are homomorphisms, then  $\gamma: H \times K \rightarrow H' \times K': (h, k) \mapsto (\alpha(h), \beta(k))$  is a homomorphism.

### Proof.

Define  $\tilde{\alpha}: H \rightarrow H' \times K': h \mapsto (\alpha(h), e)$  and  $\tilde{\beta}: K \rightarrow H' \times K': k \mapsto (e, \beta(k))$ .

From the homework,  $\tilde{\alpha}$  and  $\tilde{\beta}$  are homomorphisms, and that  $\tilde{\alpha}(x)\tilde{\beta}(y) = \tilde{\beta}(y)\tilde{\alpha}(x)$  for all  $x \in H$  and  $y \in K$ .

Then  $\gamma((x, y)) = (\alpha(x), \beta(y)) = \tilde{\alpha}(x) \cdot \tilde{\beta}(y)$  so  $\gamma = \tilde{\alpha} \cdot \tilde{\beta}$ .

□

Notation: the homomorphism  $\gamma$  is called  $\alpha \times \beta$  (more standard).

### Corollary

If  $\alpha: H \rightarrow H'$  and  $\beta: K \rightarrow K'$  are isomorphisms, then  $\alpha \times \beta: H \times K \rightarrow H' \times K'$  is an isomorphism.

*Proof.*

$\alpha \times \beta$  has inverse  $\alpha^{-1} \times \beta^{-1}$ . □

### Proposition

$G \rightarrow G \times \{e\} : g \mapsto (g, e)$  is an isomorphism.

*Proof.*

See homework for equivalent proof. □

## Groups of small order (revised)

We can use products to complete the list of groups of order  $p^2$ .

### Proposition

Suppose  $p$  is prime and  $|G| = p^2$ . Then either  $G$  is cyclic, or  $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ .

*Proof (homework).*

□

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}, D_6 = S_3, ??$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}, D_8, ??$
9	$\mathbb{Z}/9\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

## How do we know if a group is a product?

Recall:

### Proposition

Suppose  $G = H \times K$ . Let  $\tilde{H} = \{(h, e_K) : h \in H\}$  and  $\tilde{K} = \{(e_H, k) : k \in K\}$ . Then

1.  $\tilde{H}, \tilde{K} \leq G$ .
2.  $H \rightarrow \tilde{H} : h \mapsto (h, e)$  and  $K \rightarrow \tilde{K} : k \mapsto (e, k)$  are isomorphisms.

Corollary:  $H \times K \rightarrow \tilde{H} \times \tilde{K} : (h, k) \mapsto ((h, e), (e, k))$  is an isomorphism.

Other properties of  $\tilde{H}$  and  $\tilde{K}$  (homework):

- If  $h \in \tilde{H}$  and  $k \in \tilde{K}$ , then  $hk = kh$ .
- Every  $g \in G$  can be written as  $g = \tilde{h}\tilde{k}$  for unique  $\tilde{h} \in \tilde{H}$  and  $\tilde{k} \in \tilde{K}$ .

## Unique factorizations

Given  $S, T \subseteq G$ , let  $ST = \{gh : g \in S, h \in T\}$ .

### Lemma

$G = ST$  if and only if every  $g \in G$  can be written as  $g = hk$  for some  $h \in S$  and  $k \in T$ .

Example:  $D_{2n} = \{s^i r^j\} = \langle s \rangle \langle r \rangle$ .

Question: if  $G = HK$  for  $H, K \leq G$ , when does  $g = hk$  for unique  $h \in H$  and  $k \in K$ ? (Uniqueness means that if  $g = hk = h'k'$  for  $h, h' \in H$  and  $k, k' \in K$ , then  $h = h'$  and  $k = k'$ .)

Notice if  $e \neq g \in H \cap K$ , then  $g = ge = eg$  so the factorization is not unique. So a necessary condition for unique factorization is that  $H \cap K = \{e\}$ . This is actually sufficient:

### Lemma

Suppose  $G = HK$  for  $H, K \leq G$  for  $H, K \leq G$ . Then every element  $g \in G$  can be written as  $g = hk$  for unique  $h \in H$  and  $k \in K$  if and only if  $H \cap K = \{e\}$ .

### Proof.

We already proved  $H \cap K = \{e\}$  is necessary.

Suppose  $H \cap K = \{e\}$ . If  $g = hk = h'k'$ , then  $(h')^{-1}h = k'k^{-1} \in H \cap K$ . So  $(h')^{-1}h = k'k^{-1} = e$  implying  $h = h'$  and  $k = k'$ .  $\square$

## Internal (direct) products

### Definition — internal direct product

$G$  is the **internal direct product** of subgroups  $H, K \leq G$  if

1.  $HK = G$ ,
2.  $H \cap K = \{e\}$ , and
3.  $hk = kh$  for all  $h \in H$  and  $k \in K$ .

### Example

- $H \times K$  is the internal direct product of  $\tilde{H} = H \times \{e\}$  and  $\tilde{K} = \{e\} \times K$ .
- $D_{2n}$  is not the internal direct product of  $\langle s \rangle$  and  $\langle r \rangle$  because  $sr \neq rs$ .

### Theorem

Suppose  $G$  is the internal direct product of  $H$  and  $K$ . Then  $\phi: H \times K \rightarrow G : (h, k) \mapsto hk$  is an isomorphism.

### Proof.

Let  $i_H: H \rightarrow G : h \mapsto h$  and  $i_K: K \rightarrow G : k \mapsto k$ . By part (3) of the definition,  $i_H(h)i_K(k) = i_K(k)i_H(h)$  for all  $h \in H$  and  $k \in K$ , so  $\phi = i_H \cdot i_K$  is a homomorphism.

By lemma, every element  $g \in G$  can be written as  $g = hk$  for unique  $h \in H$  and  $k \in K$ . Thus  $\phi$  is a bijection.  $\square$

## A weaker condition

### Lemma

If  $G$  is an internal direct product of  $H$  and  $K$ , then  $H, K \trianglelefteq G$ .

### Proof.

Suppose  $g \in G$ , so  $g = hk$  for  $h \in H$  and  $k \in K$ . Then  $kHk^{-1} = \{khk^{-1} : h \in H\} = \{kk^{-1}h : h \in H\} = H$ , so  $gHg^{-1} = hkHk^{-1}h^{-1} = hHh^{-1} \subseteq H$ . Then  $H \trianglelefteq G$ .

Similar for  $K$ . □

### Proposition

$G$  is the internal direct product of  $H, K \leq G$  if and only if

1.  $G = HK$ ,
2.  $H \cap K = \{e\}$ , and
3.  $H, K \trianglelefteq G$ .

### Definition — commutator

The **commutator** of  $g, h \in G$  is  $[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$ .

### Lemma

If  $g, h \in G$ , then  $[g, h] = e$  if and only if  $gh = hg$ .

### Proof (proposition).

We already saw the forward implication.

If  $h \in H$  and  $k \in K$ , then  $[h, k] = (hkh^{-1})k^{-1} \in K$  since  $K \trianglelefteq G$ . But  $[h, k] = h(kh^{-1}k^{-1}) \in H$  since  $H \trianglelefteq G$ . So  $[h, k] \in H \cap K = \{e\}$  which implies  $[h, k] = e$ . Hence  $hk = kh$ , which completes the definition of an internal direct product. □

## **Week 4: Quotients and the Isomorphism Theorems**



## 9: Quotient groups

### Left cosets and functions

If  $H \leq G$ , then  $G/H$  is the set of left cosets.

Defining an equivalence relation  $\sim_H$  by  $g \sim_H k \iff g^{-1}k \in H$ , the equivalence class of  $g \in G$  is  $[g] = gH$ .

For example,  $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \leq a < n\}$ . Here,  $\mathbb{Z}/n\mathbb{Z}$  is a group with operation  $[a] + [b] = [a + b]$ .

Can we generalize this by defining a group structure on  $G/H$  by  $[g] \cdot [h] = [gh]$ ? (Or,  $gH \cdot hH = ghH$  as elements of  $G/H$ .) A big problem: this might not be well-defined.

#### Definition — function

A **relation**  $R$  between sets  $X$  and  $Y$  is a subset of  $X \times Y$ . Notation:  $a R b$  if  $(a, b) \in R$ .

A relation  $R$  is a **function** from  $X \rightarrow Y$  if

1. for all  $x \in X$ , there is  $y \in Y$  such that  $x R y$ , and
2. for all  $x \in X$  and  $y, z \in Y$ , if  $x R y$  and  $x R z$  then  $y = z$ .

We can define a relation  $\rightarrow$  between  $G/H \times G/H$  and  $G/H$  by  $([g], [h]) \rightarrow [gh]$  for all  $g, h \in G$ .

Is this relation a function? For (1), if  $x = ([g], [h])$  we can take  $y = [gh]$ . What about (2)?

#### Lemma

The relation  $\rightarrow$  between  $G/H \times G/H$  and  $G/H$  defined by  $([g], [h]) \rightarrow [gh]$  is a function if and only if  $H$  is normal.

Furthermore, if  $H$  is normal, then  $ghH = gh \cdot hH$  (the setwise product).

#### Proof.

In the forward direction, suppose  $\rightarrow$  is a function.

Suppose  $g \in G$  and  $h \in H$ . Then  $([g], [g^{-1}]) \rightarrow [e]$ . But  $[g] = [gh]$ , and  $([gh], [g^{-1}]) \rightarrow [ghg^{-1}]$ . Since  $\rightarrow$  is a function,  $[ghg^{-1}] = [e]$ .

This means  $ghg^{-1} \sim_H e$ , or  $ghg^{-1} \in H$ . This holds for all  $g \in G$  and  $h \in H$ , so  $H \trianglelefteq G$ .

In the reverse direction, suppose  $H$  is normal.

Then  $h^{-1}Hh \subseteq H$  so  $(h^{-1}Hh) \cdot H \subseteq H$ . Since  $e \in h^{-1}Hh$ , we actually get  $(h^{-1}Hh) \cdot H = H$ . Hence  $gH \cdot hH = gh(h^{-1}Hh) \cdot H = ghH$ .

Finally, say  $(S, T) \rightarrow R$  and  $(S, T) \rightarrow R'$  for  $S, T, R, R' \in G/H$ . Then  $R = S \cdot T = R'$ . So  $\rightarrow$  is a function.  $\square$

The converse of the ‘furthermore’ actually holds as well, giving two new characterizations of a subgroup being normal.

## Quotient groups

### Theorem

Let  $N \trianglelefteq G$ . Then the setwise product  $gN \cdot hN = ghN$  makes  $G/N$  into a group. Furthermore, the function  $q: G \rightarrow G/N : g \mapsto gN$  is a surjective homomorphism with  $\ker q = N$ .

$G/N$  is called the **quotient** of  $G$  by  $N$ , or a **quotient group**.

Elements of  $G/N$  can be written as  $gN$  or  $[g]$  or  $\bar{g}$ .

The group operation can be stated as  $gN \cdot hN = ghN$  or  $[g] \cdot [h] = [gh]$  or  $\bar{g} \cdot \bar{h} = \overline{gh}$ .

$q$  is called the **quotient map** or **quotient homomorphism**.

### Proof.

Let  $[g], [h], [k] \in G/N$ .

Then

$$([g] \cdot [h]) \cdot [k] = [gh] \cdot [k] = [ghk] = [g] \cdot [hk] = [g] \cdot ([h] \cdot [k])$$

so  $\cdot$  is associative. Next,

$$[e] \cdot [g] = [eg] = [g] = [ge] = [g] \cdot [e]$$

so  $[e] = N$  is an identity. Finally,

$$[g] \cdot [g^{-1}] = [gg^{-1}] = [e] = [g^{-1}g] = [g^{-1}] \cdot [g]$$

so  $g$  has inverse  $[g^{-1}]$ .

Note  $q$  is clearly surjective, and  $q(gh) = [gh] = [g] \cdot [h] = q(g)q(h)$ . Also,  $q(g) = [g] = [e]$  if and only if  $g \in N$ , so  $\ker q = N$ .  $\square$

## Normal subgroups are kernels

Previously, we proved that if  $\phi: G \rightarrow K$  is a homomorphism then  $\ker \phi \trianglelefteq G$ .

### Corollary

Let  $N \trianglelefteq G$ . Then there is a group  $K$  and homomorphism  $\phi: G \rightarrow K$  such that  $N = \ker \phi$ .

### *Proof.*

Take  $K = G/N$  and  $q: G \rightarrow G/N$  the quotient homomorphism. Then  $\ker q = N$ .  $\square$

## Examples of quotient groups

### Example: $\mathbb{Z}/n\mathbb{Z}$

We can now define this using the theorem instead of relying on the pre-existing definition.

### Example: $D_{2n}/\langle s \rangle$

The cosets are  $\langle s \rangle = \{s^i : 0 \leq i < n\}$  and  $\langle s \rangle r = \{s^i r : 0 \leq i < n\}$ .

Multiplication table:

	$\langle s \rangle$	$\langle s \rangle r$
$\langle s \rangle$	$\langle s \rangle$	$\langle s \rangle r$
$\langle s \rangle r$	$\langle s \rangle r$	$\langle s \rangle$

so  $D_{2n}/\langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$ .

### Example: $N$ not normal

Consider  $\langle r \rangle$ , which has left cosets  $s^i \langle r \rangle = \{s^i, s^i r\}$  for  $0 \leq i < n$ . But  $\langle r \rangle \cdot s \langle r \rangle = \{s, sr, s^{-1}r, s^{-1}\}$  which is not a left coset of  $\langle r \rangle$ .

Also,  $es = s$  is in a different coset from  $rs = s^{-1}r$ , so  $[g] \cdot [h] = [gh]$  is not well-defined here.

### Example: $D_{2n}/Z(D_{2n})$

Homework.

### Example: $\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$

Recall  $Z(\mathrm{GL}_n(\mathbb{K})) = \{\lambda 1 : \lambda \neq 0\}$ .

If  $M$  is invertible, then  $[M] = \{\lambda M : \lambda \neq 0\}$ .

$[M] \cdot [N] = \{\lambda_1 \lambda_2 MN : \lambda_1, \lambda_2 \neq 0\} = [MN]$ .

We think of  $\mathrm{GL}_n(\mathbb{K})$  as the group of invertible linear transformations on  $\mathbb{K}^n$  (acting on vectors).

We can then think of  $\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$  as the invertible transformations of lines through the origin in  $\mathbb{K}^n$ .

$\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$  is called the **projective general linear group**, and is denoted by  $\mathrm{PGL}_n(\mathbb{K})$ .

In general, we can look at:

- $G/Z(G)$  for any group  $G$
- $G/\ker \phi$  for any homomorphism  $\phi: G \rightarrow K$

- $G/N$  for any group  $G$  and normal subgroup  $N \trianglelefteq G$

How do we find the group structure on  $G/N$ ? We will build up techniques for approaching this problem.

## 10: First isomorphism and correspondence theorems

### Homomorphisms from quotients

Suppose  $N \trianglelefteq G$ . What are the homomorphisms  $\psi: G/N \rightarrow K$ ?

$$\begin{array}{ccc} G & \xrightarrow{\psi \circ q} & K \\ & \searrow q \quad \nearrow \psi & \\ & G/N & \end{array}$$

Every such  $\psi$  gives a homomorphism  $\psi \circ q: G \rightarrow K$  (called the **lift** or **pullback** of  $\psi$ ). What homomorphisms  $G \rightarrow K$  do we get?

$$\begin{array}{ccc} G & \xrightarrow{\phi} & K \\ & \searrow q \quad \dashrightarrow \psi & \\ & G/N & \end{array}$$

Given  $\phi$ , when can we fill in  $\psi$  so that the diagram **commutes** (the paths are equivalent)?

#### Theorem — Universal property of quotients

Suppose  $\phi: G \rightarrow K$  is a homomorphism and  $N \trianglelefteq G$ . Let  $q: G \rightarrow G/N$  be the quotient homomorphism. Then there is a homomorphism  $\psi: G/N \rightarrow K$  such that  $\psi \circ q = \phi$  if and only if  $N \subseteq \ker \phi$ . Furthermore, if  $\psi$  exists then it is unique.

In other words, we can fill in  $\psi$  if and only if  $N \subseteq \ker \phi$ .

#### Definition — set of morphisms

If  $G, K$  are groups, let  $\text{Hom}(G, K)$  be the set of morphisms  $G \rightarrow K$ .

#### Corollary

For any groups  $G, K$  and  $N \trianglelefteq G$ , the function

$$q^*: \text{Hom}(G/N, K) \rightarrow \{\phi \in \text{Hom}(G, K) : N \subseteq \ker \phi\} : \psi \mapsto \psi \circ q$$

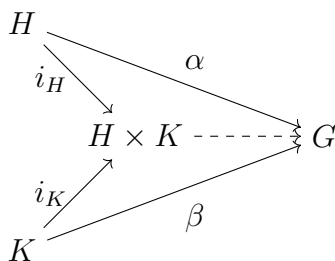
is a bijection.

## Comparison to universal property of products

From before (but without the name):

### Theorem — Universal property of products

Let  $\alpha: H \rightarrow G$  and  $\beta: K \rightarrow G$  be homomorphisms, and let  $i_H: H \rightarrow H \times K$  and  $i_K: K \rightarrow H \times K$  be the inclusions of  $H$  and  $K$  in  $H \times K$ . Then there is a homomorphism  $\phi: H \times K \rightarrow G$  such that  $\phi \circ i_H = \alpha$  and  $\phi \circ i_K = \beta$  if and only if  $\alpha(h)\beta(k) = \beta(k)\alpha(h)$  for all  $h \in H$  and  $k \in K$ .



### Corollary

There is a bijection between  $\text{Hom}(H \times K, G)$  and  $\{(\alpha, \beta) \in \text{Hom}(H, G) \times \text{Hom}(K, G) : \alpha(h)\beta(k) = \beta(k)\alpha(h) \text{ for all } h \in H \text{ and } k \in K\}$ .

We need some more machinery to justify why these are “universal properties”, but for now we can think of them as setting up important bijections.



## Proving the universal property of quotients

### Lemma

If  $\alpha: G \rightarrow H$  is surjective and  $\psi_1, \psi_2: H \rightarrow K$  are such that  $\psi_1 \circ \alpha = \psi_2 \circ \alpha$ , then  $\psi_1 = \psi_2$ .

### Proof.

If  $h \in H$ , then there is  $g \in G$  with  $\alpha(g) = h$ . So  $\psi_1(h) = \psi_1(\alpha(g)) = \psi_2(\alpha(g)) = \psi_2(h)$ .  $\square$

Restatement for reference:

### Theorem — Universal property of quotients

Suppose  $\phi: G \rightarrow K$  is a homomorphism and  $N \trianglelefteq G$ . Let  $q: G \rightarrow G/N$  be the quotient homomorphism. Then there is a homomorphism  $\psi: G/N \rightarrow K$  such that  $\psi \circ q = \phi$  if and only if  $N \subseteq \ker \phi$ . Furthermore, if  $\psi$  exists then it is unique.

### Proof.

If  $\psi$  exists and  $n \in N$ , then  $\phi(n) = \psi(q(n)) = \psi(e) = e$  so  $N \subseteq \ker \phi$ .

Suppose  $N \subseteq \ker \phi$ . Define  $\psi: G/N \rightarrow K: [g] \mapsto \phi(g)$ . To show  $\psi$  is well-defined, note that if  $[g] = [h]$  then  $g^{-1}h \in N \subseteq \ker \phi$ , so  $\phi(g^{-1}h) = e$ , so  $\phi(g) = \phi(h)$ .

Clearly  $\psi \circ q(g) = \psi([g]) = \phi(g)$  for all  $g \in G$ , so  $\psi \circ q = \phi$ .

If  $[g], [h] \in G/N$ , then

$$\psi([g] \cdot [h]) = \psi([gh]) = \phi(gh) = \phi(g)\phi(h) = \psi([g])\psi([h])$$

so  $\psi$  is a homomorphism.

If  $\psi': G/N \rightarrow K$  is another homomorphism with  $\psi' \circ q = \phi$ , then  $\psi' \circ q = \psi \circ q$  which implies  $\psi' = \psi$  by the lemma ( $q$  is surjective). So uniqueness holds.  $\square$

Note  $\phi(gN) = \phi(g)\phi(N) = \phi(g)\{e\} = \{\phi(g)\}$ . So if  $S \in G/N$ , then  $\phi(S) = \{b\}$ , a singleton set. Thus an equivalent way of defining  $\psi$  is by  $\psi(S) = b$  for  $b \in K$  such that  $\phi(S) = \{b\}$ .

## The first isomorphism theorem

Recall: if  $\phi: G \rightarrow K$  is a homomorphism then  $[G : \ker \phi] = |\operatorname{Im} \phi|$ .

Proof: there is a bijection  $\psi: G/\ker \phi \rightarrow \operatorname{Im} \phi$  defined by  $\psi(S) = b$  where  $b \in K$  is such that  $\phi(S) = \{b\}$ .

This looks like what we just did!

Now we also know  $G/\ker \phi$  is a group, so  $|G/\ker \phi| = [G : \ker \phi] = |\operatorname{Im} \phi|$ . Maybe this bijection is an isomorphism?

### Theorem — First isomorphism theorem

Suppose that  $\phi: G \rightarrow K$  is a homomorphism. Then there is an isomorphism  $\psi: G/\ker \phi \rightarrow \operatorname{Im} \phi$  such that  $\phi = \psi \circ q$ , where  $q: G \rightarrow G/\ker \phi$  is the quotient homomorphism.

#### Proof.

First,  $\ker \phi \subseteq \ker \phi$ , so by the universal property there is a homomorphism  $\psi: G/\ker \phi \rightarrow K$  with  $\psi \circ q = \phi$ .

Next  $\psi([g]) = \phi(g)$  so clearly  $\operatorname{Im} \psi = \operatorname{Im} \phi$ . Thus we can regard  $\psi$  as a surjective homomorphism  $G/\ker \phi \rightarrow \operatorname{Im} \phi$ .

To see  $\psi$  is a bijection, note  $\psi$  agrees with the function  $G/\ker \phi \rightarrow \operatorname{Im} \phi$  defined previous to the theorem.

Alternatively, notice if  $\psi([g]) = e$ , then  $\phi(g) = e$ , so  $g \in \ker \phi$  and thus  $[g] = [e]$ . Then  $\psi$  is injective by proposition.  $\square$

### Example

The first isomorphism theorem is usually the best way to determine  $G/N$ :

- Recall  $\operatorname{SL}_n \mathbb{K} \trianglelefteq \operatorname{GL}_n \mathbb{K}$  is defined as the kernel of the determinant homomorphism  $\det: \operatorname{GL}_n \mathbb{K} \rightarrow \mathbb{K}^\times$ . The image is  $\operatorname{Im} \det = \mathbb{K}^\times$ .

By first isomorphism theorem,  $\operatorname{GL}_n \mathbb{K} / \operatorname{SL}_n \mathbb{K} \cong \mathbb{K}^\times$ . (Here, we only use the existence of  $\psi$ .)

- Consider  $\mathbb{Z} \trianglelefteq \mathbb{R}^+$ . What is  $\mathbb{R}/\mathbb{Z}$ ?

We have a homomorphism  $\exp: \mathbb{R} \rightarrow \mathbb{C}^\times : x \mapsto e^{2\pi i x}$  and we know  $e^{2\pi i x} = 1$  if and only if  $x \in \mathbb{Z}$  (so  $\ker \exp = \mathbb{Z}$ ). Then  $\operatorname{Im} \exp = \{a \in \mathbb{C} : |a| = 1\} =: S^1$  (the **circle group**).

So  $\mathbb{R}/\mathbb{Z} \cong S^1$ .

In general, to find  $G/N$  we can try finding a group  $K$  and homomorphism  $\phi: G \rightarrow K$  where  $\ker \phi = N$ . Then the first isomorphism theorem yields  $G/N \cong \text{Im } \phi$ .

There are several more examples on the homework.

Sometimes, we can also turn this around and use the first isomorphism theorem to find  $\text{Im } \phi$ .

## Images and pullbacks

We want to understand subgroups of  $G/N$  using  $q: G \rightarrow G/N$ .

Recall: if  $f: X \rightarrow Y$  is a function and  $S \subseteq X$  and  $T \subseteq Y$ , then

- $f(S) := \{f(x) : x \in S\}$  and
- $f^{-1}(T) := \{x \in X : f(x) \in T\}$ .

From week 2:

### Proposition

If  $\phi: G \rightarrow H$  is a homomorphism and  $K \leq G$ , then  $\phi(K) \leq H$ .

The “pushforward” or image of a subgroup is a subgroup.

### Proposition

If  $\phi: G \rightarrow H$  is a homomorphism and  $K \leq H$ , then  $\phi^{-1}(K) \leq G$ .

The pullback of a subgroup is a subgroup.

## Subgroup correspondence for isomorphisms

If  $f: X \rightarrow Y$  is a bijection, then  $f^{-1}(f(S)) = S$  and  $f(f^{-1}(T)) = T$ . Thus if  $\phi: G \rightarrow H$  is an isomorphism, we get a bijection

$$\begin{array}{ccc} \text{Subgroups} & \xrightarrow{K \mapsto \phi(K)} & \text{Subgroups} \\ \text{of } G & \xleftarrow{\phi^{-1}(K') \mapsto K'} & \text{of } H \end{array}$$

Furthermore:

- $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$
- $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$
- $K \text{ is normal} \iff \phi(K) \text{ is normal}$
- $\phi(\langle S \rangle) = \langle \phi(S) \rangle$
- $[G : K] = [H : \phi(K)]$

## Set operation identities

Some identities for bijections don't hold for general functions.

Always hold	Don't always hold
$A \subseteq B \implies f(A) \subseteq f(B)$	$f(A \cap B) = f(A) \cap f(B)$
$A \subseteq B \implies f^{-1}(A) \subseteq f^{-1}(B)$	$f^{-1}(f(A)) = A$
$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$	$f(f^{-1}(B)) = B$
$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$	
$f(A \cup B) = f(A) \cup f(B)$	

The left column holds for all functions; the right column holds for bijections but not for general functions.

One consequence of these identities is that order is preserved:

### Lemma

If  $\phi: G \rightarrow H$  is a homomorphism, then:

1. If  $K_1 \leq K_2 \leq G$ , then  $\phi(K_1) \leq \phi(K_2)$ .
2. If  $K_1 \leq K_2 \leq H$ , then  $\phi^{-1}(K_1) \leq \phi^{-1}(K_2)$ .

Note we can't say that  $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$  since  $\phi^{-1}(\phi(K)) \neq K$  in general.

Another consequence is that pullbacks preserve intersection:

### Lemma

If  $\phi: G \rightarrow H$  is a homomorphism and  $K_1, K_2 \leq H$ , then  $\phi^{-1}(K_1 \cap K_2) = \phi^{-1}(K_1) \cap \phi^{-1}(K_2)$ .

## Set operation identities for surjections

If we suppose  $f: X \rightarrow Y$  is surjective, the table changes:

Always hold	Don't always hold
$A \subseteq B \implies f(A) \subseteq f(B)$	$f(A \cap B) = f(A) \cap f(B)$
$A \subseteq B \implies f^{-1}(A) \subseteq f^{-1}(B)$	$f^{-1}(f(A)) = A$
$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$	$f(f^{-1}(B)) = B$
$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$	
$f(A \cup B) = f(A) \cup f(B)$	
$f(f^{-1}(B)) = B$	

### Lemma

If  $\phi: G \rightarrow H$  is a surjective homomorphism and  $K \leq H$ , then  $\phi(\phi^{-1}(K)) = K$ .

### Definition — set of subgroups

If  $G$  is a group, let  $\text{Sub}(G)$  denote the set of subgroups of  $G$ .

If  $\phi: G \rightarrow H$  is a homomorphism, we get the induced functions  $\phi: \text{Sub}(G) \rightarrow \text{Sub}(H)$  and  $\phi^{-1}: \text{Sub}(H) \rightarrow \text{Sub}(G)$ .

If  $\phi$  is surjective, the lemma shows  $\phi$  is a left inverse to  $\phi^{-1}$ . So  $\phi^{-1}: \text{Sub}(H) \rightarrow \text{Sub}(G)$  is injective (from homework 1).

Question: what's the image of  $\phi^{-1}$  in  $\text{Sub}(G)$ ?

## The set of pullbacks in $\text{Sub}(G)$

### Lemma

Let  $\phi: G \rightarrow H$  be a homomorphism. Then:

1. If  $K \leq H$ , then  $\ker \phi \leq \phi^{-1}(K)$ .
2. If  $\ker \phi \leq K \leq G$ , then  $\phi^{-1}(\phi(K)) = K$ .

### Proof.

1.  $\ker \phi = \phi^{-1}(\{e\}) \subseteq \phi(H)$ .
2.  $K \leq \phi^{-1}(\phi(K))$  is easy. Suppose  $y \in \phi^{-1}(\phi(K))$ . Then  $\phi(y) \in \phi(K)$ , so  $\phi(y) = \phi(k)$  for some  $k \in K$ . Since  $\phi(k^{-1}y) = e$ , we get  $k^{-1}y \in \ker \phi \subseteq K \implies y \in K$ . We conclude that  $\phi^{-1}(\phi(K)) \subseteq K$ .

□

Conclusion:  $K = \phi^{-1}(K') \iff \ker \phi \leq K$  ( $K$  is a pullback iff  $K$  contains the kernel).

### Theorem — Correspondence theorem

Let  $\phi: G \rightarrow H$  be a surjective homomorphism. Then there is a bijection

$$\begin{array}{ccc}
 \text{Subgroups} & & \\
 K \text{ of } G \text{ with} & \xrightarrow{K \mapsto \phi(K)} & \text{Subgroups} \\
 \ker \phi \leq K & \xleftarrow{\phi^{-1}(K') \mapsto K'} & K' \text{ of } H
 \end{array}$$

Furthermore, if  $\ker \phi \leq K, K_1, K_2 \leq G$  then

1.  $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$ ,
2.  $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$ , and
3.  $K$  is normal  $\iff \phi(K)$  is normal.

### Proof.

Since  $\phi$  is surjective,  $\phi(\phi^{-1}(K')) = K'$  for all  $K' \leq H$ . Conversely, if  $\ker \phi \leq K \leq G$  then  $\phi^{-1}(\phi(K)) = K$ . So  $\phi$  and  $\phi^{-1}$  are inverses on the specified sets.

1. Follows from the fact that  $\phi$  and  $\phi^{-1}$  are inverses and preserve  $\leq$ .
2. By lemma,  $\phi^{-1}(\phi(K_1) \cap \phi(K_2)) = \phi^{-1}(\phi(K_1)) \cap \phi^{-1}(\phi(K_2)) = K_1 \cap K_2$ . Applying  $\phi$  to both sides, we see also  $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$ .
3. (Homework.)

□



## Correspondence theorem for quotient groups

If  $N \trianglelefteq G$ , then  $q: G \rightarrow G/N$  is a surjection.

### Theorem — Correspondence theorem for quotient groups

Let  $N \trianglelefteq G$ . Then there is a bijection

$$\begin{array}{ccc} \text{Subgroups} & \xrightarrow{K \mapsto q(K)} & \text{Subgroups} \\ N \leq K \leq G & \xleftrightarrow{q^{-1}(K') \leftarrow K'} & K' \text{ of } G/N \end{array}$$

Furthermore, if  $N \leq K, K_1, K_2 \leq G$  then

1.  $K_1 \leq K_2 \iff q(K_1) \leq q(K_2)$ ,
2.  $q(K_1 \cap K_2) = q(K_1) \cap q(K_2)$ , and
3.  $K$  is normal  $\iff q(K)$  is normal.

This seems like a specialization of the correspondence theorem, but they are actually equivalent (with some work).

Recall the first isomorphism theorem tells us that if  $\phi: G \rightarrow H$  is a surjective homomorphism, then  $G/\ker \phi \cong H$ . So there is a bijection between  $\text{Sub}(H)$  and  $\text{Sub}(G/\ker \phi)$ .

As an exercise, check that (first isomorphism theorem) + (subgroup correspondence for isomorphisms) + (correspondence theorem for quotient groups) implies (correspondence theorem for surjective homomorphisms).

## Identifying $q(K)$

Suppose  $N \trianglelefteq G$  and  $N \leq K \leq G$ . Let  $q_G: G \rightarrow G/N$  be the quotient map. Since  $N \trianglelefteq K$ , we also have the quotient map  $q_K: K \rightarrow K/N$ .

$$\begin{array}{ccc}
 K & \xrightarrow{i_K} & G \\
 q_K \downarrow & \searrow q_G \circ i & \downarrow q_G \\
 K/N & \xrightarrow{kN \mapsto kN} & G/N
 \end{array}$$

Since  $\ker q_G \circ i = N$ , the first isomorphism theorem tells us there is an isomorphism  $\psi: K/N \rightarrow \text{Im } q \circ i_K = q(K)$  such that  $\psi \circ q_K = q_G \circ i$ .

In other words, if  $k \in K$  then  $\psi(kN) = q(k) = kN$ .

### Proposition

Suppose  $N \trianglelefteq G$  and  $N \leq K \leq G$ . Let  $q: G \rightarrow G/N$  be the quotient map. Then the function  $K/N \rightarrow q(K) \leq G/N: kN \mapsto kN$  is an isomorphism.

Because of this isomorphism, we use the following notation:

### Definition — subgroup $q(K)$

If  $N \trianglelefteq G$  and  $N \leq K \leq G$ , then the subgroup  $q(K)$  corresponding to  $K$  in  $G/N$  is denoted by  $K/N$ .

### Example

- Let  $G = D_{2n}$  and  $N = \langle s \rangle$  where  $s$  is the rotation generator.

Subgroups of  $D_{2n}$  containing  $N$  correspond to subgroups of  $D_{2n}/N = \mathbb{Z}/2\mathbb{Z}$ .  $\mathbb{Z}/2\mathbb{Z}$  only has two subgroups, itself and  $\{e\}$ . So there are only two subgroups of  $D_{2n}$  containing  $N$ .

- $\text{GL}_n \mathbb{K} / \text{SL}_n \mathbb{K} \cong \mathbb{K}^\times$ , so subgroups of  $\text{GL}_n \mathbb{K}$  containing  $\text{SL}_n \mathbb{K}$  correspond to subgroups of  $\mathbb{K}^\times$  (of which there can be many).

## 11: Second and third isomorphism theorems

### Third isomorphism theorem

What about quotients of quotients?

Suppose  $N \trianglelefteq G$  and  $N \leq K \leq G$ .

From the correspondence theorem (homework),  $K \trianglelefteq G$  if and only if  $K/N \trianglelefteq G/N$ . Then suppose  $K/N \trianglelefteq G/N$ . What is  $(G/N)/(K/N)$ ?

#### Theorem — Third isomorphism theorem (informal version)

$$(G/N)/(K/N) \cong G/K.$$

#### Example

Suppose  $n \mid m$ , so  $m\mathbb{Z} \leq n\mathbb{Z}$  (and both are normal).

Then  $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ . For example,  $(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$ .

#### Theorem — Third isomorphism theorem

Let  $N \trianglelefteq G$  and  $N \leq K \trianglelefteq G$ . Let

- $q_1$  be the quotient map  $G \rightarrow G/N$ ,
- $q_2$  be the quotient map  $G/N \rightarrow (G/N)/(K/N)$ , and
- $q_3$  be the quotient map  $G \rightarrow G/K$ .

Then there is an isomorphism  $\psi: G/K \rightarrow (G/N)/(K/N)$  such that  $\psi \circ q_3 = q_2 \circ q_1$ .

$$\begin{array}{ccc} G & \xrightarrow{q_1} & G/N \\ q_3 \downarrow & & \downarrow q_2 \\ G/K & \xrightarrow{\psi} & (G/N)/(K/N) \end{array}$$

#### Proof.

Note that  $\ker q_2 \circ q_1 = (q_2 \circ q_1)^{-1}(\{e\}) = q_1^{-1}(q_2^{-1}(\{e\})) = q_1^{-1}(K/N) = K$ .

Since  $q_2$  and  $q_1$  are surjective,  $\text{Im } q_2 \circ q_1 = (G/N)/(K/N)$ .

By the first isomorphism theorem, there is an isomorphism  $\psi: G/K \rightarrow (G/N)/(K/N)$  such that  $\psi \circ q_3 = q_2 \circ q_1$ .  $\square$

## What if $K$ isn't normal?

Then  $G/K$  isn't a group, and neither is  $(G/N)/(K/N)$ .

However, we can still talk about  $[G : K]$  and  $[G/N : K/N]$ .

### Proposition

If  $N \trianglelefteq G$  and  $N \leq K \leq G$ , then  $[G : K] = [G/N : K/N]$ .

In fact, this doesn't even need quotient spaces. This holds for surjective homomorphisms.

### Proposition

Let  $\phi: G \rightarrow H$  be a surjective homomorphism and suppose  $\ker \phi \leq K \leq G$ . Then  $[G : K] = [H : \phi(K)]$ .

These are equivalent by the first isomorphism theorem.

### Proof.

Define a function  $f: G/K \rightarrow H/\phi(K) : gK \mapsto \phi(g)\phi(K)$ .

Well-defined: if  $gK = hK$ , then  $h^{-1}g \in K \implies \phi(h)^{-1}\phi(g) = \phi(h^{-1}g) \in \phi(K)$ . So  $\phi(g)\phi(K) = \phi(h)\phi(K)$ .

Since  $\phi$  is surjective,  $f$  is surjective.

Suppose  $f(gK) = f(hK)$  so  $\phi(g)\phi(K) = \phi(h)\phi(K)$ . Then  $\phi(h^{-1}g) = \phi(h)^{-1}\phi(g) \in \phi(K)$  which shows  $h^{-1}g \in \phi^{-1}(\phi(K)) = K$  by the correspondence theorem. So  $gK = hK$  and  $f$  is injective.

Then  $f$  is a bijection, so the indices must be equal.  $\square$

## Revisiting products

Recall this lemma:

### Lemma

Suppose  $G = HK$  for  $H, K \leq G$ . Then every element  $g \in G$  can be written as  $g = hk$  for unique  $h \in H$  and  $k \in K$  if and only if  $H \cap K = \{e\}$ .

Which motivated this definition:

### Definition — internal direct product

$G$  is the **internal direct product** of subgroups  $H, K \leq G$  if

1.  $HK = G$ ,
2.  $H \cap K = \{e\}$ , and
3.  $hk = kh$  for all  $h \in H$  and  $k \in K$ .

But the proof of the lemma did not use the fact that  $G = HK$ , so we can generalize it.

### Lemma

Suppose  $H, K \leq G$ . Then every element of  $HK$  can be written as  $hk$  for unique  $h \in H$  and  $k \in K$  if and only if  $H \cap K = \{e\}$ .

If  $H \cap K = \{e\}$ , then  $|HK| = |H| \cdot |K|$ .

What if  $H \cap K \neq \{e\}$ ? Here,  $HK = \bigcup_{h \in H} hK$ , a union of cosets of  $K$ . Let  $X = \{hK : h \in H\} \subseteq G/K$ . Then  $X$  is a partition of  $HK$ , so  $|HK| = |X| \cdot |K|$ . But how large is  $X$ ?

### Lemma

Let  $H, K \leq G$ . If  $h_1, h_2 \in H$ , then  $h_1K = h_2K$  if and only if  $h_1(H \cap K) = h_2(H \cap K)$ .

### Proof.

$h_1K = h_2K \iff h_1^{-1}h_2 \in K \iff h_1^{-1}h_2 \in H \cap K$ . But  $h_1^{-1}h_2 \in H \cap K$  if and only if  $h_1(H \cap K) = h_2(H \cap K)$ .  $\square$

Rephrasing, consider the equivalence relations  $\sim_K$  on  $G$  and  $\sim_{H \cap K}$  on  $H$ : if  $h_1, h_2 \in H$ , then  $h_1 \sim_K h_2 \iff h_1 \sim_{H \cap K} h_2$ .

**Corollary**

$H/(H \cap K) \rightarrow X: h(H \cap K) \rightarrow hK$  is a bijection.

**Proof.**

By the lemma, this is well-defined and injective. Surjectivity is obvious.  $\square$

Now we see  $|X| = [H : H \cap K]$ , so  $|HK| = [H : H \cap K]|K|$ . Lagrange's theorem yields  $[H : H \cap K] \cdot |H \cap K| = |H|$ , so we have:

**Proposition**

If  $H, K \leq G$ , then  $|HK||H \cap K| = |H||K|$ .

If  $H$  and  $K$  are finite, another way to think of this formula is  $[H : H \cap K] = |X| = \frac{|HK|}{|K|}$ .

Is the fraction an index as well? Maybe  $HK$  is not necessarily a group.

**Proposition**

Let  $H, K \leq G$ . Then  $HK \leq G \iff HK = KH \iff KH \subseteq HK$ .

**Proof.**

If  $HK \leq G$  and  $h \in H$  and  $k \in K$ , then  $h, k \in HK$  so  $kh \in HK$ . Also,  $k^{-1}h^{-1} \in HK$ , so  $k^{-1}h^{-1} = h_0k_0$ . Hence  $hk = (k^{-1}h^{-1})^{-1} = k_0^{-1}h_0^{-1} \in KH$ . So  $KH \subseteq HK$  and  $HK \subseteq KH$ , hence  $HK = KH$ .

Now suppose  $KH \subseteq HK$ , we need to show  $HK \leq G$ . We always have  $e \in HK$ . If  $x, y \in HK$ , then  $x = h_0k_0$  and  $y = h_1k_1$  for some  $h_0, h_1 \in H$  and  $k_0, k_1 \in K$ . Since  $KH \subseteq HK$ ,  $k_0^{-1}h_0^{-1}h_1 = h_2k_2$  for some  $h_2 \in H$  and  $k_2 \in K$ . So  $x^{-1}y = k_0^{-1}h_0^{-1}h_1k_1 = h_2k_2k_1 \in HK$ .  $\square$

Corollary: if  $KH \subseteq HK$ , then  $[H : H \cap K] = [HK : K]$  (exercise: even for infinite  $HK$  or  $K$ ).

When is  $KH \subseteq HK$ ?

A sufficient condition is that for all  $h \in H$ , there is  $h' \in H$  such that  $Kh = h'K$ . Recall that if  $Kh = h'K$ , then  $h'K = Kh$ . So we can rephrase this condition as  $hKh^{-1} = K$  for all  $h \in H$ , or  $H \subseteq N_G(K)$ .

**Corollary**

If  $H \subseteq N_G(K)$ , then  $HK \leq G$ , and hence  $[H : H \cap K] = [HK : K]$ .

What else does  $H \subseteq N_G(K)$  imply?

We know  $hKh^{-1} = K$  and  $kKk^{-1} = K$ , so  $H, K \subseteq N_{HK}(K) \implies N_{HK}(K) = HK \implies K \trianglelefteq HK$ .

If  $k \in H \cap K$  and  $h \in H$ , then  $hkh^{-1} \in H \cap K$ . So  $H \cap K \trianglelefteq H$ .

## Second isomorphism theorem

### Theorem — Second isomorphism theorem

Suppose  $H \subseteq N_G(K)$ . Then  $HK \leq G$ ,  $K \trianglelefteq HK$ , and  $H \cap K \trianglelefteq H$ . Furthermore, if  $i_H: H \rightarrow HK$  is the inclusion and  $q_1: H \rightarrow H/(H \cap K)$  and  $q_2: HK \rightarrow HK/K$  are the quotient maps, then there is an isomorphism  $\psi: H/(H \cap K) \rightarrow HK/K$  such that  $\psi \circ q_1 = q_2 \circ i_H$ .

$$\begin{array}{ccc} H & \xrightarrow{i_H} & HK \\ q_1 \downarrow & & \downarrow q_2 \\ H/H \cap K & \xrightarrow{\psi} & HK/K \end{array}$$

#### Proof.

We've already shown  $HK \leq G$ ,  $K \trianglelefteq HK$ , and  $H \cap K \trianglelefteq H$ .

If  $h \in H$  and  $k \in K$ , then  $hkk = hk$ . So  $HK/K = \{gK : g \in HK\} = \{hK : h \in H\}$ . Hence  $\text{Im } q_2 \circ i_H = \{hK : h \in H\} = HK/K$ .

Next,  $\ker q_2 \circ i_H = i_H^{-1}(q_2^{-1}(\{e\})) = i_H^{-1}(K) = H \cap K$ .

By the first isomorphism theorem, there is an isomorphism  $\psi$  as desired.  $\square$

#### Example: $\text{PGL}_n \mathbb{C}$

Recall  $\text{PGL}_n \mathbb{C} = \text{GL}_n \mathbb{C} / Z(\text{GL}_n \mathbb{C})$ .

Let  $K = Z(\text{GL}_n \mathbb{C}) = \{\lambda 1 : \lambda \neq 0\}$ .

Since  $K \trianglelefteq \text{GL}_n \mathbb{C}$ ,  $N_{\text{GL}_n \mathbb{C}}(K) = \text{GL}_n \mathbb{C}$ .

Take  $H = \text{SL}_n \mathbb{C} = \{M \in \text{GL}_n \mathbb{C} : \det M = 1\} \trianglelefteq \text{GL}_n \mathbb{C} = N_{\text{GL}_n \mathbb{C}}(K)$ , so  $HK \leq \text{GL}_n \mathbb{C}$  by the second isomorphism theorem.

Suppose  $M \in \text{GL}_n \mathbb{C}$  and let  $\lambda = \det M$ . Then  $\det \lambda^{-1/n} M = \lambda^{-1} \det M = 1$ , so  $\lambda^{-1/n} M \in H$  (for any choice of  $\lambda^{-1/n}$ ).

We conclude  $\text{GL}_n \mathbb{C} = HK$ .

Now define  $C_n := H \cap K = \{\lambda 1 : \lambda^n = 1\} = \{e^{2\pi i k/n} : k = 0, \dots, n-1\}$ . (Note  $C_n \cong \mathbb{Z}/n\mathbb{Z}$ .)

By the second isomorphism theorem,  $\text{PGL}_n \mathbb{C} \cong \text{SL}_n \mathbb{C} / C_n$ .