

# **PMATH 347: Groups and Rings**

University of Waterloo  
William Slofstra  
Spring 2021

Marco Yang

Last updated: July 15, 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	

## **5 Group Actions**

<b>12</b>	<b>Group actions and Cayley's theorem</b> .....	<b>118</b>
	Group actions	
	Invariant subsets	
	Actions on functions	
	Actions on subsets	
	Left regular actions	

	Right actions	
	Permutation representations	
	Permutation representations of the dihedral group	
	Faithful actions	
<b>13</b>	<b>Orbits and stabilizers</b> .....	130
	Orbits	
	Equivalence relation from a $G$ -action	
	Stabilizers	
	Example: $S_n$	
	Example: $G/H$	
	Kernel versus stabilizer	
	Conjugation actions	
	Example: matrices	
	Class equation and Cauchy's theorem	
	Center of $p$ -groups	
<b>6</b>	<b>Classification of Groups</b>	
<b>14</b>	<b>Classification of groups</b> .....	143
	Groups of order $p$ squared	
	Groups of order $pq$	
	What can we say?	
	Decomposing finite abelian groups	
<b>7</b>	<b>Rings</b>	
<b>15</b>	<b>Rings and fields</b> .....	152
	Rings	
	Basic properties	
	Multiplicative identities	
	Units	
	The trivial ring	
	Fields and division rings	
	Example: $\mathbb{Z}/n\mathbb{Z}$	
	Division rings	
<b>16</b>	<b>Subrings and homomorphisms</b> .....	161
	Subrings	
	Alternative approach: non-unital subrings	
	Characteristics and prime subrings	
	Centre of a ring	
	Ring homomorphisms	
	Basic properties of ring homomorphisms	
<b>17</b>	<b>Polynomials and group rings</b> .....	169
	Polynomials, formally	

Terminology/notation for polynomial rings  
 Degree and coefficients  
 Constant polynomials  
 Commutativity  
 Evaluation  
 Polynomials over fields  
 Multivariable polynomials  
 Multivariate evaluation  
 Group rings  
 $G$  versus  $RG$   
 Ring operations of a group ring  
 Group ring homomorphisms

## 8 Ideals and Quotient Rings

<b>18</b>	<b>Ideals</b> .....	184
	Example: $m\mathbb{Z}$	
	Simplifying conditions	
	Example: evaluation	
	Ideals containing 1	
	Ideals in fields	
<b>19</b>	<b>Quotient rings</b> .....	190
	Review on quotient groups	
	Are ideals always the kernel of some homomorphism?	
	Universal property of quotient groups, and quotient rings	
	First isomorphism theorem for rings	
<b>20</b>	<b>Ideals generated by a subset</b> .....	196
	Ideal generated by a subset	
	The sum of ideals	
	Lattice of ideals	
	Quotients by a subset	
	Ideals generated by a finite subset	
	Principal ideals	
	Principal ideals in non-commutative rings	
	More examples in polynomial rings	
<b>21</b>	<b>Correspondence, second and third isomorphism theorems</b> .....	205
	Connecting ideals and homomorphisms (correspondence theorem)	
	Second isomorphism theorem	
	Third isomorphism theorem	

## 9 Maximal and Prime Ideals

<b>22</b>	<b>Maximal ideals and fields</b> .....	212
	Constructing complex numbers from real numbers	

	The complex numbers	
	Generalizations	
	Maximal ideals	
	Ideals in fields	
	Maximal ideals and fields	
	Partially-ordered sets	
	Proper ideals ordered under inclusion	
	Maximal elements for the set of proper ideals?	
	Chains of ideals	
	Zorn's lemma	
	Maximal elements for the set of proper ideals, continued	
<b>23</b>	<b>Prime ideals and integral domains</b> .....	<b>227</b>
	Zero divisors	
	Units and zero divisors	
	Cancellation laws	
	Integral domains	
	Interesting domains?	
	Prime ideals	
	Primality and factoring	
	A related idea	

## **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.

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

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  $|g| = |g^{-1}|$ .  $\square$



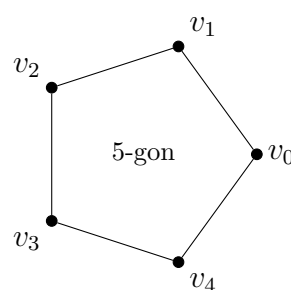
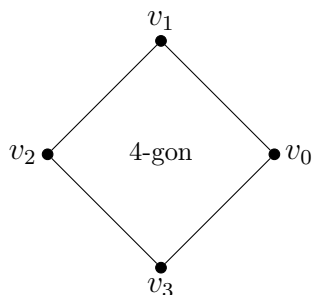
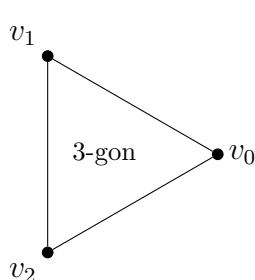
## 2: Dihedral and permutation groups

### 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**

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

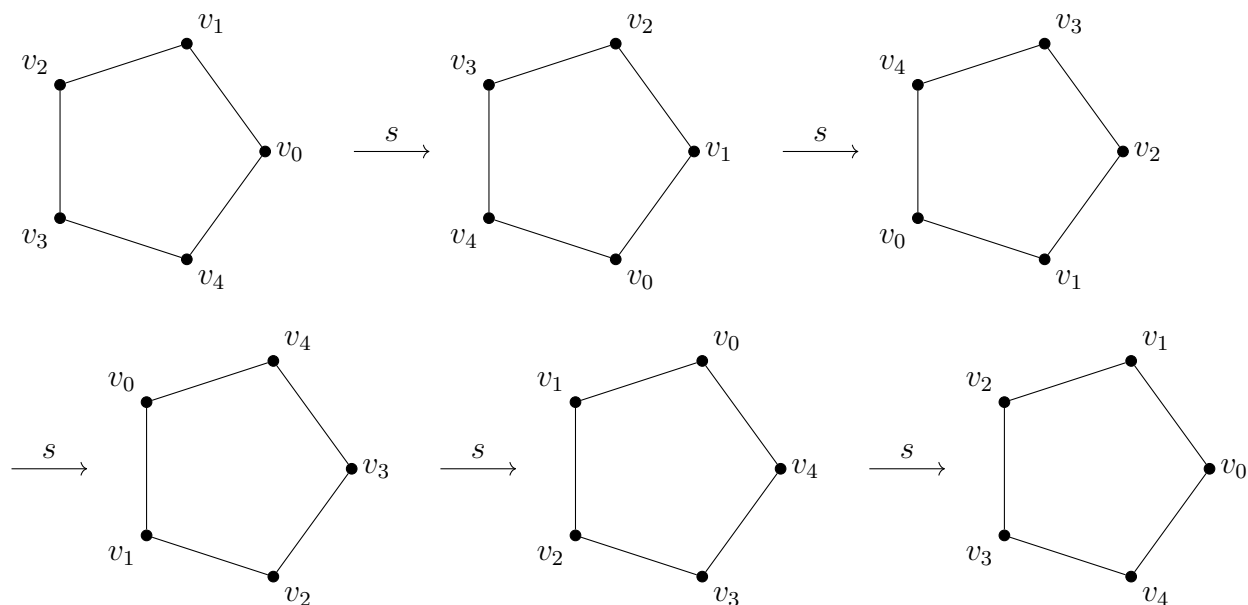
*Proof.*

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. □

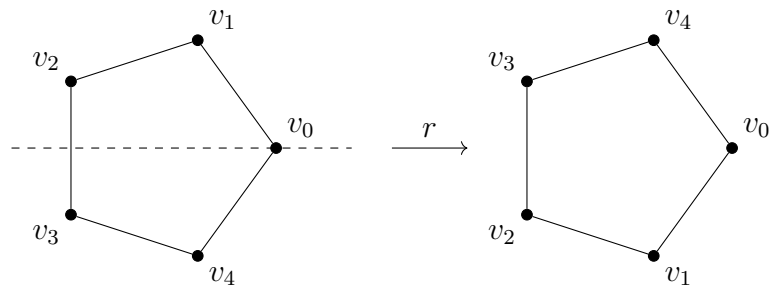
Intuitively, we can ask: for every pair of adjacent vertices  $(v_i, v_j)$ , is there an element  $T \in D_{2n}$  with  $T(v_0) = v_i$  and  $T(v_1) = v_j$ ? If yes, then  $|D_{2n}| = 2n$ .

### 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.



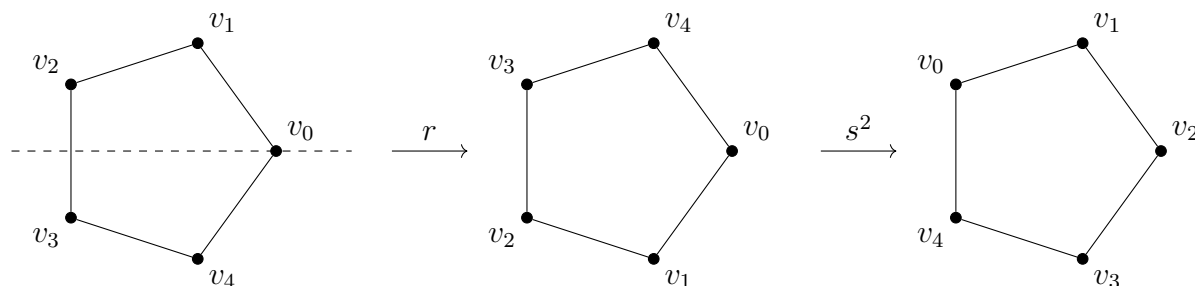
$|r| = 2$ , that is,  $r^2 = e$  and  $r \neq e$ .

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  $\langle S \rangle = K$ . □

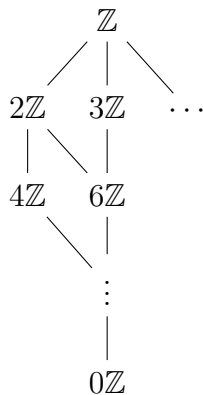
## Lattice of subgroups

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



## 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,  $\text{PGL}_n \mathbb{C} \cong \text{SL}_n \mathbb{C} / C_n$ .

## **Week 5: Group Actions**

## 12: Group actions and Cayley's theorem

### Group actions

#### Example

Permutations  $S_n$  of  $\{1, \dots, n\}$  form a group.

This means we can multiply permutations together: e.g.  $(12)(34)(24) = (1234)$ .

But we can also plug in numbers from  $\{1, \dots, n\}$ : e.g.  $((12)(34))(3) = 4$ .

We say that  $S_n$  **acts** on  $\{1, \dots, n\}$ .

#### Example

Similarly, for  $\text{GL}_n \mathbb{C}$ , we can do more than multiply matrices: we can also multiply matrices and vectors.

Given  $A \in \text{GL}_n \mathbb{C}$  and  $v \in \mathbb{C}^n$ , we get  $Av \in \mathbb{C}^n$ .

We say that  $\text{GL}_n \mathbb{C}$  **acts** on  $\mathbb{C}^n$ .

Group actions can reveal a lot about a group.

#### Definition — (left) action

Let  $G$  be a group. A **(left) action** of  $G$  on a set  $X$  is a function  $\cdot : G \times X \rightarrow X$  such that

1.  $e \cdot x = x$  for all  $x \in X$ , and
2.  $g \cdot (h \cdot x) = (gh) \cdot x$  for all  $g, h \in G$  and  $x \in X$ .

#### Example

- $S_n$  acts on  $\{1, \dots, n\}$  for  $n \geq 1$  (proof: below).
- $\text{GL}_n \mathbb{K}$  acts on  $\mathbb{K}^n$  (proof: exercise).
- If  $X$  is any set and  $G$  is any group, we can define an action of  $G$  on  $x$  by  $g \cdot x = x$  for all  $g \in G$  and  $x \in X$ . This is the **trivial action** of  $G$  on  $X$ . Proof: (1) clear; (2)  $g \cdot (h \cdot x) = g \cdot x = x = (gh) \cdot x$ .

**Proposition**

Let  $X$  be a set. The group  $S_X$  (of invertible functions  $X \rightarrow X$  under composition  $\circ$ ) acts on  $X$  via  $f \cdot x = f(x)$ .

**Proof.**

The identity  $1$  in  $S_X$  is the identity function, so  $1 \cdot x = 1(x) = x$ . If  $f, g \in S_X$ , then  $(f \circ g)(x) = f(g(x)) = f \cdot (g \cdot x)$ .  $\square$

Note: usually we use notation  $f(x)$  rather than  $f \cdot x$ . Also, recall  $S_n = S_{\{1, \dots, n\}}$ .

**Lemma**

If  $G$  acts on  $X$  and  $H \leq G$ , then  $H$  acts on  $X$  by the restricted action  $H \times X \rightarrow X : (h, x) \mapsto h \cdot x$ .

Hence an alternative way to show  $\mathrm{GL}_n \mathbb{K}$  acts on  $\mathbb{K}^n$  is to observe  $\mathrm{GL}_n \mathbb{K} \leq S_{\mathbb{K}^n}$ . (Invertible  $n \times n$  matrices are invertible functions  $\mathbb{K}^n \rightarrow \mathbb{K}^n$ .)

## Invariant subsets

Groups aren't tied to a particular action.

### Example

$D_{2n}$  was defined as a subgroup of  $\text{GL}_2 \mathbb{R}$ , so it acts on  $\mathbb{R}^2$ .

However,  $D_{2n}$  also acts on the vertices  $v_0, \dots, v_{n-1}$  of the  $n$ -gon.

In fact, this action determines elements of  $D_{2n}$ :

- $s^i$  sends  $v_0 \mapsto v_i$  and  $v_1 \mapsto v_{i+1}$
- $s^i r$  sends  $v_0 \mapsto v_i$  and  $v_1 \mapsto v_{i-1}$

This dihedral group action on the vertices of the  $n$ -gon is a special case of a pattern.

### Definition — invariant under an action

If  $G$  acts on  $X$ , a subset  $Y \subseteq X$  is **invariant under the action of  $G$**  if  $g \cdot y \in Y$  for all  $g \in G$  and  $y \in Y$ .

### Lemma

If  $G$  acts on  $X$  and  $Y$  is an invariant subset, then  $G$  acts on  $Y$  via  $G \times Y \rightarrow Y : (g, y) \mapsto g \cdot y$ .

### Example

$\{0\}$  is an invariant subset of  $\mathbb{K}^n$  under the action of  $\text{GL}_n \mathbb{K}$ . In this case, the action of  $\text{GL}_n \mathbb{K}$  on  $\{0\}$  is the trivial action.

## Actions on functions

### Proposition

Suppose  $G$  acts on  $X$  and  $Y$ , and let  $\text{Fun}(X, Y)$  denote the set of functions from  $X$  to  $Y$ .

If  $g \in G$  and  $f \in \text{Fun}(X, Y)$ , let  $g \cdot f$  be the function

$$g \cdot f: X \rightarrow Y : x \mapsto g \cdot f(g^{-1} \cdot x).$$

Then  $G \times \text{Fun}(X, Y) : (g, f) \mapsto g \cdot f$  is a left action of  $G$  on  $\text{Fun}(X, Y)$ .

*Proof (homework).*

□

Often we apply this function with the trivial action on  $Y$ , so the action looks like  $g \cdot f(x) = f(g^{-1} \cdot x)$ .



## Actions on subsets

### Proposition

Suppose  $G$  acts on  $X$ , and let  $2^X$  denote the set of subsets of  $X$ . Then  $g \cdot S = \{g \cdot s : s \in S\}$  defines an action of  $G$  on  $2^X$ .

#### *Proof.*

Let  $S \in 2^X$ .

First,  $e \cdot S = \{e \cdot s : s \in S\} = \{s : s \in S\} = S$ .

Next, let  $g, h \in G$ . Then

$$\begin{aligned} g \cdot (h \cdot S) &= g \cdot \{h \cdot s : s \in S\} \\ &= \{g \cdot (h \cdot s) : s \in S\} \\ &= \{gh \cdot s : s \in S\} \\ &= gh \cdot S. \end{aligned}$$

□

Alternative proof: use  $2^X$  as the set of functions  $X \rightarrow \{0, 1\}$ . Realize action of  $G$  on  $2^X$  by taking action on functions with trivial action on  $\{0, 1\}$  (homework).

## Left regular actions

Does every group act on some set?

### Lemma

If  $G$  is a group, then the multiplication map  $\cdot : G \times G \rightarrow G$  is a left action of  $G$  on  $G$ .

### Proof.

Immediate from group definition. □

So every group acts on itself by left multiplication. This action is called the **left regular action** of  $G$  on  $G$ .

### Lemma

If  $H \leq G$ , then  $G$  acts on  $G/H$  by  $g \cdot (kH) = gkH$ .

### Proof.

$G/H$  is an invariant subset of  $2^G$ . □

Since  $G/\{e\} = G$ , this generalizes the left regular action.

## Right actions

### Example

Let  $G$  be a group where the product of  $g$  and  $h$  is denoted  $gh$ .

For  $g, k \in G$ , define  $g \cdot k = kg$  (right multiplication). If  $g, h, k \in G$ , then  $g \cdot (h \cdot k) = g \cdot kh = khg$ , but  $gh \cdot k = kgh$ , which is not equal to  $kgh$  if  $hg \neq gh$ .

So right multiplication does not define a left action in general.

Can we fix this?

### Definition — (right) action

Let  $G$  be a group. A **(right) action** of  $G$  on a set  $X$  is a function  $\cdot : X \times G \rightarrow X$  such that

1.  $x \cdot e = x$  for all  $x \in X$ , and
2.  $(x \cdot g) \cdot h = x \cdot (gh)$  for all  $g, h \in G$  and  $x \in X$ .

### Example

- There is a right action of  $G$  on itself by right multiplication. This is called the **right regular action** of  $G$  on  $G$ . More generally, if  $H \leq G$  then  $G$  acts on  $H \backslash G$ .
- If  $G$  is a group and  $X$  is a set, then there is a trivial right action of  $G$  on  $X$  defined by  $x \cdot g = x$  for all  $g \in G$  and  $x \in X$ .
- If there is a right action of  $G$  on  $X$ , and  $Y$  is any set, then  $(g \cdot f)(x) = f(g \cdot x)$  defines a *left* action of  $G$  on  $\text{Fun}(X, Y)$ .

Can we reconcile right and left actions somehow?

### Proposition

If  $\cdot$  is a right action of  $G$  on  $X$ , then  $g \cdot x = x \cdot g^{-1}$  defines a left action of  $G$  on  $X$ .

*Proof.*

First  $e \cdot x = x \cdot e = x$ , and for  $g, h \in G$  and  $x \in X$ , we get

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot (x \cdot h^{-1}) \\ &= (x \cdot h^{-1}) \cdot g^{-1} \\ &= x \cdot h^{-1} g^{-1} \\ &= x \cdot (gh)^{-1} \\ &= gh \cdot x. \end{aligned}$$

□

Combined with the last example, this proposition explains why if  $\cdot$  is a left action of  $G$  on  $X$ , we can define a left action of  $G$  on  $\text{Fun}(X, Y)$  by setting  $(g \cdot f)(x) = f(g^{-1} \cdot x)$ .

## Permutation representations

### Lemma

If  $G$  has a left action on a set  $X$ , and  $g \in G$ , let  $\ell_g: X \rightarrow X$  be defined by  $\ell_g(x) = g \cdot x$ . Then:

1.  $\ell_g \circ \ell_h = \ell_{gh}$  for all  $g, h \in G$ .
2.  $\ell_e = 1$ , the identity function.
3.  $\ell_g$  is a bijection for all  $g \in G$ .

### Proof.

1.  $\ell_g \circ \ell_h(x) = g \cdot (h \cdot x) = gh \cdot x = \ell_{gh}(x)$ .
2.  $\ell_e(x) = e \cdot x = x$ .
3.  $\ell_g \circ \ell_{g^{-1}} = \ell_e = 1 = \ell_{g^{-1}} \circ \ell_g$ , so  $\ell_g$  is invertible.

□

### Corollary

Every left action of  $G$  on  $X$  gives a homomorphism  $\phi: G \rightarrow S_X : g \mapsto \ell_g$  with  $\phi(g)(x) = g \cdot x$ .

### Definition — permutation representation

If  $X$  is a set, a **permutation representation** of  $G$  on  $X$  is a homomorphism  $\phi: G \rightarrow S_X$ .

If  $|X| = n$ , then  $S_X \cong S_n$ . So an action on a finite set  $X$  with  $|X| = n$  gives a homomorphism to  $S_n$ .

Example:  $D_{2n}$  acts on  $n$  vertices of the  $n$ -gon, so there is a homomorphism  $D_{2n} \rightarrow S_n$ .

## Permutation representations of the dihedral group

Let  $X = \{v_0, \dots, v_{n-1}\}$  be the vertices of the  $n$ -gon. We identify  $X$  with  $\{1, \dots, n\}$  by mapping  $v_i \mapsto i + 1$  so we can write elements of  $S_X$  as elements of  $S_n$ .

Let  $\phi: D_{2n} \rightarrow S_n$  be a permutation representation given by the action of  $D_{2n}$  on  $X$ .

What is  $\phi(s)$ ? We see  $s \cdot v_0 = v_1$ ,  $s \cdot v_1 = v_2$ ,  $\dots$ ,  $s \cdot v_n = v_0$ , so  $\phi(s) = (1 \ 2 \ 3 \ \dots \ n)$ .

What is  $\phi(r)$ ? We see  $r \cdot v_0 = v_0$ ,  $r \cdot v_1 = v_{n-1}$ ,  $r \cdot v_2 = v_{n-2}$ , and in general  $r \cdot v_i = v_{n-i}$ , so

$$\phi(r) = \begin{cases} (2 \ n)(3 \ n-1) \cdots (\frac{n+1}{2} \ \frac{n+3}{2}) & n \text{ odd} \\ (2 \ n)(3 \ n-1) \cdots (\frac{n}{2} \ \frac{n}{2} + 2) & n \text{ even} \end{cases}.$$

In general,  $\phi(s^i r^j) = \phi(s)^i \phi(r)^j$ .

(Note a different choice of  $r$  could have yielded a different representation.)

### Theorem

1. If  $G$  acts on  $X$ , then there is a homomorphism  $\phi: G \rightarrow S_X$  defined by  $\phi(g)(x) = g \cdot x$ .
2. If  $\phi: G \rightarrow S_X$  is a homomorphism, then  $g \cdot x = \phi(g)(x)$  defines a group action of  $G$  on  $X$ .

In other words, group actions are equivalent to permutation representations. Because of this theorem, we treat the two as interchangeable.

### Proof.

1. Already done.
2. First,  $e \cdot x = \phi(e)(x) = 1(x) = x$  for all  $x \in X$ . Next, if  $g, h \in G$  and  $x \in X$ , then

$$g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x).$$

□

## Faithful actions

### Definition — kernel, faithful

Let  $G$  act on a set  $X$ , and let  $\phi: G \rightarrow S_X$  be the corresponding permutation representation. The **kernel** of the action is  $\ker \phi$ , and the action is **faithful** if  $\ker \phi = \{e\}$ .

That is, an action is faithful if the corresponding permutation representation is injective.

### Lemma

An action of  $G$  on  $X$  is faithful if and only if for every  $g \in G$  with  $g \neq e$ , there is  $x \in X$  such that  $g \cdot x \neq x$ .

#### Proof.

$\ell_g \neq 1$  if and only if there is  $x \in X$  such that  $g \cdot x = \ell_g(x) \neq x$ . □

### Example

- $S_X$  acts faithfully on  $X$ .
- If  $A \cdot e_i = e_i$  for all  $i = 1, \dots, n$ , then  $A = 1$ , so the action of  $\text{GL}_n \mathbb{K}$  on  $\mathbb{K}^n$  is faithful.
- $D_{2n}$  acts faithfully on vertices on the  $n$ -gon (exercise).
- The trivial action is not faithful.

Does every group act faithfully on some set?

### Theorem — Cayley's theorem

The left regular action of  $G$  on  $G$  is faithful.  
Consequently,  $G$  is isomorphic to a subgroup of  $S_G$ . In particular, if  $|G| = n < \infty$ , then  $G$  is isomorphic to a subgroup of  $S_n$ .

#### Proof.

If  $g \in G$  with  $g \neq e$ , then  $g \cdot e = g \neq e$ . So the left regular action is faithful.

Hence the permutation representation  $\phi: G \rightarrow S_G$  is injective, and thus  $G$  is isomorphic to  $\text{Im } \phi \leq S_G$  (first isomorphism theorem).

If  $|G| = n < \infty$ , then  $S_G \cong S_n$ . □

The homomorphism  $G \rightarrow S_G$  given by this theorem is called the **left regular representation** of  $G$ .

### Example

Let  $G = \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$ .

By Cayley's theorem,  $G$  is isomorphic to a subgroup of  $S_2$ .

$[0] + [0] = [0]$  and  $[0] + [1] = [1]$ , so  $[0] \mapsto e$  in  $S_2$ .

$[1] + [0] = [1]$  and  $[1] + [1] = [0]$ , so  $[1] \mapsto (12)$  in  $S_2$ .

Note the left regular representation may not be the most efficient permutation representation.

### Example

$D_6$  has order 6, so it is isomorphic to a subgroup of  $S_6$ .

But  $D_6$  acts faithfully on the vertices of the 3-gon, so there is an injective homomorphism  $D_6 \rightarrow S_3$ ; since  $|D_6| = |S_3| = 6$ , this is an isomorphism.

But  $|S_6| = 6! \gg 6$ , so the left regular representation may be much larger in terms of space.



## 13: Orbits and stabilizers

### Orbits

#### Definition — orbit

Let  $G$  act on  $X$ . The  **$G$ -orbit** of  $x$  is  $\mathcal{O}_x = \{g \cdot x : g \in G\}$ . A subset  $\mathcal{O} \subseteq X$  is an **orbit** if  $\mathcal{O} = \mathcal{O}_x$  for some  $x \in X$ . A group action is **transitive** if  $\mathcal{O}_x = X$  for some  $x \in X$ .

#### Example

- Let  $H \leq G$  act on  $G$  by left multiplication. The orbit of  $g \in G$  is  $\mathcal{O}_g = Hg$ , a right coset.

Since  $Hg$  is a proper subset of  $G$  if  $H < G$ , we see the action is not transitive unless  $H = G$ .

- Consider the action of  $\mathrm{GL}_n \mathbb{K}$  on  $\mathbb{K}^n$ . Then

$$\mathcal{O}_v = \begin{cases} \{0\} & v = 0 \\ \mathbb{K}^n \setminus \{0\} & v \neq 0 \end{cases}.$$

So this action is not transitive, and there are two orbits.

- If  $1 \leq i \neq j \leq n$ , then we can find  $\pi \in S_n$  where  $\pi(i) = j$ . So  $\mathcal{O}_i = \{1, \dots, n\}$  for all  $i$ . We conclude the action of  $S_n$  on  $\{1, \dots, n\}$  is transitive and has one orbit.
- More generally, the action of  $S_X$  on  $X$  is transitive and has one orbit.
- Suppose  $\sigma \in S_n$ . What are the orbits of  $\langle \sigma \rangle$  on  $\{1, \dots, n\}$ ?

For example, take  $\sigma = (137)(26)(48) \in S_8$ . Then  $\mathcal{O}_1 = \mathcal{O}_3 = \mathcal{O}_7 = \{1, 3, 7\}$ ,  $\mathcal{O}_2 = \mathcal{O}_6 = \{2, 6\}$ ,  $\mathcal{O}_4 = \mathcal{O}_8 = \{4, 8\}$ , and  $\mathcal{O}_5 = \{5\}$ .

In general, if  $\sigma = (i_{11} \cdots i_{1k_1})(i_{21} \cdots i_{2k_2}) \cdots (i_{m1} \cdots i_{mk_m})$  (including 1-cycles), then the orbits are  $\{i_{j1}, \dots, i_{jk_j}\}$  for  $1 \leq j \leq m$ .

## Equivalence relation from a $G$ -action

Note that in all the previous examples, the orbits partitioned  $X$ . Recall that partitions correspond to equivalence relations.

### Definition

If  $G$  acts on  $X$ , say that  $x \sim_G y$  if there is  $g \in G$  such that  $g \cdot x = y$ .

### Lemma

If  $G$  acts on  $X$ , then  $\sim_G$  is an equivalence relation on  $X$ .

#### *Proof.*

Since  $e \cdot x = x$ ,  $x \sim_G x$  for all  $x \in X$ .

If  $g \cdot x = y$ , then  $g^{-1} \cdot y = x$ , so  $x \sim_G y \implies y \sim_G x$ .

Finally, if  $g \cdot x = y$  and  $h \cdot y = z$ , then  $hg \cdot x = z$ , so  $x \sim_G y$  and  $y \sim_G z \implies x \sim_G z$ .  $\square$

Then if  $x \in X$ , the equivalence class  $[x]_{\sim_G}$  of  $x$  is  $\{y \in X : x \sim_G y\} = \{y \in X : y = g \cdot x \text{ for some } g \in G\} = \mathcal{O}_x$ .

Thus we conclude the equivalence classes of  $\sim_G$  are the orbits of  $G$  acting on  $X$ .

### Proposition

If  $G$  acts on  $X$ , then orbits of  $G$  form a partition of  $X$ . In particular, the action is transitive if and only if there is only one orbit.

### Definition — set of representatives

Let  $\sim$  be an equivalence relation on a set  $X$ . A subset  $S \subseteq X$  is said to be a **set of representatives** for  $\sim$  if each equivalence class of  $\sim$  contains exactly one element of  $S$ .

A set of representatives exists for every  $\sim$ .

**Corollary**

Suppose  $G$  acts on a set  $X$  and let  $S$  be a set of representatives for  $\sim_G$ . Then

$$|X| = \sum_{x \in S} |\mathcal{O}_x|.$$

What is  $|\mathcal{O}_x|$ ?

We can use the function  $G \rightarrow \mathcal{O}_x : g \mapsto g \cdot x$ . This is clearly surjective, but what if the function is not injective (i.e.,  $g \cdot x = h \cdot x$  for some  $g \neq h$ )?

## Stabilizers

### Definition — stabilizer

If  $G$  acts on  $X$ , and  $x \in X$ , the **stabilizer** of  $x$  is  $G_x := \{g \in G : g \cdot x = x\}$ .

### Proposition

If  $G$  acts on  $X$ , and  $x \in X$ , then  $G_x$  is a subgroup of  $G$ .

#### *Proof.*

First,  $e \in G_x$ .

Second, if  $g, h \in G_x$ , then  $gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in G_x$ .

Third, if  $g \in G_x$ , then  $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = e \cdot x = x \implies g^{-1} \in G_x$ . □

### Theorem — Orbit-stabilizer theorem

If  $G$  acts on  $X$ , and  $x \in X$ , then there is a bijection  $G/G_x \rightarrow \mathcal{O}_x : gG_x \mapsto g \cdot x$ .

#### *Proof.*

Well-defined: if  $gG_x = hG_x$ , then  $g^{-1}h \in G_x$ . So  $g^{-1}h \cdot x = x \implies h \cdot x = g \cdot x$ .

Injective: if  $g \cdot x = h \cdot x$ , then  $g^{-1}h \cdot x = x$ , so  $g^{-1}h \in G_x \implies gG_x = hG_x$ .

Surjective: if  $y \in \mathcal{O}_x$ , then  $y = g \cdot x$  by definition. □

### Corollary

If  $G$  acts on  $X$  and  $x \in X$ , then  $|\mathcal{O}_x| = [G : G_x]$ .

**Example:**  $S_n$ 

Let  $G = S_n$  and  $X = \{1, \dots, n\}$ .

We know the action of  $G$  on  $X$  is transitive, so  $\mathcal{O}_i = X$  for any  $i$ .

Then  $n = |\mathcal{O}_i| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{n!}{|G_i|}$ . Hence  $|G_i| = (n-1)!$  for any  $i$ .

Thus the stabilizer of  $i$  is  $G_i = \{\pi \in S_n : \pi(i) = i\}$ .

For a concrete example, if  $n = 4$ , then  $G_1 = \{e, (23), (24), (34), (234), (243)\}$ .

In general,  $G_i \cong S_{n-1}$  (add 1 to each number in  $S_{n-1}$  which is  $\geq i$ ), so we see  $|G_i| = (n-1)!$  directly.

**Example:**  $G/H$ 

Recall that the action of  $G$  on  $G/H$  is  $g \cdot kH = gkH$  (i.e. usual set multiplication).

**Proposition**

Suppose  $H \leq G$ . Then the left multiplication action of  $G$  on  $G/H$  is transitive, and  $G_{eH} = H$ .

*Proof.*

If  $gH \in G/H$ , then  $gH = g \cdot eH$ , so  $\mathcal{O}_{eH} = G/H$ .

Also,  $g \cdot eH = eH \iff gH = H \iff g \in H$ . □

In this case, the orbit-stabilizer theorem states that  $\mathcal{O}_{eH} = G/H$  is in bijection with  $G/H$  (tautology).

## Kernel versus stabilizer

If  $G$  acts on  $X$ , then the kernel of the action is  $\{g \in G : g \cdot x = x \text{ for all } x\}$ .

Meanwhile, the stabilizer  $G_x = \{g \in G : g \cdot x = x\}$  has  $x$  fixed.

Consequently, if  $H$  is the kernel of the action, then  $H \leq G_x$  for all  $x \in X$ .

### Proposition

If  $G$  acts on  $X$ , then the kernel of the action is  $\bigcap_{x \in X} G_x$ , the intersection of the stabilizers.

### Proof.

$g$  is in the kernel if and only if  $g \in G_x$  for all  $x \in X$ . □

An application:

### Theorem

If  $G$  is finite and  $H \leq G$  has index  $[G : H] = p$  where  $p$  is the smallest prime dividing  $|G|$ , then  $H \trianglelefteq G$ .

### Proof.

Let  $K$  be the kernel of the action of  $G$  on  $G/H$  (so  $K$  is normal).

By the proposition,  $K \leq H = G_{eH}$ . Then let  $k = [H : K] = \frac{|H|}{|K|}$ .

Now  $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \frac{|H|}{|K|} = pk$ .

By the first isomorphism theorem,  $G/K$  is isomorphic to a subgroup of  $S_p$ . So  $|G/K| = kp \mid p! = |S_p| \implies k \mid (p-1)!$ .

But we also have  $k \mid |G|$ . Since  $p$  is the smallest prime dividing  $|G|$ , we must have  $k = 1$ . Hence  $|H| = |K|$  so  $H = K$ . □

## Conjugation actions

Recall left multiplication defines a left action of  $G$  on  $G$ . There is, however, another natural left action.

### Lemma

$G \times G \rightarrow G : (g, k) \mapsto gkg^{-1}$  defines an action of  $G$  on  $G$ .

This action is called the **conjugation action** of  $G$  on  $G$ .

To avoid confusion with the left multiplication action here, we'll denote it by  $g \bullet k = gkg^{-1}$ . (In practice, there is no convention about  $\cdot$  and  $\bullet$ ; specify your choices when writing.)

### Proof.

If  $k \in G$ , then  $e \bullet k = eke = k$ .

If  $g, h, k \in G$ , then  $g \bullet (h \bullet k) = g \bullet hkh^{-1} = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = gh \bullet k. \quad \square$

### Definition — conjugacy class, centralizer

The orbit of  $k \in G$  under the conjugation action is called the **conjugacy class** of  $k$ , denoted by  $\text{Conj}_G(k)$ .

The stabilizer of  $k \in G$  is called the **centralizer** of  $k$  in  $G$ , denoted by  $C_G(k)$ .

By definition,  $\text{Conj}_G(k) = \{gkg^{-1} : g \in G\}$ .

$C_G(k) = \{g \in G : gkg^{-1} = k\} = \{g \in G : gk = kg\}$ , namely the centralizer is the set of elements in  $G$  which commute with  $k$ .

By the orbit-stabilizer theorem,  $|\text{Conj}_G(k)| = [G : C_G(k)]$ .

For example:  $\text{Conj}(e) = \{geg^{-1} : g \in G\} = \{e\}$  and  $C_G(e) = G$ .

Note the conjugation action of  $G$  on  $G$  induces an action of  $G$  on  $2^G$ . In particular, if  $g \in G$  and  $S \subseteq G$ , then  $g \bullet S = \{g \bullet h : h \in S\} = \{ghg^{-1} : h \in S\} = gSg^{-1} = N_G(S)$  (the normalizer of  $S$  in  $G$ ).



### Example: matrices

One important instance of the conjugation action is with  $\mathrm{GL}_n \mathbb{K}$ .

Actually, if  $A, B$  are  $n \times n$  matrices and  $A$  is invertible, then  $ABA^{-1}$  makes sense even if  $B$  is not invertible.

#### Exercise

Show  $\mathrm{GL}_n \mathbb{K}$  acts on  $M_n \mathbb{K}$  by conjugation, where  $M_n \mathbb{K}$  is the set of  $n \times n$  matrices over  $\mathbb{K}$ .

Recall matrices  $A$  and  $B$  are **similar** if there is  $C \in \mathrm{GL}_n \mathbb{K}$  such that  $CAC^{-1} = B$ . This is the equivalence relation  $\sim_{\mathrm{GL}_n \mathbb{K}}$ .

The orbits of the conjugation action of  $\mathrm{GL}_n \mathbb{K}$  on  $M_n \mathbb{K}$  are called **similarity classes**.

A matrix  $A$  is **diagonalizable** if it is similar to a diagonal matrix.

When  $\mathbb{K} = \mathbb{C}$ , every similarity class contains exactly one matrix in Jordan normal form; matrices in Jordan normal form give a set of representatives for  $\sim_{\mathrm{GL}_n \mathbb{K}}$ .

## Class equation and Cauchy's theorem

Using standard facts about orbits,

$$|G| = \sum_{g \in S} |\text{Conj}(g)| = \sum_{g \in S} [G : C_G(g)]$$

where  $S$  is a set of representatives for conjugacy classes.

We could simplify this by pulling out conjugacy classes of size 1:

### Lemma

$$|\text{Conj}(k)| = 1 \iff C_G(k) = G \iff k \in Z(G).$$

### Proof.

$|\text{Conj}(k)| = 1$  if and only if  $gkg^{-1} = k$  for all  $g \in G$  (since  $k \in \text{Conj}(k)$  always) if and only if  $C_G(k) = G$  if and only if  $k \in Z(G)$ .  $\square$

### Theorem — Class equation

If  $G$  is a finite group, then

$$|G| = |Z(G)| + \sum_{g \in T} |\text{Conj}(g)|$$

where  $T$  is a set of representatives for conjugacy classes not contained in the center.

### Theorem — Cauchy's theorem

If  $G$  is a finite group and  $p$  is a prime dividing  $|G|$ , then  $G$  contains an element of order  $p$ .

### Proof.

Let  $|G| = pm$ . Note the theorem is clear when  $G$  is cyclic.

First assume  $G$  is abelian; proof by induction on  $m$ .

Base case: if  $m = 1$ , then  $G$  is cyclic, so we are done.

Inductive step: pick  $a \in G$ ,  $a \neq e$ . We can assume  $|a| < |G|$  (otherwise  $G$  is cyclic). If  $p \mid |a|$ , then by induction we get  $b \in \langle a \rangle$  with  $|b| = p$ . Otherwise,  $N = \langle a \rangle \trianglelefteq G$  since  $G$  is abelian. Thus  $|G/N| = \frac{|G|}{|N|} < |G|$ . Since  $p \mid |G|$  but  $p \nmid |N|$ , we get  $p \mid |G/N|$ . By

induction,  $G/N$  has an element  $gN$  of order  $p$ . Let  $n = |g|$ . Since  $g^n = 1$ ,  $q(g)^n = 1$  where  $q$  is the quotient map, so  $p \mid n$ . If  $G = \langle g \rangle$ , we are done, otherwise apply induction to  $\langle g \rangle$ .

Now take a general  $G$  (possibly non-abelian); induction on  $|G|$ .

By the class equation,  $|G| = |Z(G)| + \sum_{g \in T} |\text{Conj}(g)|$ .

If  $p \nmid |\text{Conj}(g)| = |G|/|C_G(g)|$  for some  $g \in T$ , then  $p \mid |C_G(g)|$ . Since  $g \notin Z(G)$ ,  $|\text{Conj}(g)| > 1 \implies |C_G(g)| < |G|$ . By induction,  $C_G(g)$  contains an element of order  $p$ .

If  $p \mid |\text{Conj}(g)|$  for all  $g \in T$ , then  $p \mid |Z(G)|$ .  $Z(G)$  is an abelian group, so by the abelian case,  $Z(G)$  contains an element of order  $p$ .  $\square$

## Center of $p$ -groups

### Definition — $p$ -group

Let  $p$  be prime. A group  $G$  is a  **$p$ -group** if  $|G| = p^k$  for some  $k \geq 1$ .

### Theorem

If  $G$  is a  $p$ -group, then  $Z(G) \neq \{e\}$ .

#### *Proof.*

$$|G| = |Z(G)| + \sum_{g \in T} [G : C_G(g)].$$

Note  $[G : C_G(g)] \mid |G|$ .

If  $g \notin Z(G)$ , then  $[G : C_G(g)] > 1 \implies p \mid [G : C_G(g)]$ .

So  $p \mid |Z(G)|$ . □

As shown in the proof, the order of  $Z(G)$  is a non-zero power of  $p$ . Alternatively, get this from the theorem and Lagrange's theorem.

## **Week 6: Classification of Groups**

## 14: Classification of groups

Classification problem: identify all groups up to isomorphism. (We could replace groups with any algebraic structure. Classification is one of the big questions in modern mathematics.)

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	$\mathbb{Z}/9\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

## 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.

Suppose  $G$  is not cyclic, so choose  $a \in G \setminus \{e\}$ .

We know  $\langle a \rangle \neq G$ , so  $|a| = p$  and we can find  $b \in G \setminus \langle a \rangle$ .

Since  $\langle b \rangle \neq G$ , we get  $|b| = p$  as well. Let  $H = \langle a \rangle$  and  $K = \langle b \rangle$ .

Since  $H \cap K < K$ , we see  $|H \cap K| = 1$  so  $H \cap K = \{e\}$ . Then  $|HK| = \frac{|H||K|}{|H \cap K|} = p^2$  so  $HK = G$ .

Finally,  $[G : H] = [G : K] = p$ , the smallest prime dividing  $|G|$ . Hence  $H, K \trianglelefteq G$  so  $G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ .  $\square$

## Groups of order $pq$

### Lemma

Suppose  $H, K \trianglelefteq G$  where  $\gcd(|H|, |K|) = 1$  and  $|H||K| = |G|$ . Then  $G \cong H \times K$ .

### Proof.

Since  $|H \cap K|$  divides both  $|H|$  and  $|K|$ , we get  $|H \cap K| = 1$  so  $H \cap K = \{e\}$ .

Also,  $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$  so  $HK = G$ .

The result follows from the characterization of products.  $\square$

Suppose  $|G| = pq$  for distinct primes  $p < q$ . What can we say about  $G$ ?

By Cauchy's theorem,  $G$  has elements  $a, b$  with  $|a| = p$  and  $|b| = q$ . Let  $H = \langle a \rangle$  and  $K = \langle b \rangle$ . Note  $\gcd(|H|, |K|) = 1$  and  $|H||K| = |G|$ . Is it true that  $H, K \trianglelefteq G$ ?

We know  $[G : K] = p$ , which is the smallest prime dividing  $|G|$ , so  $K \trianglelefteq G$ . But is  $H \trianglelefteq G$ ? Not necessarily.

Counterexample:  $G = D_6$ ,  $H = \langle r \rangle$ ,  $K = \langle s \rangle$ .

What if we suppose  $H, K \leq G$ ,  $HK = G$ ,  $H \cap K = \{e\}$ , and  $K \trianglelefteq G$ ? Is  $G \cong H \times K$  here? Again, no!

In our counterexample, that would mean  $D_6 \cong H \times K \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ , but  $D_6$  is

non-abelian.

However, there is a set bijection  $H \times K \rightarrow G : (h, k) \mapsto hk$ , and we can say that  $G \cong H \ltimes K$ , the **semidirect product** of  $H$  and  $K$  (later, optional).

For  $p = 2$  and  $q = 3$ , it turns out the only groups of order  $pq = 6$  are  $\mathbb{Z}_2 \times \mathbb{Z}_3$ ,  $\mathbb{Z}_6$ , and  $D_6 \cong S_3$ .



## What can we say?

The difficulty in analyzing the  $pq$  case was that  $H \leq G$  might not be normal. This concern is not present if  $G$  is abelian, so we will focus on finite abelian groups this week.

There are lots of other ways to approach classification. Notice that for small orders, we are essentially describing groups as being built out of other groups.

We say a group is **simple** if it contains no (non-trivial) normal subgroups. Simple groups are the minimal building blocks for other groups.

Finally, by looking at the isomorphism problem for **finitely-presented groups** (later, optional), we will see that the classification problem for infinite groups cannot be solved.

## Decomposing finite abelian groups

From the earlier lemma, we can disregard the normality constraint when considering abelian groups. Then, how can we find groups of coprime order?

### Lemma

Suppose  $G$  is an abelian group. Let  $G^{(m)} = \{g \in G : g^m = e\}$ . Then  $G^{(m)} \leq G$  for all  $m \geq 1$ .

### Proof.

Clearly  $e \in G^{(m)}$  for all  $m \geq 1$ . If  $g, h \in G^{(m)}$ , then  $(g^{-1}h)^m = g^{-m}h^m = e \in G^{(m)}$ .  $\square$

$G^{(m)}$  is the  $m$ -torsion subgroup.

### Proposition

Suppose  $|G| = mn$  where  $\gcd(m, n) = 1$ . Then

1.  $\phi: G \rightarrow G^{(m)} \times G^{(n)} : g \mapsto (g^n, g^m)$  is an isomorphism.
2.  $|G^{(m)}| = m$  and  $|G^{(n)}| = n$ .

### Proof.

1. If  $g \in G$ , then  $g^{mn} = e$ , so  $g^n \in G^{(m)}$  and  $g^m \in G^{(n)}$ . Hence  $\phi$  is well-defined.

Now find  $a, b \in \mathbb{Z}$  such that  $an + bm = 1$ . If  $\phi(g) = e$ , then  $g^n = g^m = e \implies g = g^{an+bm} = e$ , so  $\phi$  is injective.

If  $g \in G^{(m)}$  and  $h \in G^{(n)}$ , then  $g = g^{an+bm} = g^{an}$  and similarly  $h = h^{an+bm} = h^{bm}$ , so  $\phi(g^a h^b) = (g^{an} h^{bm}, g^{am} h^{bn}) = (g, h)$ . Hence  $\phi$  is also surjective.

We also need to show  $\phi$  is a homomorphism:

$$\phi(gh) = ((gh)^n, (gh)^m) = (g^n h^n, g^m h^m) = (g^n, g^m) \cdot (h^n, h^m) = \phi(g)\phi(h).$$

2. Since  $G \cong G^{(m)} \times G^{(n)}$ ,  $|G| = |G^{(m)}||G^{(n)}|$ .

Suppose  $|G| = p_1^{a_1} \cdots p_k^{a_k}$  is the prime factorization of  $|G|$ . Since  $|G| = mn$  and  $\gcd(m, n) = 1$ , we have  $m = p_1^{b_1} \cdots p_k^{b_k}$  and  $n = p_1^{c_1} \cdots p_k^{c_k}$  where for each  $i$ ,  $a_i = b_i + c_i$  and only one of  $b_i$  and  $c_i$  is non-zero.

Suppose  $b_i > 0$ . If  $p_i \mid |G^{(n)}|$ , then  $G^{(n)}$  has an element  $a$  of order  $p_i$  by Cauchy's theorem. Then  $p_i \mid m \implies a \in G^{(m)} \implies a \in \ker \phi \implies a = e$ , which is impossible. So  $p_i \nmid |G^{(n)}| \implies p_i^{a_i} \mid |G^{(m)}|$ .

Conclusion:  $m \mid |G^{(m)}|$  and  $n \mid |G^{(n)}|$ . So  $|G^{(m)}| = m$  and  $|G^{(n)}| = n$ .

□

### Example

Suppose  $\gcd(m, n) = 1$  and let  $G = \mathbb{Z}/mn\mathbb{Z}$ .

If  $m[x] = 0$  for  $0 \leq x < mn$ , then  $mn \mid mx \iff n \mid x$ . So  $G^{(m)} = \{[x] \in G : m[x] = 0\} = n\mathbb{Z}/mn\mathbb{Z}$ .

Since  $\mathbb{Z} \rightarrow n\mathbb{Z} : x \mapsto nx$  is an isomorphism sending  $m\mathbb{Z} \mapsto mn\mathbb{Z}$ ,  $n\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$ . Similarly,  $G^{(n)} \cong m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ .

The proposition gives  $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ . (Chinese remainder theorem.)

### Corollary

Let  $G$  be a finite abelian group and let  $|G| = p_1^{a_1} \cdots p_k^{a_k}$  where  $p_1, \dots, p_k$  are distinct primes and  $a_i > 0$  for all  $i$ . Then  $G \cong G_1 \times G_2 \times \cdots \times G_k$  where  $|G_i| = p_i^{a_i}$ .

#### Proof.

Let  $G_1 = G^{(p_1^{a_1})}$  and let  $r = p_2^{a_2} \cdots p_k^{a_k}$ .

Since  $p_1^{a_1}$  and  $r$  are coprime and  $p_1^{a_1} \cdot r = |G|$ , the proposition implies  $G \cong G_1 \times G^{(r)}$  and that  $|G_1| = p_1^{a_1}$  and  $|G^{(r)}| = r$ .

We can continue to get  $G^{(r)} = G_2 \times \cdots \times G_k$  as desired. □

We can go further, and decompose into cyclic groups.

### Proposition

If  $G$  is a finite abelian group, then  $G \cong C_{a_1} \times C_{a_2} \times \cdots \times C_{a_k}$  for some sequence  $a_1, \dots, a_k$  where every  $a_i$  is a prime power.

(Recall that  $C_n$  is the multiplicative form of  $\mathbb{Z}/n\mathbb{Z}$ .)

#### Proof.

By the previous corollary, we can assume  $G$  is a  $p$ -group, i.e.  $|G| = p^n$  for some  $n$ . Proof by induction on  $n$ ; for base case  $n = 0$ , take  $k = 0$ .

Choose an element  $x \in G$  of maximal order, so say  $|x| = p^r$ . Since  $G$  is abelian,  $N = \langle x \rangle \trianglelefteq G$ .

Then  $|G/N| < |G|$ , so by induction,  $G/N = C_{b_1} \times \cdots \times C_{b_\ell}$  for some sequence  $b_1, \dots, b_\ell$  of prime powers. By Lagrange's theorem,  $b_i = p^{s_i}$  for all  $i$ .

For each  $i$ , let  $\tilde{y}_i$  be the generator of  $C_{b_i}$ . Let  $y_i N \in G/N$  be the element of  $G/N$  corresponding to  $(e, \dots, e, \tilde{y}_i, e, \dots, e)$  (that is,  $\tilde{y}_i$  in the  $i$ -th position). Say  $|y_i| = p^{t_i}$ ; note  $r \geq t_i \geq s_i$ .

We know that  $y_i^{b_i} \in N$ , so  $y_i^{b_i} = x^{c_i}$  for some  $c_i$ . Now  $b_i = p^{s_i}$ , so  $|y_i^{b_i}| = p^{t_i}/p^{s_i} = p^{t_i-s_i}$ . We conclude that  $c_i = d_i p^{r-(t_i-s_i)} = d_i p^{r-t_i+s_i}$  for some  $d_i$ .

Let  $z_i = y_i x^{-d_i p^{r-t_i}}$ . Then  $z_i N = y_i N$ , and  $z_i^{b_i} = y_i^{b_i} x^{-d_i p^{r-t_i+s_i}} = y_i^{b_i} x^{-c_i} = e$ , so  $|z_i| = b_i$ .

Let  $H = \langle z_1, \dots, z_\ell \rangle \leq G$  and suppose  $w \in H \cap N$ . Then  $w = z_1^{n_1} \cdots z_\ell^{n_\ell}$  where  $0 \leq n_i < b_i$  for all  $i$ .

Let  $q: G \rightarrow G/N$  be the quotient map. Then

$$q(w) = q(z_1)^{n_1} \cdots q(z_\ell)^{n_\ell} = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (y_1 N)^{n_1} \cdots (y_\ell N)^{n_\ell} \cong (\tilde{y}_1^{n_1}, \dots, \tilde{y}_\ell^{n_\ell}).$$

But since  $w \in N = \ker q$ ,  $q(w) = e$ , so  $n_1 = \cdots = n_\ell = 0$ . We conclude  $w = e$ , or in other words  $H \cap N = \{e\}$ .

Suppose  $g \in G$ . Then  $gN \cong (\tilde{y}_1^{n_1}, \dots, \tilde{y}_\ell^{n_\ell})$  for some  $n_1, \dots, n_\ell$  which implies  $gN = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (z_1^{n_1} \cdots z_\ell^{n_\ell})N$ . In particular,  $g \in HN$ . We conclude  $HN = G$ .

Since  $G$  is abelian,  $H, N \trianglelefteq G$ . So  $G = N \times H$ .

Now  $N \cong C_{p^r}$  and  $|H| < |G|$ , so by induction,  $H$  is also a product of prime-power cyclic groups.  $\square$

Now, the main result.

### Theorem — Classification of finite abelian groups

If  $G$  is a finite abelian group, then  $G \cong C_{a_1} \times \cdots \times C_{a_k}$  where  $a_1 \leq \cdots \leq a_k$  is a sequence of prime powers.

Furthermore, if  $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$  where  $b_1 \leq \cdots \leq b_\ell$  is another sequence of prime powers, then  $k = \ell$  and  $a_i = b_i$  for all  $1 \leq i \leq k = \ell$ .

### Example

We saw earlier that  $C_2 \times C_3 \cong C_6$  (or generally  $C_m \times C_n \cong C_{mn}$  for coprime  $m$  and  $n$ ), so the requirement that  $a_i$  be a prime power is required for uniqueness.

### Proof.

We just need to prove uniqueness.

If  $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$ , then  $G^{(m)} \cong C_{b_1}^{(m)} \times \cdots \times C_{b_\ell}^{(m)}$ .

If  $p, q$  are distinct primes, then  $C_{p^r}^{(q^s)} = \{e\}$ . Otherwise if  $p = q$ ,  $|C_{p^r}^{(p^s)}| = p^{\min(r,s)}$ .

Now

$$|G^{(p^r)}| = \prod_{s \geq 1} \prod_{i: b_i = p^s} |C_{b_i}^{(p^r)}| = \prod_{s \geq 1} \prod_{i: b_i = p^s} p^{\min(r,s)}$$

and hence

$$\frac{|G^{(p^r)}|}{|G^{(p^{r-1})}|} = \prod_{s \geq r} \prod_{i: b_i = p^s} p.$$

So  $\log_p |G^{(p^r)}| - \log_p |G^{(p^{r-1})}| = |\{i : b_i = p^s \text{ for some } s \geq r\}|$ .

Exercise: recover  $\ell$  and  $b_1, \dots, b_\ell$  from these numbers. □

## **Week 7: Rings**

## 15: Rings and fields

### Rings

Rings abstract sets with operations addition  $+$  and multiplication  $\cdot$ .

#### Definition — ring

A **ring** is a tuple  $(R, +, \cdot)$ , where

1.  $(R, +)$  is an abelian group, and
2.  $\cdot$  is an associative binary operation on  $R$  such that  $(a + b) \cdot c = a \cdot c + b \cdot c$  and  $a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b, c \in R$  ((left/right) distributive property).

The operation  $+$  is called **addition**, and  $\cdot$  is called **multiplication**.

A ring is **commutative** if  $\cdot$  is commutative.

#### Example

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are all commutative rings.
- $(\mathbb{N}, +, \cdot)$  is not a ring, since  $(\mathbb{N}, +)$  is not a group.
- $\mathbb{Z}/n\mathbb{Z}$  is a commutative ring.)
- If  $R$  is a ring and  $X$  is a set, then  $\text{Fun}(X, R)$  is a ring with pointwise multiplication and addition.
- If  $R$  is a (commutative) ring, then polynomials  $R[x]$  with coefficients in  $R$  is a (commutative) ring (see later).
- If  $R$  is a ring and  $n \geq 1$ , the the set of  $n \times n$  matrices  $M_n R$  with coefficients in  $R$  is a ring under usual matrix operations.
- If  $\circ: M_n \mathbb{C} \times M_n \mathbb{C} \rightarrow M_n \mathbb{C} : (A, B) \mapsto \frac{AB+BA}{2}$  then  $(M_n \mathbb{C}, +, \circ)$  is not a ring since  $\circ$  is not associative (homework #1).

Notation for rings:

- As with groups, we may refer to the ring  $(R, +, \cdot)$  by  $R$  when the operations are clear.
- We always use additive notation for the group  $(R, +)$ , and almost always use  $+$  as the symbol. (Sometimes  $\oplus$  for  $\mathbb{Z}/2\mathbb{Z}$ , etc.)
- In particular, denote identity of  $(R, +)$  by  $0$  and inverse of  $x \in R$  with respect to  $+$  by  $-x$ .
- Some variation in notation permitted for multiplication  $(\cdot, \times, \otimes, \boxtimes, \text{etc.})$ .

- Usually just use  $ab$  for multiplication of  $a$  and  $b$ .



## Basic properties

### Proposition

If  $R$  is ring, then:

1.  $0 \cdot a = a \cdot 0 = 0$  for all  $a \in R$ .
2.  $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$  for all  $a, b \in R$ .
3.  $(-a) \cdot (-b) = a \cdot b$  for all  $a, b \in R$ .

### *Proof.*

1.  $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 \cdot a = 0$ . Similarly,  $a \cdot 0 = 0$ .
2.  $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \implies (-a) \cdot b = -(a \cdot b)$ . Similarly,  $a \cdot (-b) = -(a \cdot b)$ .
3.  $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$ .

□

## Multiplicative identities

### Definition — ring with identity

A **ring with identity** is a ring  $(R, +, \cdot)$  where  $\cdot$  has an identity.

In this course, “ring” means “ring with identity” unless otherwise noted.

This is a common assumption outside of the course. If a ring doesn’t have an identity, we can call it a “ring without an identity” or “ring not necessarily having an identity” (or a “rng”, haha). (Will encounter these with subrings.)

All rings mentioned so far are rings with identities.

For  $\text{Fun}(X, R)$ ,  $R[x]$ ,  $M_n R$  to have identities, we need to assume that  $R$  has an identity.

Notation: use  $1_R$  or  $1$  for identity of  $R$ .

### Proposition

If  $R$  is a ring (with identity), then  $-a = (-1) \cdot a$  for all  $a \in R$ .

*Proof.*

$$0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a.$$

□

## Units

### Definition — unit

Let  $R$  be a ring. An element  $x \in R$  is a **unit** if  $x$  has an inverse with respect to multiplication  $\cdot$  (*i.e.*, there is  $y \in R$  where  $xy = yx = 1$ ).

The set of units in  $R$  is denoted by  $R^\times$ .

If  $x$  is a unit, then the inverse of  $x$  is unique, and is denoted by  $x^{-1}$ .

From homework, the set of units  $R^\times$  forms a group under multiplication, and thus is called the **group of units** of  $R$ .

### Example

- $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ .
- $\mathbb{Q}^\times = \{x \in \mathbb{Q} : x \neq 0\}$ .

Rings with (without) identity are also called **unital (non-unital) rings**.

## The trivial ring

The smallest possible ring is  $R = \{0\}$ , with multiplication  $0 \cdot 0 = 0$ . This is a ring with  $1 = 0$ . This ring is called the **trivial ring** or **zero ring**.

Unlike the trivial group, which is crucial in group theory, the trivial ring is often an annoyance, since there's a special property which holds only for the trivial ring.

### Lemma

Let  $R$  be a ring. Then  $1 = 0$  if and only if  $R$  is trivial.

### *Proof.*

If  $1 = 0$ , then  $x = 1 \cdot x = 0 \cdot x = 0$  for all  $x \in R$ . □

## Fields and division rings

If  $R$  is a ring with  $1 \neq 0$ , then  $0 \cdot y = 0 \neq 1$  for all  $y \in R$  and hence  $0 \notin R^\times$ .

### Definition — division ring

A **division ring** is a ring  $R$  with  $1 \neq 0$ , such that  $R^\times = R \setminus \{0\}$ .

A **field** is a commutative division ring.

### Example

$\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  are all fields.

Reminder: if  $\alpha = a + bi \in \mathbb{C}$ , then  $\alpha\bar{\alpha} = |\alpha|^2 = a^2 + b^2$ , and  $|\alpha| = 0$  if and only if  $\alpha = 0$ , so if  $\alpha \neq 0$ , then  $\alpha^{-1} = \bar{\alpha}/|\alpha|^2$ .

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

We're used to working with  $\mathbb{Z}/n\mathbb{Z}$  as a group under  $+$ . It also has multiplication  $[x] \cdot [y] = [xy]$ , making it a ring.

**Lemma**

$[x]$  is a unit in  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $\gcd(x, n) = 1$ .

*Proof.*

If  $\gcd(x, n) = 1$ , then  $ax + bn = 1$  for some  $a, b \in \mathbb{Z}$ . Since  $n \mid ax - 1$ ,  $[ax] = 1$  in  $\mathbb{Z}/n\mathbb{Z}$ .

Conversely, if  $[ax] = 1$ , then  $ax - 1 = bn$  for some  $b \in \mathbb{Z}$ . Hence  $\gcd(x, n) = 1$ .  $\square$

Corollary:  $\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $n$  is prime (every non-zero element coprime to  $n$ ).

In particular, there are fields  $\mathbb{K}$  where  $\mathbb{K}$  is finite.

## Division rings

### Theorem — Wedderburn

Any finite division ring is a field.

### Definition — ring of quaternions

The **ring of quaternions** is the ring  $Q = (\mathbb{R}^4, +, \cdot)$  where  $+$  is vector addition, and for  $\cdot$  we denote the standard basis vectors by  $1, i, j, k$ , and set  $i^2 = j^2 = k^2 = -1$  and  $ijk = -1$ .

In this ring, we have  $ij = k$  and  $jk = i$  so  $ji = -k$ , and hence  $Q$  is non-commutative.  $Q$  is an example of a non-commutative division ring.

## 16: Subrings and homomorphisms

### Subrings

#### Definition — subring

Let  $R$  be a ring. A subset  $S \subseteq R$  is a **subring** of  $R$  if

1.  $S$  is a subgroup of  $(R, +)$ ,
2.  $ab \in S$  for all  $a, b \in S$ , and
3.  $1 \in S$ .

#### Lemma

If  $S$  is a subring of  $(R, +, \cdot)$ , then  $(S, +, \cdot)$  is a ring.

#### Example

Subrings:

- $\mathbb{Z}$  is a subring of  $\mathbb{Q}$  is a subring of  $\mathbb{R}$  is a subring of  $\mathbb{C}$  is a subring of the quaternions  $\mathbb{H}$ .
- The ring  $\mathbb{R}[x]$  of polynomial functions with coefficients over  $\mathbb{R}$  is a subring of  $\text{Fun}(\mathbb{R}, \mathbb{R})$ .
- $M_n\mathbb{Z}$  is a subring of  $M_n\mathbb{R}$ .

Not subrings:

- $\mathbb{Q}^\times$  is not a subring of  $\mathbb{Q}$  (not a subgroup).
- $\text{Span}\{1, x\}$  is not a subring of  $\mathbb{R}[x]$  (not closed under multiplication).
- $2\mathbb{Z}$  is not a subring of  $\mathbb{Z}$  ( $1 \notin 2\mathbb{Z}$ ).
- $\{0\}$  is not a subring of any non-trivial ring  $R$  ( $1_R \notin \{0\}$ )!



## Alternative approach: non-unital subrings

If we work with non-unital rings, then we might not care that subrings contain the identity.

### Definition — subring (non-unital approach)

Let  $R$  be a not-necessarily-unital ring. A subset  $S \subseteq R$  is a **subring** of  $R$  if

1.  $S$  is a subgroup of  $(R, +, \cdot)$ , and
2.  $ab \in S$  for all  $a, b \in S$ .

If, in addition,  $R$  is a unital ring and

3.  $1 \in S$ ,

then  $S$  is a **unital subring**.

In this course, “ring” = “unital ring” and “subring” = “unital subring”. We’ll call sets satisfying (1) and (2) “non-unital subrings”.

One reason for interest in non-unital subrings is that many unital rings have interesting non-unital subrings.

### Example

Let  $R = \mathbb{R}[x]$ , so  $R$  is unital.

Let  $x\mathbb{R}[x] = \{f \in \mathbb{R}[x] : \text{constant term of } f \text{ is } 0\}$ . (Alternatively,  $f \in x\mathbb{R}[x] \iff f(0) = 0$ .)

If  $f, g \in x\mathbb{R}[x]$ , then  $f - g \in x\mathbb{R}[x]$  so  $x\mathbb{R}[x]$  is a subgroup of  $\mathbb{R}[x]$ . Also,  $f \cdot g \in x\mathbb{R}[x]$  since  $(fg)(0) = f(0)g(0) = 0$ . But  $1 \notin x\mathbb{R}[x]$ , so  $x\mathbb{R}[x]$  is a non-unital subring of  $R$ .

Exercise: show  $(x\mathbb{R}[x], +, \cdot)$  is a non-unital ring.

### Example

Let  $R = \text{Fun}(\mathbb{R}, \mathbb{R})$ .

A function  $f: \mathbb{R} \rightarrow \mathbb{R}$  is **compactly supported** if there is some interval  $[a, b]$  with  $a < b \in \mathbb{R}$  such that  $f(x) = 0$  for all  $x \notin [a, b]$ .

Suppose  $f, g: \mathbb{R} \rightarrow \mathbb{R}$  are compactly supported. We can choose  $a < b$  such that  $f(x) = g(x) = 0$  for all  $x \notin [a, b]$ . Then  $(f - g)(x) = (fg)(x) = 0$  for  $x \notin [a, b]$ , so  $f - g$  and  $f \cdot g$  are compactly supported.

The identity in  $\text{Fun}(\mathbb{R}, \mathbb{R})$  is the constant-1 function, which is not compactly supported.

So compactly supported functions are a non-unital subring.

Claim: compactly supported functions are a non-unital ring.

Proof: Suppose  $f$  is an identity element of the ring. There is some interval  $[a, b]$  such that  $f(x) = 0$  for all  $x \notin [a, b]$ . There is a compactly supported function  $g$  such that  $g(x) \neq 0$  for some  $x \notin [a, b]$ . But then  $fg(x) = f(x)g(x) = 0 \neq g(x)$  for this  $x$ , so  $f$  is not an identity.

## Characteristics and prime subrings

Suppose  $x \in R$  where  $R$  is a ring and  $n \in \mathbb{Z}$ . Since  $(R, +)$  is an abelian group,  $nx$  is well-defined. We can think of  $n$  as the element  $n1 \in R$ , in the sense that if  $x \in R$ , we can talk about  $n \cdot x$  or  $x \cdot n$  or  $x \pm n$ . (For example, in  $\mathbb{Z}/10\mathbb{Z}$ ,  $10 \cdot 1 = 0$ .)

### Lemma

If  $R$  is a ring,  $x \in R$ , and  $n, m \in \mathbb{Z}$ , then

- $n1 \cdot x = x \cdot n1 = nx$ , and
- $n(mx) = (nm)x$ .

### Proof.

Exercise. Idea: if  $n \geq 0$ , then  $n1 \cdot x = (1 + \cdots + 1) \cdot x = x + \cdots + x = nx$ . □

### Lemma

Let  $R$  be a ring. The set  $R_0 = \{n1 : n \in \mathbb{Z}\}$  is a subring of  $R$  and is contained in every other subring. Furthermore, as a group,  $R_0 \cong \mathbb{Z}/k\mathbb{Z}$ , where  $k = \min\{m \in \mathbb{N} : m1 = 0\}$  (or  $k = 0$  if this set is empty).

### Definition — prime subring, characteristic

$R_0$  is called the **prime subring** of  $R$ , and  $k$  is called the **characteristic** of  $R$ , denoted  $\text{char}(R)$ .

### Example

- $\text{char}(\mathbb{Z}/n\mathbb{Z}) = n$ .
- $\text{char}(\mathbb{Z}/\mathbb{Z}) = 0$ .
- $\text{char}(R) = 1$  if and only if  $R = \{0\}$ .

### Proof of lemma.

$R_0$  is the cyclic subgroup of  $(R, +)$  generated by 1. As a cyclic group,  $R_0 \cong \mathbb{Z}/k\mathbb{Z}$  where  $k = \min\{m \in \mathbb{N} : m1 = 0\}$  or  $k = 0$ .

If  $n, m \in \mathbb{Z}$ , then  $n1 \cdot m1 = nm1 \in R_0$ .

Also  $1 \in R_0$ , so  $R_0$  is a unital subring.

■ If  $S$  is a unital subring of  $R$ , then  $1 \in S$ , so  $S$  contains  $\langle 1 \rangle = R_0$ . □

## Centre of a ring

### Definition — centre

If  $R$  is a ring, the **centre** of  $R$  is the set  $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$ .

Note this is different from the group centre of  $R$  (which is  $R$  since  $R$  is abelian).

### Lemma

$Z(R)$  is a subring of  $R$ .

*Proof.*

Exercise. □

### Corollary

If  $R$  is a non-zero ring, then  $Z(R)$  is non-trivial.

*Proof.*

$Z(R)$  contains the prime subring  $R_0$ . □

## Ring homomorphisms

### Definition — homomorphism

Let  $R, S$  be rings. A function  $\phi: R \rightarrow S$  is a **(unital) homomorphism** if

1.  $\phi: (R, +) \rightarrow (S, +)$  is a group homomorphism,
2.  $\phi(ab) = \phi(a)\phi(b)$  for all  $a, b \in R$ , and
3.  $\phi(1_R) = 1_S$ .

If (1) and (2) but not (3) are satisfied, then  $\phi$  is a **non-unital homomorphism**.

In this course, “homomorphism” = “unital homomorphism”.

### Example

- If  $S$  is a subring of  $R$ , then  $i: S \rightarrow R: x \mapsto x$  is a homomorphism.
- The quotient maps  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}: x \mapsto [x]$  and  $\mathbb{Z}/mn\mathbb{Z} \rightarrow (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}: [x] \mapsto [x]$  are homomorphisms since  $[xy] = [x] \cdot [y]$ .

### Definition — isomorphism

A homomorphism  $\phi: R \rightarrow S$  is an **isomorphism** if  $\phi$  is bijective.

### Proposition

Let  $R_0 = \mathbb{Z}1_R$  be the prime subring of a ring  $R$ , and let  $n = \text{char}(R)$ . Then  $\phi: \mathbb{Z}/n\mathbb{Z} \rightarrow R_0: [x] \mapsto x1$  is a ring isomorphism.

### Proof.

We already showed  $\phi$  is a well-defined group isomorphism, so  $\phi$  is bijective.

If  $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ , then

$$\phi([a] \cdot [b]) = \phi([ab]) = ab1 = a(b1) = (a1) \cdot (b1) = \phi([a])\phi([b]).$$

Since  $\phi([1]) = 1$ ,  $\phi$  is a homomorphism. □

## Basic properties of ring homomorphisms

### Proposition

Let  $\phi: R \rightarrow S$  be a homomorphism.

1. If  $a \in R$  and  $n \geq 0$ , then  $\phi(a^n) = \phi(a)^n$ .
2. If  $u \in R^\times$ , then  $\phi(u) \in S^\times$  and  $\phi(u^n) = \phi(u)^n$  for all  $n \in \mathbb{Z}$ .
3. If  $\phi$  is an isomorphism, then  $\phi^{-1}$  is a ring homomorphism.

### Proof.

1. By induction.
2.  $1 = \phi(1) = \phi(uu^{-1}) = \phi(u)\phi(u^{-1})$ , so  $\phi(u) \in S^\times$  and  $\phi(u^{-1}) = \phi(u)^{-1}$ . It follows from (1) that  $\phi(u^n) = \phi(u)^n$  for all  $n \in \mathbb{Z}$ .
3. We already know  $\phi^{-1}$  is a group homomorphism.

Note  $\phi(1_R) = 1_S$ , so  $\phi^{-1}(1_S) = 1_R$ .

If  $a, b \in S$ , then  $a = \phi(\phi^{-1}(a))$  and  $b = \phi(\phi^{-1}(b))$ , so  $ab = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = \phi(\phi^{-1}(a)\phi^{-1}(b))$  and hence  $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$ .

□

### Proposition

Let  $\phi: R \rightarrow S$  be a homomorphism where  $S$  is not zero.

1.  $\text{Im } \phi$  is a subring of  $S$ .
2.  $\ker \phi$  is a non-unital subring of  $R$ .

### Proof.

1. We already  $\text{Im } \phi$  is a subgroup of  $(S, +)$ .

Since  $\phi(1_R) = 1_S$ ,  $1_S \in \text{Im } \phi$ .

Finally, if  $a, b \in \text{Im } \phi$ , then  $a = \phi(x)$  and  $b = \phi(y)$  for some  $x, y \in R$  and  $ab = \phi(x)\phi(y) = \phi(xy) \in \text{Im } \phi$ .

2. Revisit this when we study ideals.

□

Note about (2): if  $1 \in \ker \phi$  and  $\phi$  is unital, then  $1_S = \phi(1_R) = 0_S$ , so  $S$  is the zero ring.

## 17: Polynomials and group rings

### Polynomials, formally

Let  $R$  be a ring.

The **ring of polynomials** in variable  $x$  with coefficients in  $R$  is the ring with elements  $\sum_{i=0}^n a_i x^i$  for  $n \geq 0$  and  $a_0, \dots, a_n \in R$ .

Addition and multiplication are as usual:

$$\left( \sum_{i=0}^n a_i x^i \right) \left( \sum_{j=0}^m b_j x^j \right) = \sum_{k=0}^{n+m} \sum_{i=0}^k a_i b_{k-i} x^k$$

where  $a_i = b_j = 0$  when  $i > n$  and  $j > m$ .

As usual, we can talk about degree, monomials, evaluation, etc., but how can we do it formally?

#### Definition

Given a ring  $R$ , let  $R[x]$  be the set

$$\{(a_i)_{i=0}^\infty \subseteq R : \exists N \geq 0 \text{ such that } a_i = 0 \forall i \geq N\}.$$

We define binary operations  $+$  and  $\cdot$  on  $R[x]$  by

$$(a_i)_{i=0}^\infty + (b_i)_{i=0}^\infty = (a_i + b_i)_{i=0}^\infty$$

and

$$(a_i)_{i=0}^\infty \cdot (b_i)_{i=0}^\infty = (c_k)_{k=0}^\infty \text{ where } c_k = \sum_{i=0}^k a_i b_{k-i}.$$

The variable choice only matters in that we let  $\sum_{i=0}^n a_i x^i$  denote  $(a_0, \dots, a_n, 0, 0, \dots)$  (not unique representation). Changing the variable changes the notation.

#### Lemma

$(R[x], +, \cdot)$  is a ring.

#### Proof.

Need to show  $+$  and  $\cdot$  are well-defined for some sequences  $(a_i)_{i=0}^\infty$  and  $(b_i)_{i=0}^\infty$ .

Let  $N_1, N_2 \geq 0$  where  $a_i = 0$  for all  $i \geq N_1$  and  $b_j = 0$  for all  $b \geq N_2$ . Then  $a_i + b_j = 0$  for  $i \geq \max(N_1, N_2)$ , so  $(a_i)_{i=0}^\infty + (b_i)_{i=0}^\infty \in R[x]$ .



If  $k \geq N_1 + N_2$  and  $0 \leq i < N$ , then  $k - i > N_2$ . So  $\sum_{i=0}^k a_i b_{k-i} = 0$  if  $k \geq N_1 + N_2$ , so  $(a_i)_{i=0}^\infty \cdot (b_i)_{i=0}^\infty \in R[x]$ .

Exercise:  $(R[x], +)$  is an abelian group with  $0 = (0, 0, \dots)$ .

Next, suppose  $(a_i)_{i=0}^\infty, (b_i)_{i=0}^\infty, (c_i)_{i=0}^\infty \in R[x]$ .

(Lots of useless algebra...)

Exercise:  $1 = (1, 0, 0, \dots)$  is an identity for  $\cdot$ .

For distributivity, (more useless algebra...).

Conclusion:  $R[x]$  is a ring. □

## Terminology/notation for polynomial rings

- $R[x]$  is called the **ring of polynomials in variable  $x$  with coefficients in  $R$** .
- $x$  is the **variable** or **indeterminate**. Any variable works.
- We only use  $(a_i)_{i=0}^{\infty}$  for elements of  $R[x]$  for formal definitions or proofs.
- Use  $\sum_{i=0}^n a_i x^i$  when working with  $R[x]$ . If coefficients not needed, denote elements by  $p$  or  $p(x)$ .
- Exercise: there is an isomorphism  $R[x] \rightarrow R[y] : p(x) \mapsto p(y)$  for any variables  $x, y$ .

## Degree and coefficients

### Definition — degree

The **degree** of  $p(x) \in R[x]$  is the smallest integer  $n$  such that  $p(x) = \sum_{i=0}^n a_i x^i$  with  $a_n \neq 0$ , or  $-\infty$  if no such  $n$  exists. Notation:  $\deg(p)$ .

Examples:  $\deg(1) = 0$ ,  $\deg(1 + x - x^3) = 3$ ,  $\deg(0) = -\infty$ .

### Definition — coefficient, monomial, term

The **coefficient** of  $x^i$  in  $(a_i)_{i=0}^\infty \in R[x]$  is  $a_i$ .

A **monomial** is a polynomial of the form  $x^i$  for some  $i \geq 0$ , and a polynomial of the form  $a_i x^i$  is called a **term**.

If  $p(x) = \sum_{i=0}^n a_i x^i$  is a polynomial of degree  $n$ , then the polynomials  $a_i x^i$ ,  $i = 0, \dots, n$ , are the **terms** of  $p(x)$ .  $a_n x^n$  is the **leading term**, and  $a_n$  is the **leading coefficient**.

## Constant polynomials

Polynomials of degree  $\leq 0$  are **constant polynomials**.

There is a constant polynomial  $ax^0 \in R[x]$  for every  $a \in R$ . Usually just denote this by  $a$ .

### Lemma

Let  $R$  be a ring. The set of constant polynomials in  $R[x]$  is a subring of  $R[x]$ , and is isomorphic to  $R$ .

Because of this isomorphism, we think of  $R$  as a subring of  $R[x]$ .

## Commutativity

### Lemma

If  $R$  is commutative, then  $R[x]$  is commutative.

*Proof.*

$$\begin{aligned} \sum_{i=0}^n a_i x^i \cdot \sum_{j=0}^m b_j x^j &= \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j} \\ &= \sum_{j=0}^n \sum_{i=0}^n b_j a_i x^{j+i} \\ &= \sum_{j=0}^m b_j x^j \cdot \sum_{i=0}^n a_i x^i. \end{aligned}$$

□

$R[x]$  makes sense even if  $R$  is not commutative, but note that  $x \in Z(R[x])$ , so it's not very natural.

## Evaluation

### Definition — evaluation

If  $p(x) = \sum_{i=0}^n a_i x^i \in R[x]$  and  $c \in R$ , then the **evaluation** of  $p(x)$  at  $c$  is  $p(c) := \sum_{i=0}^n a_i c^i$ .

### Proposition

If  $R$  is commutative and  $c \in R$ , then  $R[x] \rightarrow R : p(x) \mapsto p(c)$  is a homomorphism.

This homomorphism is called **evaluation at  $c$**  or **substitution at  $c$** . When necessary, refer to it by  $\text{ev}_c$ . Note  $\text{ev}_c$  being a homomorphism means that  $(p + q)(c) = \text{ev}_c(p + q) = \text{ev}_c(p) + \text{ev}_c(q) = p(c) + q(c)$ , and similarly that  $(p \cdot q)(c) = p(c)q(c)$  and  $1(c) = 1$ .

### Proof.

If  $p = \sum_i a_i x^i$  and  $q = \sum_j b_j x^j$ , then

$$(p + q)(c) = \sum_i (a_i + b_i) c^i = \sum_i a_i c^i + \sum_i b_i c^i = p(c) + q(c).$$

Also,

$$\begin{aligned} (p \cdot q)(c) &= \sum_k \sum_{i=0}^k a_i b_{k-i} c^k \\ &= \sum_i \sum_j (a_i c^i) (b_j c^j) \\ &= \left( \sum_i a_i c^i \right) \left( \sum_j b_j c^j \right) \\ &= p(c)q(c). \end{aligned}$$

Finally  $1(c) = 1c^0 = 1$ . □

## Polynomials over fields

Most common type of polynomial rings are  $\mathbb{K}[x]$  for  $\mathbb{K}$  a field.

### Proposition

Let  $\mathbb{K}$  be a field. Then

1.  $\deg(fg) = \deg(f) + \deg(g)$  for all  $f, g \in \mathbb{K}[x]$ .
2.  $\mathbb{K}[x]^\times = \mathbb{K}^\times$ .

### Proof.

Homework. □

### Example

$\deg(0 \cdot f) = -\infty = -\infty + \deg(f) = \deg(0) + \deg(f)$ , which explains why we define  $\deg(0) = -\infty$ .

### Example

Let  $p(x) = 1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]$ . Then  $p(x)^2 = 1 + 4x + 4x^2 = 1$ . So  $p(x)$  is a unit.

## Multivariable polynomials

### Definition — multivariable polynomial ring

or any sequence of variables  $x_1, \dots, x_n$  and ring  $R$ , we define the **multivariable polynomial ring**  $R[x_1, \dots, x_n]$  recursively by  $R[x_1, \dots, x_n] := R[x_1, \dots, x_{n-1}][x_n]$ .

Elements of  $R[x_1, \dots, x_n]$  are technically of the form  $\sum_i a_i(x_1, \dots, x_{n-1})x_n^i$  where  $a_i \in R[x_1, \dots, x_{n-1}]$ , but usually we write these elements as  $\sum_{i=(i_1, \dots, i_n)} a_i x^i$  where  $x^i := x_1^{i_1} \cdots x_n^{i_n}$ .

### Example

Typical element of  $R[x_1, x_2]$  is  $x_1 x_2^2 - 7x_1^2 x_2^2 + 3x_1^5 x_2 + 2$ .

What if we reorder  $x_1, \dots, x_n$ ?

### Lemma

Let  $R$  be a ring,  $x_1, \dots, x_n$  a sequence of variables, and  $\sigma \in S_n$ . Then there is an isomorphism  $R[x_{\sigma(1)}, \dots, x_{\sigma(n)}] \rightarrow R[x_1, \dots, x_n]$  given by

$$\sum_{(i_1, \dots, i_n)} a_i x_{\sigma(1)}^{i_1} \cdots x_{\sigma(n)}^{i_n} \mapsto \sum_{(i_1, \dots, i_n)} a_i x_1^{i_{\sigma^{-1}(1)}} \cdots x_n^{i_{\sigma^{-1}(n)}}.$$

### Example

Consider  $3yx - 7y^2x^3 + 2y + 3x + 1 \in \mathbb{Z}[y, x]$ .

The isomorphism above sends this to  $3xy - 7x^3y^2 + 2y + 3x + 1 \in \mathbb{Z}[x, y]$ .

The isomorphism in the lemma is not to be confused with the isomorphism (exercise)  $\mathbb{Z}[y, x] \rightarrow \mathbb{Z}[x, y] : p(y, x) \mapsto p(x, y)$ , which would instead send the above to  $3xy - 7x^2y^3 + 2x + 3y + 1$ .



## Multivariate evaluation

### Definition

If  $p(x_1, \dots, x_n) = \sum_i a_i x^i \in R[x_1, \dots, x_n]$  and  $c = (c_1, \dots, c_n) \in R^n$ , then we define  $p(c) = p(c_1, \dots, c_n) := \sum_i a_i c_1^{i_1} \cdots c_n^{i_n}$ .

### Lemma

Let  $c = (c_1, \dots, c_n) \in R^n$ . The function

$$\text{ev}_c: R[x_1, \dots, x_n] \rightarrow R : p(x_1, \dots, x_n) \mapsto p(c_1, \dots, c_n)$$

is the composition

$$\text{ev}_{c_1} \circ \cdots \circ \text{ev}_{c_n}: R[x_1, \dots, x_{n-1}][x_n] \rightarrow R[x_1, \dots, x_{n-1}] \rightarrow \cdots \rightarrow R,$$

and hence is a homomorphism if  $R$  is commutative.

*Proof.*

Exercise. □

## Group rings

### Definition — group ring

Let  $G$  be a group and  $R$  be a ring. The **group ring**  $RG$  of  $G$  with coefficients in  $R$  is the set of formal sums

$$\left\{ \sum_{g \in G} c_g \cdot g \right\}$$

where  $(c_g)_{g \in G} \subseteq R$  is such that there is a finite subset  $X \subset G$  with  $c_g = 0$  for all  $g \notin X$ , with operations

$$\left( \sum_{g \in G} a_g g \right) + \left( \sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g$$

and

$$\left( \sum_{g \in G} a_g g \right) \cdot \left( \sum_{g \in G} b_g g \right) = \sum_{g, h \in G} a_g b_h gh = \sum_{k \in G} \left( \sum_{g \in G} a_g b_{g^{-1}k} \right) k.$$

A formal sum  $\sum_{g \in G} a_g g$  with coefficients in  $R$  is a fancy way of writing a finitely support function  $G \rightarrow R : g \mapsto a_g$ . Recall a function is finitely support if it is 0 except at finitely many points of  $G$ .

The group elements  $g \in G$  are “placeholders” in this formal sum.

### Example

Let  $R = \mathbb{Z}$  and  $G = D_6 = \{e, r, s, sr, s^2, s^2r\}$ . Some elements of  $\mathbb{Z}D_6$  are:

- $1e + 7s - 2r + sr - s^2r$
- $2e + 2s + 2s^2$
- $r$
- $e$

A general element of  $RG$  is  $a_e e + a_r r + a_s s + a_{sr} sr + a_{s^2} s^2 + a_{s^2r} s^2r$  where  $a_x \in R$  for each  $x \in G$ .

**$G$  versus  $RG$** 

Group elements  $g \in G$  can be regarded as elements of  $RG$ . For example,  $g = 1 \cdot g + \sum_{h \neq g} 0 \cdot h$ .

Technically speaking, though,  $g \in G$  and  $1 \cdot g \in RG$  are different.

Sometimes, write  $\underline{g}$  for  $g$  considered as an element of  $RG$ .

Can also write  $\sum_{g \in G} a_g g$  as  $\sum_{g \in G} a_g \underline{g}$  if it's helpful.

**Example**

Consider  $G = \mathbb{Z}^+$  and  $R = \mathbb{Z}$ . Elements of  $RG = \mathbb{Z}\mathbb{Z}$  look like:

- $3 \cdot \underline{0} - 2 \cdot \underline{1} + 5 \cdot \underline{10} - 6 \cdot \underline{-6}$
- $\underline{1} + \underline{2} + \underline{3}$
- $\underline{0}$  (in particular, not equal to  $0_{RG} = 0 \cdot \underline{0} + 0 \cdot \underline{1} + \cdots$ )

## Ring operations of a group ring

Use component-wise addition:

### Example

$$\text{In } \mathbb{Z}D_6, (2 \cdot e - s + 3 \cdot s^2r) + (3 \cdot e + s + r) = (5 \cdot e + r + 3 \cdot s^2r).$$

For multiplication, use principle that  $\underline{g} \cdot \underline{h} = \underline{gh}$ . Extend to  $RG$  so distributivity holds:

### Example

In  $\mathbb{Z}D_6$ :

- $s \cdot (e + 2s + 3r + 4s^2r) = s + 2s^2 + 3sr + 4r$
- $(e + 2s)(2e - 3r) = 2e + 4s - 3r - 6sr$
- $(e - r)^2 = (e - r)(e - r) = e - r - r + r^2 = 2e - 2r = 2(e - r)$

### Example

$$\text{In } \mathbb{Z}\mathbb{Z}, (\underline{0} + 2 \cdot \underline{-6})(3 \cdot \underline{1} - 4 \cdot \underline{2}) = 3 \cdot \underline{1} - 4 \cdot \underline{2} + 6 \cdot \underline{-5} - 8 \cdot \underline{-4}.$$

### Proposition

Let  $R$  be a ring and  $G$  be a group. Then  $RG$  is a ring with identity  $\underline{e}$ . If  $G$  is commutative, then  $RG$  is commutative.

Group rings are very important examples of not-necessarily-commutative rings.

However, we will focus on commutative rings in this course, so we won't prove this proposition.

Let's check that  $\underline{e}$  is an identity:

$$\underline{e} \cdot \left( \sum_{g \in G} a_g \underline{g} \right) = \sum_{g \in G} a_g \underline{e \cdot g} = \sum_{g \in G} a_g \underline{g}$$

and similarly for right identity.

The remainder of the proof reduces to the fact that  $\cdot$  is associative.

## Group ring homomorphisms

### Proposition

Let  $R$  be a ring and  $\phi: G \rightarrow H$  be a group homomorphism. Then  $\psi: RG \rightarrow RH$  defined by  $\psi\left(\sum_{g \in G} a_g \underline{g}\right) = \sum_{g \in G} a_g \underline{\phi(g)}$  is a ring homomorphism.

### Proof.

Exercise: check well-definedness (two things: that  $\sum_{g: \phi(g)=h} a_g$  is finite for  $h \in H$ , and  $\psi(x)$  is finitely supported for all  $x \in RG$ ).

$\psi(\underline{e_G}) = \underline{\phi(e)} = \underline{e_H}$ , so  $\psi$  is unital.

Let  $x = \sum_{g \in G} a_g \underline{g}$  and  $y = \sum_{h \in G} b_h \underline{h}$ . Then

$$\begin{aligned} \psi(x + y) &= \psi\left(\sum_{g \in G} (a_g + b_g) \underline{g}\right) \\ &= \sum_{g \in G} (a_g + b_g) \underline{\phi(g)} \\ &= \sum_{g \in G} a_g \underline{\phi(g)} + \sum_{g \in G} b_g \underline{\phi(g)} \\ &= \psi(x) + \psi(y). \end{aligned}$$

Also,

$$\begin{aligned} \psi(xy) &= \psi\left(\sum_{g, h \in G} a_g b_h \underline{gh}\right) \\ &= \sum_{g, h \in G} a_g b_h \underline{\phi(gh)} \\ &= \sum_{g, h \in G} a_g b_h \underline{\phi(g)\phi(h)} \\ &= \left(\sum_{g \in G} a_g \underline{\phi(g)}\right) \left(\sum_{h \in H} b_h \underline{\phi(h)}\right). \end{aligned}$$

□

## **Week 8: Ideals and Quotient Rings**

## 18: Ideals

Recall:

### Proposition

Let  $\phi: R \rightarrow S$  be a homomorphism, where  $S$  is not zero.

1.  $\text{Im } \phi$  is a subring of  $S$ .
2.  $\ker \phi$  is an ideal of  $R$ .

What's an ideal? But first, what's special about kernels?

### Lemma

If  $\phi: R \rightarrow S$  is a homomorphism, and  $m \in \ker \phi$ , then  $rm$  and  $mr$  are in  $\ker \phi$  for all  $r \in R$ .

### Proof.

$$\phi(rm) = \phi(r)\phi(m) = \phi(r) \cdot 0_S = 0 = \cdots = \phi(mr).$$

□

### Definition — ideal

An **ideal** of a ring  $R$  is a subgroup  $\mathcal{I}$  of  $(R, +)$  such that if  $m \in \mathcal{I}$  and  $r \in R$ , then  $rm, mr \in \mathcal{I}$ .

The lemma shows that the kernel of a homomorphism is an ideal (and so proves the proposition).

Note if  $R$  is commutative, we only need to check that  $rm \in \mathcal{I}$  for all  $m \in \mathcal{I}$  and  $r \in R$ .

**Example:**  $m\mathbb{Z}$ **Lemma**

$m\mathbb{Z}$  is an ideal of  $\mathbb{Z}$  for every  $m \in \mathbb{Z}$ .

**Proof.**

We already know  $m\mathbb{Z} \leq (\mathbb{Z}, +)$  (which is abelian).

If  $r \in \mathbb{Z}$  and  $km \in m\mathbb{Z}$ , then  $rk m \in m\mathbb{Z}$ .

So  $m\mathbb{Z}$  is an ideal. □

Intuition behind the ideal condition here: if  $m \mid x$ , then  $m \mid rx$  for all  $r \in \mathbb{Z}$ . (Once we are inside the ideal, we can never move out of it.)

Special case: when  $m = 0$ , then  $m\mathbb{Z} = \{0\}$ .

Exercise:  $\{0_R\}$  is an ideal of any ring  $R$ , called the **trivial ideal**, often denoted by  $(0)$  (notation later).



## Simplifying conditions

To show that  $\mathcal{I}$  is a subgroup of  $(R, +)$ , we need to check that

1.  $0 \in \mathcal{I}$ ,
2.  $\mathcal{I}$  is closed under addition, and
3.  $\mathcal{I}$  is closed under negation (additive inverses).

Of course, we could speed this up by checking that

- 1'.  $\mathcal{I}$  is non-empty, and
- 2'.  $f, g \in \mathcal{I} \implies f - g \in \mathcal{I}$ .

We can speed this up in a different way with the ideal condition:

### Lemma

Let  $R$  be a ring and  $\mathcal{I} \subseteq R$ . Then  $\mathcal{I}$  is an ideal if and only if

1.  $\mathcal{I}$  is non-empty, and
2. if  $r \in R$  and  $f, g \in \mathcal{I}$ , then  $rf + g, fr + g \in \mathcal{I}$ .

### *Proof.*

If  $f, g \in \mathcal{I}$ , then  $(-1) \cdot g + f = f - g \in \mathcal{I}$ , so (1') and (2') are satisfied. So  $\mathcal{I} \leq (R, +)$ .

Hence  $0 \in \mathcal{I}$ . If  $m \in \mathcal{I}$  and  $r \in R$ , then  $rm = rm + 0 \in \mathcal{I}$ . So  $\mathcal{I}$  is an ideal.  $\square$

### Example: evaluation

Let  $R$  be a commutative ring and pick  $c \in R$ .

The kernel of  $\text{ev}_c: R[x] \rightarrow R$  is  $\mathcal{I} = \{f \in R[x] : f(c) = 0\}$ .

By the previous lemma, this is an ideal, but let's check:

- $0 \in \mathcal{I}$ , so  $\mathcal{I}$  is non-empty.
- If  $f, g \in \mathcal{I}$  and  $r \in R[x]$ , then  $(rf + g)(c) = r(c)f(c) + g(c) = r(c) \cdot 0 + 0 = 0$  so  $rf + g \in \mathcal{I}$ .

Question: what do elements of this ideal look like?

First, consider  $c = 0$ .

Suppose  $f(x) = \sum_{i=0}^n a_i x^i$ . Then  $f(0) = \sum_i a_i 0^i = a_0$ , so  $f(0) = 0 \iff a_0 = 0$ . (Note: in the context of polynomial evaluation, we use  $0^0 := 1$ .)

So elements of  $\mathcal{I} = \ker \text{ev}_0$  look like  $a_1 x + a_2 x^2 + \dots$ . Because we can factor this as  $a_1 x + a_2 x^2 \dots = x(a_1 + a_2 x + \dots)$ , we sometimes denote  $\mathcal{I}$  by  $xR[x]$ , or by  $(x)$ .

Intuition behind  $xR[x]$  being an ideal: if  $f(x)$  has no constant term, then multiplying  $f(x)$  by another polynomial can't add in a constant term.

Next, for general  $c$ .

#### Lemma

If  $f(x) \in R[x]$  has degree  $\leq n$  and  $c \in R$ , then there are  $a_0, \dots, a_n \in R$  such that  $f(x) = \sum_{i=0}^n a_i (x - c)^i$ , where  $(x - c)^0 := 1$ .

#### Proof.

Clearly true if  $n = 0$ . Proof by induction on  $n$ .

General case: if coefficient of  $x^n$  in  $f(x)$  is  $a_n$ , then  $f(x) - a_n(x - c)^n = a_n x^n + \text{lower terms} - (a_n x^n) + \text{lower terms}$  is a polynomial of degree at most  $n - 1$ . By induction,  $f(x) - a_n(x - c)^n = \sum_{i=0}^{n-1} a_i (x - c)^i$ . Rearrange for  $f(x)$ .  $\square$

Because evaluation is homomorphism,

$$\text{ev}_c((x - c)^i) = \text{ev}_c(x - c)^i = \begin{cases} 0 & i > 0 \\ 1 & i = 0 \end{cases}.$$

So if  $f(x) = \sum_{i=0}^n a_i (x - c)^i$ , then  $f(c) = a_0$ . Conclusion:  $\ker \text{ev}_c = (x - c)R[x] = (x - c)$ .

Caution:  $2x = 2(x - 2) \in (\mathbb{Z}/4\mathbb{Z})[x]$ , so  $2x \in \ker \text{ev}_2$ .

## Ideals containing 1

Note that  $(x - c)R[x]$  doesn't contain 1 for any  $c \in R$ . That's because:

### Lemma

If  $\mathcal{I}$  is an ideal of a ring  $R$ , and  $1 \in \mathcal{I}$ , then  $\mathcal{I} = R$ .

### Proof.

If  $r \in R$  and  $1 \in \mathcal{I}$ , then  $r = r \cdot 1 \in \mathcal{I}$ . □

We typically consider **proper ideals**, that is, ideals  $\mathcal{I} \subsetneq R$ .

## Ideals in fields

We can use the previous lemma to consider ideals in a field.

### Corollary

The only ideals in a field  $\mathbb{K}$  are  $(0)$  and  $\mathbb{K}$ .

#### *Proof.*

Suppose  $\mathcal{I} \subseteq \mathbb{K}$  is an ideal. If  $x \in \mathcal{I}$  and  $x \neq 0$ , then  $x^{-1}x = 1 \in \mathcal{I}$ . So  $\mathcal{I} = \mathbb{K}$ .  $\square$

### Corollary

Let  $\phi: \mathbb{K} \rightarrow R$  be a ring homomorphism, where  $\mathbb{K}$  is a field and  $R$  is non-zero. Then  $\phi$  is injective.

#### *Proof.*

$\ker \phi$  is an ideal of  $\mathbb{K}$ , so  $\ker \phi$  is  $(0)$  or  $\mathbb{K}$ .

If  $\ker \phi = \mathbb{K}$ , then  $0 = \phi(1_{\mathbb{K}}) = 1_R$ , so  $R$  is zero. Since we are assuming  $R$  is non-zero,  $\ker \phi = (0)$ . Then we know from group theory that  $\phi$  is injective.  $\square$

### Example

There are no homomorphisms from an infinite field to a finite field, since such a homomorphism would have to have a kernel (that is, be injective).

### Example

$\mathbb{R}$  is uncountable, while  $\mathbb{Q}$  is countable. So there is no injection  $\mathbb{R} \rightarrow \mathbb{Q}$  as sets. Therefore there is no homomorphism  $\mathbb{R} \rightarrow \mathbb{Q}$ .

## 19: Quotient rings

### Review on quotient groups

Recall in group theory:

- Kernels of homomorphisms are normal subgroups.
- Normal subgroups are kernels of homomorphisms, since if  $N \trianglelefteq G$  then the quotient map  $G \rightarrow G/N$  has kernel  $N$ .

Suppose  $G$  is an abelian group using additive notation. Then:

- Elements of  $G/N$  are equivalence classes  $[x] = x + N$  for  $x \in G$ .
- $[x] = [y]$  if and only if  $x - y \in N$ .
- A group operation is  $[x] + [y] = [x + y]$ .
- The quotient map  $G \rightarrow G/N$  sends  $x \in G$  to  $[x]$ .

## Are ideals always the kernel of some homomorphism?

In ring theory:

- Kernels of homomorphism are ideals.
- Is it true that ideals are kernels of homomorphisms? If  $\mathcal{I}$  is an ideal of  $R$ , is there a “quotient ring”  $R/\mathcal{I}$ ?

Since  $(R, +)$  is commutative,  $\mathcal{I} \trianglelefteq R$ , so the quotient group  $R/\mathcal{I}$  exists. Can we put a ring structure on  $R/\mathcal{I}$ ?

We want multiplication  $\cdot$  such that the quotient map  $q: R \rightarrow R/\mathcal{I}$  is a ring homomorphism. This means we want  $[x] = q(xy) = q(x)q(y) = [x] \cdot [y]$ , so we know what the multiplication should be (assuming this idea works).

### Theorem

Let  $\mathcal{I}$  be an ideal of a ring  $R$ , and define operations  $+$  and  $\cdot$  on  $R/\mathcal{I}$  by  $[x] + [y] = [x + y]$  and  $[x] \cdot [y] = [xy]$  for  $x, y \in R$ . Then  $(R/\mathcal{I}, +, \cdot)$  is a ring. Furthermore, the quotient map  $q: R \rightarrow R/\mathcal{I} : x \mapsto [x]$  is a surjective ring homomorphism with  $\ker q = \mathcal{I}$ .

$R/\mathcal{I}$  is called the **quotient** of  $R$  by the ideal  $\mathcal{I}$ , or just a **quotient ring**.

### Corollary

Every ideal is the kernel of some homomorphism.

### Example

$\mathbb{Z}/m\mathbb{Z}$  is a ring with operations  $[x] + [y] = [x + y]$  and  $[x] \cdot [y] = [xy]$ . We can use this as the definition of  $\mathbb{Z}/m\mathbb{Z}$ .

### Proof of theorem.

We already know  $(R/\mathcal{I}, +)$  is an abelian group.

First, we show  $\cdot$  is **well-defined**.

Suppose  $[x] = [x']$  and  $[y] = [y']$  for  $x, x', y, y' \in R$ . We want to show that  $[xy] = [x'y']$ , or equivalent  $xy - x'y' \in \mathcal{I}$ . We see  $xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y')$ . Since  $[x] = [x']$  and  $[y] = [y']$ , we know  $x - x', y - y' \in \mathcal{I}$ . By the ideal property,  $(x - x')y, x'(y - y') \in \mathcal{I}$ , so  $xy - x'y' \in \mathcal{I}$ .

Next, we show  $\cdot$  is **associative**.

Suppose  $x, y, z \in R$ . Then  $[x] \cdot ([y] \cdot [z]) = [x] \cdot [yz] = [xyz] = ([x] \cdot [y]) \cdot [z]$ .

Next, we show  $\cdot$  has an **identity**.

Note  $[1] \cdot [x] = [1 \cdot x] = [x] = [x] \cdot [1]$ , so  $[1]$  is an identity for  $\cdot$ .

Next, we show **distributivity**.

If  $x, y, z \in R$ . Then

$$[x] \cdot ([y] + [z]) = [x] \cdot [y + z] = [x \cdot (y + z)] = [xy + xz] = [xy] + [xz] = [x] \cdot [y] + [x] \cdot [z],$$

and similarly  $([y] + [z]) \cdot [x] = [y] \cdot [x] + [z] \cdot [x]$ .

Since  $(R/\mathcal{I}, +)$  is an abelian group,  $\cdot$  is associative with identity, and  $+$  and  $\cdot$  satisfy distributivity,  $R/\mathcal{I}$  is a ring.

Now, we show  $q$  is a **homomorphism**.

We already know  $q$  is a group homomorphism. Also,  $q(xy) = [xy] = [x] \cdot [y] = q(x)q(y)$  and  $q(1) = [1]$  is the identity for  $R/\mathcal{I}$ . So  $q$  is a ring homomorphism.  $\square$

## Universal property of quotient groups, and quotient rings

### Theorem — Universal property of quotient groups

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.

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

Can we extend this to rings?

Let  $\phi: R \rightarrow S$  be a ring homomorphism and  $\mathcal{I}$  an ideal of  $R$ . Suppose  $\mathcal{I} \subseteq \ker \phi$ . By the universal property of quotient groups, there is a unique group homomorphism  $\psi: R/\mathcal{I} \rightarrow S$  such that  $\phi = \psi \circ q$ .

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ & \searrow q & \nearrow \psi \\ & R/\mathcal{I} & \end{array}$$

Is  $\psi$  a ring homomorphism?

### Lemma

Let  $R, S, T$  be rings. Suppose that  $\psi_1: R \rightarrow T$  is a ring homomorphism and  $\psi_2: T \rightarrow S$  is a group homomorphism, such that  $\psi_2 \circ \psi_1$  is a ring homomorphism. If  $\psi_1$  is surjective, then  $\psi_2$  is a ring homomorphism.

### Proof.

Let  $\phi = \psi_2 \circ \psi_1$ .

Suppose  $x, y \in T$ . Let  $a, b \in R$  such that  $\psi_1(a) = x$  and  $\psi_1(b) = y$ . Then  $\psi_2(xy) = \psi_2(\psi_1(a)\psi_1(b)) = \psi_2(\psi_1(ab)) = \phi(ab) = \phi(a)\phi(b) = \psi_2(\psi_1(a))\psi_2(\psi_1(b)) = \psi_2(x)\psi_2(y)$ .

Also,  $\psi_2(1_T) = \psi_2(\psi_1(1_R)) = \phi(1_R) = 1_S$ .

So  $\psi_2$  is a ring homomorphism. □

As a corollary of the lemma and the universal property of quotient groups:



**Theorem — Universal property of quotient rings**

Suppose  $\phi: R \rightarrow S$  is a ring homomorphism and  $\mathcal{I}$  is an ideal of  $R$ . Let  $q: R \rightarrow R/\mathcal{I}$  be the quotient homomorphism. Then there is a ring homomorphism  $\psi: R/\mathcal{I} \rightarrow S$  such that  $\psi \circ q = \phi$  if and only if  $\mathcal{I} \subseteq \ker \phi$ . Furthermore, if  $\psi$  exists then it is unique.

*Proof.*

**Existence:** If  $\mathcal{I} \subseteq \ker \phi$ , then  $\psi$  exists as a group homomorphism. Applying the lemma with  $\psi_1 = q$ ,  $\psi_2 = \psi$ , and  $T = R/\mathcal{I}$  shows  $\psi$  is a ring homomorphism.

**Uniqueness:** Any ring homomorphism  $\psi: R/\mathcal{I} \rightarrow S$  such that  $\psi \circ q = \phi$  is equal to the unique group homomorphism with this property.

**Necessity of  $\mathcal{I} \subseteq \ker \phi$ :** If  $\psi$  exists, then it is a group homomorphism, so apply the universal property of quotient groups.  $\square$

## First isomorphism theorem for rings

### Theorem — First isomorphism theorem for rings

If  $\phi: R \rightarrow S$  is a ring homomorphism, then there is a ring isomorphism  $\psi: R/\ker \phi \rightarrow \text{Im } \phi$  such that  $\phi = \psi \circ q$ , where  $q: R \rightarrow R/\ker \phi$  is the quotient homomorphism.

#### Proof.

By the universal property, we have a ring homomorphism  $\psi: R/\ker \phi \rightarrow \text{Im } \phi$  such that  $\psi \circ q = \phi$ . From the first isomorphism theorem for groups, there is a group isomorphism  $\psi': R/\ker \phi \rightarrow \text{Im } \phi$  such that  $\psi' \circ q = \phi$ .  $\psi$  is also a group homomorphism. By the universal property of quotient groups,  $\psi = \psi'$ , so  $\psi$  is bijective.

(Or, apply the lemma to  $\psi'$ .) □

The first isomorphism theorem is very useful for finding quotient rings.

### Proposition

Let  $R$  be a commutative ring and let  $c \in R$ . Then  $R[x]/(x - c)R[x] \cong R$ .

#### Proof.

$(x - c)R[x] = \ker \text{ev}_c$ , where  $\text{ev}_c: R[x] \rightarrow R$  is the evaluation map. If  $r \in R$ , then  $\text{ev}_c(r) = r$ , so  $\text{Im } \text{ev}_c = R$ . By the first isomorphism theorem,  $R[x]/(x - c)R[x] \cong R$ . □

### Example

Let  $\mathcal{I} = (y - x^2)\mathbb{Z}[x, y] = \{(y - x^2)p(x, y) : p(x, y) \in \mathbb{Z}[x, y]\}$ .

To see that  $\mathcal{I}$  is an ideal, note that  $\mathcal{I} = \ker \text{ev}_{x^2}$ , where  $\text{ev}_{x^2}: \mathbb{Z}[x, y] = \mathbb{Z}[x][y] \rightarrow \mathbb{Z}[x]$  is evaluation at  $x^2$ . (From the recursive definition and our previous investigation.)

By the proposition,  $\mathbb{Z}[x, y]/\mathcal{I} \cong \mathbb{Z}[x]$ .

## 20: Ideals generated by a subset

### Ideal generated by a subset

#### Proposition

Let  $\mathcal{F}$  be a family of ideals in a ring  $R$ . Then

$$\bigcap_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$$

is an ideal of  $R$ .

*Proof.*

Homework. □

#### Definition — ideal generated by a subset

Let  $X \subseteq R$ . The **ideal generated by  $X$**  is

$$(X) := \bigcap_{\mathcal{I} \in \mathcal{F}} \mathcal{I},$$

where  $\mathcal{F}$  is the set of ideals of  $R$  containing  $X$ .

Key properties:

- By proposition,  $(X)$  is an ideal.
- By definition, if  $\mathcal{I}$  is an ideal containing  $X$ , then  $X \subseteq (X) \subseteq \mathcal{I}$ . Say that  $(X)$  is the smallest ideal containing  $X$ .
- Example:  $(0) = (\emptyset) = \{0\}$ .

Notation:

- Sometimes use  $\langle X \rangle$  instead of  $(X)$ .
- If  $X = \{f_1, f_2, \dots\}$ , can replace  $(X) = (\{f_1, f_2, \dots\})$  by  $(f_1, f_2, \dots)$ . Example:  $(0)$  instead of  $(\{0\})$ .

**Proposition**

If  $R$  is a ring and  $X \subseteq R$ , then

$$(X) = \left\{ \sum_{i=1}^k s_i x_i t_i : k \geq 0, s_i, t_i \in R, x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

**Corollary**

If  $R$  is a commutative ring and  $X \subseteq R$ , then

$$(X) = \left\{ \sum_{i=1}^k r_i x_i : k \geq 0, r_i \in R, x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

*Proof.*

$s_i x_i t_i = (s_i t_i) x_i$ , so set  $r_i = s_i t_i$ . □

*Proof of proposition.*

Let  $\mathcal{I}$  be the set in question.

First, show  $\mathcal{I}$  is an ideal. Taking  $k = 0$ , we get  $0_R \in \mathcal{I}$ . Suppose  $r \in R$  and  $x, y \in \mathcal{I}$ . Let  $x = \sum_{i=1}^k s_i x_i t_i$  and  $y = \sum_{i=1}^\ell s'_i y_i t'_i$  for  $s_i, t_i, s'_i, t'_i \in R$  and  $x_i, y_i \in X$ . Then  $rx + y = \sum_{i=1}^k (rs_i) x_i t_i + \sum_{i=1}^\ell s'_i y_i t'_i \in \mathcal{I}$  and similarly  $xr + y \in \mathcal{I}$ , so  $\mathcal{I}$  is an ideal.

Next, show  $(X) \subseteq \mathcal{I}$ . Taking  $k = 1$  and  $s_1 = t_1 = 1$ , we get  $X \subseteq \mathcal{I}$  so  $(X) \subseteq \mathcal{I}$ .

Finally, show  $\mathcal{I} \subseteq (X)$ . Suppose  $k \geq 0$ ,  $s_i, t_i \in R$ , and  $x_i \in X$  for  $1 \leq i \leq k$ . Since  $X \subseteq (X)$ ,  $x_i \in (X)$  means  $s_i x_i t_i \in (X)$  for all  $1 \leq i \leq k$ . So  $\sum_{i=1}^k s_i x_i t_i \in (X)$ . Hence  $\mathcal{I} \subseteq (X)$ . □

## The sum of ideals

### Definition — ideal sum

If  $\mathcal{I}, \mathcal{J} \subseteq R$  are ideals, then  $\mathcal{I} + \mathcal{J} := \{x + y : x \in \mathcal{I}, y \in \mathcal{J}\}$ .

### Corollary

$(\mathcal{I} \cup \mathcal{J}) = \mathcal{I} + \mathcal{J}$  is the smallest ideal containing both  $\mathcal{I}$  and  $\mathcal{J}$ .

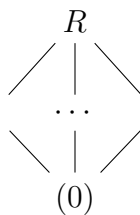
### *Proof.*

By proposition, clearly  $\mathcal{I} + \mathcal{J} \subseteq (\mathcal{I} \cup \mathcal{J})$ .

For the reverse inclusion, suppose  $s_i, t_i \in R$  and  $x_i \in \mathcal{I} \cup \mathcal{J}$  for  $1 \leq i \leq k$ . Let  $S = \{1 \leq i \leq k : x_i \in \mathcal{I}\}$ , so if  $i \in S$ , then  $s_i x_i t_i \in \mathcal{I}$ . So  $\sum_{i \in S} s_i x_i t_i \in \mathcal{I}$ , and similarly  $\sum_{i \notin S} s_i x_i t_i \in \mathcal{J}$ . We conclude that  $\sum_{i=1}^k s_i x_i t_i = \sum_{i \in S} s_i x_i t_i + \sum_{i \notin S} s_i x_i t_i \in \mathcal{I} + \mathcal{J}$ .  $\square$

## Lattice of ideals

Ideals of  $R$  are ordered by set inclusion  $\subseteq$ . The set of ideals of  $R$  with order  $\subseteq$  is called the **lattice of ideals** of  $R$ .



The subgroup below  $\mathcal{I}_1$  and  $\mathcal{I}_2$  in the lattice is  $\mathcal{I}_1 \cap \mathcal{I}_2$  (maximal subgroup contained in both).

The subgroup above  $\mathcal{I}_1$  and  $\mathcal{I}_2$  is  $\mathcal{I}_1 + \mathcal{I}_2$  (minimal subgroup containing both).

## Quotients by a subset

We get a new way of constructing rings: take  $R/(X)$  for any subset  $X$ . We know  $R/(X)$  is a unital ring, but when is it non-zero?

From group theory, we know that  $R/\mathcal{I}$  is zero if and only if  $\mathcal{I} = R$ . We proved that  $\mathcal{I} = R$  if and only if  $1 \in \mathcal{I}$ .

### Corollary

Let  $R$  be a ring and  $X \subseteq R$ . Then  $R/(X) = \{0\}$  if and only if there are  $s_i, t_i \in R$  and  $x_i \in X$  for  $1 \leq i \leq k$  such that

$$\sum_{i=1}^k s_i x_i t_i = 1.$$

If  $R$  is commutative, we can instead just show  $\sum_{i=1}^k r_i x_i = 1$  for  $r_i \in R$  and  $x_i \in X$ .

## Ideals generated by a finite subset

We often take ideals  $(x_1, \dots, x_n)$  generated by finite sets  $\{x_1, \dots, x_n\}$ .

### Corollary

If  $R$  is a commutative ring and  $X \subseteq R$ , then

$$(X) = \left\{ \sum_{i=1}^k r_i x_i : k \geq 0, r_i \in R, x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

### Corollary

If  $R$  is a commutative ring and  $X = \{x_1, \dots, x_n\} \subseteq R$ , then

$$(X) = \left\{ \sum_{i=1}^n r_i x_i : r_i \in R, 1 \leq i \leq n \right\}.$$

### *Proof.*

RHS  $\subseteq (X)$  is clear. For the other inclusion, note that  $rx_i + r'x_i = (r + r')x_i$ , so we can collect like terms; if  $x_i$  is unneeded, then set  $r_i = 0$ .  $\square$



## Principal ideals

### Definition — principal ideal

An ideal generated by a single element is called a **principal ideal**.

If  $R$  is a commutative ring, then  $(x) = \{rx : r \in R\}$ , so a principal ideal  $(x)$  is often denoted by  $xR$  or  $Rx$ .

### Example

Let  $R = \mathbb{Z}$  and  $m \in \mathbb{Z}$ . Then  $(m) = m\mathbb{Z}$  is a principal ideal.

All subgroups of  $\mathbb{Z}$  are of the form  $m\mathbb{Z}$  for some  $m \in \mathbb{Z}$ , so all subgroups of  $\mathbb{Z}$  are principal ideals. In particular, all ideals of  $\mathbb{Z}$  are principal ideals.

### Example

If  $R$  is commutative and  $p(x) \in R[x]$ , then  $(p) = pR[x]$  is an ideal.

## Principal ideals in non-commutative rings

If  $R$  is non-commutative, then  $(x)$  is not necessarily equal to  $\{rx : r \in R\}$  since  $xr \in (x)$  for  $r \in R$ . But is  $(x) = \{srx : s, r \in R\}$ ? In general, no.

### Example

Let  $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2\mathbb{R}$ .

We know  $AE_{11}B$  has rank  $\leq 1$  for every  $A, B \in M_2\mathbb{R}$ , hence  $\{AE_{11}B : A, B \in M_2\mathbb{R}\} \subsetneq M_2\mathbb{R}$ .

Let  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Then  $XE_{11}X = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ .

So  $E_{11} + XE_{11}X = I \in (E_{11})$ , and we conclude that  $(E_{11}) = M_2\mathbb{R}$ .

## More examples in polynomial rings

Principal ideals:

- We've already mentioned the principal ideals  $(x - c)\mathbb{Z}[x]$  for  $c \in \mathbb{Z}$ . For example,  $x\mathbb{Z}[x]$  is the ideal of polynomials with no constant term.
- Another good example is  $m\mathbb{Z}[x]$  for  $m \in \mathbb{Z}$ . This is  $m\mathbb{Z}[x] = \{\sum_{i=0}^n a_i x^i : n \geq 0, a_i \in m\mathbb{Z} \text{ for } 0 \leq i \leq n\}$ .
- The previous example doesn't work in  $\mathbb{Q}[x]$ , though, since  $2\mathbb{Q}[x] = \mathbb{Q}[x]$  ( $2 \cdot \frac{1}{2} = 1$ ). Also,  $\mathbb{Z}[x]$  is not an ideal in  $\mathbb{Q}[x]$  (in general, subrings are very different from ideals).

What about non-principal ideals?

In  $\mathbb{Z}[x, y]$ ,  $(x, y) = \{p(x, y)x + q(x, y)y : p, q \in \mathbb{Z}[x, y]\}$ . So  $(x, y)$  contains  $x, y, xy, x^2, y^2$ , etc. Note  $p, q$  aren't unique:  $xy = 0 + x \cdot y = y \cdot x + 0$ . To see that  $(x, y)$  is a proper ideal of  $\mathbb{Z}[x, y]$ , observe that

$$(x, y) = \left\{ \sum_{i,j=0}^n a_{ij} x^i y^j : n \geq 0, a_{ij} \in \mathbb{Z} \text{ for } 0 \leq i, j \leq n, a_{00} = 0 \right\}.$$

### Exercise

Suppose there are polynomials  $f, p, q \in \mathbb{Z}[x, y]$  such that  $p \cdot f = x$  and  $q \cdot f = y$ . Show  $f \in \{\pm 1\}$ .

Consequence: the only principal ideal containing  $(x, y)$  is  $\mathbb{Z}[x, y]$ . In particular,  $(x, y)$  is not principal.

All ideals of  $\mathbb{Z}$  are principal, whereas  $\mathbb{Z}[x, y]$  has non-principal ideals.

What about  $\mathbb{Z}[x]$ ? Consider the ideal

$$\begin{aligned} (2, x) &= \{2p(x) + xq(x) : p, q \in \mathbb{Z}[x]\} \\ &= \left\{ \sum_{i=0}^n a_i x^i : n \geq 0, a_i \in \mathbb{Z} \text{ for } 0 \leq i \leq n, a_0 \in 2\mathbb{Z} \right\}. \end{aligned}$$

Can this ideal be principal?

### Exercise

Show that if  $p, f \in \mathbb{Z}[x]$  such that  $p(x)f(x) = 2$ , then  $f \in \{\pm 1, \pm 2\}$ .  
Show that  $x \notin \pm 2\mathbb{Z}[x]$ .

Conclusion: the only principal ideal containing  $(2, x)$  is  $\mathbb{Z}[x]$ .

## 21: Correspondence, second and third isomorphism theorems

### Connecting ideals and homomorphisms (correspondence theorem)

#### Proposition

Let  $\phi: R \rightarrow S$  be a ring homomorphism.

1. If  $\mathcal{I}$  is an ideal of  $S$ , then  $\phi^{-1}(\mathcal{I})$  is an ideal of  $R$ .
2. If  $\mathcal{I}$  is an ideal of  $R$  and  $\phi$  is surjective, then  $\phi(\mathcal{I})$  is an ideal of  $S$ .

#### Proof.

Homework. (Also provide counterexample for (2) when  $\phi$  is not surjective.)  $\square$

Recall from group theory:

#### Theorem — Correspondence theorem for groups

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

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

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.

We can get a version for rings immediately.

#### Theorem — Correspondence theorem for rings

Let  $\phi: R \rightarrow S$  be a surjective ring homomorphism. Then there is a bijection

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

Furthermore, if  $\ker \phi \leq K, K_1, K_2 \leq R^+$ , then  $K$  is an ideal if and only if  $\phi(K)$  is an ideal.

*Proof.*

Apply proposition and use the fact that  $K = \phi^{-1}(\phi(K))$ . □

In the special case of  $q: R \rightarrow R/\mathcal{I}$ , if  $\mathcal{I} \subseteq \mathcal{K} \leq R^+$ , then  $\mathcal{K}$  is an ideal of  $R$  if and only if  $\mathcal{K}/\mathcal{I}$  is an ideal of  $R/\mathcal{I}$ .

### Example

Let  $R$  be a commutative ring. What are the ideals of  $R[x]$  containing  $(x)$ ?

$(x)$  is the kernel of the surjective homomorphism  $\text{ev}_{x=0}: R[x] \rightarrow R$ . So ideals of  $R[x]$  containing  $(x)$  correspond to ideals  $\mathcal{I}$  of  $R$ .

If  $\mathcal{I}$  is an ideal of  $R$ , what is the corresponding ideal in  $R[x]$ ?

Answer:

$$\begin{aligned} \text{ev}_{x=0}^{-1}(\mathcal{I}) &= \{f \in R[x] : f(0) \in \mathcal{I}\} \\ &= \left\{ \sum_{i=0}^n a_i x^i : n \geq 0, a_i \in R \text{ for } 0 \leq i \leq n, a_0 \in \mathcal{I} \right\}. \end{aligned}$$

## Second isomorphism theorem

Recall from group theory:

### Theorem — Second isomorphism theorem for groups

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  $\psi \circ q_1 = q_2 \circ i_H$ .

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

Let's restate this for abelian groups with additive notation.

### Theorem — Second isomorphism theorem for abelian groups

Suppose  $H, K \leq G$ . Then  $H + K \leq G$ , and furthermore, if  $i_H: H \rightarrow H + K$  is the inclusion,  $q_1: H \rightarrow H/H \cap K$  and  $q_2: H + K \rightarrow H + K/K$  are the quotient maps, then there is an isomorphism  $\psi: H/H \cap K \rightarrow H + K/K$  such that  $\psi \circ q_1 = q_2 \circ i_H$ .

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

Now we can extend this to rings.

### Theorem — Second isomorphism theorem for rings

Let  $S$  be a subring of  $R$  and let  $\mathcal{I}$  be an ideal of  $R$ . Then  $S + \mathcal{I}$  is a subring of  $R$  and  $S \cap \mathcal{I}$  is an ideal of  $S$ . Furthermore, if  $i_S: S \rightarrow S + \mathcal{I}$  is the inclusion and  $q_1: S \rightarrow S/S \cap \mathcal{I}$  and  $q_2: S + \mathcal{I} \rightarrow S + \mathcal{I}/\mathcal{I}$  are the quotient maps, then there is a (ring) isomorphism  $\psi: S/S \cap \mathcal{I} \rightarrow S + \mathcal{I}/\mathcal{I}$  such that  $\psi \circ q_1 = q_2 \circ i_S$ .

$$\begin{array}{ccc}
 S & \xrightarrow{i_S} & S + \mathcal{I} \\
 q_1 \downarrow & & \downarrow q_2 \\
 S/S \cap \mathcal{I} & \xrightarrow{\psi} & S + \mathcal{I}/\mathcal{I}
 \end{array}$$

Here  $S + \mathcal{I} = \{s + x : s \in S, x \in \mathcal{I}\}$  (same definition as for ideals).

*Proof.*

$S, \mathcal{I}$  are subgroups of  $R^+$  and  $S + \mathcal{I}$  is a subgroup of  $R^+$ .

To show that  $S + \mathcal{I}$  is a subring, note that  $1 \in S + \mathcal{I}$ . If  $x, y \in S + \mathcal{I}$ , then  $x = s + a$  and  $y = t + b$  for some  $s, t \in S$  and  $a, b \in \mathcal{I}$ . So  $xy = st + (st + at + ab) \in S + \mathcal{I}$  and hence  $S + \mathcal{I}$  is a subring.

Exercise: show  $S \cap \mathcal{I}$  is an ideal of  $S$ .

By second isomorphism theorem for groups, there is an isomorphism  $\psi: S/S \cap \mathcal{I} \rightarrow S + \mathcal{I}/\mathcal{I}$  such that  $\psi \circ q_1 = q_2 \circ i_S$ .

By applying the lemma below, we see  $\psi$  is a ring isomorphism.  $\square$

**Lemma — From universal property of quotient rings**

Let  $R, S, T$  be rings. Suppose that  $\psi_1: R \rightarrow T$  is a ring homomorphism and  $\psi_2: T \rightarrow S$  is a group homomorphism such that  $\psi_2 \circ \psi_1$  is a ring homomorphism. If  $\psi_1$  is surjective, then  $\psi_2$  is a ring homomorphism.

**Example**

Let  $\mathcal{J}$  be an ideal of a commutative ring  $R$ .

Let  $\mathcal{I} = \{f \in R[x] : f(0) \in \mathcal{J}\} = \text{ev}_0^{-1}(\mathcal{J})$ .

Then

- $R$  is a subring of  $R[x]$ ,
- $R + \mathcal{I} = R[x]$ , and
- $R \cap \mathcal{I} = \mathcal{J}$ .

So  $R/\mathcal{J} \cong R[x]/\mathcal{I}$  by the second isomorphism theorem.

## Third isomorphism theorem

From group theory:

### Theorem — Third isomorphism theorem for groups

Let  $N \trianglelefteq G$  and  $N \leq K \leq G$ . 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  $\psi \circ q_3 = q_2 \circ q_1$ .

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

Now for rings:

### Theorem — Third isomorphism theorem for groups

Suppose  $\mathcal{I} \subseteq \mathcal{K}$  are ideals of a ring  $R$ , and let

- $q_1$  be the quotient map  $R \rightarrow R/\mathcal{I}$ ,
- $q_2$  be the quotient map  $R/\mathcal{I} \rightarrow (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$ , and
- $q_3$  be the quotient map  $R \rightarrow R/\mathcal{K}$ .

Then there is a (ring) isomorphism  $\psi: R/\mathcal{K} \rightarrow (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$  such that  $\psi \circ q_3 = q_2 \circ q_1$ .

$$\begin{array}{ccc} R & \xrightarrow{q_1} & R/\mathcal{I} \\ q_3 \downarrow & & \downarrow q_2 \\ R/\mathcal{K} & \xrightarrow{\psi} & (R/\mathcal{I})/(\mathcal{K}/\mathcal{I}) \end{array}$$

### Proof.

Apply the lemma from the universal property of quotient rings again. □

### Example

$(\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$  as groups, and also as rings.



**Example**

As in the previous example, let  $\mathcal{J}$  be an ideal of  $R$  and  $\mathcal{I} = \text{ev}_0^{-1}(\mathcal{J}) \subseteq R[x]$ .

Now  $\mathcal{I}$  contains  $(x)$ , so by the third isomorphism,  $R[x]/\mathcal{I} \cong (R[x]/(x))/(\mathcal{I}/(x))$ .

By first isomorphism theorem,  $R[x]/(x) \cong R$  since  $(x) = \ker \text{ev}_0$ . This isomorphism sends  $f(x) + (x) \in R[x]/(x)$  to  $\text{ev}_0(f) = f(0)$ , and hence identifies  $\mathcal{I}/(x)$  with  $\mathcal{J}$ .

Conclusion:  $R[x]/\mathcal{I} \cong (R/(x))/(\mathcal{I}/(x)) \cong R/\mathcal{J}$ .

Exercise: show that this isomorphism is the same as the isomorphism  $R/\mathcal{J} \cong R[x]/\mathcal{I}$  from the second isomorphism theorem.

## **Week 9: Maximal and Prime Ideals**

## 22: Maximal ideals and fields

### Constructing complex numbers from real numbers

From last week: we can construct new rings  $R/(X)$  by taking  $X \subseteq R$ . What sets  $X$  might we like to look at?

Suppose we didn't know about  $\mathbb{C}$ , and we want a square root of  $-1$ . We want to take  $\mathbb{R}$  and add an element  $x$  such that  $x^2 = -1$ .

So let's look at  $\mathbb{R}[x]/(x^2 + 1)$  (note  $x^2 + 1 = 0 \iff x^2 = -1$ ). If we look at  $\bar{x} = [x]$  in  $\mathbb{R}[x]/(x^2 + 1)$ , then

$$\bar{x}^2 + 1 = [x]^2 + [1] = [x^2 + 1] = x^2 + 1 + (x^2 + 1) = (x^2 + 1) = 0.$$

What ring is  $\mathbb{R}[x]/(x^2 + 1)$ ?

#### Theorem

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

If we didn't know about  $\mathbb{C}$ , we could use  $\mathbb{R}[x]/(x^2 + 1)$  as the definition.

## The complex numbers

Let's clarify what  $\mathbb{C}$  is:

- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$
- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

How does  $\mathbb{R}[x]/(x^2 + 1)$  correspond to  $\mathbb{C}$ ? We know that  $\bar{x}$  acts like  $i$ .

### Lemma

Every element of  $\mathbb{R}[x]/(x^2 + 1)$  can be written uniquely in the form  $a + b\bar{x}$  for some  $a, b \in \mathbb{R}$ .

### Proof.

**Existence:** Since the quotient map  $\mathbb{R}[x] \rightarrow \mathbb{R}[x]/(x^2 + 1)$  is surjective, every element of  $\mathbb{R}[x]/(x^2 + 1)$  can be written as  $\sum_{i=0}^n a_i \bar{x}^i$ . (Note the bar on  $a_i$  is dropped for brevity.)

If  $n \geq 2$ , then  $a_n x^{n-2}(x^2 + 1) \in (x^2 + 1)$ , so  $a_n \bar{x}^n + a_n \bar{x}^{n-2} = 0$ . Thus

$$\begin{aligned} \sum_{i=0}^n a_i \bar{x}^i &= \sum_{i=0}^n a_i \bar{x}^i - (a_n \bar{x}^n + a_n \bar{x}^{n-2}) \\ &= 0 \cdot \bar{x}^n + a_{n-1} \bar{x}^{n-1} + (a_{n-2} - a_n) \bar{x}^{n-2} + \cdots \end{aligned}$$

We can lower  $n$  until we get  $\sum_{i=0}^n a_i \bar{x}^i = a + b\bar{x}$  for some  $a, b$ .

**Uniqueness:** Suppose  $a + b\bar{x} = c + d\bar{x}$ . Then  $(a - c) + (b - d)\bar{x} = 0$ , so  $(a - c) + (b - d)x \in (x^2 + 1)$ .

If  $f \in (x^2 + 1)$  and  $f \neq 0$ , then  $f = g(x^2 + 1)$  for  $g \in \mathbb{R}[x]$  with  $g \neq 0$ . So  $\deg(f) = \deg(g) + \deg(x^2 + 1) \geq 2$ .

Hence every non-zero element of  $(x^2 + 1)$  has degree  $\geq 2$ . Then the only way  $(a - c) + (b + d)x$  can be in  $(x^2 + 1)$  is if it is zero, so  $a = c$  and  $b = d$ .  $\square$

Now for the theorem:

### Theorem

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

*Proof.*

Since  $\mathbb{R}$  is a subring of  $\mathbb{C}$ , we can consider  $\mathbb{R}[x]$  as a subring of  $\mathbb{C}[x]$ .

Let  $j: \mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$  be the inclusion. Let  $\phi = \text{ev}_{x=i} \circ j: \mathbb{R}[x] \rightarrow \mathbb{C}[x] \rightarrow \mathbb{C}$ . Then  $\phi(x) = i$ , so  $\phi(x^2 + 1) = i^2 + 1 = 0$ . So  $x^2 + 1 \in \ker \phi$ , so  $(x^2 + 1) \subseteq \ker \phi$ .

By the universal property of quotient rings, there is a homomorphism  $\psi: \mathbb{R}[x]/(x^2+1) \rightarrow \mathbb{C}$  such that  $\psi \circ q = \phi$ . So  $\psi(a + b\bar{x}) = \phi(a + bx) = a + bi$ . By the lemma,  $\psi$  is a bijection.  $\square$

This is a common line of proof (see Homework #4 Q9).

## Generalizations

We constructed  $\mathbb{C}$  by asking for an element  $x$  such that  $x^2 + 1 = 0$ .

If we start from a field  $\mathbb{K}$ , can we ask for an element  $x$  satisfying any polynomial equation(s), and then just construct a ring containing  $\mathbb{K}$  with such an element?

Yes! But the ring might be zero if we ask for too much.

### Example

- $1 \neq 0$  in  $\mathbb{K}[x]/(x^2 + 1)$  as we've seen.
- If  $p$  is a polynomial of degree  $n \geq 1$ , then  $\mathbb{K}[x]/(p)$  is a  $\mathbb{K}$ -vector space of dimension  $n$  (exercise similar to lemma). So  $1 \neq 0$  in  $\mathbb{K}[x]/(p)$ .
- $1 = 0$  in  $\mathbb{K}[x]/(x^2 + 1, x^3 + x + 1)$ , since  $x^3 + x + 1 - x(x^2 + 1) = 1 \in (x^2 + 1, x^3 + x + 1)$ .

## Maximal ideals

Let  $\mathcal{I}$  be an ideal of a commutative ring  $R$ . When is  $R/\mathcal{I}$  a field?

We know that the only ideals in a field  $\mathbb{K}$  are  $(0)$  and  $\mathbb{K}$ . Suppose  $\mathbb{K} = R/\mathcal{I}$  is a field, and  $q: R \rightarrow \mathbb{K}$  is the quotient map. By the correspondence theorem, the only ideals of  $R$  containing  $\mathcal{I}$  are  $q^{-1}((0)) = \ker q = \mathcal{I}$  and  $q^{-1}(\mathbb{K}) = R$ .

### Definition — maximal ideal

An ideal  $\mathcal{I}$  of a ring  $R$  is **maximal** if the only ideals containing  $\mathcal{I}$  are  $\mathcal{I}$  and  $R$ .

Intuition: a maximal ideal is a maximal proper ideal under  $\subseteq$ .

### Lemma

If  $R/\mathcal{I}$  is a field, then  $\mathcal{I}$  is maximal.

## Ideals in fields

### Proposition

A commutative ring  $R$  is a field if and only if  $1 \neq 0$ , and the only ideals in  $R$  are  $(0)$  and  $R$ .

Requiring  $1 \neq 0$  is the same as requiring  $(0) \neq R$ .

### *Proof.*

We already saw the forward implication.

For the reverse, suppose  $x \in R$  where  $x \neq 0$ . Then  $(x) = R$ . Then  $1 \in (x) = xR$ , so there is  $y \in R$  such that  $xy = 1$ . So  $x$  is a unit. Since all non-zero elements of  $R$  are units,  $R$  is a field.  $\square$



## Maximal ideals and fields

### Theorem

Let  $\mathcal{I}$  be an ideal in a commutative ring  $R$ . Then  $R/\mathcal{I}$  is a field if and only if  $\mathcal{I}$  is maximal.

### Proof.

By correspondence theorem, the only ideals of  $R/\mathcal{I}$  are  $(0)$  and  $R/\mathcal{I}$  if and only if the only ideals of  $R$  containing  $\mathcal{I}$  are  $\mathcal{I}$  and  $R$ . So by the proposition,  $R/\mathcal{I}$  is a field if and only if  $\mathcal{I}$  is maximal.  $\square$

### Example

- $\mathbb{K}[x]/(x - c) \cong \mathbb{K}$  for all  $c \in \mathbb{K}$ , so  $(x - c)$  is a maximal ideal of  $\mathbb{K}[x]$  for any field  $\mathbb{K}$ .
- $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ , so  $(x^2 + 1)$  is a maximal ideal of  $\mathbb{R}[x]$ .

### Example

$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$  is not a field, so  $(x)$  is not a maximal ideal of  $\mathbb{Z}[x]$ .

Indeed, we know that  $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$ . We also know that  $(2, x) = \{f \in \mathbb{Z}[x] : f(0) \in (2)\} = \text{ev}_{x=0}^{-1}((2))$  for ideal  $(2) \subseteq \mathbb{Z}$ . By the second isomorphism theorem,  $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ , which is a field.

Exercise:  $\mathbb{Z}[x]/(n, x) \cong \mathbb{Z}/n\mathbb{Z}$  and hence  $(n, x)$  is maximal for  $n \in \mathbb{Z}$  if and only if  $n$  is prime.

### Example

If  $R$  is commutative ring, we have

$$\text{ev}_{(a,b)} = \text{ev}_{x=a} \circ \text{ev}_{y=b} : R[x, y] = R[x][y] \rightarrow R[x] \rightarrow R.$$

Then  $\ker \text{ev}_{(a,b)} = \text{ev}_{(a,b)}^{-1}((0)) = \text{ev}_{y=b}^{-1}((x - a)) = \{f \in R[x][y] : f(x, b) \in (x - a)R[x]\} = (x - a, y - b)$ . By the first isomorphism theorem,  $R[x, y]/(x - a, y - b) \cong R$ . So  $(x - a, y - b)$  is a maximal ideal of  $R[x, y]$  if and only if  $R$  is a field.

For  $(y - x^2) \subseteq R[x, y]$ , we know  $R[x, y]/(y - x^2) \cong R[x]$ .  $R[x]$  is not a field since  $x$  is not a unit. So  $(y - x^2)$  is not maximal. (Indeed,  $(y - x^2) \subsetneq (x, y)$ .)

**Example**

Let  $c \in \mathbb{R}$ . In the homework, you'll show

$$\mathbb{R}[x]/(x^2 - c) \cong \begin{cases} \mathbb{C} & c < 0 \\ \mathbb{R} \times \mathbb{R} & c > 0 \\ \mathbb{R}[x]/(x^2) & c = 0 \end{cases}.$$

Exercise:  $\mathbb{R} \times \mathbb{R}$  and  $\mathbb{R}[x]/(x^2)$  are not fields. Hence  $\mathbb{R}[x]/(x^2 - c)$  is a field if and only if  $c < 0$ . So  $(x^2 - c)$  is maximal if and only if  $c < 0$ .

Exercise: find proper ideals properly containing  $(x^2 - c)$  for  $c \geq 0$ .

## Partially-ordered sets

### Definition — partial order

A **partial order** on a set  $X$  is a relation  $\leq$  on  $X$  such that for all  $x, y, z \in X$ :

1.  $x \leq x$ ;
2. if  $x \leq y$  and  $y \leq x$ , then  $x = y$ ; and
3. if  $x \leq y$  and  $y \leq z$ , then  $x \leq z$ .

We say that  $x < y$  if  $x \leq y$  and  $x \neq y$ .

A **maximal element of a subset**  $S \subseteq X$  is an element  $x \in S$  such that if  $x \leq y$  for  $y \in S$ , then  $x = y$ .

An **upper bound of a subset**  $S \subseteq X$  is an element  $x \in X$  such that  $y \leq x$  for all  $y \in S$ .

A **maximum element of a subset**  $S \subseteq X$  is an element  $x \in S$  which is an upper bound for  $S$  (unique if it exists).

A maximum element (if it exists) of a subset  $X$  is maximal. But a subset  $S$  can have maximal elements without having a maximum element.

### Example

Consider  $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$  ordered by  $\subseteq$ .

Then  $\{1, 2\}$  is a maximum element for  $2^{\{1,2\}}$ , but the subset  $\{\emptyset, \{1\}, \{2\}\}$  has no maximum element. Instead it has two maximal elements:  $\{1\}$  and  $\{2\}$ .

Ideals of a ring  $R$  are ordered under  $\subseteq$ .  $R$  is a maximum element for the whole set. We are more interested in the set of proper ideals ordered under  $\subseteq$ .

## Proper ideals ordered under inclusion

Let  $R$  be a non-zero ring, so the set of proper ideals is non-empty. Does the set of proper ideals of  $R$  have a maximum element? Once a set has more than one maximal element, it can't have a maximum.

### Example

$\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $n$  is prime. So  $(n)$  is maximal if and only if  $n$  is prime. So  $(2)$  and  $(3)$  are both maximal.

Does the set of proper ideals always have a maximal element?

## Maximal elements for the set of proper ideals?

Does the set of proper ideals always have a maximal element? Maybe we can construct one:

- Pick a proper ideal  $\mathcal{I}_0$ .
- If  $\mathcal{I}_0$  is not maximal, find a proper ideal  $\mathcal{I}_1$  with  $\mathcal{I}_0 \subsetneq \mathcal{I}_1$ .
- Continue until we get to a maximal element.

Of course, this might not work. We might be in a poset (partially ordered set) like  $(\mathbb{N}, \leq)$ , where we have infinitely long increasing sequences like  $1 < 2 < 3 < \cdots$ . In that case, we're only guaranteed to get a sequence  $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$  of proper ideals.

## Chains of ideals

If  $x_0 \leq x_1 \leq x_2 \leq \cdots$  in a partially ordered set  $X$ , then the subset  $S = \{x_0, x_1, x_2, \dots\}$  is a chain.

### Definition — chain

If  $(X, \leq)$  is a partially ordered set, we say that a subset  $S \subseteq X$  is a **chain** if for every  $s, t \in S$ , either  $s \leq t$  or  $t \leq s$  (or both).

Is the set of proper ideals like  $\mathbb{N}$ , a chain with no upper bound?

### Lemma

Let  $R$  be a commutative ring, and let  $\mathcal{F}$  be a chain of ideals. Then

$$\bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$$

is an ideal of  $R$ .

*Proof.*

Homework. □

Note that this doesn't work if  $\mathcal{F}$  is not a chain, since the union of ideals is typically not closed under addition.

### Example

$(2) \cup (3) \subseteq \mathbb{Z}$  doesn't contain  $5 = 2 + 3$ .

If  $\mathcal{F}$  is a chain of proper ideals, then  $1 \notin \mathcal{I}$  for all  $\mathcal{I} \in \mathcal{F}$ . So  $1 \notin \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$ .

### Corollary

If  $\mathcal{F}$  is a chain of proper ideals of  $R$ , then there is a proper ideal which is an upper bound for  $\mathcal{F}$ .

Suppose we try to construct a maximal ideal, and end up with a sequence  $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$  of proper ideals.

By the corollary, there is a proper ideal  $\mathcal{J}_0$  which is an upper bound for  $\{\mathcal{I}_0, \mathcal{I}_1, \dots\}$ , that is,  $\mathcal{I}_k \subseteq \mathcal{J}_0$  for all  $k$ .

If  $\mathcal{J}_0$  is maximal, then we are done. If not, we can find a proper ideal  $\mathcal{J}_1$  with  $\mathcal{J}_0 \subsetneq \mathcal{J}_1$ , and our search continues.

Is this going to end? It looks like we face a never-ending (infinite) succession of choices. We need some help.

## Zorn's lemma

### Axiom — Axiom of choice

Let  $X \subseteq 2^Y$  for some  $Y$ , such that if  $A \in X$ , then  $A \neq \emptyset$ . Then there is a function  $f: X \rightarrow Y$  such that  $f(A) \in A$  for all  $A \in X$ .

The function  $f$  is called a **choice function** (it “chooses” an element from each set). We rarely use the axiom of choice in this form. However, it has a number of useful equivalent formulations:

### Axiom — Equivalent form of the axiom of choice #1

A function  $f: X \rightarrow Y$  is surjective if and only if it has a right inverse.

(We called this a theorem earlier in the course because the axiom of choice is one of our standard axioms.)

### Axiom — Equivalent form of the axiom of choice #2: Zorn's lemma

Let  $(X, \leq)$  be a partially ordered set, such that if  $S$  is a chain in  $X$ , then there is an element  $x \in X$  which is an upper bound for  $S$ . Then  $X$  contains a maximal element.



## Maximal elements for the set of proper ideals, continued

### Proposition

Suppose that  $\mathcal{J}$  is a proper ideal in a commutative ring  $R$ . Then there is a maximal ideal  $\mathcal{K}$  of  $R$  containing  $\mathcal{J}$ .

#### Proof.

Let  $\mathcal{P} = \{\mathcal{I} \subsetneq R : \mathcal{I} \text{ is an ideal and } \mathcal{J} \subseteq \mathcal{I}\}$ , ordered under  $\subseteq$ . Let  $\mathcal{F}$  be a chain in  $\mathcal{P}$ .

By the lemma,  $\mathcal{I}' = \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$  is an ideal of  $R$ . Clearly  $\mathcal{J} \subseteq \mathcal{I}'$ , and since  $1 \notin \mathcal{I}'$  we have that  $\mathcal{I}' \in \mathcal{P}$ . So  $\mathcal{I}'$  is an upper bound for  $\mathcal{F}$  in  $\mathcal{P}$ .) By Zorn's lemma,  $\mathcal{P}$  has a maximal element.  $\square$

### Example

Take  $(0)$  in  $\mathbb{Z}$ . Then  $(0)$  is contained in  $(p)$  for any prime  $p$ , all of which are maximal. So the ideal  $\mathcal{K}$  in the proposition isn't necessarily unique.

In particular, every non-zero commutative ring has a maximal ideal. Or equivalently:

### Corollary

For every non-zero commutative ring  $R$ , there is a field  $\mathbb{K}$  such that there is a homomorphism  $\phi: R \rightarrow \mathbb{K}$ .

#### Proof.

Take  $\mathcal{I}$  to be a maximal ideal of  $R$ , and let  $\phi: R \rightarrow R/\mathcal{I}$  be the quotient map.  $\square$

## 23: Prime ideals and integral domains

### Zero divisors

If  $\mathbb{K}$  is a field and  $f, g \in \mathbb{K}[x]$ , then  $\deg(fg) = \deg(f) + \deg(g)$ .

In contrast, in an arbitrary ring like  $R = \mathbb{Z}/6\mathbb{Z}$ , we can have things like  $(1 + 2x)(1 + 3x) = 1 + 5x + 6x^2 = 1 - x$ . This happens when there are elements  $x, y \in R \setminus \{0\}$  with  $xy = 0$ .

#### Definition — zero divisor

Let  $R$  be a ring. A non-zero element  $x \in R$  is a **zero divisor** if there is a non-zero element  $y \in R$  such that  $xy = 0$  or  $yx = 0$ .

That is,  $x$  (and  $y$ ) divide 0.

#### Example

If  $n$  is not prime, then  $n = ab$  for  $2 \leq a, b < n$ . So  $[a], [b] \neq 0$  in  $\mathbb{Z}/n\mathbb{Z}$ , but  $[a] \cdot [b] = [ab] = 0$ , so  $[a], [b]$  are zero divisors.

#### Example

If  $R$  and  $S$  are non-zero rings and  $a \neq 0$  in  $R$  and  $b \neq 0$  in  $S$ , then  $(a, 0)$  and  $(0, b)$  are non-zero in the product ring  $R \times S$ .

But  $(a, 0) \cdot (0, b) = (0, 0) = 0$  in  $R \times S$ , so  $(a, 0)$  and  $(0, b)$  are zero divisors.

#### Example

For any ring  $R$ ,  $\bar{x}$  is a zero divisor in  $R[x]/(x^2)$  since  $\bar{x}^2 = 0$ .

#### Example

For any ring  $R$ ,  $\bar{x}$  and  $\bar{y}$  are zero divisors in  $R[x]/(xy)$ .

For these examples, we still need to show  $\bar{x}$  or  $\bar{y}$  are non-zero; there are techniques for this later and on the homework.

#### Example

Suppose  $\mathbb{K}$  is a field. Let  $E_{ij} \in M_n\mathbb{K}$  be the matrix with a 1 in position  $ij$  and 0's elsewhere.

Then  $E_{ij}E_{kl} = \delta_{jk}E_{il}$ , so  $E_{ij}$  is a zero divisor for all  $i, j$  as long as  $n \geq 2$ .

Exercise: show that  $A \in M_n\mathbb{K}$  is a zero divisor if and only if the rank of  $A$  is less than

$n$  (i.e.,  $A$  is not invertible).

**Example**

Let  $G$  be a group, and let  $g \in G \setminus \{e\}$  with  $|g| = 2$ .

Then  $(e + g)(e - g) = e - g^2 = e - e = 0$  in  $\mathbb{Z}G$ .

**Kaplansky zero divisor conjecture:** if every element of  $G \setminus \{e\}$  has infinite order, and  $\mathbb{K}$  is a field, then  $\mathbb{K}G$  has no zero divisors.

## Units and zero divisors

### Lemma

Let  $u$  be a unit in a ring  $R$ . Then  $u$  is not a zero divisor.

### *Proof.*

$$uv = 0 \implies v = u^{-1}uv = 0 \text{ and } vu = 0 \implies v = vuu^{-1} = 0. \quad \square$$

Every non-zero element of a field is a unit, so fields have no zero divisors.

In general, an element can be not a zero divisor but also not a unit:

- $\mathbb{Z}$  has no zero divisors, but the only units are  $\pm 1$ .
- If  $f \in \mathbb{K}[x]$  with  $f \neq 0$  and  $\mathbb{K}$  a field, then by the degree formula,  $fg = 0$  if and only if  $g = 0$ .

So  $\mathbb{K}[x]$  has no zero divisors, but  $\mathbb{K}[x]^\times = \mathbb{K}^\times$ .

## Cancellation laws

### Proposition

Suppose a non-zero element  $x$  in a ring  $R$  is not a zero divisor. If  $xa = xb$  or  $ax = bx$  for some  $a, b \in R$ , then  $a = b$ .

### Proof.

If  $xa = xb$ , then  $x(a-b) = 0$ . Since  $x \neq 0$  and  $x$  is not a zero divisor,  $a-b = 0 \implies a = b$ . Similar if  $ax = bx$ .  $\square$

### Corollary

Let  $R$  be a finite ring. If a non-zero element  $x$  is not a zero divisor, then  $x$  is a unit.

### Proof.

Consider the function  $\ell_x: R \rightarrow R: y \mapsto xy$ . If  $\ell_x(a) = \ell_x(b)$ , then  $xa = xb$  and so  $a = b$ . So  $\ell_x$  is injective.

Since  $R$  is finite, by the pigeonhole principle  $\ell_x$  is also surjective. Thus there is  $y \in R$  such that  $\ell_x(y) = xy = 1$ , so  $x$  has a right inverse.

A similar argument with  $y \mapsto yx$  shows  $x$  has a left inverse. Hence  $x$  is invertible.  $\square$

## Integral domains

### Definition — integral domain

An **integral domain** (or **domain**) is a commutative ring  $R$  such that  $1 \neq 0$  and  $R$  has no zero divisors.

### Example

- Every field is an integral domain.
- $\mathbb{Z}$  is an integral domain.
- All the examples of rings we've looked at with zero divisors are not domains ( $\mathbb{Z}/n\mathbb{Z}$  for  $n$  not prime,  $\mathbb{R} \times \mathbb{R}$ ,  $\mathbb{R}[x]/(x^2)$ ).
- $\{0\}$  has no zero divisors, but is not a domain.

Since all non-zero divisors in finite rings are units:

### Corollary

All finite integral domains are fields.

### Proposition

If  $R$  is an integral domain, then:

1. If  $f, g \in R[x]$ , then  $\deg(fg) = \deg(f) + \deg(g)$ .
2.  $R[x]$  is an integral domain.

### Proof.

1. True if  $f$  or  $g$  is zero, so suppose  $f, g \neq 0$ . Let  $f = \sum_{i=0}^n a_i x^i$  and  $g = \sum_{i=0}^m b_i x^i$  where  $a_n, b_m \neq 0$ . Then  $fg = a_n b_m x^{n+m} + \text{lower degree terms}$ . Since  $R$  is a domain,  $a_n b_m \neq 0$ , so  $\deg(fg) = n + m = \deg(f) + \deg(g)$ .
2. Suppose  $f, g \neq 0$  and  $fg = 0$ . Then  $\deg(fg) = -\infty$  so by part (a), we must have  $\deg(f) = -\infty$  or  $\deg(g) = -\infty$ . So one of  $f, g$  is zero, so neither  $f$  nor  $g$  can be a zero divisor.

□

## Interesting domains?

### Proposition

If  $R$  is a subring of a field  $\mathbb{K}$ , then  $R$  is a domain.

#### *Proof.*

$\mathbb{K}$  is commutative with  $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ . So  $R$  is commutative and  $1_R \neq 0_R$ .

If  $x$  is a non-zero element of  $R$  and  $xy = 0$  for  $y \in R$ , then  $y = x^{-1}xy = 0$  in  $\mathbb{K}$ , so  $y = 0$  in  $R$ . So  $R$  has no zero divisors.  $\square$

### Example

$\mathbb{Z}$  is a subring of  $\mathbb{Q}$ , and hence a domain.

### Proposition

If  $\alpha \in \mathbb{C}$  satisfies  $\alpha^2 \in \mathbb{Z}$ , then

$$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$$

is a subring of  $\mathbb{C}$ .

#### *Proof.*

Homework.  $\square$

This leads to interesting domains like the Gaussian integers  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ .

## Prime ideals

Can we construct interesting domains of the form  $R[x]/(p)$ ?

First, we need to answer: if  $\mathcal{I}$  is an ideal of a commutative ring  $R$ , when is  $R/\mathcal{I}$  an integral domain?

Suppose  $R/\mathcal{I}$  is an integral domain. If  $\bar{a} \cdot \bar{b} = 0$  in  $R/\mathcal{I}$  for some  $a, b \in R$ , then one of  $\bar{a}, \bar{b}$  is 0 in  $R/\mathcal{I}$ .

Of course,  $\bar{r} = 0$  in  $R/\mathcal{I}$  if and only if  $r \in \mathcal{I}$ . So  $\bar{a} \cdot \bar{b} = 0$  in  $R/\mathcal{I}$  if and only if  $ab \in \mathcal{I}$ , and one of  $\bar{a}, \bar{b}$  is zero in  $R/\mathcal{I}$  if and only if one of  $a, b$  is in  $\mathcal{I}$ .

### Definition — prime ideal

Let  $R$  be a commutative ring. Then an ideal  $\mathcal{I}$  is **prime** if  $\mathcal{I} \subsetneq R$  and whenever  $ab \in \mathcal{I}$  for  $a, b \in R$ , at least one of  $a, b$  is in  $\mathcal{I}$ .

### Theorem

Let  $\mathcal{I}$  be an ideal in a commutative ring  $R$ . Then  $R/\mathcal{I}$  is an integral domain if and only if  $\mathcal{I}$  is a prime ideal.

### Example

- If  $\mathcal{I}$  is a maximal ideal of a commutative ring  $R$ , then  $R/\mathcal{I}$  is a field and hence a domain. So maximal ideals are prime.
- $\mathbb{Z}/n\mathbb{Z}$  is an integral domain if and only if  $n$  is prime. So  $n\mathbb{Z}$  is a prime ideal if and only if  $n$  is prime.
- Previously we saw  $\mathbb{K}[x, y]/(y - x^2) \cong \mathbb{K}[x]$ , which is a domain but not a field. So  $(y - x^2)$  is a prime ideal which is not maximal.

### Proof.

Since  $R$  is commutative and  $R \rightarrow R/\mathcal{I} : r \mapsto \bar{r}$  is surjective,  $R/\mathcal{I}$  is commutative for any ideal  $\mathcal{I}$ , and  $R/\mathcal{I}$  is zero if and only if  $\mathcal{I} = R$ .

Using surjectivity of  $R \rightarrow R/\mathcal{I}$  again,  $R/\mathcal{I}$  has no zero divisors if and only if for all  $a, b \in R$ , if  $\bar{a} \cdot \bar{b} = 0$  in  $R/\mathcal{I}$  then one of  $\bar{a}, \bar{b}$  is 0 in  $R/\mathcal{I}$ .

Since  $\bar{r} = 0$  in  $R/\mathcal{I}$  if and only if  $r \in \mathcal{I}$ , we have that  $R/\mathcal{I}$  has no zero divisors if and only if  $ab \in \mathcal{I}$  means one of  $a, b$  is in  $\mathcal{I}$  for all  $a, b \in R$ .

So  $R/\mathcal{I}$  is an integral domain if and only if  $\mathcal{I}$  is prime. □



## Primality and factoring

We'll have more to say in a week about when an ideal is prime. For now, we consider one reason why an ideal might not be prime.

### Lemma

If  $R$  is an integral domain and  $f, g \in R[x]$  have  $\deg \geq 1$ , then  $fgR[x]$  is not prime (so  $R/fgR[x]$  is not an integral domain).

Intuition: if  $h \in R[x]$  factors into a product of lower degree polynomials, then the principal ideal  $hR[x]$  is not prime.

### Proof.

We know  $\deg(fgh) \geq \deg(fg) = \deg(f) + \deg(g) > \deg(f), \deg(g)$  for all non-zero  $h \in R[x]$ . So  $fg \in fgR[x]$ , but  $f, g \notin fgR[x]$ .  $\square$

### Example

Since  $(x^2 + 1)$  is maximal in  $\mathbb{R}[x]$ , we have  $(x^2 + 1)$  is prime.

However,  $(x^2 + 1)$  is not prime in  $\mathbb{C}[x]$ , since  $x^2 + 1 = (x - i)(x + i)$  in  $\mathbb{C}[x]$ .

As the previous example shows, whether or not a polynomial factors can be subtle, since it depends on the coefficient ring.

### Example

$(x^2 + 1)$  is not prime in  $\mathbb{Z}_2[x]$  as  $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ .

On the other hand, in  $\mathbb{Z}_3[x]$ , we can check that  $(ax + b)(cx + d) \neq x^2 + 1$  for all  $a, b, c, d \in \mathbb{Z}_3$ , so  $x^2 + 1$  does not factor. Later we will see  $(x^2 + 1)$  is actually prime here.

## A related idea

$\mathbb{C}[x]/(x^2 + 1)$  is a ring containing  $\mathbb{C}$  and an additional element  $x \notin \mathbb{C}$  such that  $x^2 = -1$ . However,  $\mathbb{C}[x]/(x^2 + 1)$  is not a domain.

What if we wanted a domain containing  $\mathbb{C}$  and an additional element  $x \notin \mathbb{C}$  such that  $x^2 = -1$ ?

### Proposition

Suppose  $R$  is a subring of a domain  $S$  and  $x$  is an element of  $S$  such that  $x^2 = t^2$  for some  $t \in S$ . Then  $x = t$  or  $x = -t$ .

### *Proof.*

If  $x^2 = t^2$ , then  $x^2 - t^2 = 0$ , so  $(x - t)(x + t) = 0$ . Since  $S$  is a domain, one of  $x - t$  or  $x + t$  must be 0.  $\square$

Since  $i^2 = -1$  in  $\mathbb{C}$ , there is no domain containing  $\mathbb{C}$  and an additional element  $x \notin \mathbb{C}$  such that  $x^2 = -1$ .