Groups and Rings

PMATH 347

William Slofstra

LaTeXed by Sibelius Peng

Preface

Disclaimer Much of the information on this set of notes is transcribed directly/indirectly from the lectures of PMATH 347 during Spring 2020 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

Spring 2020 classes online only. So the grading scheme:

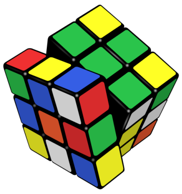
- Participation: 4%
- Quizzes: 32%
- Written homework: 32%
- Final takehome exam: 32%

For any questions, send me an email via `https://notes.sibeliusp.com/contact/`.

You can find my notes for other courses on `https://notes.sibeliusp.com/`.

Sibelius Peng

Contents



Part I:

Group Theory

It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these characteristics.

Abstract Algebra, Third Edition

1

Introduction to Groups

1.1 Binary Operations

week 1

If we randomly ask someone on the street: *What's math about?* The answer we might get is **numbers**. It always comes with **operations**.

Objects	Operations
Natural numbers $\mathbb{N}$	addition $+$ subtraction $-$ multiplication $\cdot$ division with remainders
Integers $\mathbb{Z}$	negation $x \mapsto -x$
Rational number $\mathbb{Q}$	multiplicative inversion $x \mapsto 1/x$
Real numbers $\mathbb{R}$	kth roots, etc
$\mathbb{Z}/n\mathbb{Z}$	modular arithmetic and operations

Then we realizd that math is not just about numbers. We later have **elementary algebra**:

Objects	Operations
Expressions with variables	operations with variables
Functions	Pointwise operations $+, -, \cdot$ and Composition $\circ$

Then ..., and (leaving lots of stuff out), we have **linear algebra**:

Objects	Operations
Vectors	Vector addition $+$, scalar multiplication $\cdot$
Matrices	$+, -$, scalar and matrix multiplication $\cdot$

Then *what's algebra about?*

Pre-university answer:

- manipulating expr involving indeterminates (variables):

If $a, b \in \mathbb{R}$, $ax = b$ and $a \neq 0$, then $x = \frac{b}{a}$.

- solving eqs by applying ops to both sides:
  If A, B are matrices, $AX = B$ and A is invertible, then $X = A^{-1}B$.

Key idea: algebra is about operations

Then *what operations should we study?* Polynomials in several vars; functions, pointwise ops and function composition... *Are there other operations we should study?* Then we introduce **abstract algebra**: try to answer this question by studying operations abstractly, and seeing what the possibilities are.

binary operation

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

Notation:

- Any letter (b, m) or symbol $(+, \cdot)$
- function notation
  $$b : X \times X \to X : (x, y) \mapsto b(x, y)$$
  or inline notation
  $$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto x + y$$
  Typically use inline notation with symbols and function notation with letters.
- There are lots of symbols to choose from: $a + b, a \times b, a \cdot b, a \circ b, a \oplus b, a \otimes b, a \odot b, a \diamond b, a \Diamond b, a \blacklozenge b, a * b, a \bullet b, a \boxplus b, a \boxtimes b, a \uplus b$
- If there's no chance of confusion, can even drop symbol completely:
  $$X \times X \to X : (a, b) \mapsto ab$$

Example:

- Addition $+$ is a binary op on $\mathbb{N}$, but subtraction $-$ is not, since $a - b$ is not necessarily a natural number.
- Subtraction $=$ is a binary op on $\mathbb{Z}$.
- If $(V, +, \cdot)$ is a vector space over a field $\mathbb{K}$, then $+$ is a binary op on V, but $\cdot$ is not, since $\cdot$ is a function $\mathbb{K} \times V \to V$.[a]

[a] We'll define fields later, now think of $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$.

k-ary operation

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

$$\underbrace{X \times X \times \cdots X}_{k \text{ times}} \to X$$

A 1-ary operation is called a unary operation.

Example:
Negation $\mathbb{Z} \to \mathbb{Z} : x \mapsto -x$ 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

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

Now let's discuss some properties that binary ops might satisfy.

1.2 Associativity and commutativity

associative

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

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

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

Many operations we've 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

Note that Subtraction and division are not associative. Subtraction is adding negative numbers, same for division. So we aren't that interested in subtraction and division, and focus on associative operations.

Here we introduce an informal definition: A **bracketing** of a sequence $a_1, \ldots, a_n \in X$ is a way of inserting brackets into $a_1 \boxtimes \ldots \boxtimes a_n$ so that the expression can be evaluated.

Example:
The bracketings of $a_1, \ldots, a_4$ 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 1.1

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

Note

If $\boxtimes$ is associative, can use notation $a_1 \boxtimes a_2 \boxtimes \ldots \boxtimes a_n$ without choosing a bracketing.

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.

$\Rightarrow$ Proof is by induction. Base cases are $n = 1, 2, 3$.

For $n = 1, 2$, there's only one bracketing. For $n = 3$ follows from defn of associativity.

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

Let w be a bracketing of $a_1, \ldots, a_n$.

$w = w_1 \boxtimes w_2$ where w_1 is a bracketing of $a_1, \ldots, a_k$, w_2 is a bracketing of $a_{k+1}, \ldots, a_n$, for some $k < n$.

By induction,

$$w_1 = (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \quad \text{and} \quad w_2 = (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots)$$

Therefore

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

$\square$

commutative

A binary operation $\boxtimes : X \times X \to X$ is commutative (also known as abelian) if $a \boxtimes b = b \boxtimes a$ for all $a, b \in X$.

Fact The word "abelian" comes from the surname of Niels Henrik Abel (1802-1829).

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 operation are **not** commutative: subtraction and division; function composition; matrix multiplication.

Therefore, subtraction and division are not commutative or associative. Function composition and matrix multiplication are not commutative, but are associative. We are not going to worry about the first type of operation, but we are interested in operations of the second type.

First half of the course: group theory – single associative operation, not necessarily commutative.

Second half of the course: ring theory – two associative operations (like addition and multiplication on $\mathbb{Z}$), focus on commutative case.

1.3 Identities and inverses

Let $\boxtimes$ be a binary operation on a set X.

identity

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 $+$. $1 \in \mathbb{Q}$ is identity for $\cdot$. $0 \in \mathbb{Q}$ is not identity for $\cdot$

Lemma 1.2

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

Proof:
$e = e \boxtimes e' = e'$ □

inverse

Let $\boxtimes$ be a binary operation on X with identity element e. An element y is a left inverse for x (w.r.t. $\boxtimes$) 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 $n \in \mathbb{Z}$ w.r.t. $+$.

$n \in \mathbb{Z}$ does not have an inverse w.r.t. $\cdot$ unless $n = \pm 1$.

If $x \in \mathbb{Q}$ is non-zero, then $1/x$ is an inverse of x w.r.t. $\cdot$. The element 0 does not have an inverse.

Lemma 1.3

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

Proof:
$y_L = y_L \boxtimes e = y_L \boxtimes (x \boxtimes y_R) = (y_L \boxtimes x) \boxtimes y_R = e \boxtimes y_R = y_R$ □

Corollary 1.4

- If x has both a left and right inverse, then x has an inverse.
- Inverses are unique.

invertible

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

Exercise
It's possible to have a left (resp. right inverse), but not be invertible. Also, left and right inverses don't have to be unique (unless an element has both).

Lemma 1.5

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

□

Proposition 1.6

Let $\boxtimes$ be an associative binary operation on X with 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

$$a \boxtimes x = b \text{ and } y \boxtimes a = b$$

have unique solutions for all $b \in X$.

Proof:

$\Leftarrow$ A solution to $ax = e$ is a right inverse of a, and a solution to $ya = e$ is a left inverse. If a both have a left and right inverse, then it has an inverse.

$\Rightarrow$ Suppose a is invertible. Then

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

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 $y \boxtimes a = b$. □

Proposition 1.7: Cancellation property

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

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

Proof:

1. $u = a^{-1} \boxtimes a \boxtimes u = a^{-1} \boxtimes a \boxtimes v = v$
2. similar.

□

1 and 2 also hold for $n \in \mathbb{Z}$ w.r.t. $\cdot$ if $n \geq 0$, even though n is not invertible for $n \neq \pm 1$.

1.4 Groups

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 $\boxtimes$.

abelian

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

finite

A group is **finite** if G is a finite set.

order

The **order** of G the number of elements in G if G is finite, and $+\infty$ if G is infinite. The order of G is denoted by $|G|$.

1.4.1 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 $\boxtimes$ all the time, so usually we use one of the following options:

- Use $\cdot$ as the standard symbol, write $g \cdot h$ for the product of $g, h \in G$
- Drop the symbol entirely, write gh for the product of $g, h \in G$.

The identity of G is denoted by e (or e_G when we want to make the group clear). 1 and 1_G are also used.

Since every element of a group G is invertible, g^{-1} is defined for all $g \in G$. The function $G \to G : G \mapsto g^{-1}$ can be regarded as a unary operation on G.

Consider $\iota : G \to G : g \mapsto g^{-1}$. Since $(g^{-1})^{-1} = g$, $\iota \circ \iota = \mathrm{Id}_G$, the identity map $G \to G$. In particular, ι is a bijection, both injective and surjective.

If $g \in G$, then

$$g^n := \underbrace{g \cdot \dots \cdot g}_{n \text{ times}} \text{ and } g^{-n} := (g^{-1})^n = (g^n)^{-1}$$

Exercise

If $m, n \in \mathbb{Z}$, then $(g^n)^m = g^{mn}$.

If $g, h \in G$, then

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

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

Example: Groups

$\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups under operation $+$. The identity is 0 and the inverse of n is $-n$. These groups have infinite order. They are infinite abelian groups.

$\mathbb{Z}/n\mathbb{Z}$ is also a group under $+$. The identity is $0 = [0]$, and the inverse of $[m]$ is $-[m] = [-m]$. This group is finite, with order $|\mathbb{Z}/n\mathbb{Z}| = n$. It is a finite abelian group.

If $(V, +, \cdot)$ is a vector space, then $(V, +)$ is group. The identity element is 0, and the inverse of v is $-v$.

Example: Not a group?! & Trivial group

$\mathbb{Z}$ 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 called the **trivial group**.

A non-abelian example

All the examples previously are abelian.

Let $\mathrm{GL}_n(\mathbb{K})$ denote the invertible $n \times n$ matrices with entries in a field $\mathbb{K}$.

Proposition 1.8

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

Proof:

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

Exercise

Find matrices A, B such that $AB \neq BA$.

$\square$

1.4.2 Additive notation

Standard notation for operation in a group is gh. This is called **multiplicative notation**. For groups like $(\mathbb{Z}, +)$, it is confusion to write mn instead of $m+n$, since mn already has another meaning. For abelian groups G, there is another convention called **additive notation**. In additive notation, we write the group operation as $g+h$. The identity is denoted by 0 or 0_G. Inverse are denoted by $-g$. Writing g^n in additive notation gives

$$\underbrace{g+g+\ldots+g}_{n \text{ times}},$$

so rather than g^n we use ng. Similarly g^{-n} is $-ng$.

For nonabelian groups we always use multiplicative notation. For abelian groups, we can choose either.

Note the potential for conflict between the two conventions. We must be clear about what convention we are using!.

For groups like $(\mathbb{Z}, +)$, we could denote the operation by mn, but it's clearer to write $m+n$. For groups like $(Q^\times, \cdot)$, we could denote the operation by $x+y$, but it is clearer to write $x \cdot y$ or xy.

1.4.3 Multiplicative table

multiplicative table

The multiplicative 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 info of the group G. It is defined for finite and infinite groups, but makes the most sense for finite groups.

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

The multiplication table for $\mathbb{Z}/2\mathbb{Z}$ is

	0	1
0	0	1
1	1	0

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

Table 1.1: Comparison between multiplicative and additive notation

1.4.4 Order of elements

order

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

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

Some 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: $\mathbb{Z}/n\mathbb{Z}$

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

Lemma 1.9

$g^n = e$ 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,

$$g^n = e \text{ if and only if } (g^n)^{-1} = e^{-1} = e.$$

But g^{-n} also equals $(g^{-1})^n$, so

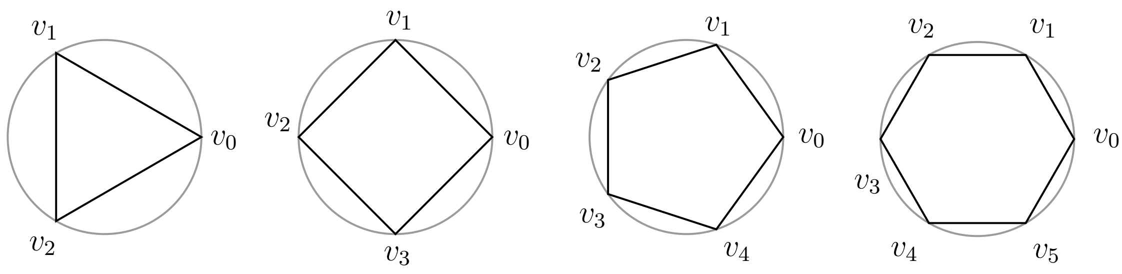
$$\left\{k \geq 1 : g^k = e\right\} = \left\{k \geq 1 : \left(g^{-1}\right)^k = e\right\}$$

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

1.5 Dihedral groups

n-gon

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



To be specific: set $v_k = (\cos 2\pi k/n, \sin 2\pi k/n) = e^{2\pi ik/n}$

Get n-gon by drawing line segment from v_k to v_{k+1} for all $0 \leq k \leq n$ (where $v_n := v_0$)

symmetry

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

dihedral group

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

In this course, we use D_{2n}.

Note
We think of matrices and invertible linear transformations interchangeably.

Matrix multiplication = composition of transformations.

Proposition 1.10

D_{2n} is a group under composition.

Proof:
Later. Key point: $S, T \in D_{2n} \implies ST \in D_{2n}$. $\square$

v_i and v_j are **adjacent** in P_n if connected by line segment.

Lemma 1.11

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

Proof:

1. v_0, v_1 are adjacent, T is linear
2. v_0 and v_1 are linearly independent.

$\square$

Corollary 1.12

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

Proof:
Let A be the set of adjacent pairs (v_i, v_j)[a], so $|A| = 2n$. By Lemma 1.11, $D_{2n} \to A : T \mapsto (T(v_0), T(v_1))$ is well-defined and injective. $\square$

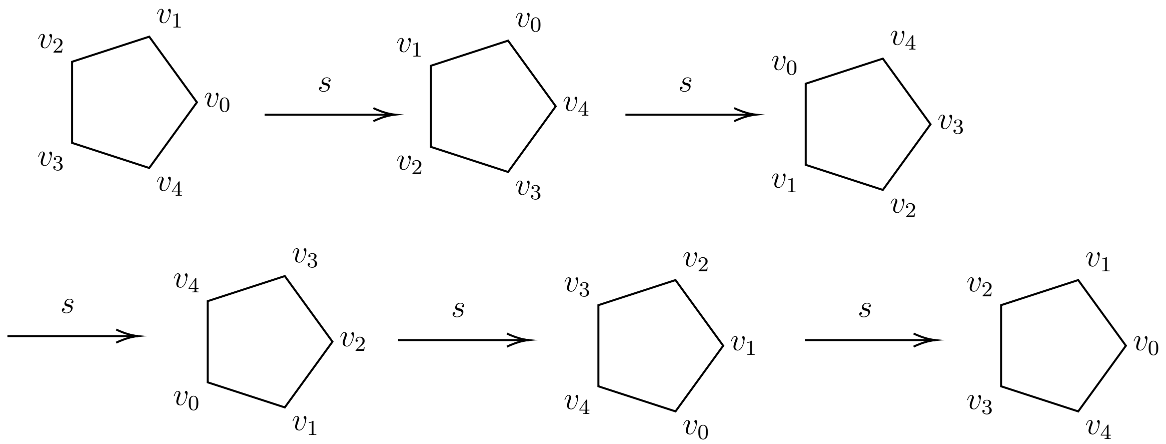
[a]ordered pairs

For every pair of adjacent vertices (v_i, v_j), is there an element $T \in D_{2n}$ with $T(v_0) = v_i, T(v_1) = v_j$?

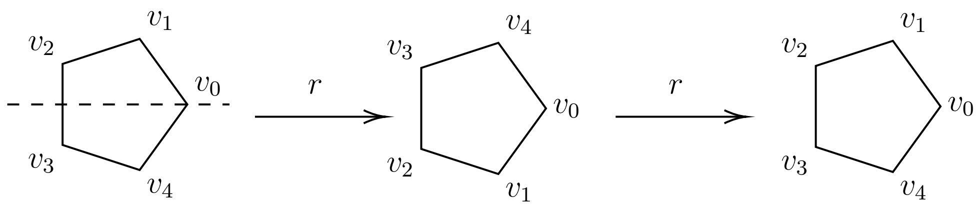
If the answer is yes, then $|D_{2n}| = 2n$.

1.5.1 Special elements of D_{2n}

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



Let r be reflection through the x-axis:

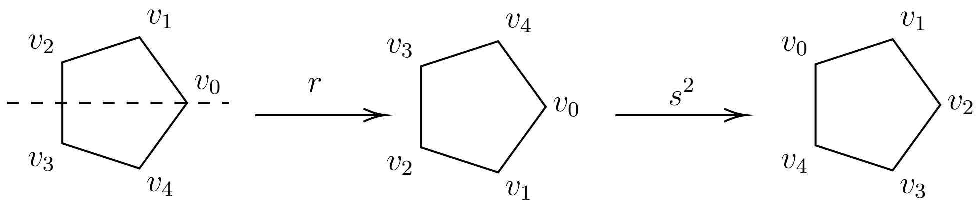


$|r| = 2$, i.e. $r^2 = e, r \neq e$.

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

If we try to put these two elements together:

1. s^i, $0 \leq i < n$: sends $v_0 \mapsto v_i, v_1 \mapsto v_{i+1}$ (notes: $v_n = v_0$, s^0 is the identity)
2. $s^i r, 0 \leq i < n$: sends $v_0 \mapsto v_i$, $v_1 \mapsto v_{i-1}$ (notes: $v_{-1} = v_{n-1}$)



Proposition 1.13

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

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 1.14

D_{2n} is a finite nonabelian group.

Exercise

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

$|D_{2n}| = 2n$

$s^n = e, r^2 = e, rs = s^{-1}r$

These relations are enough to completely determine D_{2n}.

What's group theory about?

Basic answer: study sets with one binary op. A better answer: group theory is study of symmetry. If we resize or rotate P_n, then symmetries are the same.

Kleinian view of geometry:

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

1.6 Permutation groups

If X is a set, let $\mathrm{Fun}(X, X)$ be set of functions $X \to X$. Then

$$\circ : \mathrm{Fun}(X, X) \times \mathrm{Fun}(X, X) \to \mathrm{Fun}(X, X) : (f, g) \mapsto f \circ g$$

is an associative operation with an identity Id_X. Let $S_X = \{f \in \mathrm{Fun}(X, X) : f \text{ is a bijection}\}$

Proposition 1.15

S_X is a group under $\circ$.

Proof:
See homework. $\square$

symmetric/permutation group

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

Elements of S_n are bijections $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$

What makes a function $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ a bijection?

Every element of $\{1, \ldots, n\}$ must appear in the list $\pi(1), \ldots, \pi(n)$, and no element can appear twice ($\Leftarrow$ redundant by pigeon-hole principle.)

How many elements in S_n?

n choices for $\pi(1)$, $n-1$ choices for $\pi(2)$, ..., 1 choice for $\pi(n)$. So $n(n-1)\cdots 1 = n!$ choices $\implies |S_n| = n!$.

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

1.6.1 Representations

Elements of S_n are called **permutations**. There are a number of different ways to represent 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**:

$$\pi = 651423$$

This representation saves space than the previous one, but it is hard to do operations in group theory. The one below seems counter-intuitive, but convenient for doing operations.

3. Note $\pi(1) = 6, \pi(6) = 3, \pi(3) = 1$. Say (163) is a **cycle** of π.

Disjoint cycle representation: write down cycles of π

$$\pi = (163)(25)(4) = (163)(25)$$

We typically drop cycles of length 1.

Identity is empty in disjoint cycle notation, so just use e.

The convention is that we start from the lowest item in the cycle, and sort the cycles by their lowest items.

Multiplication

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

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

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix} = (126)(345)$$

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

Note i comes from the right: $\pi(\sigma(i))$.

(It's a bit of a pain in one-line notation, so we don't use one-line notation often in group theory)

Inversion

We can also take inverse in two-line or disjoint cycle notation

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

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

$*$: swap two rows and sort the columns by the first row. Disjoint cycle notation is even easier.

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

fixed points

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

support set

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

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

disjoint

π and σ are disjoint if $\text{supp}(\pi) \cap \text{supp}(\sigma) = \varnothing$

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

Remark:
In general, $\text{supp}(\pi)$ are numbers that appear in disjoint cycle representation of π (when cycles of length one are dropped).

$\text{supp}(\pi) = \varnothing$ if and only if $\pi = e$

$\text{supp}(\pi^{-1}) = \text{supp}(\pi)$

If $i \in \text{supp}(\pi)$, then $\pi(i) \in \text{supp}(\pi)$

commute

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

Lemma 1.16

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

Proof:
Suppose $1 \leq i \leq n$. If $i \in \text{supp}(i)$, then $\pi(i) \in \text{supp}(\pi)$. Since π, σ disjoint, $i, \pi(i) \notin \text{supp}(\sigma)$. 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 $\pi(\sigma(i)) = i = \sigma(\pi(i))$.

So $\pi(\sigma(i)) = \sigma(\pi(i))$ for all $i \implies \pi\sigma = \sigma\pi$. □

1.6.2 Cycles

k-cycle

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

Suppose cycles of $\pi \in S_n$ are $c_1, \ldots, c_k$. We can regard c_i as an element of S_n, $\pi = c_1 \cdot c_2 \cdot \cdots \cdot c_k$ as product in S_n. c_i and c_j are disjoint, so $c_i c_j = c_j c_i$. Note that order of cycles in disjoint cycle representation doesn't matter.

Example:
$\pi = (163)(25) = (25) \cdot (163)$

We can also get an interesting prospective on this formula for the inverse of π in the disjoint cycle notation. If $c_1, \ldots, c_k$ are cycles of π, then $\pi = c_1 c_2 \cdots c_k$ as product in S_n.

c_i and c_j are disjoint, so $c_i c_j = c_j c_i$.
$\pi^{-1} = c_k^{-1} \cdots c_1^{-1} = c_1^{-1} \cdots c_k^{-1}$

> 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 π is a permutation, then π commutes with π^i for all i since $\pi^{i+1} = \pi\pi^i = \pi^i\pi$, so π and π^i commute. However, note that they don't necessarily have disjoint support sets.

2

Subgroups

2.1 Subgroups

week 2

subgroup

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

(a) for all $g, h \in H$, $g \cdot h \in H$ (H is **closed under products**),

(b) for all $g \in H$, $g^{-1} \in H$ (H is **closed under inverses**), and

(c) $e_G \in H$.

Notation $H \leq G$.

Example:
$\mathbb{Z} \leq \mathbb{Q}^{+} := (\mathbb{Q}, +)$

$\mathbb{Q}_{>0} := \{x \in \mathbb{Q} : x > 0\} \leq \mathbb{Q}^{\times}$.

To check this: if $x, y \in \mathbb{Q}$, $x, y > 0$, 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: More complicated
Let $G = D_{2n}$, s rotation.

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

Proof:

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

Proof Let $i = nk + r, 0 \leq r < n$. Then $s^i = s^{nk+r} = (s^n)^k s^r = s^r$, since $s^n = e$. ■

Now check subgroup: if $s^i, s^j \in H$, then $s^{i+j} \in H$. If $s^i \in H$, then $s^{-i} \in H$. Finally, $e \in H$ by construction. □

H is the smallest subgroup containing s. The notation for H is $\langle s \rangle$.

Example: $\mathbb{Z}$

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

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

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

trivial subgroup

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

proper subgroup

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

H is proper nontrivial subgroup if $\{e\} \neq H < G$.

Example: Not subgroups

$\mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} : x \geq 0\}$ is not a subgroup of $\mathbb{Q}^+$. We can verify as follows: 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 2.1

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

(a) the identity of H is $e_H = e_G$, and

(b) the inverse of $g \in H$ is the same as the inverse of g in G.

Proof:

First, why is $\boxtimes|_{H \times H}$ a binary operation on H?

Recall $\boxtimes$ is a function $G \boxtimes G \to G$ which implies $\boxtimes|_{H \times H}$ is a function $H \times H \to G$ if we restrict its domain. But if $g, h \in H$, then $g \boxtimes h \in H$. So we can think of $\boxtimes|_{H \times H}$ as function $H \times H \to H$. For the rest of this proof, we just denote this function by $\tilde{\boxtimes}$.

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

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

If $g \in H$, then inverse g^{-1} with respect to $\boxtimes$ is in H by the definition of subgroup.

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

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

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

Example:
$\mathbb{Z}$ is subgroup $\mathbb{Q}$ with operation $+$.

If H is group of $(G, \cdot)$, then H is group with operation $\cdot$.

Proposition 2.2

H is subgroup if and only if

(a) H is non-empty, and

(b) $gh^{-1} \in H$ for all $g, h \in H$.

Proof:
$\Rightarrow$ If H is a subgroup of G, then $e_G \in H$, so $H \neq \varnothing$. Also if $g, h \in H$, then $h^{-1} \in H$, so $gh^{-1} \in H$.

$\Leftarrow$ By (a), there is some element $x \in H$. In part (b), let $g = h := x$, then $xx^{-1} = e_G = e_H \in H$.

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

If $x, y \in H$, then $y^{-1} \in H$, so $xy = x(y^{-1})^{-1} \in H$ (closed under inverses). □

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 $v - w \in W$.

Conclusion: W is subgroup.

Proposition 2.3

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

(a) H is non-empty, and

(b) $gh \in H$ for all $g, h \in H$.

Proof:
Since H is nonempty, suppose $g \in H$. By induction, we can show $g^n \in H$ for all $n \in \mathbb{N}$. Since H is finite, sequence $g, g^2, g^3, \ldots \in H$ must eventually repeat. So $g^i = g^j$ for some $1 \leq i < j \implies g^n = e$ for $n = j - i$. Since $i < j$, then $n \geq 1$, therefore $g^n = e \in H$.

Now we need to show it is closed under inverses.

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

2.2 Subgroups generated by a set

Proposition 2.4

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

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

is a subgroup of G.

Proof:
First we check it is non-empty. Since $e_G \in H$ for all $H \in \mathcal{F}$, then $e_G \in K \implies K$ is non-empty.

Suppose $x, y \in K$, then

$$\begin{aligned} &\implies x, y \in H \quad \forall H \in \mathcal{F} \\ &\implies y^{-1} \in H \quad \forall H \in \mathcal{F} \\ &\implies xy^{-1} \in H \quad \forall H \in \mathcal{F} \\ &\implies xy^{-1} \in K \end{aligned}$$

By Proposition 2.3, K is a subgroup of G. □

subgroup generated by S in G

Let S be a subset of group G. The **subgroup generated by S in G** is

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

Note
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 smallest subgroup of G containing S.

To simplify the notation: If $S = \{s_1, s_2, \ldots\}$, often write $\langle S \rangle = \langle s_1, s_2, \ldots \rangle$.

We can write the trivial subgroup as $\langle \varnothing \rangle = \langle e \rangle = \{e\}$.

Example: D_{2n}
Let s be the rotation generator of D_{2n}. Let $K = \{s^0 = e, s^1, s^2, \ldots, s^{n-1}\}$.

As previously checked, K is a subgroup of D_{2n}.

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

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

So $K \subseteq \langle s \rangle \implies \langle s \rangle = K$.

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

Here we introduce a notation: If $S \subset G$, let $S^{-1} = \{s^{-1} : s \in S\}$.

Proposition 2.5

If $S \subset G$, let

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

Then $\langle S \rangle = K$.

Proof:

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

Proof It is easy to show that $S \subseteq K$. We simply let $k = 1$ and s_1 to be any element of S.

To show the second part, we know $e \in \langle S \rangle$. Then we can prove by induction that $s_1 \cdots s_k \in \langle S \rangle$ for all $k \geq 1$, $s_1, \ldots, s_k \in S \cup S^{-1}$. ■

Claim 2 K is a subgroup of G.

Proof $e \in K$ by construction.

Suppose $x, y \in K$,

$$x = s_1 \cdots s_k, k \geq 0, s_1, \ldots, s_k \in S \cup S^{-1}$$
$$y = t_1 \cdots t_\ell, \ell \geq 0, t_1, \ldots, t_\ell \in S \cup S^{-1}$$

Then $xy = s_1 \cdots s_k t_1 \cdots t_\ell \in K$ by construction. Also, $x^{-1} = s_k^{-1} \cdots s_1^{-1} \in K$ since $s_k^{-1}, \cdots, s_1^{-1} \in S \cup S^{-1}$. So K is a subgroup. ■

$S \subseteq K$, and $\langle S \rangle$ is smallest subgroup containing $S \implies \langle S \rangle \subseteq K$. Thus $\langle S \rangle = K$. □

2.2.1 Lattice of subgroups

Before concluding this section, it is interesting to mention one closed related subject which the lattice of subgroups of G.

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 $\leq$. Set of subgroups of G with order $\leq$ is called the **lattice of subgroups of** G. We don't need to deal with formal definitions and properties here.

The picture below shows the subgroups of $\mathbb{Z}$, where $k\mathbb{Z}$ denotes the set containing all integers that are divisible by k.

$$
\begin{tikzcd}
 & \mathbb{Z} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
2\mathbb{Z} \arrow[d, dash] \arrow[dr, dash] & 3\mathbb{Z} \arrow[d, dash] & \cdots \\
4\mathbb{Z} \arrow[dr, dash] & 6\mathbb{Z} \arrow[d, dash] & \\
 & \vdots \arrow[d, dash] & \\
 & 0\mathbb{Z} &
\end{tikzcd}
$$

Subgroup below $H_1, H_2 \leq G$ in the lattice is $H_1 \cap H_2$. In the picture above, it is $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. Intuitively, a number is divisible by 2 and 3, which is the same thing as being divisible by 6.

What about the subgroup above H_1 and H_2? The subgroup above H_1, H_2 is $\langle H_1 \cup H_2 \rangle$.

2.3 Cyclic groups

generate

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

cyclic

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

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 2.6

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 Proposition 2.5 about $\langle S \rangle$.
2. See argument for $\langle s \rangle$ in D_{2n}.

$\square$

Remark:
In the first part of Lemma 2.6, it does not mean each element in the subgroup can be uniquely represented in the form of a^i.

Then we have two questions:

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

Proposition 2.7

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

This proposition also applies to infinite groups.

Proof:
From part 2 of Proposition 2.6, we know that there are at most n elements in $\langle a \rangle$, then $|G| \leq |a|$.

Suppose $|G| = n < +\infty$. Then the sequence $a^0, a^1, \ldots, a^n \in G$ must have repetition. Thus there is $0 \leq i < j \leq n$ with $a^i = a^j$. Then with the similar argument before, $a^{j-i} = e$, which implies that $|a| \leq n$.

Thus $|a| \leq |G| \implies |a| = |G|$. $\square$

Remark:
It is worth thinking that what happens if $|G| = \infty$ and it seems the proof only works with finite order. If $|G| = \infty$, then $|G| \leq |a|$ will force $|a|$ to be infinite.

Example: $\mathbb{Z}$
$G = \mathbb{Z}$:

- Infinite cyclic group
- Generators are $+1$ and -1

- Order of $m \in \mathbb{Z}$ is
$$|m| = \begin{cases} +\infty & m \geq 0 \\ 1 & m = 0 \end{cases}$$

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

  All subgroups of $\mathbb{Z}$ are cyclic

2.3.1 $\mathbb{Z}/n\mathbb{Z}$

Can we analyze $\mathbb{Z}/n\mathbb{Z}$ in the same way? Recall $\mathbb{Z}/n\mathbb{Z}$ is the set of congruence classes mod n. We denote congruence class of $a \in \mathbb{Z}$ by $[a]$, or just a. For example, in $\mathbb{Z}/5\mathbb{Z}$, $3 = 8$.

Then we might wonder:

- What are the generators?
- What are the orders of elements?
- What are the subgroups?

Before we explore these questions, it is nice to have the following lemma which works for arbitrary group G.

Generators

Lemma 2.8

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

Proof:
It's relatively easy to prove.

$\Rightarrow$ If $G = \langle T \rangle$, and we know $S \subseteq G$, then $S \subseteq \langle T \rangle$.

$\Leftarrow$ If $S \subseteq \langle T \rangle$, and we know $\langle S \rangle$ is the smallest subgroup containing S, then $\langle T \rangle$ must contain the subgroup generated by S, which is $\langle S \rangle = G$, thus $G \subseteq \langle T \rangle$. And $\langle T \rangle$ is a subgroup as well, then $G = \langle T \rangle$. $\square$

What does this mean in our example? So $\mathbb{Z}/n = \langle [a] \rangle$ if and only if $[1] \in \langle [a] \rangle$.

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

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

Order of elements

Lemma 2.9

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

Proof:
Exercise. □

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

Lemma 2.10

Suppose $a|n$. 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 2.11

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

Proof:
Since $b|a$, there is k such that $a = kb$, then $[a] \in \langle [b] \rangle \implies \langle [a] \rangle \subseteq \langle [b] \rangle$.

By properties of gcd, there is $x, y \in \mathbb{Z}$ such that $xa + yn = b$. So $[b] = x[a] \implies [b] \in \langle [a] \rangle \implies \langle [b] \rangle \subseteq \langle [a] \rangle$.

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

Using these lemmas, we can find order for a general element in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.12

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

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

Finally

$$|[b]| = \frac{n}{b}$$

□

Subgroups

Corollary 2.13

Let $n \geq 1$.

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

Proof:

If $|\langle [a] \rangle| = d$, then $d = |[a]| \Bigm| n$ by Lemma 2.9. Also, $d = \frac{n}{\gcd(a,n)}$, and by Lemma 2.11, $\langle [a] \rangle = \left\langle \left[\frac{n}{d}\right] \right\rangle$.

Conversely, if $d|n$ and $a = \dfrac{n}{d}$, then $|\langle [a] \rangle| = d$. $\square$

Example:

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

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

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

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

Every subgroup of a cyclic group is cyclic. So Corollary 2.13 is a complete list of subgroups of $\mathbb{Z}/n\mathbb{Z}$. Every cyclic group is isomorphic to one of $\mathbb{Z}/n\mathbb{Z}, n \geq 1$, or $\mathbb{Z}$.

3 Homomorphisms

3.1 Homomorphisms

homomorphism

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

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

for all $g, h \in G$.

Example:

$\mathbb{K}$ field, $\mathbb{K}^\times = \{a \in \mathbb{K}, a \neq 0\}$ with operation $\cdot$.

$\mathrm{GL}_n\, \mathbb{K} \to \mathbb{K}^\times : A \mapsto \det(A)$ is a homomorphism because $\det(AB) = \det(A)\det(B)$ for all invertible matrices A, B.

Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\} \leq \mathbb{R}^\times$. $\mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto \sqrt{x}$ is a homomorphism since $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Additive notation: $\phi : (G, +) \to (H, +)$ is a homomorphism if $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in G$. For example, $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ is a homomorphism for any $m \in \mathbb{Z}$, since

$$\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y) \quad \forall x, y \in \mathbb{Z}$$

If V, W are vector spaces, and $T : V \to W$ 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: $\mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$ is a homomorphism since $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}^+$.

$\mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto e^x$ is not a homomorphism since $e^{x+y} \neq e^x + e^y$ for some $x, y \in \mathbb{R}^+$ (e.g. $x = y = 0$).

Lemma 3.1

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

(a) $\phi(e_G) = e_H$

(b) $\phi(g^{-1}) = \phi(g)^{-1}$

(c) $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$

(d) $|\phi(g)| \,\Big|\, |g|$ for all $g \in G$ ($n|\infty$ for all $n \in \mathbb{N}$)

Proof:

(a) $\phi(e_G) = \phi(e_G^2) = \phi(e_G) \cdot \phi(e_G)$
so $e_H = \phi\left(e_G\right)^{-1} \cdot \phi\left(e_G\right) = \phi\left(e_G\right)^{-1} \cdot \phi\left(e_G\right) \cdot \phi\left(e_G\right) = \phi\left(e_G\right)$.

(b) $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ and similarly $\phi(g^{-1})\phi(g) = e_H$, so $\phi(g^{-1})$ is the unique inverse of $\phi(g)$.

(c) Use induction for $n \geq 0$, use part (b) for $n < 0$.

(d) If $|g| = n < +\infty$, then $g^n = e_G$ so $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. This implies[a] $|\phi(g)| \,\Big|\, n$.

$\square$

[a]See homework

Lemma 3.2

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

Proof:
$i(g \cdot h) = g \cdot h = i(g) \cdot i(h)$ $\square$

Lemma 3.3

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

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

Corollary 3.4

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

Proof:
$\phi_K = \phi \circ i$, where $i : K \to G$ is the inclusion $x \mapsto x$. $\square$

3.2 Homomorphisms and subgroups

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

Proposition 3.5

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

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

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

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

image

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

Example:
Let $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$. $e^x > 0$ for all $x \in \mathbb{R}$, so $\operatorname{Im}\phi \subseteq \mathbb{R}_{>0}$. If $y \in \mathbb{R}_{>0}$, then $y = \phi(\log y)$, so $\operatorname{Im}\phi = \mathbb{R}_{>0}$.

If $K \leq G$ and $i : K \to G$ is inclusion, then $\operatorname{Im} i = K$.

$\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$. $\phi(\mathbb{Z}) = m\mathbb{Z}$.

Lemma 3.6

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

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. □

Usually just refer to $\tilde{\phi}$ as ϕ.

Lemma 3.7

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

Proof:
Obvious from definition. □

Corollary 3.8

ϕ induces a surjective homomorphism $\tilde{\phi} : G \to K$, where $K = \operatorname{Im}\phi$.

Remark:
From Lemma 3.7, if ϕ is not surjective, then $\operatorname{Im}\phi < H$, then we can let $K = \operatorname{Im}\phi$, and then construct a surjective homomorphism by Lemma 3.6.

Because this is a bit abstract, it is helpful to go through some examples.

Recall the previous example: Let $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$. $e^x > 0$ for all $x \in \mathbb{R}$. This is not surjective, because $\operatorname{Im}\phi = \mathbb{R}_{>0}$. If we restrict the codomain to be $\mathbb{R}_{>0}$, then it is surjective.

Similarly for $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$, but it induced surjective homomorphism $\mathbb{Z} \to m\mathbb{Z}$.

Proposition 3.9

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

Proof:
$\phi\left(S^{-1}\right) = \left\{\phi\left(s^{-1}\right) : s \in S\right\} = \left\{\phi(s)^{-1} : s \in S\right\} = \phi(S)^{-1}$. So

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

$\square$

Remark:
We used the fact that $\phi(S \cup S^{-1}) = \phi(S) \cup \phi(S^{-1})$, but it doesn't work for intersection.

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

Proposition 3.10

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

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

If $x, y \in \phi^{-1}(K)$, then $\phi(x), \phi(y) \in K$. Thus $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in K$. Hence $xy^{-1} \in \phi^{-1}(K)$. Thus it is a subgroup of G. $\square$

kernel

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

Example:

For $\det : \mathrm{GL}_n \mathbb{K} \to \mathbb{K}^\times$, $\ker\det = \{A \in \mathrm{GL}_n : \det(A) = 1\}$.
This subgroup of $\mathrm{GL}_n \mathbb{K}$ is called the **special linear group**, and is denoted by $\mathrm{SL}_n \mathbb{K}$.

If $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$, 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 $\phi : \mathbb{R} \to \mathbb{R}^\times : x \mapsto e^x$, then $e^x = 1$ if and only if $x = 0$, so $\ker\phi = \{0\}$.

We can generalize the last example into the following proposition.

Proposition 3.11

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

Proof:

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

$\Leftarrow$ 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 $x = y$ which implies that ϕ is injective. □

3.2.1 Application: subgroups of cyclic groups

Proposition 3.12

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

Proof:

We need following facts:

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

The first two are in the homework. The last one is not hard to see.

Since G is cyclic, there is a surjective homomorphism $\phi : \mathbb{Z} \to G$.

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

Let $\psi : \mathbb{Z} \to \mathbb{Z}$ be homomorphism with $\psi(k) = mk$.

Then $\phi \circ \psi : \mathbb{Z} \to G$ is homomorphism.

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

Then we can restrict codomain of $\phi \circ \psi$ to get surjective homomorphism $\mathbb{Z} \to H$.

Hence H is cyclic. □

3.3 Isomorphisms

in/sur/bi-jective

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

1. **injective** if for all $x, y \in X$, $f(x) = f(y) \implies x = y$,
2. **surjective** if for all $y \in Y$, $\exists x \in X$ with $f(x) = y$, and
3. **bijective** if f is both injective and surjective.

Proposition 3.13

$f : X \to Y$ is a bijection if and only if there is a function $g : Y \to X$ 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}.

isomorphism

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

Lemma 3.14

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

Example:
$\mathbb{R}^+ \to \mathbb{R}_{>0} : x \mapsto e^x$ is an isomorphism.

If $\phi : G \to H$ is injective, then ϕ induces an isomorphism $G \to \operatorname{Im} \phi$.

Proposition 3.15

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

Proof:
ϕ^{-1} is also a bijection, so just need to show that it is a homomorphism.

If $g, h \in H$, then

$$\phi(\phi^{-1}(g) \cdot \phi^{-1}(h)) = \phi(\phi^{-1}(g))\phi(\phi^{-1}(h)) = g \cdot h$$

So ϕ^{-1} is a homomorphism, hence isomorphism. □

Corollary 3.16

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

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

Proof:
$\Rightarrow$ If ϕ is an isomorphism, then can take $\psi = \phi^{-1}$.

$\Leftarrow$ If ψ exists, then ϕ is a bijection.

□

isomorphic

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

Notation: $G \cong H$.

Key facts:

- If $G \cong H$ then $H \cong G$.

  Proof:
  If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism. □
- If $G \cong H$ and $H \cong K$ then $G \cong K$.

  Proof:
  If $\phi : G \to H$ is an isomorphism and $\psi : H \to K$ is an isomorphism, then $\psi \circ \phi$ is an isomorphism. □
- $G \cong G$.

  Proof:
  $1_G : G \to G$ is an isomorphism. □

Idea If $G \cong H$, then G and H are identical as groups.

If $\phi : G \to H$ 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

Proposition 3.17

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

Proof:
Suppose $|G| = \langle a \rangle$, $H = \langle b \rangle$.

$\Leftarrow$ Assume that $|G| = |H|$.

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

Proof

$\Leftarrow$ If $a^i = a^j$ then $a^{j-i} = e$.

$\Rightarrow$ If $|a| \bigm| j - i$, then $j - i = k|a|$. So $a^{j-i} = a^{k|a|} = e \implies a^j = a^i$. ■

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

Then we define a function $\phi : G \to H : a^i \mapsto b^i$.

Well-defined? $|a| = |G| = |H| = |b|$.
$a^i = a^h \implies |a| \bigm| j - i \implies |b| \bigm| j - i \implies b^i = b^j$

Homomorphism? $\phi(a^i \cdot a^j) = \phi(a^{i+j}) = b^{i+j} = b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j)$ for all $a^i, a^j \in G$.

Inverse? $\psi : H \to G : b^i \mapsto a^i$ is well-defined. Clearly ψ is inverse to ϕ.

Thus ϕ is isomorphism $\implies G \cong H$.

$\Rightarrow$ If $G \cong H$, then $|G| = |H|$ which holds for all groups. Same cardinality thus same order.

□

Corollary 3.18

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 3.19

Cyclic groups are abelian.

multiplicative form of cyclic groups

Let a be formal indeterminate (can use any letter). Let

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

Of course we have $C_\infty \cong \mathbb{Z}$ via $a^i \mapsto i$, and $C_n \cong \mathbb{Z}/n\mathbb{Z}$ via $a^i \mapsto i$.

3.4 Cosets

week 3

Recall linear subspaces are motivation for definition of subgroups. Let $T : V \to W$ be a linear transformation. (so T is also a group homomorphism $(V, +) \to (W, +)$). $\ker T = \{x \in V : T(x) = 0\}$ = "solutions to $Tx = 0$".

What are solutions to $Tx = b$?

They can be empty: $Tx = b$ has a solution if and only if $b \in \operatorname{Im} T$. If $b \in \operatorname{Im} T$, and $Tx = b$ has a solution x_0, then all other solutions are of the form $x_0 + x_1$, for $x_1 \in \ker T$.

Conclusion: space of solutions has form $x_i + \ker T$. $x_0 + \ker T$ is called an **affine** subspace. (it's like a linear subspace, but doesn't have to contain 0). We can still talk about the dimension.

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

Remark:
We also refer these sets: left/right translate of S by g.

For abelian groups, $gH = Hg$.

Additive notation: coset of H in $(G, +)$ is $g + H$.

Example:
U 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

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

We can think of the cosets as the sets of solutions to system of equations.

Example: Dihedral group $\langle s \rangle$

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

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

What are the right cosets of H?

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

Conclusion: right cosets are H and Hr.

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

What about the left cosets of $H = \langle s \rangle$?

Exercise

- use $rs = s^{-1}r$ to show $s^i = rs^{-i}$ for all $i \in \mathbb{Z}$.
- if $S \subseteq G$, $g, h \in G$, then $ghS = g(hS)$. This follows from the associativity of the group.

With these facts,

$$\begin{aligned} s^i H &= H \\ s^i r H &= rs^{-i}H = rH \end{aligned}$$

Conclusion: left cosets of H are H, rH

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

Example: Dihedral group $\langle r \rangle$

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

Left cosets: $rH = \{r, e\} = H$ and $s^i H = \{s^i, s^i r\} = s^i rH$.

Conclusion: Left cosets are $s^i H, 0 \leq i < n$, and

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

Right cosets: $Hr = \{r, e\} = H$ and $Hs^i = \{s^i, rs^i\} = \{s^i, s^{-i}r\}$
$Hs^ir = \{s^ir, s^{-i}\} = Hs^{-i}$

Conclusion: Right cosets are $Hs^i, 0 \leq i < n$, and $D_{2n} = \bigsqcup_{i=0}^{n-1} Hs^i$.

In this case, left cosets and right cosets are different.

set of left/right 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

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

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

Remark:
It is read as $G \mod H$. We count each subset once.

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

Example: D_{2n}
$D_{2n}/\langle s \rangle = \{\langle s \rangle, r\langle s \rangle\}$

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

Example: $\mathbb{Z}/n\mathbb{Z}$
Consider $n\mathbb{Z} \leq \mathbb{Z}$.

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

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

Big question for next week: for $H \leq G$, is G/H always a group? spoiler: no...

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

Lemma 3.20

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 $\phi(x_0^{-1}x_1) = \phi(x_0)^{-1}\phi(x_1) = b^{-1}b = e$. Thus $x_0^{-1}x_1 \in H$. Therefore $x_1 = x_0(x_0^{-1}x_1) \in H$.

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

Same argument for right cosets shows set of solutions is Hx_0. □

In this case, left cosets are right cosets.

Lemma 3.21

Suppose $\phi(x_0) = b$. Then set of solutions to $\phi(x) = b$ is $x_0 \cdot \ker \phi$.

Proposition 3.22

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

Proof:
$g \cdot \ker\phi \in G/\ker\phi$ is the set of solutions to $\phi(x) = b$ where $b = \phi(g)$. As a result, $\phi(g \cdot \ker\phi) = \{b\}$, $b \in \operatorname{Im}\phi$.

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

From Lemma 3.21, we see these two mappings are inverses of each other, thus bijection. □

Example:
Suppose $G = \mathbb{Z}$, $K = \mathbb{Z}/n\mathbb{Z}$.

From tutorial: there is a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]$.

$\ker\phi = \mathbb{Z}$, $\operatorname{Im}\phi = \mathbb{Z}/n\mathbb{Z}$.

Elements of $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \le a < n\} = \{a + n\mathbb{Z} : 0 \le a < n\}$

$a + n\mathbb{Z}$ is the set of solutions of $[x] \equiv [a]$ in $\mathbb{Z}/n\mathbb{Z}$.

3.5 The index and Lagrange's theorem

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

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 3.23: Lagrange's theorem

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

Remark:
Why are we use left cosets here for index? Why not right cosets? Anything holds for left cosets should also be expected hold for right cosets with the order of product reversed. Lagrange's theorem didn't mention the order of product. Thus we should expect it holds for right cosets as well. Thus when G is finite, Lagrange's theorem should imply the number of left cosets is equal to the number of right cosets.

Proposition 3.24

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

Proof:
First we check ϕ is will defined: if we are given left coset S, then S^{-1} is a right coset.

Suppose $S \in G/H$, so $S = gH$ for some $g \in G$. Then
$$\begin{aligned} S^{-1} &= \{(gh)^{-1} : h \in H\} \\ &= \{h^{-1}g^{-1} : h \in H\} \\ &\stackrel{*}{=} \{hg^{-1} : h \in H\} \\ &= Hg^{-1} \end{aligned}$$

$*$: because $H \to H : h \mapsto h^{-1}$ is a bijection.

So ϕ is well-defined, and same argument shows $\psi : H \setminus G \to G/H : S \mapsto S^{-1}$ is well-defined.

Finally, ψ is an inverse to ϕ. $\square$

Thus can use either left or right cosets to define index:

Corollary 3.25

If $H \leq G$ then
$$[G : H] = \begin{cases} |H \setminus G| & H \setminus G \text{ is finite} \\ +\infty & H \setminus G \text{ is infinite} \end{cases}$$

Theorem 3.26: Lagrange's theorem (detailed)

If $H \leq G$, then $|G| = [G : H] \cdot |H|$. (In particular, $|H|$ divides $|G|$.) Furthermore, if G is finite, then $[G : H] = \dfrac{|G|}{|H|}$.

Remark:
We don't want to use the second formula if $|G|$ and $|H|$ both are infinite. See proof in the next section.

Example:
$G = D_{2n}$, $H = \langle s \rangle$, $|D_{2n}| = 2n$, $|H| = n$, so $[G : H] = 2$.

$G = D_{2n}$, $H = \langle r \rangle$, $|D_{2n}| = 2n$, $|H| = 2$, so $[G : H] = n$.

$G = \mathbb{Z}$, $H = m\mathbb{Z}$. $|G| = |H| = +\infty$, $[G : H] = |\mathbb{Z}/m\mathbb{Z}| = m$. So $|G| = [G : H] \cdot |H|$, but we don't get any info about $[G : H]$ from Lagrange's theorem. However, it still gives us some info in many cases.

Corollary 3.27

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

Proof:
$|x| = |\langle x \rangle|$ and $|\langle x \rangle|$ divides $|G|$. $\square$

Proposition 3.28

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

Proof:
Here we don't treat $+\infty$ as a prime number, and 1 is not a prime number.

Let $x \in G$, $x \neq e$. Then $|x| \neq 1$, and $|x| \,\Big|\, |G|$, so $|x| = |G|$. Since $|\langle x \rangle| = |x| = |G|$, $G = \langle x \rangle$. $\square$

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	$\mathbb{Z}/9\mathbb{Z}$, ??

Table 3.1: Groups of small order

?? = could be more groups.

Corollary 3.29

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

Proof:
There is a bijection $G/\ker\phi \to \operatorname{Im}\phi$, so $|\operatorname{Im}\phi| = [G : \ker\phi]$. Then Lagrange's theorem implies $[G : H]$ divides $|G|$ for any $H \leq G$. $\square$

Note
Lagrange's theorem also implies that $|\operatorname{Im}\phi|$ divides $|K|$.

Exercise
If G, K are groups, then $\phi : G \to K : g \mapsto e_K$ is a homomorphism (called the **trivial homomorphism**).

$\phi : G \to K$ is the trivial homomorphism if and only if $\operatorname{Im}\phi = \{e\}$, the trivial subgroup.

Corollary 3.30

If G and K have coprime order, then the only homomorphism $\phi : G \to K$ is the trivial homomorphism.

3.6 Proof of Lagrange's theorem

How to prove this theorem?

Recall

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

In example, cosets of H are disjoint, we can divide G into $[G : H]$ sets of size $|H|$. Does this work in general? Need to better understand cosets.

Proposition 3.31

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

(a) $g^{-1}k \in H$

(b) $k \in gH$

(c) $gH = kH$

(d) $gH \cap kH \neq \varnothing$

Example:
$hH = H$ if and only if $h \in H$. (This is from (c) and (a))

Proof:
(a) $\Rightarrow$ (b) If $g^{-1}k = h \in H$, then $k = gh \in gH$.

(b) $\Rightarrow$ (c) Suppose $k = gh$ for $h \in H$. If $h' \in H$, then $kh' = g(hh') \in gH$, since

$hh' \in H$. So $kU \subseteq gH$.

For the reverse inclusion, notice that $g = kh^{-1} \in kH$. If $h' \in H$, then $gh' = k(h^{-1}h') \in kH$, so $gH \subseteq kH$.

(c) $\Rightarrow$ (d) Since $e \in H$, then $g \in gH$, so $gH \neq \varnothing$. If $gH = kH$, then $gH \cap kH = gH \neq \varnothing$.

(d) $\Rightarrow$ (a) Suppose $x \in gH \cap kH$. Then $x = gh_1 = kh_2$ for $h_1, h_2 \in H$. Multiply on the left by g^{-1}, right by h_2^{-1}. So $g^{-1}k = h_1 h_2^{-1} \in H$.

□

partition

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

(a) $\bigcup_{S \in \mathcal{Q}} S = X$, and

(b) $S \cap T = \varnothing$ for all $S \neq T \in \mathcal{Q}$.

Here 2^X denotes set of subsets of X.

Exercise

If $\mathcal{Q} \subseteq 2^X$, then the following are equivalent:

- $\mathcal{Q}$ is a partition
- $X = \bigsqcup_{S \in \mathcal{Q}} S$
- Every element of X is contained in exactly one element of $\mathcal{Q}$.

Corollary 3.32

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

Proof:

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

Suppose $S \neq T \in G/H$ (so $S = gH$, $T = kH$ for some $g, k \in G$). If $S \cap T \neq \varnothing$, then $S = T$ by parts (c) and (d) of Proposition 3.31. So $S \cap T = \varnothing$. □

Lemma 3.33

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

Proof:

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

Consequence: If H is finite, and $g \in G$, then $|gH| = |H|$.

Now we can prove the Lagrange's theorem.

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

Suppose $|H|, [G : H]$ are finite.

By Lemma 3.33, $|gH| = |H|$ 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 $|H|$.

Conclude that $|G| = [G : H] \cdot |H|$. $\square$

3.6.1 Equivalence relations

relation $\sim$

Let X be a set. A **relation** $\sim$ on 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.

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

Example:
$=$ on X. $\equiv_m$, congruence mod m, is an equivalence relation on $\mathbb{Z}$.

$\leq, <$ on $\mathbb{N}, \mathbb{R}$, etc. are not equivalence relations.

Isomorphism $\cong$ is an equivalence relation on the *proper class* of groups. Note that there is no set of all sets, or set of all groups.

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 3.34

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

(a) $x \sim y$

(b) $y \in [x]$

(c) $[x] = [y]$

(d) $[x] \cap [y] \neq \varnothing$

Proof:

(a) $\Rightarrow$ (b) Follows immediately from definition of equivalent classes.

(b) $\Rightarrow$ (c) Assume $y \in [x]$. If $z \in [y]$, then $x \sim y \sim z$, and by transitivity, $z \in [x]$. Thus $[y] \subseteq [x]$. Also $x \sim y \implies y \sim x$, which implies $[x] \subseteq [y]$.

(c) $\Rightarrow$ (d) Assume $[x] = [y]$, $[x] \cap [y] = [x] \supset \{x\} \neq \varnothing$.

(d) $\Rightarrow$ (a) If $x \in [x] \cap [y]$, then $x \sim z \sim y \implies x \sim y$. $\square$

Corollary 3.35

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

Proof:

Since $x \sim x$, $x \in [x]$. Therefore, every element x belongs to some equivalent class. If two equivalent class intersect, they must be equal. Thus X is a disjoint union of its equivalent classes. $\square$

Thus equivalence relation $\implies$ partition. It turns out we can go the opposite direction:

Lemma 3.36

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 $x \sim y$ if and only if $S_x = S_y$. This defines an equivalence relation. $\square$

Proposition 3.37

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 $[g] = gH$.

Remark:

From the proposition, we would say $h \sim e$ if and only if $h \in H$.

Proposition 3.37 follows from that cosets partition G. Proposition 3.31 is a special case of Proposition 3.34. Thus we can prove that $\sim_H$ is equivalence class directly, and use Proposition 3.37 to prove Proposition 3.31.

3.7 Normal subgroups

Recall Proposition 3.31, by symmetry:

Proposition 3.38

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

(a) $kg^{-1} \in H$

(b) $k \in Hg$

(c) $Hg = Hk$

(d) $Hg \cap Hk \neq \varnothing$

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

Lemma 3.39

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

Proof:
$g \in Hg = hH$, so $gH = hH$. □

normal subgroup

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

Notation: $N \trianglelefteq G$.

conjugate of h by g

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

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

Recall: $gS = \{gh : h \in S\}$, $Sg = \{hg : h \in S\}$. So $gSg^{-1} = \{ghg^{-1} : h \in S\}$.

As previously mentioned, $g(hS) = (gh)S$, $(Sg)h = S(gh)$, $g(Sh) = (gS)h$, $eS = S = Se$.

So $gN = Ng$ if and only if $gNg^{-1} = N$. Here we

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

Proposition 3.40

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

(1) $N \trianglelefteq G$ ($gN = Ng\ \forall g \in G$)

(2) $gNg^{-1} = N$ for all $g \in G$

(3) $gNg^{-1} \subseteq N$ for all $g \in G$

(4) $G/N = N \setminus G$

(5) $G/N \subseteq N \setminus G$

(6) $N \setminus G \subseteq G/N$

Proof:

We've already done (1) $\iff$ (2). Clearly (2) $\implies$ (3).

To see (3) $\implies$ (2), suppose $gNg^{-1} \subseteq N$ for all $g \in G$. Given $g \in G$, we know $g^{-1}Ng \subseteq N$ by apply assumption to g^{-1}. Thus $N \subseteq gNg^{-1}$. Hence $N = gNg^{-1}$, so (2) holds.

By definition, (1) $\implies$ (4) $\implies$ (5), (6).

(5) $\implies$ (1): Suppose $G/N \subseteq N \setminus G$. If $g \in G$, then $gN = Nh$ for some $h \in G$. By Lemma 3.39, $gN = Ng$.

(6) $\implies$ (1): Similar. $\square$

Example:

$\langle s \rangle \leq D_{2n}$: Already seen $G/\langle s \rangle = \langle s \rangle \backslash G$. So $\langle s \rangle \trianglelefteq D_{2n}$. Can also check $s^i \langle s \rangle s^{-i} = \langle s \rangle$, $r \langle s \rangle r^{-1} = \langle s \rangle$ (since $rs^ir^{-1} = s^{-i}$).

$\langle r \rangle \leq D_{2n}$: $G/\langle r \rangle \neq \langle r \rangle \setminus G$, 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 $\phi : G \to K$ is a homomorphism, then $\ker\phi$ is normal. Previously, we have proved $G/\ker\phi \equiv$ solution sets to equations $\phi(x) = b, b \in \operatorname{Im}\phi = \ker\phi \setminus G$. Alternatively, we can use statement (2): if $x \in \ker\phi, g \in G$, then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$, so $gxg^{-1} \in \ker\phi \implies g(\ker\phi)g^{-1} \subseteq \ker\phi$.

The subgroup relation $\leq$ is transitive: If $H \leq G$ (G considered as group) and $K \leq H$ (H considered as group) then $K \leq G$. Normally we just say $K \leq H \leq G \implies K \leq G$.

The normal subgroup relation $\trianglelefteq$ is **not** transitive: Consider $H = \langle r, s^2 \rangle \leq D_8$. $rs^2 = s^{4-2}r = s^2r \implies rs^2r^{-1} = s^2$. We know $H \trianglelefteq D_8$, and H is abelian. Since H is abelian, then $\langle r \rangle \trianglelefteq H$. However, $\langle r \rangle \ntrianglelefteq D_8$.

3.8 Normalizers and the center

normalizer of S in G

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

Lemma 3.41

$N_G(S) \leq G$.

Proof:
$eSe = S$, so $e \in N_G(S)$.

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

If $g \in N_G(S)$, then $g^{-1}Sg = g^{-1}(gSg^{-1})g = eSe = S$. So $g^{-1} \in N_G(S)$. □

Lemma 3.42

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

Corollary 3.43

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 $S \subseteq N_G(H)$. □

Remark:
It will be helpful to check a subgroup is normal. Warning: it is possible to have $gHg^{-1} \subseteq H$ and $g \notin N_G(H)$.

Lemma 3.44

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

Proof:
Prove by induction. If $gHg^{-1} \subseteq H$, then $g^iHg^{-i} \subseteq H$ for all $i \geq 0$. (Use $g(g^{i-1}Hg^{-(i-1)})g^{-1} \subseteq gHg^{-1}$).

If $|g| = n < +\infty$, then $g^{-1}Hg = g^{n-1}Hg^{-(n-1)} \subseteq H$. We multiply g on the left and g^{-1} on the right, then $H \subseteq gHg^{-1}$, conclude $gHg^{-1} = H$. □

Corollary 3.45

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

Remark:
If G is a finite group, this process makes checking whether the group is normal even faster.

center of G

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

Example:
$Z(\mathrm{GL}_n\,\mathbb{C}) = \{\lambda 1 : \lambda \neq 0\}$

Proposition 3.46

$Z(G) \trianglelefteq G$.

Proof:
Exercise. $\square$

4 Products

4.1 Product groups

Proposition 4.1

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

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

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

Proof:
Exercise. $\square$

product of G_1 and G_2

If G_1, G_2 are groups, the group $G_1 \times G_2$ with operation from Proposition 4.1 is called the **product of G_1 and G_2**.

Example: the 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. Called the **Klein 4-group**.

Multiplication table:

	(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)

All elements have order 2, so it's not cyclic. Identity is $(0, 0)$. In general, identity of $G_1 \times G_2$ is (e_{G_1}, e_{G_2}).

Proposition 4.2

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

(a) $\tilde{H}, \tilde{K} \leq G$.

(b) $H \to \tilde{H} : h \mapsto (h, e)$ and $K \to \tilde{K} : k \mapsto (e, k)$ are isomorphisms.

Proof:
Exercise. □

Remark:
So we can think of H and K as subgroups of $H \times K$. $H \times K$ can have lots of other subgroups as well. Here we listed the two particularly important ones.

Let $G = H \times K$, $\tilde{H} = H \times \{e\}$, $\tilde{K} = \{e\} \times K \leq H \times K$.

Lemma 4.3

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

Proof:
Exercise. □

4.2 Homomorphisms between products

Corollary 4.4

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

Proof:
Immediate. □

Now consider the converse of this corollary.

Lemma 4.5

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

Proof:

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

for all $x, z \in H$, $y, w \in K$. □

Notation: the homomorphism γ is called $\alpha \cdot \beta$. This is not entirely standard. You should mention this homomorphism if you use this notation.

Remark:
You might wonder why Lemma 4.5 is called the converse of corollary. In Corollary 4.4, given ϕ, we can get homomorphisms: $H \to G : h \mapsto (h, e)$ and apply ϕ to it, similar for K.

Corollary 4.6

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

Proof:
Define $\tilde{\alpha} : H \to H' \times K' : h \mapsto (\alpha(h), e)$ and $\tilde{\beta} : K \to H' \times K' : K \mapsto (e, \beta(k))$. $\tilde{\alpha}, \tilde{\beta}$ are homomorphisms (exercise), and that $\tilde{\alpha}(x)\tilde{\beta}(y) = \tilde{\beta}(y)\tilde{\alpha}(x)$ for all $x \in H, y \in K$.

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 γ is called $\alpha \times \beta$. This notation is quite standard, which is safer to use.

Corollary 4.7

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

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

Proposition 4.8

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

Proof:
Exercise. □

Using products, can complete list of groups of order p^2:

Proposition 4.9

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

Proof:
Exercise. □

Recall our table of small order:

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 4.2. Corollary: $H \times K \to \tilde{H} \times \tilde{K} : (h,k) \to ((h,e),(e,k))$ is an isomorphism. So we are looking for two subgroups $\tilde{H}, \tilde{K}$ which satisfy these properties:

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

4.3 Unique factorizations & internal direct products

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

Lemma 4.10

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

Example:

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

Suppose $G = HK$ for $H, K \leq G$. *When does $g = hk$ for unique $h \in H, k \in K$?* Uniqueness means that if $g = hk = h'k'$ for $h, h' \in H, k, k' \in K$, then $h = h'$ and $k = k'$.

It is easy to find necessary condition: If $e \neq g \in H \cap K$, then $g = g \cdot e = e \cdot g$, then factorization is not unique. So if factorization is unique, $H \cap K = \{e\}$. It turns out this is also a sufficient condition.

Lemma 4.11

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

Proof:

We've proved it is necessary. Suppose $H \cap K = \{e\}$. If $g = hk = h'k'$, then $(h')^{-1}h = k'k^{-1} \in H \cap K$. Thus $(h')^{-1}h = k'k^{-1} = e$. This implies $h = h', k = k'$. $\square$

internal direct product

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

(a) $HK = G$,

(b) $H \cap K = \{e\}$, and

(c) $hk = kh$ for all $h \in H, k \in K$.

Remark:
To make the condition (b) and (c) hold, we put the word "direct" here.

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 4.12

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

Proof:
Let $i_H : H \to G : h \mapsto h$ and $i_K : K \to G : k \mapsto k$. By part (c) of definition, $i_H(h)i_K(k) = i_K(k)i_H(h)$ for all $h \in H, k \in K$. So $\phi = i_H \cdot i_K$ is a homomorphism.

By Lemma 4.11, every element $g \in G$ can be written as $g = hk$ for unique $h \in H, k \in K$. Thus ϕ is a bijection, then ϕ is an isomorphism. $\square$

Lemma 4.13

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

Proof:
Suppose $g \in G$, so $g = hk$, $h \in H, k \in K$. Then

$$kHk^{-1} = \{khk^{-1} : h \in H\} = \{kk^{-1}h : h \in H\} = H,$$

so $gHg^{-1} = hkHk^{-1}h^{-1} = hHh^{-1} \subseteq H$. So $H \trianglelefteq G$. Proof for K is similar. $\square$

Proposition 4.14

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

(a) $G = HK$, and

(b) $H \cap K = \{e\}$.

(c) $H, K \trianglelefteq G$.

Before proving the proposition, we introduce a definition:

commutator

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

Lemma 4.15

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

Proof:
This is the proof of Proposition 4.14.

We have proved $\Rightarrow$.

If $h \in H, k \in K$, 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 $[h, k] \in H \cap K = \{e\} \implies [h, k] = e$. Therefore, $hk = kh$ for all $h \in H, k \in K$, thus G is indeed an internal direct product. $\square$

5 Quotient groups and the isomorphism theorems

week 4

5.1 Quotient groups

Recall an example: $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \leq a < n\}$. In this example, $\mathbb{Z}/n\mathbb{Z}$ is a group, with operation $[a] + [b] = [a + b]$. *Can we generalize this example? Can we define a group structure on G/H by $[g] \cdot [h] = [gh]$?* or $gH \cdot hH = ghH$? (Here we regard gH and hH as elements in G/H instead of sets.) Big problem: this might not be **well-defined**.

relation

A **relation** R between two 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 $X \to Y$ if

(a) for all $x \in X$, there is $y \in Y$ such that $x\ R\ y$, and

(b) for all $x \in X$, $y, z \in Y$, if $x\ R\ y$ and $x\ R\ z$ then $y = z$.

Can define relation $\to$ between $G/H \times G/H$ and G/H by $([g], [h]) \to [gh]$ for all $g, h \in G$? Yes. It is properly defined, we just need to find a subset of $X \times Y$ (in this case $(G/H \times G/H) \times G/H$).

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

Lemma 5.1

The relation $\to$ between $G/H \times G/H$ and G/H defined by $([g], [h]) \to [gh]$ is a function if and only if H is normal. Furthermore, if H is normal, then $ghH = gH \cdot hH$, the setwise product. (Recall $S \cdot T = \{xy : x \in S, y \in T\}$)

Proof:

$\Rightarrow$ Suppose $\to$ is a function. Suppose $g \in G, h \in H$. Then $([g],[g^{-1}]) \to [e]$. Since $g^{-1} \cdot gh = h \in H$ from Proposition 3.37, then $g \sim_H gh$, then $[g] = [gh]$, and $([gh],[g^{-1}]) \to [ghg^{-1}]$. Since $\to$ is a function, $[ghg^{-1}] = [e]$. But this means $ghg^{-1} \sim_H e$, i.e., $ghg^{-1} \in H$. Since this holds for all $g \in G, h \in H$. Hence $H \trianglelefteq G$.

$\Leftarrow$ First let's prove H normal $\implies ghH = gH \cdot hH$.

Note that $gH \cdot hH = gh(h^{-1}Hh) \cdot H$. If H is normal, then $h^{-1}Hh \subseteq H$, then $(h^{-1}Hh) \cdot H \subseteq H$. Since $e \in H^{-1}Hh$, $(h^{-1}Hh) \cdot H = H$ if we take e on the left and every element of H on the right. Thus if H is normal, then $gH \cdot hH = ghH$.

Suppose that $(S,T) \to R$ and $(S,T) \to R'$ for $S,T,R,R' \in G/H$. Then $R = S \cdot T = R'$ by the definition of equivalent class. So $\to$ is a function. $\square$

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 $\overline{g}$.

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

q (defined in the following theorem) is called the **quotient map** or **quotient homomorphism**.

Theorem 5.2

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

Proof:

$([g] \cdot [h]) \cdot [k] = [gh] \cdot [k] = [ghk] = [g] \cdot ([h] \cdot [k])$ for all $[g],[h],[k] \in G/N$, so $\cdot$ is associative.

$[e] \cdot [g] = [e \cdot g] = [g] = [g \cdot e] = [g] \cdot [e]$ for all $[g] \in G/N$, so $[e] = N$ is an identity.

$[g] \cdot [g^{-1}] = [gg^{-1}] = [e] = [g^{-1}g] = [g^{-1}] \cdot [g]$ for all $[g] \in G/N$, so every element of G/N has an inverse.

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

We previously proved that if $\phi : G \to K$ is a homomorphism then $\ker \phi \trianglelefteq G$.

Corollary 5.3

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

Proof:

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

Example:

$\mathbb{Z}/n\mathbb{Z}$: can now define this using theorem, no need to rely on pre-existing definition.

$D_{2n}/\langle s\rangle$: Cosets are $\langle s\rangle = \{s^i : 0 \le i < n\}$ and $\langle s\rangle r = \{s^i r : 0 \le i < n\}$

Multiplication table: $\begin{array}{c|cc} & \langle s\rangle & \langle s\rangle r \\ \hline \langle s\rangle & \langle s\rangle & \langle s\rangle r \\ \langle s\rangle r & \langle s\rangle r & \langle s\rangle \end{array}$

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

If N *not normal*: $\langle r\rangle$ has left cosets $s^i\langle r\rangle = \{s^i, s^i r\}, 0 \le i < n$. If we take two left cosets and do setwise product:

$$\langle r\rangle \cdot s\langle r\rangle = \{s, sr, s^{-1}r, s^{-1}\}$$

is not a left coset of $\langle r\rangle$. Also $e \sim_{\langle r\rangle} r$, $e \cdot s = s$ is in a different coset from $r \cdot s = s^{-1}r$ so $[g]\cdot[h] = [gh]$ is not a well-defined operation.

See $D_{2n}/Z(D_{2n})$ on homework.

Example: projective general linear group

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

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

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

We can view $\mathrm{GL}_n(\mathbb{K})$ as group of invertible linear transformations of $\mathbb{K}$ (acts on vectors).

$\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n\,\mathbb{K})$ is invertible transformations of lines through 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 $\mathrm{PGL}_n(\mathbb{K})$. It is a very important group in some areas of geometry.

In general, can look at:

- $G/Z(G)$, any group G
- $G/\ker\phi$, any homomorphism $\phi : G \to K$
- G/N, any group G and normal subgroup $N \trianglelefteq G$

How do we find the group structure on G/N? It might be hard.

5.2 The universal property of quotients

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

$$\begin{tikzcd}
G \arrow[rr, "\psi \circ q"] \arrow[dr, "q"'] & & K \\
& G/N \arrow[ur, "\psi"'] &
\end{tikzcd}$$

Every such ψ gives a homomorphism $\psi \circ q : G \to K$ (this homomorphism is sometimes also called lift, pullback of ψ to G). Not every homomorphism from $G \to K$ is a lift of ψ. What homomorphisms $G \to K$ are lift of some homomorphism ψ?

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "q"'] & & K \\
& G/N \arrow[ur, dashed, "\psi?"'] &
\end{tikzcd}$$

If we start with $\phi : G \to K$, when does there exist ψ such that $\phi = \psi \circ q$? Given ϕ, when can fill in ψ so that diagram **commutes**? Here "commute" means if we start at any point in the diagram and go to any other point, it doesn't matter what path we take to get there, we get the same function.

Theorem 5.4: Universal property of quotients

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

In other words, can fill in dashed line so that diagram "commutes" if and only if $N \subseteq \ker \phi$.

Hom(G, K)

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

Corollary 5.5

For any groups G, K, and $N \trianglelefteq G$, the function $q^* : \mathrm{Hom}(G/N, K) \to \{\phi \in \mathrm{Hom}(G, K) : N \subseteq \ker \phi\} : \psi \mapsto \psi \circ q$ is a bijection.

Recall we previously proved:

Theorem 5.6: Universal property of products

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

$$\begin{tikzcd}
H \arrow[dr, "i_H"'] \arrow[drr, "\alpha"] & & \\
& H \times K \arrow[r, dashed] & G \\
K \arrow[ur, "i_K"] \arrow[urr, "\beta"'] & &
\end{tikzcd}$$

Corollary 5.7

There is a bijection between $\mathrm{Hom}(H \times K, G)$ and

$$\{(\alpha, \beta) \in \mathrm{Hom}(H, G) \times \mathrm{Hom}(K, G) : \alpha(h)\beta(k) = \beta(k)\alpha(h) \text{ for all } h \in H, k \in K\}$$

Remark:
We won't formally define the term *universal property*. Often that's held off until grad level. But even if we want to define it now, we would need some category theory. Intuitively, we can think about it as a type of theorem setting up a bijection between some sets and set of homomorphisms.

We still need to prove Theorem 5.4. Before we get into the proof, let's prove the following lemma:

Lemma 5.8

If $\alpha : G \to H$ is surjective, $\psi_i : H \to K, i = 1, 2$ 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 $\psi_1(h) = \psi_2(\alpha(g)) = \psi_2(h)$. We conclude that $\psi_1 = \psi_2$. □

With this lemma, we can dive into the proof of Theorem 5.4:

Proof:

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

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

If $\psi' : G/N \to K$ is another homomorphism with $\psi' \circ q = \phi$ then $\psi' \circ q = \psi \circ q$. Since q is surjective, by Lemma 5.8, $\psi' = \psi$. So uniqueness holds. □

Remark:

Equivalent way to define ψ: $\phi(gN) = \phi(g)\phi(N) = \phi(g)\{e\} = \{\phi(g)\}$. So if $S \in G/N$, then $\phi(S) = \{b\}$, a singleton set. Can define $\psi(S) = b$ for $b \in K$ such that $\phi(S) = \{b\}$.

5.3 The first isomorphism theorem

Recall: If $\phi : G \to K$ is a homomorphism then $[G : \ker\phi] = |\operatorname{Im}\phi|$. We prove this by setting up a bijection $\psi : G/\ker\phi \to \operatorname{Im}\phi$ defined by $\psi(S) = b$, where $b \in K$ is such that $\phi(S) = \{b\}$. This looks like what we just did! Now we know $G/\ker\phi$ is a group, $|G/\ker\phi| = [G : \ker\phi] = |\operatorname{Im}\phi|$. Maybe this bijection is an isomorphism?

Theorem 5.9: First isomorphism theorem

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

Proof:

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

For $g \in G$, $\psi([g]) = \phi(g)$, so plainly $\operatorname{Im}\psi = \operatorname{Im}\phi$. Thus we can regard ψ as surjective homomorphism $G/\ker\phi \to \operatorname{Im}\phi$.

ψ agrees with the function $G/\ker\phi \to \operatorname{Im}\phi$ defined previously, so ψ is a bijection. Therefore ψ is an isomorphism.

Alternatively, we can prove it from the scratch. If $\psi([g]) = e$, then $\phi(g) = e$, so $g \in \ker\phi$ which implies $[g] = [e]$. So ψ is injective. Thus it is isomorphism. □

The first isomorphism theorem is the best way to determine G/N.

Example: $\operatorname{GL}_n \mathbb{K}/\operatorname{SL}_n \mathbb{K}$

Recall $\operatorname{SL}_n(\mathbb{K}) \trianglelefteq \operatorname{GL}_n(\mathbb{K})$ is defined as the kernel of homomorphism $\det : \operatorname{GL}_n \mathbb{K} \to \mathbb{K}^\times$.

The image of det is $\operatorname{Im}\det = \mathbb{K}^\times$. By first isomorphism theorem, $\operatorname{GL}_n \mathbb{K}/\operatorname{SL}_n \mathbb{K} \cong \mathbb{K}^\times$.

Example: $\mathbb{R}/\mathbb{Z}$

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

Have homomorphism exp: $\mathbb{R} \to \mathbb{C}^\times : x \mapsto e^{2\pi i x}$. Thus $e^{2\pi i x} = 1$ if and only if $x \in \mathbb{Z}$.

$\operatorname{Im}\exp = \{a \in \mathbb{C} : |a| = 1\} =: S^1$ (the **circle group**).

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

In general, to find G/N, we can find a group K and homomorphism $\phi : G \to K$ such that $\ker\phi = N$. Then we can conclude $G/N \cong \operatorname{Im}\phi$.

Sometimes we can also turn this around and use first isomorphic theorem to find $\operatorname{Im}\phi$.

5.4 The correspondence theorem

a.k.a. the fourth isomorphism theorem. We want to understand subgroups of G/N using $q : G \to G/N$. Recall: Suppose $f : X \to Y$ is a function, $S \subseteq X, T \subseteq Y$. Then

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

We previously proved:

Proposition 3.5

If $\phi : G \to H$ is a homomorphism, $K \leq G$, then $\phi(K) \leq H$. (a.k.a. pushfoward, image of K)

Proposition 3.10

If $\phi : G \to H$ is a homomorphism, $K \leq H$, then $\phi^{-1}(K) \leq G$. (a.k.a. pullback of K)

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

$$\begin{tikzcd} \text{Subgroups of } G \arrow[r, shift left, "K \mapsto \phi(K)"] & \text{Subgroups of } H \arrow[l, shift left, "\phi^{-1}(K') \leftarrow\!\shortmid K'"] \end{tikzcd}$$

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 is normal $\iff$ $\phi(K)$ is normal
- $\phi(\langle S \rangle) = \langle \phi(S) \rangle$. This holds for any homomorphisms. $\phi^{-1}(\langle S \rangle) = \langle \phi^{-1}(S) \rangle$ doesn't have to hold if ϕ is not isomorphism.
- $[G : K] = [H : \phi(K)]$

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

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

Everything in the left column holds for any function f. Everything in the right column holds when f is a bijection, but not for general functions f.

Order is preserved:

Lemma 5.10

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

(a) If $K_1 \leq K_2 \leq G$, then $f(K_1) \leq f(K_2)$

(b) If $K_1 \leq K_2 \leq H$, then $f^{-1}(K_1) \leq f^{-1}(K_2)$

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

Also, pullback preserves intersection:

Lemma 5.11

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

Suppose $f : X \to Y$ is a surjection, then we can move $f(f^{-1}(B)) = B$ from the right column to the left column:

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

Lemma 5.12

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

Sub(G)

If G is a group, let Sub(G) denote set of subgroups of G.

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

If ϕ is surjective, by Lemma 5.12, then ϕ is *left* inverse to ϕ^{-1}. (It might not have inverse. Sometimes we use ϕ^*.)

So $\phi^{-1} : \text{Sub}(H) \to \text{Sub}(G)$ is injective. Question: *What's the image of ϕ^{-1} in* Sub(G)*?*

Lemma 5.13

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

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

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

Proof:

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

(b) It's clear that $K \leq \phi^{-1}(\phi(K))$.

Suppose $y \in \phi^{-1}(\phi(K))$. Then $\phi(y) \in \phi(K)$, so $\phi(y) = \phi(k)$ for some $k \in K$. Since $\phi(k^{-1}y) = e$, $k^{-1}y \in \ker\phi \subseteq K$, thus $y \in K$. We conclude that $\phi^{-1}(\phi(K)) \subseteq K$. $\square$

From this lemma, we can conclude: $K = \phi^{-1}(K') \iff \ker\phi \leq K$.

When we combine Lemma 5.12 and Lemma 5.13, we get the following theorem:

Theorem 5.14: Correspondence theorem

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

$$\begin{array}{c} \text{Subgroups} \\ K \text{ of } G \text{ s.t.} \\ \ker\phi \leq K \end{array} \quad \begin{array}{c} \xrightarrow{\quad K \mapsto \phi(K) \quad} \\ \xleftarrow[\quad \phi^{-1}(K') \leftarrow\!\shortmid K' \quad]{} \end{array} \quad \begin{array}{c} \text{Subgroups} \\ K' \text{ of } H \end{array}$$

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

(a) $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$

(b) $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$

(c) K is normal $\iff$ $\phi(K)$ is normal

Proof:

Since ϕ 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 ϕ and ϕ^{-1} are inverses on the specified sets. So they are bijections.

(a) follows from fact that ϕ and ϕ^{-1} are inverses and preserve $\leq$. For instance, if $\phi(K_1) \leq \phi(K_2)$ then $K_1 = \phi^{-1}(\phi(K_1)) \leq \phi^{-1}(\phi(K_2)) = K_2$

(b) $\phi^{-1}(\phi(K_1) \cap \phi(K_2)) = \phi^{-1}(\phi(K_1)) \cap \phi^{-1}(\phi(K_2)) = K_1 \cap K_2$ since $\phi(\phi^{-1}(K)) = K, \phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$,

(c) Exercise. $\square$

What about quotient groups?

If $N \trianglelefteq G$, then $q : G \to G/N$ is a surjection, so we have

Theorem 5.15: Correspondence theorem for quotient groups

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

$$\begin{tikzcd} \begin{array}{l}\text{Subgroups}\\ N \leq K \leq G\end{array} \arrow[r, shift left, "K \mapsto q(K)"] & \begin{array}{l}\text{Subgroups}\\ K' \text{ of } G/N\end{array} \arrow[l, shift left, "q^{-1}(K') \mapsfrom K'"] \end{tikzcd}$$

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

(a) $K_1 \leq K_2 \iff q(K_1) \leq q(K_2)$

(b) $q(K_1 \cap K_2) = q(K_1) \cap q(K_2)$

(c) K is normal $\iff$ $q(K)$ is normal

Recall from first isomorphism theorem: If $\phi : G \to H$ is a surjective homomorphism, then $G/\ker\phi \cong H$. So there is a bijection between $\mathrm{Sub}(H)$ and $\mathrm{Sub}(G/\ker\phi)$.

Exercise

Check that

$$\left.\begin{array}{r}\text{first isomorphism theorem}\\ \text{subgroup correspondence for isomorphisms}\\ \text{correspondence theorem for quotient groups}\end{array}\right\} \implies \begin{array}{l}\text{correspondence theorem}\\ \text{for surjective homomorphisms}\end{array}$$

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$, we immediately see that $N \trianglelefteq K$ since $kNk^{-1} \subseteq N$ for all $k \in K \subseteq G$.

Let $q_G : G \to G/N$ be quotient map. Since $N \trianglelefteq K$, also have quotient map $q_K : K \to K/N$.

$$\begin{tikzcd} K \arrow[r, "i_K"] \arrow[d, "q_K"'] \arrow[dr, "q_G \circ i"] & G \arrow[d, "q_G"] \\ K/N \arrow[r, "kN \mapsto kN"'] & G/N \end{tikzcd}$$

It's easy to see $\ker q_G \circ i = N$, and by first isomorphism theorem, we get an isomorphism $\psi : K/N \to \mathrm{Im}\, q \circ i_K = q(K)$ such that $\psi \circ q_K = q_G \circ i$. In other words, if $k \in K$, then $\psi(kN) = q(k) = kN$. Let's summarize this into a proposition:

Proposition 5.16

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

Because of this isomorphism, we use the following notation:

K/N

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: D_{2n}

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

Subgroups of D_{2n} contains N correspond to subgroups of $D_{2n}/N = \mathbb{Z}_2$.

$\mathbb{Z}_2$ has two subgroups, $\mathbb{Z}_2$ and $\{e\}$.

So there are only two subgroups of D_{2n} containing N.

Example: $\operatorname{GL}_n \mathbb{K}$

$\operatorname{GL}_n \mathbb{K}/\operatorname{SL}_n \mathbb{K} \cong \mathbb{K}^\times$, so subgroups of $\operatorname{GL}_n \mathbb{K}$ containing $\operatorname{SL}_n \mathbb{K}$ correspond to subgroups of $\mathbb{K}^\times$ (of which there can be lots: $\{1, -1\}, \{2^x | x \in \mathbb{Z}\}$)

5.5 The third isomorphism theorem

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$. From correspondence theorem: $K \trianglelefteq G$ if and only if $K/N \trianglelefteq G/N$. Suppose $K/N \trianglelefteq G/N$. What's $(G/N)/(K/N)$?

Third isomorphism theorem, informal version

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

Example:

Suppose $n|m$, so that $m\mathbb{Z} \leq n\mathbb{Z}$.

Then $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

$(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$

Theorem 5.17: Third isomorphism theorem

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

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

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

$$\begin{tikzcd} G \arrow[r, "q_1"] \arrow[d, "q_3"'] & G/N \arrow[d, "q_2"] \\ G/K \arrow[r, "\psi"'] & (G/N)/(K/N) \end{tikzcd}$$

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

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

By first isomorphism theorem, therre is an isomorphism $\psi : G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$. □

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 5.18

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

In fact, there's no reason to use quotient spaces. This holds for surjective homomorphisms.

Proposition 5.19

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

These two propositions are actually equivalent by the first isomorphism theorem.

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

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 ϕ is surjective, f is onto.

Suppose $f(gK) = f(hK)$, so $\phi(g)\phi(K) = \phi(h)\phi(K)$. Then $\phi(h^{-1}g) = \phi(h)^{-1}\phi(g) \in \phi(K) \implies h^{-1}g \in \phi^{-1}(\phi(K)) = K$. So $gK = hK$, and f is injective.

We conclude that f is a bijection. □

5.6 The second isomorphism theorem

Recall *internal direct product* and lemma from products:

Lemma 4.11

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

We didn't use the fact $G = HK$ in the proof. If $HK \subsetneq G$, then we won't be able to write $g = hk$, but for the g that we can write in the form of hk, the factorization is unique if and only if $H \cap K = \{e\}$. Then we can reword this lemma a little more generally.

Suppose $H, K \leq G$.

Lemma 5.20

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

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

What is $|HK|$ if $H \cap K \neq \{e\}$?

$HK = \bigcup_{h \in H} hK$, a union of cosets of K.

Let $X = \{hK : h \in H\} \subseteq G/K$.

Then X is a partition of HK, so $|HK| = |X| \cdot |K|$.

How large is X?

Lemma 5.21

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 $h_1^{-1}h_2 = H \cap K$ if and only if $h_1H \cap K = h_2H \cap K$. This uses the fact that $H \cap K \leq H$. □

Rephrasing: Consider equivalence relations $\sim_K$ on G, $\sim_{H \cap K}$ 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 5.22

$H/H \cap K \to X : hH \cap K \to hK$ is a bijection.

Proof:
From Lemma 5.21, it is well-defined, injective. Surjective obvious. $\square$

Now going back to what we are trying to do: If $H, K \leq G$, $X = \{hK : h \in H\}$ partitions HK, so $|HK| = |X| \cdot |K|$.

$|X| = [H : H \cap K]$, so $|HK| = [H : H \cap K]|K|$. Using $[H : H \cap K] \cdot |H \cap K| = |H|$ (by Lagrange's theorem), we have

Proposition 5.23

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

Note that this proposition also holds when H and K are infinite. Another way to think about this formula if H, K finite:

$[H : H \cap K] = |X| = \frac{|HK|}{|K|}$ LHS is an index, RHS is a fraction. Is RHS an index as well? The problem: HK *not necessarily a group.* Thus RHS might not be an index. But when is HK a group?

Proposition 5.24

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

Proof:

(1) $\Rightarrow$ (2) If $HK \leq G$, and $h \in H, k \in K$, 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 $hk = (k^{-1}h^{-1})^{-1} = k_0^{-1}h_0^{-1} \in KH$. Sp $KH \subseteq HK$ and $HK \subseteq KH \implies HK = KH$

(3) $\Rightarrow$ (1) Conversely, suppose $KH \subseteq HK$. We always have $e \in HK$. If $x, y \in HK$, then $x = h_0k_0$, $y = h_1k_1$ for $h_0, h_1 \in H$, $k_0, k_1 \in K$. Since $KH \subseteq HK$, $k_0^{-1}(h_0^{-1}h_1) = h_2k_2$ for $h_2 \in H, k_2 \in K$. So $x^{-1}y = k_0^{-1}h_0^{-1}h_1k_1 = h_2(k_2k_1) \in HK$. $\square$

Corollary 5.25

If $KH \subseteq HK$, then $[H : H \cap K] = [HK : K]$.

When is $KH \subseteq HK$?

Sufficient condition:

$$\text{for all } h \in H, \text{ there is } h' \in H \text{ such that } Kh = h'K.$$

Recall: if $Kh = h'K$, then $h'K = hK$.
Rephrase condition: $hKh^{-1} = K$, for all $h \in H$, i.e., $H \subseteq N_G(K)$.

Corollary 5.26

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

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

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

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

Theorem 5.27: Second isomorphism theorem

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

$$\begin{tikzcd} H \arrow[r, "i_H"] \arrow[d, "q_1"'] & HK \arrow[d, "q_2"] \\ H/H\cap K \arrow[r, "\psi"'] & HK/K \end{tikzcd}$$

Proof:
Already shown $HK \le G, K \trianglelefteq HK, H \cap K \trianglelefteq H$.

If $h \in H, k \in K$, then $hkK = hK$. So $HK/K = \{gK : g \in HK\} = \{hK : h \in H\}$.
Hence $\operatorname{Im} q_2 \circ i_H = \{hK : h \in H\} = HK/K$.

$\ker q_2 \circ i_H = i_H^{-1}(q_2^{-1}(\{e\})) = i_H^{-1}(K) = H \cap K$

By the first isomorphism theorem, there is an isomorphism ψ as desired. $\square$

Example: $\mathrm{PGL}_n \mathbb{C}$
Recall that $\mathrm{PGL}_n \mathbb{C} = \mathrm{GL}_n \mathbb{C}/Z(\mathrm{GL}_n \mathbb{C})$.

Let $K = Z(\mathrm{GL}_n \mathbb{C}) = \{\lambda 1 : \lambda \neq 0\}$. Since $K \trianglelefteq G$, $N_G(K) = G$. Let $H = \mathrm{SL}_n \mathbb{C} = \{M \in G : \det M = 1\} \trianglelefteq G = N_G(K)$, so $HK \le G$. Suppose $M \in \mathrm{GL}_n \mathbb{C}$, let $\lambda = \det M$. Then $\det \lambda^{-1/n} M = \lambda^{-1} \det M = 1$, $\lambda^{-1/n} M \in \mathrm{SL}_n \mathbb{C}$.

Conclusion: $G = HK$.

$C_n := H \cap K = \{\lambda 1 : \lambda^n = 1\} = \{e^{2\pi i k/n} 1 : k = 0, \ldots, n-1\}$ (Note: $C_n \cong \mathbb{Z}/n\mathbb{Z}$).
Second isomorphism $\implies \mathrm{PGL}_n \mathbb{C} \cong \mathrm{SL}_n \mathbb{C}/C_n$. In Lie theory, this kind of calculation can be quite useful.

6

Group actions

week 5

6.1 Group actions

6.1.1 Two group actions

Example: S_n

Permutation S_n of $\{1, \ldots, n\}$ form a group.

This means that we can multiply permutations together. e.g.,

$$(12)(34)(24) = (1234)$$

However, that's not all there is to permutations: we can also plug in numbers from $1, \ldots, n$

$$((12)(34))(3) = 4$$

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

Example: $\mathrm{GL}_n \mathbb{C}$

Similarly, for $\mathrm{GL}_n \mathbb{C}$, we can do more than multiply matrices: We can also multiply matrices and vectors. Given $A \in \mathrm{GL}_n \mathbb{C}, v \in \mathbb{C}$, can take $A \cdot v \in \mathbb{C}^n$. Say that $\mathrm{GL}_n \mathbb{C}$ **acts** on $\mathbb{C}^n$.

Clearly the notion of actions is important to groups.

left action

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

(a) $e \cdot x = x$ for all $x \in X$, and

(b) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G, x \in X$.

Example:
S_n acts on $\{1, \ldots, n\}, n \geq 1$.

$\mathrm{GL}_n \mathbb{K}$ acts on $\mathbb{K}^n$ (prove by the associativity of matrix multiplication).

Let X be any set, G any group. We can define an action of G on X by $g \cdot x = x$ for all $g \in G, x \in X$. This is called the **trivial action** of G on X.

Proof:
(a) clear, $g \cdot (h \cdot x) = g \cdot x = x = (gh) \cdot x$. □

Proposition 6.1

Let X be a set. The group S_X (of invertible functions $X \to X$ 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 $(f \circ g)(x) = f(g(x)) = g \cdot (g \cdot x)$. □

Note
We typically stick with the notation $f(x)$, rather than $f \cdot x$. Recall $S_n = S_{\{1,\ldots,n\}}$.

Lemma 6.2

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

Proof:
Immediate. □

Alternative way to show $\mathrm{GL}_n \mathbb{K}$ acts on $\mathbb{K}^n$: observe $\mathrm{GL}_n \mathbb{K} \leq S_{\mathbb{K}^n}$.

6.1.2 Invariant subsets

However, note that groups aren't tied to a particular action:

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

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

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

$$s^i \text{ sends } v_0 \text{ to } v_i,\ v_1 \text{ to } v_{i+1} \qquad s^i r \text{ sends } v_0 \text{ to } v_i,\ v_1 \text{ to } v_{i-1}$$

This dihedral group action on the vertices of the n-gon is an instance of the following pattern:

invariant under the action of G

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 $g \in G, y \in Y$.

Lemma 6.3

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

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

6.1.3 Actions on functions

Proposition 6.4

Suppose G acts on X and Y, and let $\mathrm{Fun}(X, Y)$ denote the set of functions from X to Y. If $g \in G$ and $f \in \mathrm{Fun}(X, Y)$, let $g \cdot f$ be the function

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

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

Proof:
Exercise. □

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

6.1.4 Actions on subsets

Proposition 6.5

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

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

For all $g, h \in G, S = 2^X$,

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

□

Alternative proof: 2^X is the set of functions $X \to \{0, 1\}$. Can realize action of G on 2^X by taking action on functions with trivial action on $\{0, 1\}$.

6.1.5 Left regular action

Does every group act on some set?

Lemma 6.6

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

Proof:
Immediate from group definition. $\square$

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

Lemma 6.7

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

Proof:
We can prove this by combining previous lemmas and propositions.

First we know G acts on itself by the left regular action. From Proposition 6.5, we know G acts on 2^G by the setwise product. Second, the elements of G/H are cosets, thus $G/H \subseteq 2^G$. Now setwise product gives us an action of G on 2^G. When we take the setwise product g with coset kH, we get another coset. So G/H is an invariant subset of 2^G under the induced subset product action from the left regular action. $\square$

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

6.1.6 Right multiplication

What about right multiplication?

Let G be a group, where we denote the product of g and h by gh (then we free $\cdot$ symbol and can redefine later). For $g, k \in G$, define $g \cdot k = kg$ (right multiplication). Then we might ask: does this define a left action of G on G in the same way that left multiplication did?

If $g, h, k \in G$ (k is the element being acted on), then $g \cdot (h \cdot k) = g \cdot kh = khg$, whereas $gh \cdot k = kgh$, which is not equal to khg if $hg \neq gh$. So right multiplication does not define a left action in general.

Can we fix this?

right action

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

(a) $x \cdot e = x$ for all $x \in X$, and

(b) $(x \cdot g) \cdot h = x \cdot (gh)$ for all $g, h \in G, x \in X$.

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 $H \setminus G$.

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 $g \in G, x \in X$.

If there is a right action of G on X, and Y is any set, then $(g \cdot f)(x) = f(x \cdot g)$ defomes a left action of G on $\mathrm{Fun}(X, Y)$.

Proposition 6.8

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:
$e \cdot x = x \cdot e$, and if $g, h \in G, x \in X$, then

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

□

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

6.2 Permutation representations

Lemma 6.9

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

(a) $\ell_g \circ \ell_h = \ell_{gh}$ for all $g, h \in G$.

(b) $\ell_e = 1$, the identity function.

(c) ℓ_g is a bijection for all $g \in G$.

Proof:
$\ell_g \circ \ell_h(x) = g \cdot (h \cdot x) = gh \cdot x = \ell_{gh}(x)$.

Also, $\ell_e(x) = e \cdot x = x$.

Finally, $\ell_g \circ \ell_{g^{-1}} = \ell_e = 1 = \ell_{g^{-1}} \circ \ell_g \implies \ell_g$ is invertible. □

Corollary 6.10

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

permutation representation

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

If $|X| = n$, then $S_X \cong S_n$.

So action on finite set X with $|X| = n$ gives homomorphism to S_n.

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

Let $X = \{v_0, \dots, v_{n-1}\}$ be vertices of n-gon.

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 $\phi : D_{2n} \to S_n$ be permutation representation given by action D_{2n} on X

What is $\phi(s)$?

$s \cdot v_0 = v_1, s \cdot v_1 = v_2, \dots, s \cdot v_{n-1} = v_0$. So

$$\phi(s) = (1\ 2\ 3\ \dots\ n)$$

What is $\phi(r)$?

$r \cdot v_0 = v_0, r \cdot v_1 = v_{n-1}, \dots, r \cdot v_i = v_{n-i}$. So

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

Transposition is another name for the two cycle.

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

Theorem 6.11

(a) If G acts on X, then there is a homomorphism $\phi : G \to S_X$ defiend by $\phi(g)(x) = g \cdot x$.

(b) If $\phi : G \to S_X$ is a homomorphism, then $g \cdot x = \phi(g)(x)$ defines a group action of G on X.

In other wrods, group actions $\equiv$ permutation representations.

Because of this theorem, we treat the two as interchangeable.

Proof:

(a) Already done.

(b) $e \cdot x = \phi(e)(x) = 1(x) = x$ for all $x \in X$.

If $g, h \in G, x \in X$, then

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

□

6.3 Cayley's theorem

faithful

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

Lemma 6.12

An action of G on X is faithful if and only if for every $g \in G$, $g \neq e$, 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 $g \cdot x = \ell(g)(x) \neq x$. □

Lemma 6.13

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

Example:
S_X acts faithfully on X.

If $A \cdot e_i = e_i$ for all $i = 1, \ldots, n$, then $A = 1$, so action of $\mathrm{GL}_n \mathbb{K}$ on $\mathbb{K}^n$ is faithful.

D_{2n} acts faithfully on vertices of the n-gon.

Trivial action is not faithful.

Does every group act faithfully on some set?

Theorem 6.14: 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 $g \in G, g \neq e$, then $g \cdot e = g \neq e$. So left regular action is faithful.

Hence permutation representation $\phi : G \to S_G$ is injective. So G is isomorphic to $\operatorname{Im}\phi \leq S_G$ (easy case of first isomorphism theorem). If $|G| = n < +\infty$, then $S_G \cong S_n$. $\square$

Homomorphism $G \to S_G$ given by this theorem is called **left regular representation** of G.

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

Cayley's theorem: G is isomorphic to a subgroup of S_2

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

$[1] + [0] = [1], [1] + [1] = [0]$, so $[0] \mapsto (1\ 2)$ in S_2.

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

Example: D_6
D_6 has order 6, so is isomorphic to subgroup of S_6

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

But $|S_6| = 6! \gg 6$.

Remark:
There is actually a sense in which the left regular representation is the least efficient representation of the group. We don't have the tools to fill what we mean by that. The tools will be explored in the representation theory of finite groups.

6.4 Orbits and stabilizers

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: left multiplication

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

If we take $H = G$, then $\mathcal{O}_g = G$, then transitive. Since Hg is a proper subset of G if $H < G$, G is not transitive unless $H = G$.

If H is non-trivial, $Hg = Hg'$ for some $g \neq g'$. Thus it's possible to have $\mathcal{O} = \mathcal{O}_x = \mathcal{O}_{x'}$ for $x \neq x'$. That's part of why we have two different terms: $\mathcal{O}$ and $\mathcal{O}_x$.

We can also consider right multiplication, then orbit is a left coset.

Example: $\mathrm{GL}_n \mathbb{K}$

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

$$\mathcal{O}_v = \begin{cases} \{0\} & v = 0 \\ \{w \in \mathbb{K}^n : w \neq 0\} & v \neq 0 \end{cases}$$

The second orbit can be verified by the basis extension theorem. So this action is transitive, and there are two orbits.

Example: S_X

If $1 \leq i \neq j \leq n$, then can find $\pi \in S_n$ such that $\pi(i) = j$. (for instance, $\pi = (i\ j)$). So $\mathcal{O}_i = \{1, \ldots, n\}$ for all i.

Conclusion: action of S_n on $\{1, \ldots, n\}$ is transitive, has one orbit.

More generally, action of S_X on X is transitive, has one orbit.

Suppose $\sigma \in S_n$. What are the orbits of $\langle\sigma\rangle$ on $\{1, \ldots, n\}$? E.g. $\sigma = (1\,3\,7)(2\,6)(4\,8) \in S_8$.

$\mathcal{O}_1 = \mathcal{O}_3 = \mathcal{O}_7 = \{1, 3, 7\}, \mathcal{O}_2 = \mathcal{O}_6 = \{2, 6\}$. Other orbits are $\{4, 8\}, \{5\}$.

In general, if $\sigma = (i_{11}\ \cdots\ i_{1k_1})(i_{21}\ \cdots i_{2k_2})\cdots(i_{m1}\ \cdots\ i_{mk_m})$ (with 1-cycles included), orbits are $\{i_{j1}, \ldots, i_{jk_j}\}$, $1 \leq j \leq m$

Note: in all these examples, orbits partition X.

Recall: partitions correspond to equivalence relations.

$\sim_G$

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

Lemma 6.15

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 multiply both sides by g^{-1}, 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 $y \sim_G z \implies x \sim_G z$. $\square$

If $x \in X$, then equivalence class $[x]_{\sim G}$ of x is

$$\{y \in X : x \sim_G y\} = \{y \in X : y = g \cdot x, \text{ for some } g \in G\} = \mathcal{O}_x$$

Conclusion: equivalence classes of $\sim_G$ are orbits of G acting on X.

Proposition 6.16

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 one orbit.

set of representatives for $\sim$

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.

It's always possible to pick a set of representatives.

Corollary 6.17

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

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

Example:
In the previous S_X example, we can pick $1, 2, 4, 5$, and

$$|X| = 8 = |\mathcal{O}_1| + |\mathcal{O}_2| + |\mathcal{O}_4| + |\mathcal{O}_5|$$

What's $|\mathcal{O}_x|$?

To determine $|\mathcal{O}_x|$, we can use the function $G \to \mathcal{O}_x : g \mapsto g \cdot x$. It's clearly onto, but it might have $g \cdot x = h \cdot x$ when $g \neq h$.

stabilizer of x

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

Proposition 6.18

If G acts on X, $x \in X$, 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 $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = e \cdot x = x \implies g^{-1} \in G_x$. $\square$

Theorem 6.19: Orbit-stabilizer theorem

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

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. $\square$

Corollary 6.20

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

Example: S_n
Let $G = S_n, X = \{1, \ldots, n\}$.

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

So we have $n = |\mathcal{O}_i| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{n!}{|G_i|}$.

It follows that $|G_i| = (n-1)!$, any i

Stabilizer of i is $G_i = \{\pi \in S_n : \pi(i) = i\}$,

For example, for $n = 4$, $G_1 = \{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$.

In general, $G_i \cong S_{n-1}$, we can see $|G_i| = (n-1)!$ directly.

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

Proposition 6.21

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 $\mathcal{O}_{eH} = G/H$.

$$g \cdot eH = eH \iff gH = H \iff g \in H. \qquad \square$$

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

6.4.1 Kernel versus stabilizer

If G acts on X, then kernel of the action is $\{g \in G : g \cdot x = x \quad \forall x\}$ where as $G_x = \{g \in G : g \cdot x = x\}$, i.e., with stabilizer x is fixed. Consequently, if H is kernel of action, then $H \leq G_x$ for all $x \in X$.

Proposition 6.22

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 $x \in X$. $\square$

Theorem 6.23

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 kernel of action of G on G/H. By Proposition 6.22, $K \leq H = G_{eH}$. Let $k = [H : K] = \frac{|H|}{|K|}$. Now $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = p \cdot k$.

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

But we also have $k \Bigm| |G|$. Since p is smallest prime dividing $|G|$, must have $k = 1 \implies |H| = |K| \implies H = K$. $\square$

6.5 Conjugation

Recall that left multiplication defines a left action of G on G. It turns out that there's another natural left action:

Lemma 6.24

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

Remark:
This action is called the **conjugation action of G on G**.

To avoid confusion with the left multiplication action in this section, we'll denote the conjugation action by $\bullet$, so $g \bullet k = gkg^{-1}$.

In practice, there is no convention on the meaning of $\cdot$ and $\bullet$, so we'll have to say which one you are using each time.

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

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

$$g \bullet (h \bullet k) = g \bullet hkh^{-1} = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = gh \bullet k$$

□

conjugacy class

The orbit of $k \in G$ under the conjugation action is called **conjugacy class** of k. We'll denote it by $\mathrm{Conj}_G(k)$.

centralizer of k in G

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

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

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

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

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

The conjugation action of G on G induces an action of G on 2^G

If $g \in G, S \subseteq G$, then

$$g \bullet S = \{g \bullet h : h \in S\} = \left\{ghg^{-1} : h \in S\right\} = gSg^{-1}$$

So the stabilizer of S is $\{g \in G : gSg^{-1} = S\} =: N_G(S)$, where $N_G(S)$ is the normalizer of S in G.

Example: matrices
Important instances of the conjugation action: $G = \mathrm{GL}_n \mathbb{K}$

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

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

Recall: two 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 $\sim_{\mathrm{GL}_n \mathbb{K}}$.

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

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 $\sum_{\mathrm{GL}_n \mathbb{K}}$.

6.5.1 Class equation

Using standard fact about orbits,

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

where S is set of representatives for conjugacy classes.

Lemma 6.25

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

Proof:
$\operatorname{Conj}(k)$ has size one $\iff gkg^{-1} = k$ for all $g \in G$
$\iff C_G(k) = G \iff k \in Z(G)$ □

Theorem 6.26: Class equation

If G is a finite group, then $|G| = |Z(G)| + \sum_{g \in T} |\operatorname{Conj}(g)|$, where T is a set of representatives for conjugacy classes not contained in the center.

Proof:
Immediate. □

Theorem 6.27: 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: theorem is true if G is cyclic.

First assume G is *abelian*. Proof by induction on m.

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

Inductive step: Pick $a \in G$, $a \neq e$. Can assume $|a| < |G|$ (since otherwise G is cyclic)

If $p \mid |a|$, then apply induction to get element $b \in \langle a \rangle$ with $|b| = p$.

Otherwise assume $p \nmid |a|$. Since G abelian, $N = \langle a \rangle \trianglelefteq G$. $|G/N| = |G|/|N| < |G|$. Since $p \mid |G|, p \nmid |N|$, then $p \mid |G/N|$ by prime factorization of $|G|$. Then prove by induction, G/N has element gN of order p.

Let $n = |g|$. Since $g^n = 1$, then $q(g)^n = (gN)^n = 1$ where q is quotient map. Thus $p \mid n$.

If $G = \langle g \rangle$, then done, otherwise apply induction to $\langle g \rangle$.

Now prove for general case (nonabelian G): Use induction on $|G|$ again.

Recall class equation: $|G| = |Z(G)| + \sum_{g \in T} |\operatorname{Conj}(g)|$.

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

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

6.5.2 p-groups

p-group

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

Theorem 6.28

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

Proof:

$|G| = Z(G) + \sum_{g \in T}[G : C_G(g)]$. We know that $[G : C_G(g)] \mid |G|$. If $g \notin Z(G)$ then $[G : C_G(g)] > 1 \implies [G : C_G(g)] = p^l$ for $1 < l \leq k \implies p \mid [G : C_G(g)]$. Thus $p \mid |Z(G)| \implies |Z(G)| \geq p \implies Z(G) \neq \{e\}$. □

6.6 Conjugation in permutation groups

Suppose $\pi\sigma \in S_n$. What is $\pi\sigma\pi^{-1}$?

Lemma 6.29

If $\sigma(i) = j$, then $(\pi\sigma\pi^{-1})(\pi(i)) = \pi(j)$.

Corollary 6.30

If $\sigma = (i_{11} \ \cdots \ i_{1k_1})(i_{21} \ \cdots \ i_{2k_2}) \cdots (i_{m1} \ \cdots \ i_{mk_m})$, then
$\pi\sigma\pi^{-1} = (\pi(i_{11}) \ \cdots \ \pi(i_{1k_1})) \cdots (\pi(i_{m1}) \ \cdots \ \pi(i_{mk_m}))$

Example: S_{10}

Let $\sigma = (1\ 3)(2)(4\ 8\ 10)(5\ 7\ 6)(9)$, $\pi = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$, then
$\pi\sigma\pi^{-1} = (2\ 4)(3)(5\ 9\ 1)(6\ 8\ 7)(10) = (1\ 5\ 9)(2\ 4)(3)(6\ 8\ 7)(10)$

Now given σ, what can we say about the conjugacy class $\mathrm{Conj}(\sigma) = \{\pi\sigma\pi^{-1} : \pi \in S_n\}$?

cycle type

For $n \geq 1$, let $[n] := \{1, \dots, n\}$. If $\sigma \in S_n$, the **cycle type** of σ is the function $\lambda : [n] \to \mathbb{Z}_{\geq 0}$ such that $\lambda(i)$ is the number of cycles in the disjoint cycle representation of σ of length i.

Example: S_{10}
Let $\sigma = (1\ 3)(2)(4\ 8\ 10)(5\ 7\ 6)(9)$.

Then σ has cycle type λ with $\lambda(1) = 2, \lambda(2) = 1, \lambda(3) = 2$, and $\lambda(i) = 0$ for $4 \leq i \leq 10$.

Note that if λ is a cycle type, then $\sum_{i=1}^{n} i\lambda(i) = n$.

Proposition 6.31

If $\sigma \in S_n$ has cycle type λ, then

$$\mathrm{Conj}(\sigma) = \{\tau \in S_n : \tau \text{ has cycle type } \lambda\} =: \mathrm{Conj}(\lambda)$$

Proof:
By Corollary 6.30, $\pi\sigma\pi^{-1}$ has the same cycle type as σ.

Suppose τ has the same cycle type as σ.
Let $\sigma = (i_{11}\ \cdots\ i_{1k_1})(i_{21}\ \cdots\ i_{2k_2})\cdots(i_{m1}\ \cdots\ i_{mk_m})$.

By ordering cycles, can write τ as
$\tau = (j_{11}\ \cdots\ j_{1k_1})(j_{21}\ \cdots\ j_{2k_2})\cdots(j_{m1}\ \cdots\ j_{mk_m})$.

Let π be the permutation with $\pi(i_{ab}) = j_{ab}$. Then $\pi\sigma\pi^{-1} = \tau$, so $\tau \in \mathrm{Conj}(\sigma)$. $\square$

How many conjugacy classes are there?

partition of n

A **partition of** n is a tuple λ of natural numbers $(\lambda_1, \dots, \lambda_k)$ such that

- $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$, and
- $\lambda_1 + \lambda_2 + \ldots + \lambda_k = n$.

Example:
The partitions of 4 are $(4), (3,1), (2,2), (2,1,1),$ and $(1,1,1,1)$.

Remark:
To avoid having to repeat numbers, we can write

$$\underbrace{a, a, \dots, a}_{k \text{ times}}$$

as a^k. So for instance, $(2,1,1) = (2^1, 1^2), (1,1,1,1) = (1^4)$.

Lemma 6.32

There is a bijection between partitions of n, and functions $\lambda : [n] \to \mathbb{Z}_{\geq 0}$ such that $\sum_{i=1}^{n} i\lambda(i) = n$.

Proof:
Map λ to $(n^{\lambda(n)}, (n-1)^{\lambda(n-1)}, \dots, 2^{\lambda(2)}, 1^{\lambda(1)})$. □

Corollary 6.33

The number of conjugacy classes in S_n is $p(n)$.

where $p(n) =$ number of partitions of $n = e^{\pi\sqrt{2n/3}} \ll n! \approx n^n$. $|S_n| = n!$.

Proof:
$\lambda : [n] \to \mathbb{Z}_{\geq 0}$ is the cycle type of a permutation if and only if $\sum_i i\lambda(i) = n$. □

6.6.1 Stabilizer of an element

Suppose $\sigma = (1\ 2\ \cdots\ n) \in S_n$. Then what is $C_{S_n}(\sigma) = \{\pi \in S_n : \pi\sigma\pi^{-1} = \sigma\}$? If $\pi(1) = i$, then we must have $\pi(2) = i+1, \pi(3) = i+2$, etc. So π is completely determined by $\pi(1)$.

What about $\sigma = (1\ 2)(3\ 4)$? Could have $\pi = e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)$ or $\pi = (1\ 3)(2\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 4)(2\ 3)$. i.e., we can switch cycles of the same length. In this case, π is determined by $\pi(1)$ and $\pi(3)$.

Proposition 6.34

Let $\sigma = (i_{11}\ \cdots\ i_{1k_1})(i_{21}\ \cdots\ i_{2k_2})\cdots(i_{m1}\ \cdots\ i_{mk_m})$ be a permutation of cycle type λ. If $\pi \in C_{S_n}(\sigma)$, then π is completely determined by $\pi(i_{11}), \pi(i_{21}), \dots, \pi(i_{m1})$. Consequently,

$$|C_{S_n}(\sigma)| = \prod_{i=1}^{n} i^{\lambda_i}\lambda_i!$$

Proof:
For the first part, use $\sigma(i) = j \implies \pi\sigma\pi^{-1}(\sigma(i)) = \pi(j)$.

Enumeration: note that $\pi(i_{a1})$ must go to a cycle of length $k = k_a$ so π permutes the cycles of length k, leading to $\lambda_k!$ choices.

Once we know what cycle i_{a1} is going to, there are k choices for where in the cycle in can go.

λ_k such choices gives a factor of k^{λ_k}. □

Corollary 6.35

If $\lambda : [n] \to \mathbb{Z}_{n \geq 0}$ with $\sum_i i\lambda(i) = n$, then

$$|\operatorname{Conj}(\lambda)| = \frac{n!}{\prod_i i^{\lambda_i} \lambda_i!}$$

Since the orbits partition S_n, we get the nice combinatorial identity

$$n! = \sum_{\lambda} \frac{n!}{\prod_i i^{\lambda_i} \lambda_i!}$$

where the sum is over functions $\lambda : [n] \to \mathbb{Z}_{\geq 0}$ with $\sum_i i\lambda(i) = n$. (If we want to, we can think of the sum as being over partitions.)

7 Classification of groups

week 6

Classification problem here is to identify all groups up to isomorphism. Also, we can replace the groups here with any algebraic structure. In the next part of this course, we will do classification on rings. Classification is really one of the *big questions* in modern mathematics. By big questions, we mean *where does the gravity come from* in physics, or *do we have free wills* in philosophy. So we what we have so far is a group of orders strictly less then 10,

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

Table 7.1: Groups of small order

Recall we previously mentioned,

Proposition 7.1

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. Choose $a \in G \setminus \{e\}$. Then $\langle a \rangle \neq G$, since $|a| \neq 1, |a| \,\big|\, p$, then $|a| = p$. We can find $b \in G \setminus \langle a \rangle$. We know $\langle a \rangle \neq G$ either, $|b| = p$ as well.

Let $H = \langle a \rangle, K = \langle b \rangle$. Since $H \cap K < K$, and $|H \cap K| \,\big|\, |K| = p$, thus $|H \cap K| = 1$, then $H \cap K = \{e\}$. So $|HK| = |H|\,|K|/|H \cap K| = p^2$, which implies $HK = G$.

Also $[G : H] = [G : K] = p$, which is the smallest prime dividing $|G|$, which implies $H, K \trianglelefteq G$. Therefore $G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. □

7.1 Groups of order pq

Lemma 7.2

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

Proof:
Since $|H \cap K|$ divides both $|H|, |K|$, thus $|H \cap K| = 1$, then $H \cap K = \{e\}$.

Also $|HK| = |H| \cdot |K|/|H \cap K| = |G| \implies HK = G$. Use characterization of products, then $G \cong H \times K$. □

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

Cauchy's theorem: G has elements a, b with $|a| = p, |b| = q$. Let $H = \langle a \rangle, K = \langle b \rangle$. Note $\gcd(|H|, |K|) = 1$, and $|H| \cdot |K| = |G|$. But we have to ask that *are* $H, K \trianglelefteq G$*?*

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

We already got a counterexample: $G = D_6$, $H = \langle r \rangle, K = \langle s \rangle$.

Suppose $H, K \leq G, HK = G, H \cap K = \{e\}$, and $K \trianglelefteq G$. Is it true that $G \cong H \times K$? No!

In our counterexample, that would make $D_6 \cong H \times K \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, which is abelian, but D_6 is nonabelian. It is not necessarily true that $G \cong H \times K$ if just one of the subgroup is normal.

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

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

Difficulty in analyzing pq case: $H \leq G$ might not be normal. This concern is not present of G is abelian. If G is abelian, every subgroup is normal.

Our focus in this chapter will be **finite abelian groups**.

There are lots of other ways to approach the classification problem. Notice that for small orders, we are essentially describing groups as built out of other smaller groups. For example, for the group of order 6, we have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. S_3 is the semidirect product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

When can a group be built out of smaller groups? This is covered in the Galois theory.

Group is **simple** if it contains no normal subgroups. Simple groups are the minimal building blocks for other groups in the sense they cannot be broken down any further.

Finally, by looking at the isomorphism problem for **finitely-presented groups**, we see that the classification problem for in finite groups cannot be solved.

7.2 Classification of finite abelian groups

Recall Lemma 7.2, how can we find subgroups of coprime order? Let's ask an easier question: how can find subgroups of order m for some given m inside the abelian group?

Lemma 7.3

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 $(g^{-1}h)^m = g^{-m}h^m = e$ since G is abelian. □

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

Proposition 7.4

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

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

Proof:

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

  If $g \in G^{(m)}$ and $h \in G^{(n)}$, then $g^{an} = g^{an}g^{bm} = g^{an+bm} = g$, and similarly $h^{bm} = h^{an+bm} = h$, so $\phi\left(g^a h^b\right) = \left(g^{an}h^{bn}, g^{am}h^{bm}\right) = (g, h)$. Therefore, ϕ is surjective. Hence bijective. Now we want to show ϕ is a homomorphism:

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

  as required.

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

  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

  $$m = p_1^{b_1} \cdots p_k^{b_k} \text{ and } n = p_1^{c_1} \cdots p_k^{c_k}$$

  where for each i, $a_i = b_i + c_i$, and only one of b_i, c_i is non-zero.

Suppose $b_i > 0$. If $p_i \mid |G^{(n)}|$, then by Cauchy's theorem, $G^{(n)}$ has an element a of order p_i. We also know that $p_i \mid m$, this means $a \in G^{(m)}$, then $\phi(a) = (a^m, a^n) = (e, e) = e_{G^{(m)} \times G^{(m)}}$. Thus $a \in \ker \phi$. Since ϕ is injective, thus $a = e$, contradicting to the fact that a has order p_i. Thus $p_i \nmid |G^{(n)}|$.

We know that $p_i^{a_i} \mid |G| = |G^{(m)}| \cdot |G^{(n)}|$. Then we must have $p_i^{a_i} = p_i^{b_i} \mid |G^{(m)}|$.

Therefore, $m \mid |G^{(m)}|$. Similarly, $n \mid |G^{(n)}|$. So the only possibility is $|G^{(m)}| = m$ and $|G^{(n)}| = n$. □

Example: $\mathbb{Z}/mn\mathbb{Z}$

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

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

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

From Proposition 7.4, $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

Remark:

This example shows that a cyclic group can actually be a product of two cyclic groups.

Do we really need the assumption that $\gcd(m, n) = 1$? After all, we didn't use the assumption until the final step we apply the proposition. Actually, we do need $\gcd(m, n) = 1$. When $\gcd(m, n) > 1$, $G^{(m)}$ and $G^{(n)}$ intersect with each other, then ϕ here would not be injective, thus has a non-trivial kernel.

Corollary 7.5

Let G be a finite abelian group, and let $|G| = p_1^{a_1} \cdots p_k^{a_k}$, where $p_1, \ldots, p_k$ are distinct primes and $a_i > 0$ for all $1 \le i \le k$. 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 take $r = p_2^{a_2} \cdots p_k^{a_k}$.

Since $p_1^{a_1}$ and r are coprime and $p_1^{a_1} \cdot r = |G|$, Proposition 7.4 implies $G \cong G_1 \times G^{(r)}$, and that $|G_1| = p_1^{a_1}, |G^{(r)}| = r$.

We can continue to get $G^{(r)} = G_2 \times \cdots \times G_k$ with $|G_i| = p_i^{a_i}$. □

Proposition 7.6

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 $a_1, \ldots, a_k$ where every a_i is a prime power.

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

Proof:
By Corollary 7.5, can assume that 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, let $|x| = p^r$. Since G is abelian, $N = \langle x \rangle \trianglelefteq G$.

$|G/N| < |G|$, so by induction, $G/N = C_{b_1} \times \cdots \times C_{b_\ell}$ for some sequence $b_1, \ldots, b_\ell$ of prime powers. By Lagrange's theorem, $|C_{b_i}| \bigm| |G/N|$ and $|G/N| \bigm| |G|$, then we must have $b_i = p^{s_i}$ for some s_i.

For each $1 \leq i \leq \ell$, 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 $(e, \ldots, e, \tilde{y}_i, e, \ldots, e)$ (i.e., $\tilde{y}_i$ in the i-th position). The order of $y_i N$ in G/N is the same as $(e, \ldots, e, \tilde{y}_i, e, \ldots, e)$ in the product, and the same as $\tilde{y}_i$ in C_{b_i}, which is $b_i = p^{s_i}$. However, y_i in G is the element we pick to represent class $y_i N$, thus we could possibly have larger order of y_i in G.

Let $|y_i| = p^{t_i}$, and note that $r \geq t_i \geq s_i$ since the element x is of maximal order r.

Since $y_i N$ has order b_i, then $y_i^{b_i} \in N$, so $y_i^{b_i} = x^{c_i}$. Since $b_i = p^{s_i} \bigm| |y_i| = p^{t_i}$, then $|y^{b_i}| = p^{t_i}/p^{s_i} = p^{t_i - s_i}$. To have x^{c_i} of the order $p^{t_i - s_i}$, we must have
$c_i = d_i p^{r-(t_i - s_i)} = d_i p^{r - t_i + s_i}$.

Let $z_i = y_i x^{-d_i p^{r-t_i}}$. Since $x^{-d_i p^{r-t_i}} \in N$, then $z_i \in y_i N$, then $z_i N = y_i N$. Now

$$z_i^{b_i} = y_i^{b_i} x^{-d_i p^{r-t_i} \cdot p^{s_i}} = y_i^{b_i} x^{-d_i p^{r-t_i+s_i}} = x^{c_i} x^{-c_i} = e$$

The quotient map sends z_i to $y_i N$, thus $|z_i|$ can't be less than b_i. So $|z_i| = b_i$.

Let $H = \langle z - 1, \ldots, z_\ell \rangle \leq G$, and suppose $w \in H \cap N$. Then $w = z_1^{n_1} \cdots z_\ell^{n_\ell}$ for some $0 \leq n_1 < b_1, \ldots, 0 \leq n_\ell < b_\ell$.

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

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

But since $w \in N$, $q(w) = e$, then we must have $n_1 = n_2 = \ldots = n_\ell = 0$. Thus $w = e$, i.e., $H \cap N = \{e\}$.

Suppose $g \in G$. Then $gN \cong (\tilde{y}_i^{n_1}, \ldots, \tilde{y}_\ell^{n_\ell})$ for some $n_1, \ldots, n_\ell$. Then
$gN = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (z_1^{n_1} \cdots z_\ell^{n_\ell}) N$. In particular $g \in HN$. Thus every element in G is in HN, then $HN = G$.

Since G is abelian, $H, N \trianglelefteq G$. Then from the characterization of products, $G = N \times H$.

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

Remark:
We can show that H is isomorphic to G/N, and in particular, it has the same factorizations into prime power cyclic groups.

Theorem 7.7: Classification of finite abelian groups

If G is a finite abelian group, then $G \cong C_{a_1} \times C_{a_2} \times \cdots \times C_{a_k}$, where $a_1 \leq a_2 \leq \ldots, a_k$ is a sequence of prime powers.

Furthermore, if $G \cong C_{b_1} \times C_{b_2} \times \cdots \times C_{b_\ell}$, where $b_1 \leq b_2 \leq \cdots \leq b_\ell$ is another sequence of prime powers, then $k = \ell$ and $a_i = b_i$ for all $1 \leq i \leq k$.

Example:
$C_2 \times C_3 \cong C_6$, so the requirement that a_i be a prime-power is necessary 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 $p \neq q$ are distinct primes, then $C_{p^r}^{(q^s)} = \{e\}$. Otherwise $|C_{p^r}^{(p^s)}| = p^{\min(r,s)}$.

So

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

hence

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

So

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

For every r and p, we can recover ℓ and $b_1, \ldots, b_\ell$ from these numbers. Since the LHS doesn't depend on the choice of factorization at all, LHS is exactly the same number for both choices of factorization, then we can recover ℓ, k and a_i, b_i for $1 \leq i \leq k$. $\square$

7.3 Simple Groups

Every group G has at least two normal subgroups: $\{e\}$ and G.

simple

A group G is **simple** if it has no non-trivial proper normal subgroups.

As mentioned previously, simple groups can be thought as "building blocks" for other groups.

Example:
$\mathbb{Z}/p\mathbb{Z}$ is simple for all primes p.

S_n is not simple for $n \geq 3$, since $A_n \trianglelefteq S_n$.

Any p-group G of size $> p$ is not simple, since $Z(G) \neq \{e\}$ is normal (or if $Z(G) = G$, then G has a normal subgroup of order p).

We should see at least one example of a non-abelian simple group!

Theorem 7.8

A_5 is simple.

To solve this, we'll find the conjugacy classes of A_5.

First recall that $A_n = \ker(\operatorname{sgn} : S_n \to \mathbb{R}^\times : \sigma \mapsto \det(P_\sigma))$

If $\sigma = (1\ 2)$, then $P_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, so $\operatorname{sgn}(\sigma) = \det(P_\sigma) = -1 \implies \operatorname{sgn}(\sigma) = -1$. Also $[S_n : A_n] = 2$. And since $A_n \trianglelefteq S_n$,

$$\operatorname{Conj}_{S_n}(\sigma) \cap A_n \neq \varnothing \iff \operatorname{Conj}_{S_n}(\sigma) \subseteq A_n \iff \sigma \in A_n$$

Which conjugacy classes of A_5 are contained in A_5?

$\operatorname{Conj}_{S_5}(e)$: YES

$\operatorname{Conj}_{S_5}((1\ 2)) : \operatorname{sgn}((1\ 2)) = -1$ so NO

$\operatorname{Conj}_{S_5}((1\ 2)(3\ 4)) : \operatorname{sgn}((1\ 2)(3\ 4)) = \operatorname{sgn}((1\ 2))\operatorname{sgn}((3\ 4)) = 1$ so YES

$\operatorname{Conj}_{S_5}((1\ 2\ 3)) : (1\ 2\ 3) = (1\ 2)(2\ 3)$ so YES

$\operatorname{Conj}_{S_5}((1\ 2\ 3)(4\ 5)) :$ NO

$\operatorname{Conj}_{S_5}((1\ 2\ 3\ 4)) : (1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4)$ so NO

$\operatorname{Conj}_{S_5}((1\ 2\ 3\ 4\ 5)) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)$ so YES

Just because $\operatorname{Conj}_{S_5}(\sigma) \subseteq A_n$ doesn't necessarily mean that $\operatorname{Conj}_{S_5}(\sigma) = \operatorname{Conj}_{A_5}(\sigma)$.

Proposition 7.9

Suppose $\sigma \in A_n$.

(a) If $C_{S_n}(\sigma) \not\subseteq A_n$, then $\operatorname{Conj}_{S_n}(\sigma)$.

(b) If $C_{S_n}(\sigma) \subseteq A_n$, then there is $\sigma' \in \operatorname{Conj}_{S_n}(\sigma)$ such that $\operatorname{Conj}_{S_n}(\sigma) = \operatorname{Conj}_{A_n}(\sigma) \cup \operatorname{Conj}_{A_n}(\sigma')$.

Proof:
By second isomorphism theorem, $C_{S_n}(\sigma) \cap A_n \trianglelefteq A_n$, $A_n \trianglelefteq C_{S_n}(\sigma)A_n$ and $C_{S_n}(\sigma)/C_{S_n}(\sigma) \cap A_n \cong C_{S_n}(\sigma)A_n/A_n$.

$C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$ so

$$|C_{S_n}(\sigma)| \,/\, |C_{A_n}(\sigma)| = [C_{S_n}(\sigma)A_n : A_n] \implies |C_{A_n}(\sigma)| = |C_{S_n}(\sigma)| \,/\, [C_{S_n}(\sigma)A_n : A_n]$$

Since $[S_n : A_n] = 2$, if $C_{S_n}(\sigma) \nsubseteq A_n$ then $C_{S_n}(\sigma)A_n = S_n \implies |C_{A_n}(\sigma)| = |C_{A_n}(\sigma)|/2$ so

$$|\operatorname{Conj}_{A_n}(\sigma)| = |A_n|/|C_{A_n}(\sigma)| = (|S_n|/2)/(|C_{S_n}(\sigma)/2) = |\operatorname{Conj}_{S_n}(\sigma)|$$
$$\implies \operatorname{Conj}_{A_n}(\sigma) = \operatorname{Conj}_{S_n}(\sigma)$$

If $C_{S_n}(\sigma) \subseteq A_n$, then $C_{S_n}(\sigma)A_n = A_n \implies |C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|$. So

$$\operatorname{Conj}_{A_n}(\sigma) = |A_n|/|C_{A_n}(\sigma)| = (|S_n|/2)/|C_{S_n}(\sigma)| = |\operatorname{Conj}_{S_n}(\sigma)|/2$$

Choose $\sigma' \in \operatorname{Conj}_{S_n}(\sigma) \setminus \operatorname{Conj}_{A_n}(\sigma)$.

We've shown $|\operatorname{Conj}_{A_5}(\sigma')$ is either $|\operatorname{Conj}_{S_n}(\sigma)|$ or $|\operatorname{Conj}_{S_n}(\sigma)|/2$. Since $\operatorname{Conj}_{A_5}(\sigma') \neq \operatorname{Conj}_{S_n}(\sigma')$, must be the second one.

Conjugacy classes disjoint: $\operatorname{Conj}_{S_n}(\sigma) = \operatorname{Conj}_{A_5}(\sigma) \cup \operatorname{Conj}_{S_5}(\sigma')$. □

$\operatorname{Conj}_{A_5}(e) = \operatorname{Conj}_{S_n}(e) = \{e\}$: size 1.

$C_{S_n}((1\ 2)(3\ 4))$: $(1\ 2) \in C_{S_n}((1\ 2)(3\ 4))$ and $(1\ 2) \notin A_5$
so $\operatorname{Conj}_{A_5}((1\ 2)(3\ 4)) = \operatorname{Conj}_{S_5}((1\ 2)(3\ 4))$.
Cycle type has $\lambda_1 = 1, \lambda_2 = 2$ so $|\operatorname{Conj}_{S_n}((1\ 2)(3\ 4))| = 120/(2^2 \cdot 2!) = 15$.

$C_{S_n}(1\ 2\ 3)$: $(4\ 5) \in C_{S_n}((1\ 2\ 3))$ so $\operatorname{Conj}_{A_5}((1\ 2\ 3)) = \operatorname{Conj}_{S_r}((1\ 2\ 3))$
Cycle type is $\lambda_1 = 2, \lambda_3 = 1$, so $|\operatorname{Conj}_{S_5}((1\ 2\ 3))| = 120/6 = 20$

$C_{S_n}((1\ 2\ 3\ 4\ 5))$: Cycle type is $\lambda_5 = 1$ so $|C_{S_n}((1\ 2\ 3\ 4\ 5))| = 5$
$\implies C(S_n)((1\ 2\ 3\ 4\ 5)) = \langle(1\ 2\ 3\ 4\ 5)\rangle \subseteq A_5$. Splits into two conjugacy classes of size $120/5 \cdot 2 = 12$

Now we prove A_5 is simple.

Proof:
The order of A_5 is $120/2 = 60$.

The conjugacy classes of A_5 have sizes $1, 15, 20, 12, 12/$

If $H \trianglelefteq A_5$, then H must be a union of conjugacy classes $\operatorname{Conj}_{A_5}(\sigma)$. Mandatory that H contain $\{e\}$.

Since $|H| = 1+$ some sum of 15, 20, 12, and 12. Only numbers of this form dividing 60 are 1 and 60 itself. Thus no H must be trivial or equal to A_5. □

7.4 Semidirect products

automorphism

An **automorphism** of a group G is an isomorphism $\phi : G \to G$. The set of automorphisms $G \to G$ is denoted by $\mathrm{Aut}(G)$.

Example:

If $g \in G$, then $C_g : G \to G : h \mapsto ghg^{-1}$ is a homomorphism. $C_{g^{-1}}$ is an inverse to C_g, so C_g is an isomorphism for all $g \in G$.

If G is an abelian group, then $G \to G : g \mapsto g^{-1}$ is an automorphism.

Lemma 7.10

$\mathrm{Aut}(G)$ is a group under composition.

semidirect product

Let G and H be groups, and let $\phi : G \to \mathrm{Aut}(H)$ be a homomorphism. The **semidirect product** of G and H is the set $G \times H$, with binary operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, \phi(g_1)(h_1) h_2).$$

The semidirect product is denoted by $G \ltimes H$ or $G \ltimes_\phi H$.

The idea behind this definition is that

$$(g, e)(e, h)\left(g^{-1}, e\right) = (e, \phi(g)(h)),$$

i.e., conjugating by $g \in G$ is the automorphism $\phi(g)$ of H.

Proposition 7.11

$G \ltimes H$ is a group. Furthermore

- $G \times \{e\}$ is a subgroup of $G \ltimes H$.
- $\{e\} \times H$ is a normal subgroup of $G \ltimes H$.

Proof:
See textbook. $\square$

Theorem 7.12

Suppose G is a group, and H, N are subgroups of G such that

- $N \trianglelefteq G$,
- $H \cap N = \{e\}$, and
- $HN = G$.

Then $\phi : H \to \operatorname{Aut}(N) : h \mapsto C_h$ is a homomorphism, and $G \cong H \ltimes_\phi N$.

C_h refers to the conjugation automorphism of h on G. Since N is normal, C_g defines an automorphism of N for all $g \in G$.

Proof:
See textbook. □

7.5 Free Groups

How can we get more groups? Like the dihedral group D_{2n}, where we have generators s and r and relations $r^2 = e, s^n = e$, and $rs = s^{-1}r$ determining the group.

Maybe we could just write down some generators (e.g., x_1, x_2, s, t) and some relations on them (e.g., $st = x_1x_2x_1^{-1}, s^2 = e$) and just work with them as a group?

We could even have some special notations like $\langle x_1, x_2, s, t : st = x_1x_2x_1^{-1}, s^2 = e\rangle$ for this group.

Is this possible?

What would this look like if we didn't put any relations down? Let's say that our generators are $S = \{x_1, x_2, \ldots\}$. What would the group elements look like? We'd want to include things like $e, x_1, x_1^{-1}, \ldots, x_1x_2^2x_1^{-3}x_3^{-2}x_2^4, \ldots$. Multiplication should be easy: $(x_1x_2^4x_1)(x_2x_3x_1) = x_1x_2^4x_1x_2x_3x_1$.

word

A **(group) word** over a set S is a formal expression of the form $s_1^{a_1}s_2^{a_2}\cdots s_k^{a_k}$ where $k \geq 0, s_1, \ldots, s_k$ is a sequence in S (repetitions allowed) and $a_1, \ldots, a_k \in \mathbb{Z}$.

When $k = 0$, get **empty word** ϵ (also denoted by e).

The **concatenation** of two words $w_1 = s_1^{a_1}\cdots s_k^{a_k}$ and $w_2 = t_1^{b_1}\cdots t_\ell^{b_\ell}$ is

$$w_1w_2 = s_1^{a_1}\cdots s_k^{a_k}t_1^{b_1}\cdots t_\ell^{b_\ell}$$

A word like $x_1x_2^2x_2^{-3}x_3$ should be included, but should be equal to $x_1x_2^{-1}x_3$.

reduced

A word $s_1^{a_1} \cdots s_k^{a_k}$ is **reduced** if $s_i \neq s_{i+1}$ for all $1 \leq i \leq k-1$, and $a_i \neq 0$ for all $1 \leq i \leq n$.

equivalent

Two words w_1 and w_2 are **equivalent** if w_1 can be changed to w_2 by inserting or deleting s^0, replacing s^{a+b} with $s^a s^b$ for $a, b \in \mathbb{Z}$, or replacing $s^a s^b$ with s^{a+b} for $a, b \in \mathbb{Z}$.

Lemma 7.13

Every word is equivalent to a unique reduced word.

Example:

$x_1 x_2 x_2^{-1} x_1^{-1} x_1$ is equivalent to x_1.

free group

Let S be a set. The **free group** $\mathcal{F}(S)$ generated by S is the set of reduced words over S, with group operation $w_1 \cdot w_2 = r$, where r is the reduced word equivalent to the concatenation $w_1 w_2$.

Lemma 7.14

$\mathcal{F}(S)$ is a group, with identity ϵ.

Example:

The inverse of $x_1 x_2^2 x_1^7 x_3^{-4}$ would be $x_3^4 x_1^{-7} x_2^{-2} x_1^{-1}$.

Nice property: easy to describle homomorphisms $\mathcal{F}(S) \to G$.

Proposition 7.15: Universal property of free groups

If $\phi : S \to G$ is a function, then there is a unique group homomorphisms $\tilde{\phi} : \mathcal{F}(S) \to G$ with $\tilde{\phi}(s) = \phi(s)$ for all $s \in S$.

Proof:

If $w = s_1^{a_1} \cdots s_k^{a_k}$, define $\tilde{\phi}(w) = \phi(s_1)^{a_1} \cdots \phi(s_k)^{a_k}$. It's not hard to see this is a group homomorphism. Clearly this is the only morphism with $\tilde{\phi}(s) = \phi(s)$ for all $s \in S$. $\square$

Example:

Let $A, B \in \mathrm{GL}_n \mathbb{K}$. Then there is a homomorphism $\mathcal{F}(\{a, b\}) \to \mathrm{GL}_n \mathbb{K}$ sending $a \mapsto A$ and $b \mapsto B$. This homomorphism sends $aba^{-1} \mapsto ABA^{-1}$, etc.

7.6 Group presentations

normal subgroup generated by S

Let G be a group, and let $S \subseteq G$. Then **normal subgroup generated by** S is the intersection

$$\bigcap_{S \subseteq N \trianglelefteq G} N$$

If K is the normal subgroup generated by S, then $K \trianglelefteq G$.

group presentation

Let S be a set, and let $R \subseteq \mathcal{F}(S)$. The **group presentation** $\langle S : R \rangle$ denotes the group $\mathcal{F}(S)/K$, where K is the normal subgroup of $\mathcal{F}(S)$ generated by R.

Idea: pick generators, then pick elements of $\mathcal{F}(S)$ to set to zero.

> Example:
> $G = \langle x, y : xyx^{-1}y^{-2} \rangle$.
>
> This group is $\mathcal{F}(\{x, y\})/K$, where K is normal subgroup generated by $xyx^{-1}y^{-2}$. Since $xyx^{-1}y^{-2} \in K$, $[xyx^{-1}y^{-2}] = e$ in G. This means that $[x][y][x]^{-1} = [y]^2$ in G.

We use the following conventions for group presentations:

- If $S_1, \ldots, s_k \in S, s_1, \ldots, a_k \in \mathbb{Z}$, then $[s_1]^{a_1}[s_2]^{a_2} \cdots [s_k]^{a_k} \in \langle S : R \rangle$ is just denoted by $s_1^{a_1} \cdots s_k^{a_k}$. (In the previous example, we'd just say $xyx^{-1} = y^2 \in G$.)
- We can write $w_1 = w_2$ instead of $w_1 w_2^{-1}$, for instance. We can also drop the curly braces on sets.

  For instance, $\langle s, r : s^n = r^2 = e, rs = s^{-1}r \rangle$ means $\langle \{s, r\} : \{s^n r^2, rsr^{-1}s\} \rangle$.
- If $G \cong \langle S : R \rangle$, then $\langle S : R \rangle$ is called a **presentation** of G. Presentations are not unique.

  The sets S and R don't have to be finite, so every group G has a representation

$$\langle \underline{g}, g \in G : \underline{g} \cdot \underline{h} = \underline{gh}, \underline{e_G} = \epsilon \rangle$$

finite presentable

A presentation $\langle S : R \rangle$ is **finite** if both S and R are finite sets. A group G is **finite presentable** if $G \cong \langle S : R \rangle$ for some finite presentation $\langle S : R \rangle$.

For example, D_{2n} is finitely presentable: $D_{2n} \cong \langle r, s : s^n = e, r^2 = e, rs = s^{-1}r \rangle$. Actually, all finite groups are finitely presentable.

Theorem 7.16: Universal property of finitely presented groups

Let $G = \langle S : R \rangle$ and let H be a group. If $\phi : S \to H$ is a function such that $\phi(s_1)^{a_1} \cdots \phi(s_k)^{a_k} = e$ for all $s_1^{a_1} \cdots s_k^{a_k} \in R$, then there is a unique homomorphism $\tilde{\phi} : G \to H$ such that $\tilde{\phi}(s) = \phi(s)$ for all $s \in S$.

Proof:
Let $\psi : \mathcal{F}(S) \to H$ be the morphism with $\psi(s) = \phi(s)$ for all $s \in S$. Let K be normal subgroup generated by R in $\mathcal{F}(S)$.

If $r = s_1^{a_1} \cdots s_k^{a_k} \in R$, then $\psi(r) = \phi(s_1)^{a_1} \cdots \phi(s_k)^{a_k} = e$, so

$$r \in \ker \psi \implies R \subseteq \ker \phi \implies K \subseteq \ker \phi$$

Let $q : \mathcal{F}(S) \to \mathcal{F}(S)/K$ be quotient map. By universal property of quotients, there is $\tilde{\phi} : \mathcal{F}(S)/K \to H$ with $\psi = \tilde{\phi} \circ q$. But then $\tilde{\phi}(s) = \tilde{\phi}([s]) = \psi(s) = \phi(s)$. □

Why are finitely presented groups important?

Consider the following problem: given $S, R \subseteq \mathcal{F}(S)$, and $w \in \mathcal{F}(S)$, determine if $[w] = e$ in $\langle S : R \rangle$.

Often we fix S and R, in which case this is called the **word problem** for $\langle S : R \rangle$.

Theorem 7.17

There is a finite presentation $\langle S : R \rangle$ for which the word problem is undecidable.

Remark:
It's beyond the scope of the course to define undecidable, but see a course on computability.

Another problem: given finite S and $R \subseteq \mathcal{F}(S)$, determine if $\langle S : R \rangle$ is the trivial group.

This is a special case of the **isomorphism problem**: given finite S_1, S_2 and $R_1 \subseteq \mathcal{F}(S_1)$ and $R_2 \subseteq \mathcal{F}(S_2)$, determine if $\langle S_1 : R_1 \rangle$ and $\langle S_2 : R_2 \rangle$ are isomorphic.

Theorem 7.18

The problem of determining whether $\langle S : R \rangle$ is trivial for finite S and R is undecidable.

The message is that many natural problems for groups cannot be solved in general.

Part II:

Ring Theory

The theory of groups is concerned with general properties of certain objects having an algebraic structure defined by a single binary operation. The study of rings is concerned with objects possessing two binary operations (called addition and multiplication) related by the distributive laws.

Abstract Algebra, Third Edition

8 Introduction to Rings

week 7

8.1 An intro

As we learn about mathematics, we learn about different notions of numbers:

$$\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \text{Functions} \to \text{Polynomials} \to \mathbb{C} \to M_n\mathbb{R} \to \mathbb{Z}/n\mathbb{Z}$$

All of these sets have two operations: addition $+$ and multiplication $\cdot$.

Rings are abstract structure designed to capture what all these examples have in common.

ring

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

(a) $(R, +)$ is an abelian group, and

(b) $\cdot$ is an associative binary operation on R such that

$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ and } a \cdot (b + c) = a \cdot b + a \cdot c$$

This last condition is called the **distributive property**.

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

commutative ring

A ring is **commutative** if $\cdot$ is commutative, i.e., if $a \cdot b = b \cdot a$ for all $a, b \in R$.

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 $\mathrm{Fun}(X, R)$ 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.

If R is a ring, and $n \geq 1$, then the set of $n \times n$ matrices $M_n R$ with coefficients in R is a ring under the usual matrix operations.

If $\circ : M_n\mathbb{C} \times M_n\mathbb{C} \to M_n\mathbb{C} : (A, B) \to \frac{AB+BA}{2}$ then $(M_n\mathbb{C}, +, \circ)$ is not ring, since $\circ$ is not associative.

As with groups, we usually refer to a ring $(R, +, \cdot)$ as R when the operations are clear.

We always use additive notation for the group $(R, +)$, and almost always use $+$ for the symbol. (Sometimes $\oplus$ is used, for instance for $\mathbb{Z}/2\mathbb{Z}$. XOR in computer science.)

In particular, denote identity of $(R, +)$ by 0 and inverse of $x \in R$ with respect to $+$ by $-x$.

Some variation in notation is permitted for multiplication (you might see $\cdot$ or $\times$ or $\otimes$ or $\boxtimes$, etc)

But typically just denote multiplication of a and b by ab.

Proposition 8.1

If R is a ring, then

(a) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

(b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ for all $a, b \in R$

(c) $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in R$.

Proof:

(a) $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 \cdot a = 0$. Similarly, $a \cdot 0$.

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

(c) $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. $\square$

Recall that an **identity** for a binary operation $\cdot$ on a set R is an element 1 such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$. Also, if an identity exists, it is unique.

ring with identity

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

Note
In this course, **ring** means **ring with identity** unless otherwise noted.

This assumption is common outside this course as well. If a ring doesn't have an identity, we can call it a **ring without an identity**, or a **ring not necessarily having an identity**.

The term **rng** is sometimes used for rings without identity, since it's a ring without an i.

Fitting our assumption, all the examples of rings mentioned so far are rings with identities.

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

Notation: Use 1 to denote identity in ring R.

When we talk about subrings, we'll give some examples of rings without identity.

Proposition 8.2

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

Proof:
$0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$ □

8.2 Fields and units

unit

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

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}.

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

Example:
$\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$

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

The smallest possible ring is $R = \{0\}$, with multiplication $0 \cdot 0 = 0$. This is a ring with identity $1 = 0$. 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 that holds only for the trivial ring:

Lemma 8.3

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 $x \in R$. □

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

division ring

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

field

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

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. Recall: if $\alpha = a + bi \in \mathbb{C}$, then $\alpha\overline{\alpha} = |\alpha|^2 = a^2 + b^2$, and $|\alpha| = 0$ if and only if $\alpha = 0$, so if $\alpha \neq 0$, then $\alpha^{-1} = \overline{\alpha}/|\alpha|^2$.

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

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

Lemma 8.4

$[x]$ 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 $b \in \mathbb{Z}$ implies $\gcd(x, n) = 1$. □

Corollary 8.5

$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

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

Theorem 8.6: Wedderburn

Any finite division ring is a field.

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 $1, i, j$ and k, and set $i^2 = j^2 = k^2 = -1$, and $ijk = -1$.

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

Note

Rings with identity are also called **unital rings**.

Rings without identity can be called **non-unital rings**.

This term is a little more compact than "ring with identity" and works a lot better when we start talking about subrings and homomorphisms.

Later in this course, rings will mean unital rings by default. Textbook uses the opposite: by default rings will mean non-unital rings.

8.3 Subrings

subring

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

(a) S is a subgroup of $(R, +)$,

(b) if $a, b \in S$, then $ab \in S$, and

(c) $1 \in S$.

Lemma 8.7

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

Example: Subrings

$\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$, which is a subring of the quaternions Q.

The ring $\mathbb{R}[x]$ of polynomial functions with coefficients in $\mathbb{R}$ is a subring of $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$.

$M_n\mathbb{Z}$ is a subring of $M_n\mathbb{R}$.

Example: Not subrings

$\mathbb{Q}^\times$ is not a subring of $\mathbb{Q}$.

$\mathrm{span}\{1, x\}$ is not a subring of $\mathbb{R}[x]$, since it is not closed under multiplication.

$2\mathbb{Z}$ is not a subring of $\mathbb{Z}$ since $1 \notin \mathbb{Z}$.

$\{0\}$ is not a subring of any non-trivial ring R. (a) and (b) are satisfied. (c) is not satisfied since $\{0\}$ doesn't contain the identity of R.

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

Alternative for non-unital rings

Let R be a non-necessarily-unital ring. A subset $S \subseteq R$ is a **subring** if

(a) S is a subgroup of $(R, +)$, and

(b) if $a, b \in S$, then $ab \in S$.

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

(c) $1 \in S$,

then S is said to be a **unital subring**.

In this course, ring = unital ring and subring = unital subring. We'll call sets satisfying (a) and (b) "non-unital subrings".

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

Example: Real polynomials

Let $R = \mathbb{R}[x]$, the ring of polynomials with coefficients in $\mathbb{R}$.

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

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

Exercise: check that $(x\mathbb{R}[x], +, \cdot)$ is a non-unital ring where it doesn't have an identity element at all.

Example: $\operatorname{Fun}(\mathbb{R}, \mathbb{R})$

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

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

0 is compactly supported. Suppose $f, g : \mathbb{R} \to \mathbb{R}$ are compactly supported. Can choose $a < b$ such that $f(x) = g(x) = 0$ for $x \notin [a, b]$ (here we can choose minimum of two left endpoints and maximum of two right endpoints). Then $(f - g)(x) = (fg)(x) = 0$ for $x \notin [a, b]$, so $f - g$ and $f \cdot g$ are compactly supported.

Identity in $\operatorname{Fun}(\mathbb{R}, \mathbb{R})$ is constant function 1, not compactly supported.

So compactly supported functions are a non-unital subring.

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

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

Suppose $x \in R$, where R is a (unital) ring, and $n \in \mathbb{Z}$. Since $(R,+)$ is an abelian group, nx is well-defined (from additive notation). Take $x = 1$, then can think of n as the element $n1 \in R$, in the sense that if $x \in R$, 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 8.8

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:
Idea: If $n \geq 0$, then $n1 \cdot x = (1 + 1 + \ldots + 1) \cdot x = nx$ □

8.4 Characteristic and prime subring

Lemma 8.9

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
$k = \min\{m \in \mathbb{Z} : m1 = 0\}$, (or $k = 0$ is this set is empty).

prime subring

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

Example:
$\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$.

$\mathrm{char}(\mathbb{Z}) = 0$.

$\mathrm{char}(R) = 1$ if and only if $R = \{0\}$.

Lemma 8.9

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
$k = \min\{m \in \mathbb{N} : m1 = 0\} \cup \{0\}$.

Proof:
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 $k = 0$. (k is equal to the order of 1 or 0 if the order is infinity).

If $n, m \in \mathbb{Z}$, then $n1 \cdot m1 = nm1 \in R_0$. And $1 \in R_0$, so R_0 is a unital subring.

If S is a unital subring of R, then $1 \in S$, and $S \leq (R, +)$, so S contains cyclic subgroup R_0 generated by 1. □

centre of R

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

Lemma 8.10

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

Proof:
Exercise. □

Corollary 8.11

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

Proof:
$Z(R)$ contains prime subring R_0. □

8.5 Homomorphisms

homomorphism

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

1. $\phi : (R, +) \to (S, +)$ 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 are satisfied, but 3 is not, then ϕ is a **non-unital homomorphism**.

Note
In this class, homomorphism = unital homomorphism. Textbook uses non-unital homomorphism as default.

Example:
If S is a subring of R, then $i : S \to R : x \mapsto x$ is a homomorphism.

The quotient maps $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x \mapsto [x]$ and $\mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} : [x] \mapsto [x]$ are homomorphisms since $[xy] = [x] \cdot [y]$.

isomorphism

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

Proposition 8.12

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

Proof:
We already showed that ϕ is a well-defined group isomorphism. So ϕ is bijective.

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

$$\begin{aligned}
\phi([a] \cdot [b]) &= \phi([ab]) \\
&= ab1 \\
&= a(b1) && \text{Here is abelian group operation} \\
&= (a1) \cdot (b1) && \text{Here } \cdot \text{ is ring operation} \\
&= \phi([a]) \cdot \phi([b]) && \text{Here } \cdot \text{ is ring operation}
\end{aligned}$$

Since $\phi([1]) = 1$, thus unital, then ϕ is a homomorphism. Thus ϕ is a ring isomorphism. $\square$

Proposition 8.13

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

(a) If $a \in R$ and $n \geq 0$, then $\phi(a^n) = \phi(a)^n$.

(b) If $u \in R^\times$, then $\phi(u) \in S^\times$, and $\phi(u^n) = \phi(u)^n$ for all $n \in \mathbb{Z}$.

(c) If ϕ is an isomorphism, then ϕ^{-1} is a ring homomorphism.

Proof:

(a) Standard proof by induction. Starting from $n = 2$.

(b) We know $1 = \phi(1) = \phi(uu^{-1}) = \phi(u)\phi(u^{-1})$, so $\phi(u) \in S^\times$ and $\phi(u^{-1}) = \phi(u)^{-1}$. It follows from (a) that $\phi(u^n) = \phi(u)^n$ for all $n \in \mathbb{Z}$.

(c) We already know ϕ^{-1} is a group homomorphism. $\phi(1_R) = 1_S \implies \phi^{-1}(1_S) = 1_R$. And if $a, b \in S$, then $a = \phi(\phi^{-1}(a)), b = \phi(\phi^{-1}(b))$, so

$$ab = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = \phi(\phi^{-1}(a)\phi^{-1}(b)) \implies \phi^{-1}(ab) = \phi^{-1}\phi^{-1}(b)$$

Thus ϕ^{-1} is a homomorphism. □

Proposition 8.14

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

(a) $\operatorname{Im}\phi$ is a subring of S.

(b) $\ker\phi$ is a non-unital subring of R.

Note
Here $\operatorname{Im}\phi$ and $\ker\phi$ are the group theory image and kernel.

Proof:
Proof of (a): We already know that $\operatorname{Im}\phi$ is a subgroup of $(S, +)$.

Since $\phi(1_R) = 1_S, 1_S \in \operatorname{Im}\phi$. Finally, if $a, b \in \operatorname{Im}\phi$, then $a = \phi(x), b = \phi(y)$, $x, y \in R$ and $ab = \phi(x)\phi(y) = \phi(xy) \in \operatorname{Im}\phi$. □

Remark:
If $1 \in \ker\phi$ and ϕ is unital, then $1_S = \phi(1_R) = 0_S$, so S must be zero ring, contradicting to our assumption S is not zero. Thus $\ker\phi$ must be non-unital. What we are going to see later is that $\ker\phi$ is a special type of non-unital subring, called ideal. We'll do this properly when we do ideals.

8.6 Polynomials

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 $a_0 \ldots, a_n \in R$.

Addition and multiplication are defined as usual, so

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

where $a_i = b_j = 0$ for $i > n, j > m$.

As usual, we can talk about degree, monomials, evaluation, etc. *how do we formalize all this?*

$R[x]$ and binary operations

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

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

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

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

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

The choice of variable matters only in that we let $\sum_{i=0}^{n} a_i x^i$ denote $(a_0, \ldots, a_n, 0, 0, \ldots)$ (note: not a unique representation). If we change the variable then we change this notation.

Lemma 8.15

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

Proof:
Need to show that $+$ and $\cdot$ are well-defined.

Let $(a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty} \in R[x]$. Then there are $N_1, N_2 \geq 0$ be such that $a_i = 0$ for $i \geq N_1$, $b_j = 0$ for $j \geq N_2$. Then $a_i + b_i = 0$ 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 $0 \leq i < N_1$, then $k - i > N_2$. So $\sum_{i=0}^{k} a_i b_{k-i} = 0$ if $k \geq N_1 + N_2$, which implies $(a_i)_{i=0}^{\infty} \cdot (b_i)_{i=0}^{\infty} \in R[x]$.

Then it's not hard to see $(R[x], +)$ is an abelian group with $0 = (0, 0, \ldots)$.

Next want to show that $\cdot$ is associative. Suppose that $(a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty}, (c_i)_{i=0}^{\infty} \in R[x]$.

Let $(a_i)_{i=0}^{\infty} \cdot \left((b_j)_{i=0}^{\infty} \cdot (c_k)_{i=0}^{\infty}\right) = (d_n)_{n=0}^{\infty}$. Then

$$d_n = \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{n-i-j} \right) = \sum_{i+j+k=n} a_i b_j c_k = \sum_{\ell=0}^{n} \left(\sum_{i=0}^{\ell} a_i b_{\ell-i} \right) c_{n-\ell}$$

From this, we see that $(d_n)_{n=0}^{\infty} = \left((a_i)_{i=0}^{\infty} \cdot (b_j)_{i=0}^{\infty}\right) \cdot (c_k)_{i=0}^{\infty}$. So $\cdot$ is associative.

It's not hard to show $1 = (1, 0, 0, \ldots)$ is an identity for $\cdot$

For distributivity, suppose $(a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty}, (c_i)_{i=0}^{\infty} \in R[x]$ again,
let $(d_n)_{n=0}^{\infty} = (a_i)_{i=0}^{\infty} \cdot ((b_i)_{i=0}^{\infty} + (c_i)_{i=0}^{\infty})$. Then

$$d_n = \sum_{i=0}^{n} a_i \cdot (b_{n-i} + c_{n-i}) = \sum_{i=0}^{n} a_i b_{n-i} + \sum_{i=0}^{n} a_i c_{n-i}$$

so $(d_n)_{n=0}^{\infty} = (a_i)_{i=0}^{\infty} \cdot (b_i)_{i=0}^{\infty} + (a_i)_{i=0}^{\infty} \cdot (c_i)_{i=0}^{\infty}$. Similarly we can show right distributivity.

Therefore, $R[x]$ is a ring. $\square$

$R[x]$ is called **the ring of polynomials in variable x with coefficients in R.**

x is referred to as the variable or indeterminate. Can use any variable we want, e.g., $R[x], R[y], R[\pi]$.

We only use $(a_i)_{i=0}^{\infty}$ to denote elements of $R[x]$ when we are defining or proving something formally.

Use $\sum_{i=0}^{n} a_i x^i$ when working with $R[x]$. If we don't want to specify coefficients, denote elements of $R[x]$ by p or $p(x)$.

We can show that there is an isomorphism $R[x] \cong R[y] : p(x) \mapsto p(y)$ (this works with x and y replaced by any pair of variables).

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. The degree is denoted by $\deg(p)$.

Example:

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

coefficient

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

monomial

A **monomial** is a polynomial of the form x^i for some $i \geq 0$.

term

A polynomial of the form $a_i x^i$ is called a **term**.

leading term/coefficient

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

Polynomials of degree ≤ 0 are called **constant polynomials**. There is a constant polynomial $ax^0 \in R[x]$ for every $a \in R$. Usually just denote this polynomial by a.

Lemma 8.16

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

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

Lemma 8.17

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

Proof:

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

□

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

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 8.18

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

This homomorphism is called **evaluation** at c or **substitution** at c. When necessary, we will denote it by ev_c. Note that ev_c being a homomorphism means that

$$(p+q)(c) = \mathrm{ev}_c(p+q) = \mathrm{ev}_c(p) + \mathrm{ev}_c(q) = p(c) + q(c)$$

and similarly that $(p \cdot q)(c) = p(c)q(c)$ and $1(c) = 1$.

Proof:

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

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

Finally $1(c) = 1c^0 = 1$ as desired. □

Most common type of polynomial rings are $\mathbb{K}(x)$, $\mathbb{K}$ a field.

Proposition 8.19

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

(a) $\deg(fg) = \deg(f) + \deg(g)$ for all $f, g \in \mathbb{K}[x]$

(b) $\mathbb{K}[x]^\times = \mathbb{K}^\times$

Example:
$\deg(0 \cdot f) = -\infty = -\infty + \deg(f) = \deg(0) + \deg(f)$ which explains why we set $\deg(0) = -\infty$.

Example: Not a field...
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.

8.7 Multivariable polynomials

multivariable polynomial ring

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

Elements of $R[x_1, \ldots, x_n]$ are technically of the form $\sum_i a_i(x_1, \ldots, x_{n-1})x_n^i$, where $a_i \in R[x_1, \ldots, x_{n-1}]$, but usually we write these elements as $\sum_{i=(i_1,\ldots,i_n)} a_i x^i$, where $x^i := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$.

Example:
A typical element of $R[x_1, x_2]$ is $x_1x_2^2 - 7x_1^2x_2^2 + 3x_1^5x_2 + 2$.

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

Lemma 8.20

Let R be a ring, $x_1, \ldots, x_n$ a sequence of variables, $\sigma \in S_n$. Then there is an isomorphism $R[x_{\sigma(1)}, \ldots, x_{\sigma(n)}] \to R[x_1, \ldots, x_n]$ sending

$$\sum_{(i_1,i_2,\ldots,i_n)} a_i x_{\sigma(1)}^{i_1} x_{\sigma(2)}^{i_2} \ldots x_{\sigma(n)}^{i_n} \mapsto \sum_{i_1,i_2,\ldots,i_n} a_i x_1^{i_{\sigma^{-1}(1)}} x_2^{i_{\sigma^{-1}(2)}} \ldots x_n^{i_{\sigma^{-1}(n)}}$$

Example:

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

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

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

multivariate evaluation

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

Lemma 8.21

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

$$\mathrm{ev}_c : R[x_1, \ldots, x_n] \to R : p(x_1, \ldots, x_n) \mapsto p(c_1, \ldots, c_n)$$

is the composition

$$\begin{aligned} \mathrm{ev}_{c_1} \circ \mathrm{ev}_{c_2} \circ \cdots \mathrm{ev}_{c_n} : R[x_1, \ldots, x_{n-1}][x_n] &\to R[x_1, \ldots, x_{n-1}] \\ &= R[x_1, \ldots, x_{n-2}][x_{n-1}] \to \cdots \to R[x_1] \to R \end{aligned}$$

and hence is a homomorphism if R is commutative.

8.8 Group rings

group ring

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

$$\left\{ \sum_{g\in G} c_g \cdot g : \begin{array}{l} (c_g)_{g\in G} \subseteq R \text{ such that there is a finite} \\ \text{subset } X \subset G \text{ with } c_g = 0 \text{ for all } g \notin X \end{array} \right\}$$

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

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

What's a formal sum?

A formal sum $\sum_{g\in G} a_g g$ with coefficients in R is a fancy way of writing a finitely supported function $G \to R : g \mapsto a_g$

Finitely supported: 0 except at finitely many points of G

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

Example:
$R = \mathbb{Z}, G = D_6 = \{e, r, s, sr, s^2, s^2 r\}$.

Here are some examples of elements of $\mathbb{Z}D_6$

$$\begin{gathered} 1e + 7s - 2r + sr - s^2 r \\ 2e + 2s + 2s^2 \\ r \\ e \end{gathered}$$

General element of RD_6 is

$$a_e e + a_r r + a_s s + a_{sr} sr + a_{s^2} s^2 + a_{s^2 r} s^2 r$$

where $a_e, a_r, a_s, a_{sr}, a_{s^2}, a_{s^2 r} \in R$.

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

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

Sometimes write $\underline{g}$ for g considered as an element of RG (this helps emphasize the difference)

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

$$3 \cdot \underline{0} - 2 \cdot \underline{1} + 5 \cdot \underline{10} - 6 \cdot \underline{-6}$$
$$\underline{1} + \underline{2} + \underline{3}$$
$$\underline{0}$$

Note: $\underline{0}$ is not equal to $0 = 0 \cdot \underline{0} + 0 \cdot \underline{1} + \dots$

What are the ring operations?

Use component-wise addition:

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

For multiplication, use principle that $\underline{g} \cdot \underline{h} = \underline{gh}$

Extend to RG so distributivity holds:

Example: $\mathbb{Z}D_6$
In $\mathbb{Z}D_6$ again, $s \cdot (e + 2s + 3r + 4s^2 r) = s + 2s^2 + 3sr + 4r$.

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

$(e - r)^2 = (e - r)(e - r) = e - r - r + r^2 = 2e - 2r = 2(e - r)$

Example: $\mathbb{Z}\mathbb{Z}$
$(\underline{0} + 2 \cdot \underline{-6})(3 \cdot \underline{1} - 4 \cdot \underline{2}) = 3 \cdot \underline{1} - 4 \cdot \underline{2} + 6 \cdot \underline{-5} - 8 \cdot \underline{-4}$

Note that $\underline{0} \cdot \underline{1} = \underline{0 + 1} = \underline{1}$

Proposition 8.22

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 example of noncommutative (more accurately, not-necessarily-commutative) rings. However, since we're focusing on commutative rings in this course, 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 right identity is similar.

Remainder of proof reduces to fact that $\cdot$ is associative.

Proposition 8.23

Let R be a ring, and $\phi : G \to H$ be a group homomorphism. Then $\psi : RG \to RH$ 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:
It's not hard to check well-definedness ($\sum_{g:\phi(g)=h} a_g$ 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 ψ is unital.

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

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

and

$$\begin{aligned}
\psi(xy) &= \psi\left(\sum_{g,h} a_g b_h \underline{gh}\right) \\
&= \sum_{g,h} a_g b_h \underline{\phi(gh)} \\
&= \sum_{g,h} a_g b_h \underline{\phi(g)\phi(h)} \\
&= \left(\sum_{g} a_g \underline{\phi(g)}\right)\left(\sum_{h} a_h \underline{\phi(h)}\right) \\
&= \psi(x)\psi(y)
\end{aligned}$$

So ψ is a homomorphism. □

9

Ideals and Quotient Rings

9.1 Ideals

week 8

Recall Proposition 8.14, in this section, we will learn what an ideal is. Starting point: what's special about kernels?

Lemma 9.1

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

Proof:
$\phi(rm) = \phi(r)\phi(m) = \phi(r) \cdot 0_S = 0 = \phi(mr)$. □

ideal

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

Lemma 9.1 shows that the kernel of a homomorphism is an ideal.

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

Example: $m\mathbb{Z}$

Lemma 9.2

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

Proof:
Already know that $m\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. If $r \in \mathbb{Z}$, and $km \in m\mathbb{Z}$, then $rkm \in m\mathbb{Z}$. So $m\mathbb{Z}$ is an ideal. □

Intuition: if $m \mid x$, then $m \mid rx$ for all $r \in \mathbb{Z}$.

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

Exercise

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

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

(a) $\mathcal{I}$ contains 0,

(b) $\mathcal{I}$ is closed under addition, and

(c) $\mathcal{I}$ is closed under negation (additive inverses).

Of course, can speed this checking that

(a') $\mathcal{I}$ is non-empty, and

(b') $f, g \in \mathcal{I} \implies f - g \in \mathcal{I}$.

The ideal condition can speed up this check in a different way.

Lemma 9.3

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

(a) $\mathcal{I}$ is non-empty,

(b) if $r \in R, f, g, \in \mathcal{I}$, then $rf + g, fr + g \in \mathcal{I}$.

Proof:

If $f, g \in \mathcal{I}$, since $-1 \in R$, then $(-1) \cdot g + f = f - g \in \mathcal{I}$, so (a'), (b') satisfied. Thus $\mathcal{I}$ is a subgroup of $(R, +)$.

Since $\mathcal{I}$ is a subgroup of $(R, +)$, $0 \in \mathcal{I}$. If $m \in \mathcal{I}, r \in R$, then $rm = rm + 0 \in \mathcal{I}$. So $\mathcal{I}$ is an ideal. □

Example: evaluation

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

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

By Lemma 9.3, it's an ideal, but let's doublecheck:

- $0 \in \mathcal{I}$, 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 $rf + g \in \mathcal{I}$.

What do elements of this ideal look like?

Example: evaluation cont'd

Let's first look at the case $c = 0$.

Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$. Then $f(0) = \sum_i a_i 0^i = a_0$, so $f(0) = 0 \iff a_0 = 0$. [a]

So elements of $\mathcal{I} = \ker \mathrm{ev}_0$ look like $a_1 x + a_2 x^2 + \ldots$

Because $a_1 x + a_2 x^2 + \ldots = x(a_1 + a_2 x + \ldots)$, 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.

[a] as far as evaluation of polynomials is concerned, $0^0 := 1$.

Then what about evaluation for general c?

Lemma 9.4

If $f(x) \in R[x]$ has degree $\leq n$, and $c \in R$, then there are $a_0, \ldots, a_n \in R$ 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 $\leq n-1$.

By induction, $f(x) - a_n(x-c)^n = \sum_{i=0}^{n-1} a_i (x-c)^i$. □

Because evaluation is a homomorphism,

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

So if $f(x) = \sum_{i=0}^{n} a_i (x-c)^i$, then $f(c) = a_0$. $f(c) = 0 \iff a_0 = 0$.

Conclusion: $\ker \mathrm{ev}_c = (x-c)R[x] = (x-c)$.

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

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

Lemma 9.5

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

Proof:
If $r \in R$, $1 \in \mathcal{I}$, then $r = r \cdot 1 \in \mathcal{I}$. $\square$

We typically want to look at **proper ideals**, i.e., ideals $\mathcal{I}$ with $\mathcal{I} \subsetneq R$.

9.2 Ideals in fields

From Lemma 9.5, we have the corollary:

Corollary 9.6

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

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

Corollary 9.7

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

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 that R is non-zero, $\ker \phi = (0)$. Then we know from group theory that ϕ 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.

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

9.3 Quotient rings

Recall that in group theory: Kernels of homomorphisms are normal subgroups, and normal subgroups are kernels of homomorphisms, since if $N \trianglelefteq G$, the quotient map $G \to G/N$ 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 $x - y \in N$.
- Group operation is $[x] + [y] = [x + y]$.

- Quotient map $G \to G/N$ sends $x \in G$ to $[x]$.

Are ideals always the kernel of some homomorphism?

In ring theory, kernels of homomorphisms 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 quotient group $R/\mathcal{I}$ exists.

Why not try to put a ring structure on $R/\mathcal{I}$?

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

Theorem 9.8

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, and furthermore, the quotient map $q : R \to R/\mathcal{I} : x \mapsto [x]$ 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 **quotient ring**.

Corollary 9.9

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 definition of $\mathbb{Z}/m\mathbb{Z}$.

Proof:

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

First, let's show that $\cdot$ is <u>well-defined</u>.

Suppose $[x] = [x'], [y] = [y']$ for $x, x', y, y' \in R$. We want to show that $[xy] = [x'y']$, or equivalently $xy - x'y' \in \mathcal{I}$.

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y')$$

Since $[x] = [x'], [y] = [y']$, we know $x - x', y - y' \in \mathcal{I}$. By ideal property, $(x - x')y, x'(y - y') \in \mathcal{I}$, so $xy - x'y' \in I$.

Conclusion: $[x] \cdot [y] = [xy]$ is a well-defined binary operation.

<u>Associativity</u>: suppose $x, y, z \in R$. Then $[x] \cdot ([y] \cdot [z]) = [z] \cdot [yz] = [xyz] = ([x] \cdot [y]) \cdot [z]$.

<u>Identity</u>: $[1] \cdot [x] = [1 \cdot x] = [x] = [x] \cdot [1]$, so $[1]$ is an identity for $\cdot$

Distributivity: If $x, y, z \in R$, then

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

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

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

q is a homomorphism: 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. □

9.4 The universal property of quotient rings

Recall universal property of quotient groups (Theorem 5.4). Now extend the universal property to rings.

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

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "q"'] & & S \\ & R/\mathcal{I} \arrow[ur, dashed, "\psi?"'] & \end{tikzcd}$$

Is ψ a ring homomorphism?

Lemma 9.10

Let R, S, T be rings. Suppose $\psi_1 : R \to T$ is a ring homomorphism, and $\psi_2 : T \to S$ is a group homomorphism, such that $\psi_2 \circ \psi_1$ is a ring homomorphism. If ψ_1 is surjective, then ψ_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 $\psi_1(a) = x, \psi_1(b) = y$. Then

$$\begin{aligned}
\psi_2(xy) &= \psi_2(\psi_1(a)\psi_1(b)) \\
&= \psi_2(\psi_1(ab)) \\
&= \phi(ab) \\
&= \phi(a)\phi(b) \\
&= \psi_2(\psi_1(a))\psi_2(\psi_1(b)) \\
&= \psi_2(x)\psi_2(y)
\end{aligned}$$

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

So ψ_2 is a ring homomorphism. □

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

Theorem 9.11: Universal property of quotient rings

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

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr, "q"'] & & S \\
& R/\mathcal{I} \arrow[ur, dashed, "\psi?"'] &
\end{tikzcd}$$

Proof:

Existence If $\mathcal{I} \subseteq \ker \phi$, then ψ exists as a group homomorphism. Applying Lemma 9.10 with $\psi_1 = q, \psi_2 = \psi$, and $T = R/\mathcal{I}$ shows that ψ is a ring homomorphism.

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

Necessary for $\mathcal{I} \subseteq \ker \phi$ If ψ exists, then it is a group homomorphism, so apply universal property of quotient groups. □

Theorem 9.12: First isomorphism theorem for rings

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

Proof:
By universal property, having a ring homomorphism $\psi : R/\ker \phi \to \operatorname{Im} \phi$ such that $\psi \circ q = \phi$.

From first isomorphism theorem for groups, there is a group isomorphism $\psi' : R/\ker \phi \to \operatorname{Im} \phi$ such that $\psi' \circ q = \phi$. ψ is also a group homomorphism.

By universal property of quotient groups, $\psi = \psi'$ so ψ is bijective. (Could also just apply Lemma to ψ') □

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

Proposition 9.13

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

Proof:
$(x - c)R[x] = \ker \mathrm{ev}_c$, where $\mathrm{ev}_c : R[x] \to R$ is the evaluation map. If $r \in R$, then $\mathrm{ev}_c(r) = r$, so $\operatorname{Im} \mathrm{ev}_c = R$. By 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 $\mathcal{I} = \ker \operatorname{ev}_{x^2}$, where $\operatorname{ev}_{x^2} : \mathbb{Z}[x, y] = \mathbb{Z}[x][y] \to \mathbb{Z}[x]$ is evaluation at x^2.

By Proposition 9.13, $\mathbb{Z}[x, y]/\mathcal{I} \cong \mathbb{Z}[x]$.

9.5 Ideals generated by a subset

Proposition 9.14

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:
Exercise. $\square$

ideal generated by X

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

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

where $\mathcal{F} = \{\mathcal{I} \text{ an ideal of } R : X \subseteq \mathcal{I}\}$.

Key properties:

- By Proposition 9.14, (X) is an ideal.
- By definition, if $\mathcal{I}$ is an ideal with $X \subseteq \mathcal{I}$, then $X \subseteq (X) \subseteq \mathcal{I}$. Say that (X) is the **smallest ideal containing** X.
- Example: $(0) = (\varnothing) = \{0\}$

Sometimes use $\langle X \rangle$ instead of (X).

If $X = \{f_1, f_2, \ldots\}$, can replace $(X) = (\{f_1, f_2, \ldots\})$ with $(f_1, f_2, \ldots)$.
E.g., (0) instead of $(\{0\})$

Proposition 9.15

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

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

Remark:
Note that when $k = 0$, then the list of $s_i x_i t_i$ is empty, which is just 0.

Proof:

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

$\underline{\mathcal{I} \text{ is an ideal}}$: Taking $k = 0$, get $0_R \in \mathcal{I}$. Suppose $r \in R, x, y \in \mathcal{I}$. Let $x = \sum_{i=1}^{k} s_i x_i t_i, y = \sum_{i=1}^{\ell} s_i' y_i t_i'$ for $s_i, t_i, s_i', t_i' \in R$, $s_i y_i \in X$. 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.

$\underline{(X) \subseteq \mathcal{I}}$: Take $k = 1, s_1 = t_1 = 1 \implies X \subseteq \mathcal{I} \implies (X) \subseteq \mathcal{I}$.

$\underline{\mathcal{I} \subseteq (X)}$: Suppose $k \geq 0, s_i, t_i \in R, x_i \in X$ for $1 \leq i \leq k$. Since $X \subseteq (X), x_i \in (X) \implies s_i x_i t_i \in (X)$ for all $1 \leq i \leq k$. So $\sum_{i=1}^{k} s_i x_i t_i \in (X)$. Conclusion: $\mathcal{I} \subseteq (X)$. $\square$

Corollary 9.16

If R is a commutative ring, $X \subseteq R$, 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 $r_i = s_i t_i$. $\square$

$\mathcal{I} + \mathcal{J}$

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 9.17

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

Proof:
By Proposition 9.15, clearly $\mathcal{I} + \mathcal{J} \subseteq (\mathcal{I} \cup \mathcal{J})$.

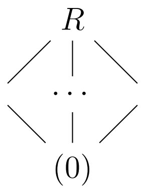
For the reverse inclusion, suppose $s_i, t_i \in R, x_i \in \mathcal{I} \cup \mathcal{J}$ for $1 \leq i \leq k$. Let $S = \{1 \leq i \leq k : x_i \in \mathcal{I}\}$, so if $i \in S, s_i x_i t_i \in \mathcal{I}$. So $\sum_{i \in S} s_i x_i t_i \in \mathcal{I}$, and similarly

$\sum_{i \notin S} s_i x_i t_i \in \mathcal{J}$.

Conclusion: $\sum_{i=1}^{k} s_i x_i t_i = \sum_{i \in S} s_i x_i t_i + \sum_{i \notin S} s_i x_i t_i \in \mathcal{I} + \mathcal{J}$ $\square$

Ideals of R are ordered by set inclusion $\subseteq$

Set of ideals of R with order $\subseteq$ is called **lattice of ideals of** R



Subgroup below $\mathcal{I}_1, \mathcal{I}_2$ in the lattice is $\mathcal{I}_1 \cap \mathcal{I}_2$. Subgroup above $\mathcal{I}_1, \mathcal{I}_2$ is $\mathcal{I}_1 + \mathcal{I}_2$.

New way of constructing rings: take $R/(X)$ for any subset X.

We know that $R/(X)$ is a unital ring, but when is it non-zero?

From group theory, know $R/\mathcal{I}$ is zero if and only if $\mathcal{I} = R$

We proved that $\mathcal{I} = R$ if and only if $1 \in \mathcal{I}$

Corollary 9.18

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

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

If R commutative, just have to show $\sum_{i=1}^{k} r_i x_i = 1, r_i \in R, x_i \in X$

9.6 Ideals generated by a finite subset

Often take ideals $(x_1, \ldots, x_n)$ generated by finite sets $\{x_1, \ldots, x_n\}$

Recall Corollary 9.16,

Corollary 9.19

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

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

Proof:
RHS $\subseteq (X)$ clear. For $(X) \subseteq RHS$, not that $rx_i + r'x_i = (r+r')x_i$, so can collect like terms, set $r_i = 0$ if x_i unneeded. $\square$

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 $R = \mathbb{Z}, m \in \mathbb{Z}$. 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 commutative and $p(x) \in R[x]$, then $(p) = pR[x]$ is an ideal

If R is noncommutative, pretty clear that (x) is not necessarily equal to $\{rx : r \in R\}$, since $xr \in (x)$ for $r \in R$.

But is $(x) = \{sxr : s, r \in R\}$? Answer is no in general.

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

We know $AE_{11}B$ has rank ≤ 1 for every $A, B \in M_2\mathbb{R}$, hence $\{AE_{11}B : A, B \in M_2\mathbb{R}\} \subsetneq M_2\mathbb{R}$ because it can't contain identity matrix.

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 $(E_{11}) = M_2\mathbb{R}$.

In general, there isn't a nice formula for the ideal generated by a single element in a non-commutative ring. We just have to use the general formula for any set.

9.6.1 More examples in polynomial rings

We've already mentioned the principle ideals $(x-c)\mathbb{Z}[x]$ for $c \in \mathbb{Z}$.
E.g., $x\mathbb{Z}[x]$ is the ideal of polynomials with no constant term.

Another good example is $m\mathbb{Z}[x]$ for $m \in \mathbb{Z}$. This is $m\mathbb{Z}[x] = \{\sum_{i=0}^{n} a_i x^i : n \geq 0, a_i \in m\mathbb{Z}$ for $0 \leq i \leq n\}$.

The last example doesn't work in $\mathbb{Q}[x]$, since $2\mathbb{Q}[x] = \mathbb{Q}[x]$. 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, since $xy = 0 + x \cdot y = y \cdot x + 0$.

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 that there are polynomials $f, p, q \in \mathbb{Z}[x,y]$ such that $p \cdot f = x$, and $q \cdot f = y$. Then f is one of ± 1.

Consequence: the only principle 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 ideal.

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 $\mathbb{Z}[x]$. In other words, $(2,x)$ is not principal.

9.7 Correspondence theorem

Proposition 9.20

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

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

(b) If $\mathcal{I}$ is an ideal of R, and ϕ is surjective, then $\phi(\mathcal{I})$ is an ideal of S.

Recall from group theory, correspondence theorem for groups (Theorem 5.14).

Theorem 9.21: Correspondence theorem for rings

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

$$\begin{array}{ccc} \text{Subgroups } K \text{ of } R^+ \text{ s.t. } \ker\phi \leq K & \underset{\phi^{-1}(K') \hookleftarrow K'}{\overset{K \mapsto \phi(K)}{\rightleftarrows}} & \text{Subgroups } K' \text{ of } S^+ \end{array}$$

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

Here R^+ is the ring R under addition.

Proof:
Apply Proposition 9.20, use fact that $K = \phi^{-1}((\phi(K))$. □

Special case $q : R \to R/\mathcal{I}$: 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 $\mathrm{ev}_{x=0} : R[x] \to R$. So ideals of $R[x]$ containing (x) correspond to ideals $\mathcal{I}$ of R. If $\mathcal{I}$ is an ideal of R, what is corresponding ideal in $R[x]$?

Answer:

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

9.8 The second isomorphism theorem

Recall from group theory, second isomorphism theorem for groups (Theorem 5.27). Now change to 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 $i_H : H \to H + K$ is the inclusion, $q_1 : H \to H/H \cap K$ and $q_2 : H + K \to H + K/K$ are the quotient maps, then there is an isomorphism $\psi : H/H \cap K \to H + K/K$ such that $\psi \circ q_1 = q_2 \circ i_H$.

Theorem 9.22: Second isomorphism theorem for rings

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

$$\begin{tikzcd} S \arrow[r, "i_S"] \arrow[d, "q_1"'] & S+\mathcal{I} \arrow[d, "q_2"] \\ S/S\cap\mathcal{I} \arrow[r, "\psi"'] & S+\mathcal{I}/\mathcal{I} \end{tikzcd}$$

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, not that $1 \in S+\mathcal{I}$.

If $x, y \in S+\mathcal{I}$, then $x = s+a, y = t+b$ where $s, t \in S$, $a, b \in \mathcal{I}$.
So $xy = st + (sb + at + ab) \in S+\mathcal{I}$, and hence $S+\mathcal{I}$ is a subring.

Then it is not hard to see that $S \cap \mathcal{I}$ is an ideal of S.

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

By applying Lemma 9.10, we see that ψ is a ring isomorphism. □

Example:

Let $\mathcal{J}$ be an ideal of a commutative ring R. Let $\mathcal{I} = \{f \in R[x] : f(0) \in \mathcal{J}\} = \mathrm{ev}_0^{-1}(\mathcal{J})$.

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.

9.9 The third isomorphism theorem

Also from group theorem, recall third isomorphism theorem for groups (Theorem 5.17), we then have

Theorem 9.23: Third isomorphism theorem for rings

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

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

Then there is an isomorphism $\psi : R/\mathcal{K} \to (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$ sicj tjat $\psi \circ q_3 = q_2 \circ q_1$.

$$\begin{tikzcd} R \arrow[r, "q_1"] \arrow[d, "q_3"'] & R/\mathcal{I} \arrow[d, "q_2"] \\ R/\mathcal{K} \arrow[r, "\psi"'] & (R/\mathcal{I})/(\mathcal{K}/\mathcal{I}) \end{tikzcd}$$

Proof:
Apply Lemma 9.10 again. □

Example:
$(\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ as rings.

Example:
Previous example: $\mathcal{J}$ ideal in R, $\mathcal{I} = \mathrm{ev}_0^{-1}(\mathcal{J}) \subseteq R[x]$.

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

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

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

Now we can show that this isomorphism $R/\mathcal{J} \cong R[x]/\mathcal{I}$ from second isomorphism theorem.

10 More on ideals

week 9

10.1 Constructing $\mathbb{C}$ from $\mathbb{R}$

From last chapter: 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 $\mathbb{R}[x]/(x^2+1)$ since $x^2 + 1 \iff x^2 = -1$. If we look at $\overline{x} = [x]$ in $\mathbb{R}[x]/(x^2+1)$, then

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

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

Theorem 10.1

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

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

Before proving the theorem, let's be clear on what $\mathbb{C}$ is:

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

How does $\mathbb{R}[x]/(x^2+1)$ correspond to $\mathbb{C}$?

We know that $\overline{x}$ acts like i.

Lemma 10.2

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

Proof:

Existence Since quotient map $\mathbb{R}[x] \to \mathbb{R}[x]/(x^2+1)$ is surjective, every element of $\mathbb{R}[x]/(x^2+1)$ can be written as $\sum_{i=0}^n a_i\overline{x}^i$.

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

$$\begin{aligned}\sum_{i=0}^n a_i\overline{x}^i &= \sum_{i=0}^n a_i\overline{x}^i - \left(a_n\overline{x}^n + a_n\overline{x}^{n-2}\right)\\ &= 0\cdot\overline{x}^n + a_{n-1}\overline{x}^{n-1} + (a_{n-2}-a_n)\,\overline{x}^{n-2} + \dots\end{aligned}$$

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

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

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

Conclusion: every non-zero element of (x^2+1) has degree ≥ 2.
Only way $(a-c)+(b-d)x \in (x^2+1)$ is $a=c, b=d$. $\square$

Now let's prove Theorem 10.1.

Proof:
Since $\mathbb{R}$ is a subring of $\mathbb{C}$, 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 $\phi = \mathrm{ev}_{x=i} \circ j : \mathbb{R}[x] \to \mathbb{C}[x] \to \mathbb{C}$. Then $\phi(x) = i$, so $\phi(x^2+1) = i^2+1 = 0$. So $x^2+1 \in \ker\phi \implies (x^2+1) \subseteq \ker\phi$.

By universal property of quotient rings, there is a homomorphism $\psi : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ such that $\psi \circ q = \phi$. So $\psi(a+b\overline{x}) = \phi(a+bx) = a+bi$. By Lemma 10.2, ψ is a bijection. $\square$

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 the 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. So $1 \neq 0$ in $\mathbb{K}[x]/(p)$.

$1 = 0$ in $\mathbb{K}[x]/(x^2+1, x^3+x+1)$, since $x^3+x+1-x(x^2+1) = 1 \in (x^2+1, x^3+x+1)$.

10.2 Maximal ideals

Let $\mathcal{I}$ be an ideal of a commutative ring R. When is $R/\mathcal{I}$ is 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 $q : R \to \mathbb{K}$ is the quotient map. By correspondence theorem, only ideals of R containing $\mathcal{I}$ are $q^{-1}((0)) = \ker q = \mathcal{I}$, and $q^{-1}(\mathbb{K}) = R$.

maximal

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 10.3

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

Proposition 10.4

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:
Already proved $\Rightarrow$, only need to prove $\Leftarrow$.

Suppose $x \in R, x \neq 0$. Then $(x) = R$. That means $1 \in (x) = xR$, 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. $\square$

Theorem 10.5

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, only ideals of $R/\mathcal{I}$ are (0) and $R/\mathcal{I}$ if and only if ideals of R containing $\mathcal{I}$ are $\mathcal{I}, R$. So by Proposition 10.4, $R/\mathcal{I}$ 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 now that $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$. Also know that $(2, x) = \{f \in \mathbb{Z}[x] : f(0) \in (2)\} = \mathrm{ev}_{x=0}^{-1}((2))$ for

ideal $(2) \subseteq \mathbb{Z}$. By 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 a commutative ring, have

$$\mathrm{ev}_{(a,b)} = \mathrm{ev}_{x=a} \circ \mathrm{ev}_{y=b} : R[x,y] = R[x][y] \to R[x] \to R$$

Then

$$\begin{aligned}\ker \mathrm{ev}_{(a,b)} &= \mathrm{ev}_{(a,b)}^{-1}((0)) = \mathrm{ev}_{y=b}^{-1}((x-a)) \\ &= \{f \in R[x][y] : f(x,b) \in (x-a)R[x]\} = (x-a, y-b)\end{aligned}$$

By first isomorphism theorem, we have $R[x,y]/(x-a,y-b) \cong R$. So $(x-a,y-b)$ is a maximal ideal of $R[x,y] \iff R$ is a field.

For $(y-x^2) \in R[x,y]$, 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 $c \in \mathbb{R}$. We have shown that

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

It's not hard to see that $\mathbb{R}\times\mathbb{R}$ and $\mathbb{R}[x]/(x^2)$ are not fields. Hence $\mathbb{R}[x]/(x-c^2)$ 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 $c \geq 0$.

10.3 Maximal ideals and Zorn's lemma

partial order

A **partial order** on a set X is a relation $\leq$ on X such that

1. $x \leq x$ for all $x \in X$,
2. if $x \leq y$ and $y \leq x$, then $x = y$ for all $x, y \in X$, and
3. if $x \leq y$ and $y \leq z$, then $x \leq z$ for all $x, y, z \in X$.

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. (These are unique if they exist.)

A maximum element (if it exists) if a subset S is maximal.

But a subset S can have maximal elements without having a maximum element.

Example: $2^{\{1,2\}}$

Consider $2^{\{1,2\}} = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$ ordered by $\subseteq$.
Then $\{1,2\}$ is a maximum element for $2^{\{1,2\}}$, but the subset $\{\varnothing, \{1\}, \{2\}\}$ 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 $\subseteq$.

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.

Thus this is a ring where the set of proper ideals does not have a maximal element. What about all commutative rings? It turns out that we can write down commutative rings even where the set of proper ideals of R has a maximum element. These rings are called local rings. But in general, we can't expect the set of proper ideals of R to have a maximum element. It's a special property to be a local ring.

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 a maximal element.

Of course, this might not work.

We might be in a poset[1] like $(\mathbb{N}, \leq)$, where we have infinitely long increasing sequences like $1 < 2 < 3 < \cdots$

In that case, we are only guaranteed to get a sequence $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \ldots$ of proper ideals.

If $x_0 \leq x_1 \leq x_2 \leq \ldots$ in a partially ordered set X, then the subset $S = \{x_0, x_1, x_2, \ldots\}$ has a special property: it's a chain!

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 $\mathbb{N}$: chains with no upper bound?

Lemma 10.6

Let R be a commutative ring, and let $\mathcal{F}$ be a chain of ideals (i.e., a family of ideals, such that if $\mathcal{I}, \mathcal{J} \in \mathcal{F}$, then either $\mathcal{I} \subseteq \mathcal{J}$, or $\mathcal{J} \subseteq \mathcal{I}$, or both). Then

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

is an ideal of R.

Note that this doesn't work if $\mathcal{F}$ is not a chain, since the union of ideals is typically not closed under addition. For 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 10.7

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 10.7, there is a proper ideal $\mathcal{J}_0$ which is an upper bound for $\{\mathcal{I}_0, \mathcal{I}_1, \ldots\}$,

[1] partially ordered set

i.e., $\mathcal{I}_k \subseteq \mathcal{J}_0$ 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!

Axiom: Axiom of choice

Let $X \subseteq 2^Y$ for some Y, such that if $A \in X$, then $A \neq \varnothing$. Then there is a function $f : X \to Y$ 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 of the axiom of choice #1

A function $f : X \to Y$ is surjective $\iff$ 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 #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.

Proposition 10.8

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 Lemma 10.6, $\mathcal{I}' = \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$ is an ideal of R. Clearly $\mathcal{J} \subseteq \mathcal{I}'$, and since $1 \notin \mathcal{I}'$, $\mathcal{I}' \in \mathcal{P}$. 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. So the ideal $\mathcal{K}$ in the proposition isn't necessarily unique.

In particular, every non-zero commutative ring R has a maximal ideal, or equivalently:

Corollary 10.9

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

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

10.4 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 $R = \mathbb{Z}/6\mathbb{Z}$, 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 $xy = 0$

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 $yx = 0$.

Example: $\mathbb{Z}/n\mathbb{Z}$
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: $R \times S$
If R and S are non-zero rings, and $a \neq 0$ in R, $b \neq 0$ in S. Then $(a, 0), (0, b)$ are non-zero in the product ring $R \times S$. But $(a, 0) \times (0, b) = (0, 0) = 0$ in $R \times S$. So $(a, 0), (0, b)$ are zero-divisors.

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

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

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. $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$, 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 $< n$ (i.e., A is not invertible).

Example: Group ring
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.

Lemma 10.10

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

Proof:
$uv = 0 \implies v = u^{-1}uv = 0$

$vu = 0 \implies v = vuu^{-1} = 0.$ □

Every non-zero element of field is a unit, so fields don't have zero divisors.

In general, an element can be a non-zero divisor without being a unit:

- $\mathbb{Z}$ does not have any zero divisors, but the only units are ± 1.
- If $f \in \mathbb{K}[x], f \neq 0$, $\mathbb{K}$ a field, then by the degree formula, $fg = 0$ if and only if $g = 0$. So $\mathbb{K}[x]$ has no zero divisors, but $\mathbb{K}[x]^\times = \mathbb{K}^\times$.

Proposition 10.11

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

Proof:
If $xa = xb$, then $x(a - b) = 0$. Since $x \neq 0$ and x is not a zero divisor, $a - b = 0 \implies a = b$. Use the same argument if $ax = bx$. □

Corollary 10.12

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 $\ell_x : R \to R : y \mapsto xy$.

If $\ell_x(a) = \ell_x(b)$, then $xa = xb \implies a = b$. So ℓ_x is injective.

Since R is finite, pigeon-hole principle implies that ℓ_x is surjective. So there is $y \in R$, such that $xy = 1 \implies x$ has right inverse.

Same argument with $y \mapsto yx$ implies x has left inverse.

So x is invertible. □

10.5 Integral domains

integral domain

An **integral domain** (or **domain**) is a commutative ring R such $1 \neq 0$, 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, $\mathbb{R} \times \mathbb{R}, \mathbb{R}[x]/(x^2)$)

$\{0\}$ doesn't have zero divisors, but not a domain.

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

Corollary 10.13

All finite integral domains are fields.

Proposition 10.14

If R is an integral domain, then

(a) If $f, g \in R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$.

(b) $R[x]$ is an integral domain.

Proof:

(a) Formula is true if f or g is zero, so suppose $f, g \neq 0$. Let $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$, where $a_n, b_m \neq 0$. Then $fg = a_n b_m x^{n+m} +$ lower degree terms. Since R is a domain, $a_n b_m \neq 0$, so $\deg(fg) = n + m = \deg(f) + \deg(g)$

(b) Suppose $f, g \neq 0$ and $fg = 0$. Then $\deg(fg) = -\infty$ so by (a), must have $\deg(f) = -\infty$ or $\deg(g) = -\infty$. □

Proposition 10.15

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

Proof:

$\mathbb{K}$ is commutative and $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$. 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 $\mathbb{K}$, and hence $y = 0$ in R. So R has no zero divisors. □

Example:

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

Proposition 10.16

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 $\mathbb{C}$.

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

10.6 Prime ideals

Can we construct interesting domains of the form $R[x]/(p)$? where R is integral domain and $p \in R[x]$. We need to know: Suppose $\mathcal{I}$ 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 $\overline{a} \cdot \overline{b} = 0$ in $R/\mathcal{I}$ for some $a, b \in R$, then one of $\overline{a}, \overline{b}$ is 0 in $R/\mathcal{I}$. Of course, $\overline{r} = 0$ if $R/\mathcal{I}$ if and only if $r \in \mathcal{I}$. So $\overline{a} \cdot \overline{b} = 0$ in $R/\mathcal{I}$ if and only $ab \in \mathcal{I}$, and one of $\overline{a}, \overline{b}$ is zero in $R/\mathcal{I}$ if and only if one of a, b is in $\mathcal{I}$.

prime ideal

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

Theorem 10.17

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: $\mathbb{K}[x, y]/(y - x^2) \cong \mathbb{K}[x]$, a domain but not a field. So $(y - x^2)$ is a prime ideal which is not maximal.

Proof:

Since R is commutative and $R \to R/\mathcal{I} : r \mapsto \overline{r}$ is surjective, $R/\mathcal{I}$ is commutative for any ideal $\mathcal{I}$, and $R/\mathcal{I}$ is zero $\iff$ $\mathcal{I} = R$. Using surjectivity of $R \to R/\mathcal{I}$ again, $R/\mathcal{I}$ has no zero divisors if and only if for $a, b \in R$, if $\overline{a} \cdot \overline{b} = 0$ in $R/\mathcal{I}$, then one of $\overline{a}, \overline{b}$ is 0 in $R/\mathcal{I}$. Since $\overline{r} = 0$ in $R/\mathcal{I}$ $\iff$ $r \in \mathcal{I}$, $R/\mathcal{I}$ has no zero divisors if and only if for all $a, b \in R$, if $ab \in \mathcal{I}$, then one of a, b is in $\mathcal{I}$.

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

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

Lemma 10.18

If R is an integral domain, and $f, g \in R[x]$ have degree ≥ 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 $f, g \notin fgR[x]$. Since if $f, g \in fgR[x]$, we have $\deg(fgh) = \deg(f)$ or $\deg(fgh) = \deg(g)$ for some h, contradiction. Thus we conclude that $fgR[x]$ is not prime. $\square$

Example:
Since (x^2+1) is maximal in $\mathbb{R}[x]$, (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 $\mathbb{Z}_3[x]$, 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 that (x^2+1) is prime.

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

However, suppose we want a <u>domain</u> containing $\mathbb{C}$ and an additional element $x \notin \mathbb{C}$ such that $x^2 = -1$.

Proposition 10.19

Suppose R is a subring of a domain S, and x is an element of S such that $x^2 = t^2$ for some $t \in R$. 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 zero. $\square$

Since $i^2 = -1$ in $\mathbb{C}$, there is no domain containing $\mathbb{C}$ and an additional element $x \notin \mathbb{C}$ such that $x^2 = -1$.

11

Fields of fractions and CRT

week 10

11.1 Fields of fractions

Recall Proposition 10.15.

Theorem 11.1

A ring R is an integral domain if and only if it is (isomorphic to) a subring of a field.

Example:

$\mathbb{Z}$ is a subring of $\mathbb{Q}$ (and also of $\mathbb{R}, \mathbb{C}$)

$\mathbb{Q}[x]$ is a subring of $\mathbb{Q}(x)$, the ring of **rational functions**

$$\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in \mathbb{Q}[x], g \neq 0 \right\}$$

Strategy for proof of theorem: we've already done $\Leftarrow$. For $\Rightarrow$: given R, need to construct a field $\mathbb{K}$ containing R. For $\mathbb{Z}$ we could pick $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Q}(x)$. Which field should we pick?

Lemma 11.2

Let $\mathbb{K}$ be a field containing $\mathbb{Z}$ as a subring. Then $\mathbb{K}$ contains $\mathbb{Q}$ as a subfield.

Note

$\mathbb{K}$ containing $\mathbb{Z}$ as a subring means that there is an isomorphism $\phi : \mathbb{Z} \to R$, where R is a subring of $\mathbb{K}$.

By the first isomorphism theorem, this is the same as saying that there is an injective homomorphism $\phi : \mathbb{Z} \to \mathbb{K}$.

ϕ is called the **subring inclusion map**, since it's like the inclusion map $R \hookrightarrow \mathbb{K} : x \mapsto x$ for the actual subring.

Proof:
Let $\phi : \mathbb{Z} \to \mathbb{K}$ be the subgroup inclusion map. Define $\psi : \mathbb{Q} \to \mathbb{K}$ by $\frac{a}{b} \mapsto \phi(a)\phi(b)^{-1}$. Is this map well-defined?

Suppose $\frac{a}{b} = \frac{c}{d}$, so $ad = bc$. Then

$$\phi(a)\phi(d) = \phi(ad) = \phi(bc) = \phi(b)\phi(c)$$

so $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1} \implies \psi$ is well-defined.

It's not hard to see ψ is a ring homomorphism. Any map from a field is injective, so ψ is an injective morphism. $\square$

How do we get $\mathbb{Q}$ from $\mathbb{Z}$?

- Elements are $\frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$.
- $\frac{a}{b} = \frac{c}{d} \iff ad = bc$
- Operations:
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
- Zero element is $\frac{0}{1}$, identity is $\frac{1}{1}$, and $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ if $a \neq 0$.
- Why can't we take $\frac{a}{0}$?

  Including $\frac{a}{0}$ for any a means we have to include $\frac{0}{1} \cdot \frac{a}{0} = \frac{0}{0}$. Since $0 \cdot a = 0 \cdot b$ for all b, we have $\frac{a}{b} = \frac{0}{0}$ for all $a, b \in \mathbb{Z}$. But then $\frac{a}{b} = \frac{a'}{b'}$ for all $a, b, a', b' \in \mathbb{Z}$.

Field of fractions Q of an integral domain R is defined as follows:

- Elements are $\frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$.
- $\frac{a}{b} = \frac{c}{d} \iff ad = bc$
- Operations:
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
- Zero element is $\frac{0}{1}$, identity is $\frac{1}{1}$, and $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ if $a \neq 0$.
- Why can't we include zero divisors?

  If $yz = 0, y, z, \neq 0$, then $\frac{0}{y} \cdot \frac{0}{z} = \frac{0}{0}$. Once again we get $\frac{a}{b} = \frac{0}{0} = \frac{a'}{b'}$ for all $a, b, a', b' \in R$.

11.2 Localization

Suppose we have a commutative ring R, and we want to make a ring of fractions $\frac{a}{b}$ with $a, b \in R$.

Operations should be

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ and } \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

so zero should be $\frac{0}{1}$ and identity should be $\frac{1}{1}$.

Let S be the set of elements that can go in the denominator. We've already seen that S shouldn't contain 0 or any zero divisors. To have identities, and for operations to be well-defined, want:

multiplicatively closed

We say that a subset S of a ring R is **multiplicatively closed** if and only if $1 \in S$, and if $b, d \in S$, then $bd \in S$.

Theorem (Informal version)

Let R be a commutative ring, and let S be a multiplicatively closed subset of R which does not contain 0 or any zero divisors.

Then there is a commutative ring Q containing R as a subring, such that

(a) every element of S is a unit in Q, and

(b) if T is a ring containing R as a subring such that every element of S is a unit in T, then T contains Q as a subring.

Part (a): because we can put $a \in S$ in denominator, then we can talk about $\frac{1}{a}$. Part (b): Q is the smallest possible commutative ring containing R satisfying (a).

Theorem 11.3: (Stronger + formal version)

Let R be a commutative ring, and let S be a multiplicatively closed subset of R which does not contain 0 or any zero divisors.

Then there is a commutative ring Q and an injective morphism $\phi : R \to Q$ such that

(a) $\phi(a) \in Q^\times$ for all $a \in S$, and

(b) if $\psi : R \to T$ is a morphism s.t. $\psi(x) \in T^\times$ for all $x \in S$, then there is a morphism $\tilde{\psi} : Q \to R$ such that $\tilde{\psi} \circ \phi = \psi$.

$$\begin{tikzcd}
R \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & T \\
& Q \arrow[ur, dashed, "\tilde{\psi}"'] &
\end{tikzcd}$$

Note since $\tilde{\psi}\circ\phi = \psi$, if $a \in S$, then $\tilde{\psi}\circ\phi(a) = \psi(a)$, and $\tilde{\psi}\left(\phi(a)^{-1}\right) = \tilde{\psi}(\phi(a))^{-1} = \psi(a)^{-1}$.

localization of R at S

The ring Q from the theorem is called the **localization of R at S** (or **with respect to S**), and is denoted by $S^{-1}R$.

Proof:
Let $Q_0 := \{(a,b) : a \in R, b \in S\}$, and define an equivalence relation $\sim$ on Q_0 by $(a,b) \sim (c,d)$ if $ad = bc$. Let's show that $\sim$ is an equivalence relation.

- $(a,b) \sim (a,b)$ since by commutativity, $ab = ba$.
- If $(a,b) \sim (c,d)$ then commutativity again implies $cb = da$, so $(c,d) \sim (a,b)$.
- If $(a,b) \sim (c,d) \sim (e,f)$, then $ad = bc$ and $cf = de$, so $afd = bcf = bed$. Since $d \in S$, d is not zero or a zero divisor, so $af = be$ by cancellation law. So $(a,b) \sim (e,f)$.

Let $Q = Q_0 / \sim$ be the set of equivalence classes of $\sim$.

Notation: If $a \in R, b \in S$, let $\frac{a}{b} := [(a,b)] \in Q$.

Now let's put a ring structure on Q.

$$\text{Define } \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We want to first show $+, \cdot$ are well-defined. Because S is multiplicatively closed, if $a, c \in R, b, d \in S$, then $[(ad+bc, bd)]$ and $[(ac, bd)]$ are well-defined elements of Q.

So $([(a,b)], [(c,d)])\ R\ [(ad+bc, bd)]$ is a well-defined relation between $Q \times Q$ and Q, and similar with $\cdot$.

Suppose $[(a,b)] = [(a',b')]$, and $[(c,d)] = [(c',d')]$, so $ab' = b'a$ and $cd' = dc'$.

Then $(ad+bc)(b'd') = ba'dd' + bb'dc' = (a'd' + b'c')(bd)$ and $(ac)(b'd') = ba'dc' = (bd)(a'c')$, so

$$\frac{ad+bc}{bd} = \frac{a'd' + b'c'}{b'd'} \text{ and } \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Thus the operations $+$ and $\cdot$ are well-defined.

Have $+, \cdot$ well-defined, so let's show that $(Q, +)$ is abelian group.

$\frac{a}{b} = \frac{0}{1}$ if and only if $a = 1 \cdot a = b \cdot 0 = 0$.

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf + bcf + ebd}{bdf} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right),$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{c}{d} + \frac{a}{b}, \qquad \frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b1} = \frac{a}{b},$$

$$\text{and } \frac{a}{b} + \frac{-a}{b} = \frac{ab - ba}{b^2} = \frac{0}{b^2} = \frac{0}{1}$$

for all $a, c, e \in R$ and $b, d, f \in S$.

$(Q, +)$ is an abelian group with zero $\frac{0}{1}$ and $-\frac{a}{b} = \frac{-a}{b}$.

Next, need to show that $(Q, +, \cdot)$ is a commutative ring.

For all $a, c, e \in R$ and $b, d, f \in S$,

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd} = \frac{ba}{dc} = \frac{c}{d} \cdot \frac{a}{b}, \qquad \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$$

so $\cdot$ is associative and commutative.

Since $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, $\frac{1}{1}$ is an identity.

Also if $a \in R$, $b, c \in S$, then $\frac{ac}{bc} = \frac{a}{b}$ since $acb = bca$.

Finally

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{acf + ade}{bdf} = \frac{acfb + adeb}{b^2 df} = \frac{ac}{bd} + \frac{ae}{bf}$$

So $(Q, +, \cdot)$ is a ring.

Now we can define $\phi : R \to Q : a \mapsto \frac{a}{1}$.

To check that this is a homomorphism, have

$$\phi(1) = \frac{1}{1}, \quad \phi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} \text{ and } \phi(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$$

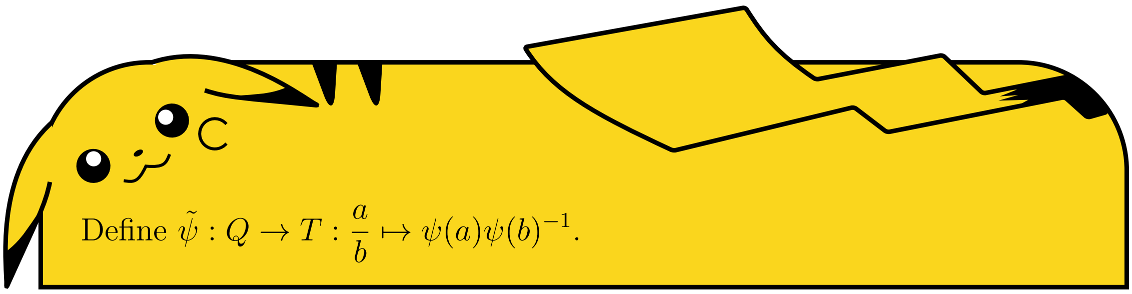
for all $a, b \in R$.

If $\phi(a) = \phi(b)$, then $\frac{a}{1} = \frac{b}{1} \implies a = a \cdot 1 = b \cdot 1 = b$. So ϕ is injective.

Also, if $a \in S$, then $\frac{a}{1} \cdot \frac{1}{a} = \frac{a}{a} = \frac{1}{1}$, so $\phi(a) \in Q^\times$ for all $a \in S$. So this proves (a) of the theorem.

This leaves part (b).

Suppose $\psi : R \to T$ is a morphism s.t. $\psi(a) \in T^\times$ for all $a \in S$. $\operatorname{Im} \psi \cong R/\ker \phi$ is commutative, so can assume T is commutative.
(Exercise: if $ab = ba$ for $a \in T^\times$, $b \in T$, then $a^{-1}b = ba^{-1}$.) With this fact, elements of T is either in $\operatorname{Im} \psi$ or $(\operatorname{Im} \psi)^{-1}$. Then every pair of elements in T commute.



Define $\tilde{\psi} : Q \to T : \frac{a}{b} \mapsto \psi(a)\psi(b)^{-1}$.

Since $\psi(b) \in T^\times$ if $b \in S$, $\psi(a)\psi(b)^{-1}$ is well-defined in T. To see that $\tilde{\psi}$ is well-defined, suppose that $\frac{a}{b} = \frac{c}{d}$. Then $ad = bc$ so $\psi(a)\psi(d) = \psi(b)\psi(c) \implies \psi(a)\psi(b)^{-1} = \psi(c)\psi(d)^{-1}$. So $\tilde{\psi}$ is well-defined.

Also $\tilde{\psi} \circ \phi(a) = \tilde{\psi}\left(\frac{a}{1}\right) = \psi(a)\psi(1)^{-1} = \psi(a)$ for all $a \in R$, so $\tilde{\psi} \circ \phi = \psi$.

To finish, just need to show that $\tilde{\psi}$ is a homomorphism:

$$\tilde{\psi}\left(\frac{1}{1}\right) = \psi(1)\psi(1)^{-1} = 1,$$

$$\begin{aligned} \tilde{\psi}\left(\frac{a}{b} + \frac{c}{d}\right) = \tilde{\psi}\left(\frac{ad+bc}{bd}\right) &= \psi(ad+bc)\psi(bd)^{-1} \\ &= \psi(a)\psi(b)^{-1} + \psi(c)\psi(d)^{-1} = \tilde{\psi}\left(\frac{a}{b}\right) + \tilde{\psi}\left(\frac{c}{d}\right) \end{aligned}$$

and

$$\begin{aligned} \tilde{\psi}\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \tilde{\psi}\left(\frac{ac}{bd}\right) &= \psi(ac)\psi(bd)^{-1} \\ &= \psi(a)\psi(b)^{-1}\psi(c)\psi(d)^{-1} = \tilde{\psi}\left(\frac{a}{b}\right) \cdot \tilde{\psi}\left(\frac{c}{d}\right) \end{aligned}$$

for all $a, c \in R$, $b, c \in S$, so $\tilde{\psi}$ is a homomorphism. □

11.3 Uniqueness of localization

Recall Theorem 11.3, is it ok to talk about **the** ring from the theorem? (rather than from the proof of the theorem)

No! We omitted a condition out of the theorem.

Lemma 11.4

If Q is the ring from the proof of Theorem 11.3, and $\phi : R \to Q$ is the inclusion, then all elements of Q are of the form $\phi(a)\phi(b)^{-1}$ for $a \in R, b \in S$.

Proof:
All elements of Q are of the form $\frac{a}{b}$ for $a \in R, b \in S$, and $\phi : R \to Q$ is defined by $\phi(a) = \frac{a}{1}$. $\square$

Theorem 11.5: Corrected localization theorem

Let R be a commutative ring, and let S be a multiplicatively closed subset of R which does not contain 0 or any zero divisors.

Then there is a commutative ring Q and an injective morphism $\phi : R \to Q$ such that

(a) $\phi(a) \in Q^\times$ for all $a \in S$, and every element of Q is of the form $\phi(a)\phi(b)^{-1}$ for $a \in R, b \in S$, and

(b) if $\psi : R \to T$ is a morphism s.t. $\psi(x) \in T^\times$ for all $x \in S$, then there is a morphism $\tilde{\psi} : Q \to R$ such that $\tilde{\psi} \circ \phi = \psi$.

Corollary 11.6

Let S be a multiplicatively closed subset of a ring R, which does not contain 0 or any zero divisors. If Q_i and ϕ_i are a commutative ring and an injective homomorphism satisfying (a) and (b) from the theorem, $i = 1, 2$ then there is an isomorphism $\alpha : Q_1 \to Q_2$ such that $\alpha \circ \phi_1 = \phi_2$.

$$\begin{tikzcd}
 & R \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\
Q_1 \arrow[rr, dashed, "\alpha"'] & & Q_2
\end{tikzcd}$$

Proof:
Since $\phi_i(a) \in Q_i^\times$ for all $a \in S$, $i = 1, 2$ can apply part (b) of the theorem to get morphisms $\alpha : Q_1 \to Q_2$ and $\beta : Q_2 \to Q_1$ with $\alpha \circ \phi_1 = \phi_2$, and $\beta \circ \phi_2 = \phi_1$.

$$\begin{tikzcd} & R \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\ Q_1 \arrow[rr, bend left, "\alpha"] & & Q_2 \arrow[ll, bend left, "\beta"] \end{tikzcd}$$

Suppose $x \in Q_1$. By part (a) of the theorem, $x = \phi_1(a)\phi_1(b)^{-1}$ for $a \in R, b \in S$. Since $\alpha(\phi_1(b)) = \phi_2(b)$, $\alpha(x) = \phi_2(a)\phi_2(b)^{-1}$. So $\beta(\alpha(x)) = \phi_1(a)\phi_1(b)^{-1} = x$. Conclusion, β is left inverse to α. By symmetry, α is a left inverse to β, so α and β are inverses, and α is an isomorphism. □

By Corollary, we can talk about **the** ring from the theorem:

localization of R at S

The ring Q from the theorem is called the **localization of R at S** (or **with respect to** S), and is denoted by $S^{-1}R$.

With this definition, $S^{-1}R$ is only defined up to isomorphism. Usually just take $S^{-1}R$ to be the ring from proof of the theorem.

Exercise

Show that if we can leave out the requirement that every element of Q is of the form $\phi(a)\phi(b)^{-1}$ for some $a \in R, b \in S$, then there can be non-isomorphic rings satisfying conditions (a) and (b).

Hint: show that you can replace Q with $Q[x]$ and it will satisfy part (a) and (b).

11.4 Examples of localization

Lemma 11.7

Let R be an integral domain. Then $S = R \setminus \{0\}$ is multiplicatively closed and does not contain 0 or any zero divisors. Also $S^{-1}R$ is a field.

Proof:

Because R is a subring of $S^{-1}R$, $S^{-1}R$ is non-zero. Suppose $\frac{a}{b} \in S^{-1}R$. Then $\frac{a}{b} = \frac{0}{1}$ if and only if $a = 0$. So if $\frac{a}{b} \neq 0$, then $\frac{a}{b}$ has an inverse, namely $\frac{b}{a}$. □

field of fractions of R

If R is an integral domain, and $S = R \setminus \{0\}$, then $S^{-1}R$ is called the **field of fractions of** R.

Theorem 11.8

A ring R is an integral domain if and only if it is (isomorphic to a subring of a field).

Proof:
Already seen that every subring of a field is an integral domain. Conversely, every domain is a subring of its field of fractions. $\square$

Lemma 11.9

The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

Proof:
Clearly from the construction of $S^{-1}R$ that we get $\mathbb{Q}$.

Alternatively, can show $\mathbb{Q}$ satisfies conditions (a) and (b) of corrected localization theorem. $\square$

rational functions

Let R be a domain. The field of fractions of $R[x]$ is denoted by $R[x]$, and is called the field of **rational functions** over R.

By construction, $R[x]$ consists of fractions $\frac{f(x)}{g(x)}$ with $f, g \in R[x]$, and $g \neq 0$.

Lemma 11.10

Let Q be the field of fractions of a domain R. Then $Q(x) = R(x)$.

Proof:
Since $R[x]$ is a subring of $Q[x]$, then there is an injective homomorphism $\phi : R[x] \to Q(x)$.

By part (b) of localization theorem, there is a homomorphism $R(x) \to Q(x)$ sending $\frac{f(x)}{g(x)} \in R(x)$ to the same fraction in $Q(x)$.

Since $R(x)$ is a field, this homomorphism is injective. But $R(x)$ contains $\frac{a}{b}$ for any $a, b \in R$, $b \neq 0$, so homomorphism $R(x) \to Q(x)$ is onto. $\square$

So for rational functions, can assume coefficients form a field.

Suppose $\mathbb{K}$ is a field. Why do we call functions $\frac{f(x)}{g(x)} \in \mathbb{K}(x)$ rational <u>functions</u>?

Suppose we are given $c \in \mathbb{K}$. If $g(c) \neq 0$, then $\frac{f(c)}{g(c)} \in \mathbb{K}$.

domain D(F)

The **domain D(F)** of $F \in \mathbb{K}(x)$ is the set of points $c \in K$ such that $F = \frac{f(x)}{g(x)}$ for some $f, g \in \mathbb{K}[x]$ with $g(c) \neq 0$.

Can have $f, g \in \mathbb{K}[x]$ such that $g(c) = 0$, but $c \in D(f/g)$.

Lemma 11.11

$F \in \mathbb{K}(x)$ defines a function $D(F) \to \mathbb{K} : c \mapsto f(c)/g(c)$, where $f, g \in \mathbb{K}[x]$ are chosen such that $F = f/g$ and $g(c) \neq 0$.

Example:

Let $F = \frac{1}{x(x-1)(x+1)} \in \mathbb{C}(x)$. If $F = \frac{f}{g}$, then $g(x) = x(x-1)(x+1)f(x)$, so $g(c) = 0$ for $c \in \{0, 1, -1\}$. Conclusion, $D(F) = \mathbb{C} \setminus \{0, 1, -1\}$.

So F defines a function $\mathbb{C} \setminus \{0, 1, -1\} \to \mathbb{C} : c \mapsto \frac{1}{c(c-1)(c+1)}$.

Exercise: $D(F) = \mathbb{C} \iff F \in \mathbb{C}[x]$ (more about this later)

Intuition: functions defined on all $\mathbb{C}$ are polynomials.

Localization of $\mathbb{C}[x]$ **at** $c \in C$ is the set of rational functions $\mathcal{F} \in \mathbb{C}(x)$ with $c \in D(F)$. (Intuition: focuse in on c, expand $\mathbb{C}[x]$)

Lemma 11.12

Let $\mathbb{K}$ be a field, and $c \in \mathbb{K}$. Then $R(c) = \{F \in \mathbb{K}(x) : c \in D(F)\}$ is a subring of $\mathbb{K}(x)$.

If R is a domain, then $R \setminus \{0\}$ is multiplicatively closed.

Lemma 11.13

Let $\mathcal{P}$ be an ideal of a commutative ring. Then $R \setminus \mathcal{P}$ is multiplicatively closed if and only if $\mathcal{P}$ is prime.

Note: iF $\mathcal{P}$ is a prime ideal of a domain R, then $S = R \setminus \mathcal{P}$ doesn't contain 0 or any zero divisors.

localization of R at $\mathcal{P}$

Let $\mathcal{P}$ be a prime ideal of a domain R. The **localization of R at $\mathcal{P}$** is the ring $R_{\mathcal{P}} := S^{-1}R$, where $S = R \setminus \mathcal{P}$.

Further reading: there's a more general version of localization where S can contain zero divisors, and this can be used to define $R_{\mathcal{P}}$ when R is not a domain.

Lemma 11.14

Let $\mathbb{K}$ be a field and $c \in \mathbb{K}$, so that $(x - c)$ is a maximal ideal in $\mathbb{K}[x]$. Then the localization $\mathbb{K}[x]_{(x-c)}$ is isomorphic to the subring $R(c) \subseteq \mathbb{K}(x)$ of rational functions with c in the domain.

This chain of examples is why $S^{-1}R$ called a "localization".

Proposition 11.15

Let $\mathcal{P}$ be a prime ideal in a domain R. Then $R_{\mathcal{P}}$ has a unique maximal ideal.

local

A commutative ring R is **local** if it has a unique maximal ideal.

Example:

Let p be a prime in $\mathbb{Z}$, so that (p) is prime.

$S = \mathbb{Z} \setminus (p)$ is the set of numbers in $\mathbb{Z}$ which are not divisible by p. Then $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \notin (p)\right\} \subseteq \mathbb{Q}$.

11.5 Products of ideals

product ideal

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. The **product ideal** $\mathcal{I}\mathcal{J}$ is the ideal

$$(\{ab : a \in \mathcal{I}, b \in \mathcal{J}\}),$$

i.e., the ideal generated by products of elements from $\mathcal{I}$ and $\mathcal{J}$.

Example:

If R is commutative, then $Rf \cdot Rg = Rfg$. For instance, in $\mathbb{Z}[x]$, $(x)^2 = (x^2)$.

In $\mathbb{Z}[x, y]$, $(x, y)^2$ contains x^2, y^2, and xy, but not x or y. Note that $x^2 + y^2$ is in $(x, y)^2$, but since it doesn't factor, it's not true that every element of $\mathcal{I}\mathcal{J}$ is a product of elements of $\mathcal{I}$ and $\mathcal{J}$.

Lemma 11.16

Let $\mathcal{I}, \mathcal{J}$ be ideals in a ring R.

1. $\mathcal{I}\mathcal{J} = \left\{\sum_{i=1}^{k} a_i b_i : k \geq 0, a_i \in \mathcal{I}, b_i \in \mathcal{J}\right\}$.
2. If R is commutative, and $\mathcal{I} = (S), \mathcal{J} = (T)$, then $\mathcal{I}\mathcal{J} = (\{ab : a \in S, b \in T\})$.

Note

Another way to say (1) is that $\mathcal{IJ}$ is the subgroup of R^+ generated by products of elements of $\mathcal{I}$ and $\mathcal{J}$.

The reason we need R to be commutative in (2) is so that we don't need to include elements of the form arb for $a \in S, b \in T$, and $r \in R$.

Proof:

1. Let K be the RHS. If $x \in K$, then $-x \in K$, and K is closed under addition, so K is a subgroup.

   If $r, s \in R$, and $x = \sum_{i=1}^{k} a_i b_i \in K$ for $a_i \in \mathcal{I}$, $b_i \in \mathcal{J}$, then $rxs = \sum_{i=1} (ra_i)(b_i s) \in K$, since $ra_i \in \mathcal{I}, b_i s \in J$.

   So K is an ideal. Since K contains the generating set for $\mathcal{IJ}$, and is clearly contained in $\mathcal{IJ}$, must have $\mathcal{IJ} = \mathcal{K}$.

2. Clearly RHS $\subseteq \mathcal{IJ}$, so just need to show $\mathcal{IJ} \subseteq$ RHS. Suppose $x \in \mathcal{I}, y \in \mathcal{J}$. Then $x = \sum a_i s_i, a_i \in R, s_i \in S$, and $y = \sum b_i t_i, b_i \in R, t_i \in T$. So $xy = \sum_{i,j} a_i b_j s_i t_j \in$ RHS.

   Since RHS contains generators for $\mathcal{IJ}$, it contains $\mathcal{IJ}$. □

Lemma 11.17

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. Then $\mathcal{IJ} \subseteq \mathcal{I} \cap \mathcal{J}$.

Proof:

If $a \in \mathcal{I}, b \in \mathcal{J}$, then $ab \in \mathcal{I} \cap \mathcal{J}$, so $\mathcal{I} \cap \mathcal{J}$ contains a generating set for $\mathcal{IJ}$. Since $\mathcal{I} \cap \mathcal{J}$ is an ideal, $\mathcal{IJ} \subseteq \mathcal{I} \cap \mathcal{J}$. □

Example:

Consider $\mathcal{I} = (xy)$ and $\mathcal{J} = (yz)$ in $R[x, y, z]$, R commutative. Then $\mathcal{IJ} = (xy^2z)$, buy $xyz \in \mathcal{I} \cap \mathcal{J}$. So it's not necessarily true that $\mathcal{IJ} = \mathcal{I} \cap \mathcal{J}$.

Lemma 11.18

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. Then $\mathcal{IJ} \subseteq \mathcal{I} \cap \mathcal{J}$.

Proof:

If $a \in \mathcal{I}, b \in \mathcal{J}$, then $ab \in \mathcal{I} \cap \mathcal{J}$, so $\mathcal{I} \cap \mathcal{J}$ contains a generating set for $\mathcal{IJ}$. Since $\mathcal{I} \cap \mathcal{J}$ is an ideal, $\mathcal{IJ} \subseteq \mathcal{I} \cap \mathcal{J}$. □

Example:

Suppose $\mathcal{I} = (x)$ and $\mathcal{J} = (y)$ in $\mathbb{Z}[x, y]$.

$f \in \mathcal{I}$ (resp $\mathcal{J}$) if and only if every monomial contains a positive power of x (resp y). So $f \in \mathcal{I} \cap \mathcal{J}$ if and only if every monomial of f contains a positive power of both x and y.

So $\mathcal{I} \cap \mathcal{J} = (xy) = \mathcal{IJ}$.

11.6 Generalizing the CRT

Recall from group theory: If $m, n \geq 0$, $\gcd(m, n) = 1$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

How did this group isomorphism work?

$$\begin{array}{ccccc} \mathbb{Z}/mn\mathbb{Z} & \to & n\mathbb{Z}/mn\mathbb{Z} \times m\mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & (nx, mx) & \mapsto & (x, x) \end{array}$$

The fact that $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is an isomorphism is called the **Chinese remainder theorem**.

It implies that for any $0 \leq a < m, 0 \leq b < n$, there is a unique $0 \leq x < mn$ such that x is a solution to

$$x \equiv a \mod m \qquad \text{and} \qquad x \equiv b \mod n$$

Is there a connection with ring theory?

Well, $\gcd(m, n) = 1$ if and only if $\text{lcm} = mn$, where lcm is the **least common multiple** of m and n: the smallest integer $k \geq 0$ such that $k = xm = yn$ for $x, y \in \mathbb{Z}$.

Lemma 11.19

$\text{lcm}(m, n) = k$, where $k \geq 0$ and $(m) \cap (n) = (k)$.

Proof:
$k = xm$ and $k = yn$ for some $x, y \in \mathbb{Z}$ if and only if $k \in (m) \cap (n)$. Since $\mathcal{I} = (m) \cap (n)$ is an ideal, $\mathcal{I} = (k)$ where k is the smallest non-negative integer in $\mathcal{I}$. $\square$

CRT: If $(m) \cdot (n) = (m) \cap (n)$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Lemma 11.20

If R, S and T are rings, and $\phi : R \to S, \psi : R \to T$ are homomorphisms, then

$$\phi \times \psi : R \to S \times T : r \mapsto (\phi(r), \psi(r))$$

is a homomorphism.

Proof:
If $x, y \in R$, then

$$(\phi \times \psi)(xy) = (\phi(xy), \psi(xy)) = (\phi(x, \psi(x)))(\phi(y), \psi(y)) = (\phi \times \psi)(x) \cdot (\phi \times \psi)(y)$$

The rest of the proof is left as an exercise. $\square$

$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : x \mapsto (x, x)$ is the product $q_1 \times q_2$, where $q_1 : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and $q_@ : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ are the quotient maps.

Let $\mathcal{I}, \mathcal{J}$ be the ideals in R. Do we get a map $R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J} : \overline{r} \mapsto (\overline{r}, \overline{r})$?

Lemma 11.21

If $\mathcal{I}, \mathcal{J}$ are ideals in a ring R, and $\phi : q_1 \times q_2 : R \to R/\mathcal{I} \times R/\mathcal{J}$ where $q_1 : R \to R/\mathcal{I}$ and $q_2 : R \to R/\mathcal{J}$ are the quotient maps, then $\ker \phi = \mathcal{I} \cap \mathcal{J}$.

As a result, there is a homomorphism $\psi : R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ such that $\psi(\overline{x}) = (q_1(x), q_2(x))$, and $\ker \psi = \mathcal{I} \cap \mathcal{J}/\mathcal{I}\mathcal{J}$.

Proof:
$x \in \ker \phi \iff (q_1(x), q_2(x)) = (0, 0) \iff x \in \ker q_1 \cap \ker q_2$.

For the second part, note that $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J} = \ker \phi$. By the universal property of quotient rings. there is a homomorphism $\psi : R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ such that $\psi(\overline{x}) = \phi(x)$ for all $x \in R$, and $\ker \psi = \mathcal{I} \cap \mathcal{J}/\mathcal{I}\mathcal{J}$ by the correspondence theorem, since $\psi(\overline{x}) = 0 \iff \phi(x) = 0$. $\square$

Let $\mathcal{I}, \mathcal{J}$ be ideals in R. Is $\phi :: R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J} : \overline{r} \mapsto (\overline{r}, \overline{r})$ a ring isomorphism?

By Lemma, ϕ is injective if and only if $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$. Is injective sufficient to prove surjectivity?

Example:
Let $R = \mathbb{Z}, \mathcal{I} = (m), \mathcal{J} = (n)$. Then $|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$. By pigeonhole principle, ϕ is surjective if and only if ϕ is injective. Conclusion: TFAE:

1. ϕ is a group isomorphism
2. ϕ is a ring isomorphism
3. $(m) \cap (m) = (mn)$, i.e., $\operatorname{lcm}(m, n) = mn$, i.e., $\gcd(m, n) = 1$.

Example:
Consider $(2), (x)$ in $\mathbb{Z}[x]$. Not hard to see that $(2) \cap (x) = 2x$.

Is $\phi : \mathbb{Z}[x]/(2x) \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x) : p \mapsto (\overline{p}, \overline{p})$ surjective?

Suppose $p \in \mathbb{Z}[x]$ such that $p(x) = 0$ in $\mathbb{Z}[x]/(2)$, so all coefficients of p are even. But then $p(x) - 1$ must have a constant term, so $p(x) - 1 \notin (x)$. Conclusion: $(0, 1) \notin \operatorname{Im} \phi$.

So ϕ is injective but not surjective.

Index

H

I

K

L

M

N

O

P

Q

R

S

T

U

W

Z