PMATH 347: Groups and Rings

University of Waterloo
William Slofstra
Spring 2021

Marco Yang

Last updated: August 1, 2021

Contents

1 Groups

2 Subgroups and Homomorphisms

6 Classification of Groups

7 Rings

8 Ideals and Quotient Rings

9 Maximal and Prime Ideals

10 Fields of Fractions and the Chinese Remainder Theorem

11 PIDs and UFDs

Week 1: Groups

1: Binary operations and definition of a group

Binary operations

Definition — binary operation

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

Notation:

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

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

  or inline notation (typically for letters)

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

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

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

Example

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

Definition — k-ary operation

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

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

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

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

Associative operations

Definition — associative

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

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

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

Many operations mentioned so far are associative:

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

Subtraction and division are not associative:

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

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

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

Example

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

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

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

Proof.

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

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

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

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

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

So by repeatedly applying associativity,

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

□

Commutative (abelian) operations

Definition — commutative (abelian)

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

Many familiar operations are commutative:

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

The following operations are **not** commutative:

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

Note:

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

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

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

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

Identities

Definition — identity

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

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

for all $x \in X$.

Example

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

Lemma

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

Proof.

$e = e \boxtimes e' = e'$. □

Inverses

Definition — inverse

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

Example

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

Lemma

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

Proof.

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

Corollaries:

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

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

Exercise

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

Properties of inverses

Lemma

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

Proof.

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

$\square$

Inverses and solving equations

Proposition

Let $\boxtimes$ be an associative binary operation on X with an identity e, and let x and y be variables taking values in X.
An element $a \in X$ is invertible if and only if the equations $a \boxtimes x = b$ and $y \boxtimes a = b$ have unique solutions for all $b \in X$.

Proof.

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

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

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

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

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

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

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

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

□

Left and right cancellation property

Proposition

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

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

Proof.

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

□

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

Groups

Definition — group

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

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

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

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

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

Terminology:

- Usually we refer to $(G, \boxtimes)$ simply as G, and just assume the operation is given. (Note: we still need to clearly specify the operation for each group we work with.)
- It's cumbersome to write $\boxtimes$, so usually we use one of the following options:
  - Use $\cdot$ as the standard symbol: $g \cdot h$ is the product of $g, h \in G$.
  - Drop the symbol entirely: gh is the product of $g, h \in G$.
- The identity of G is denoted by e (or e_G for clarity). Also used are 1 and 1_G.
- g^{-1} is defined for all $g \in G$. The function $G \to G : g \mapsto g^{-1}$ can be regarded as a unary operation on G.
- Consider $\iota\colon G \to G : g \mapsto g^{-1}$. Since $(g^{-1})^{-1} = g$, $\iota \circ \iota = \mathrm{Id}_G$, the identity map $G \to G$. In particular, ι is a bijection (injective and surjective).
- If $g \in G$, then
  $$g^n := \underbrace{g \cdots g}_{n \text{ times}}$$
  and
  $$g^{-n} := (g^{-1})^n = (g^n)^{-1}$$
  where $g^0 := e$. Exercise: if $m, n \in \mathbb{Z}$, then $(g^n)^m = g^{mn}$.
- If $g, h \in G$, then
  $$(gh)^n = gh \cdots gh,$$
  which is not necessarily the same as $g^n h^n$ if G is not abelian.

Example

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

A non-abelian example

All the previous examples are abelian.

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

Proposition

$\mathrm{GL}_n(\mathbb{K})$ 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 on $\mathrm{GL}_n(\mathbb{K})$. 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 $AB \neq BA$. □

Additive notation

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

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

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

Writing g^n in additive notation gives

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

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

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

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

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

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

Multiplication table

Definition — multiplication table

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

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

Example

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

	0	1
0	0	1
1	1	0

Order of elements

Definition — order of a group element

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

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

Easy properties:

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

Example

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

Lemma

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

Proof.

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

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

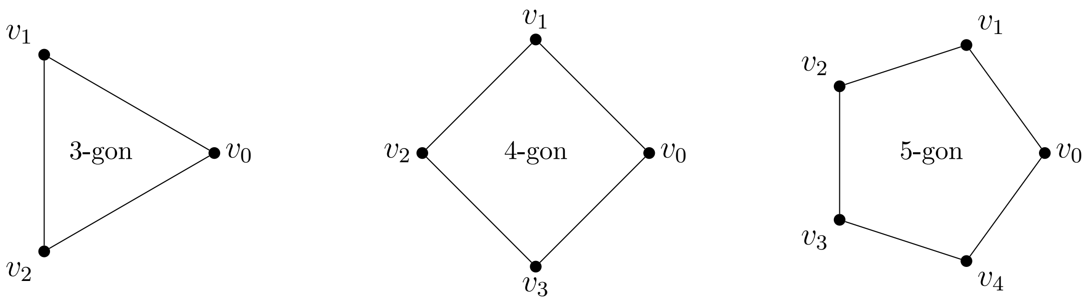
2: Dihedral and permutation groups

Dihedral groups

Definition — n-gon

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

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



Definition — symmetry, dihedral group

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

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

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

Proposition

D_{2n} is a group under composition.

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

Lemma

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

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

Proof.

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

□

Corollary

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

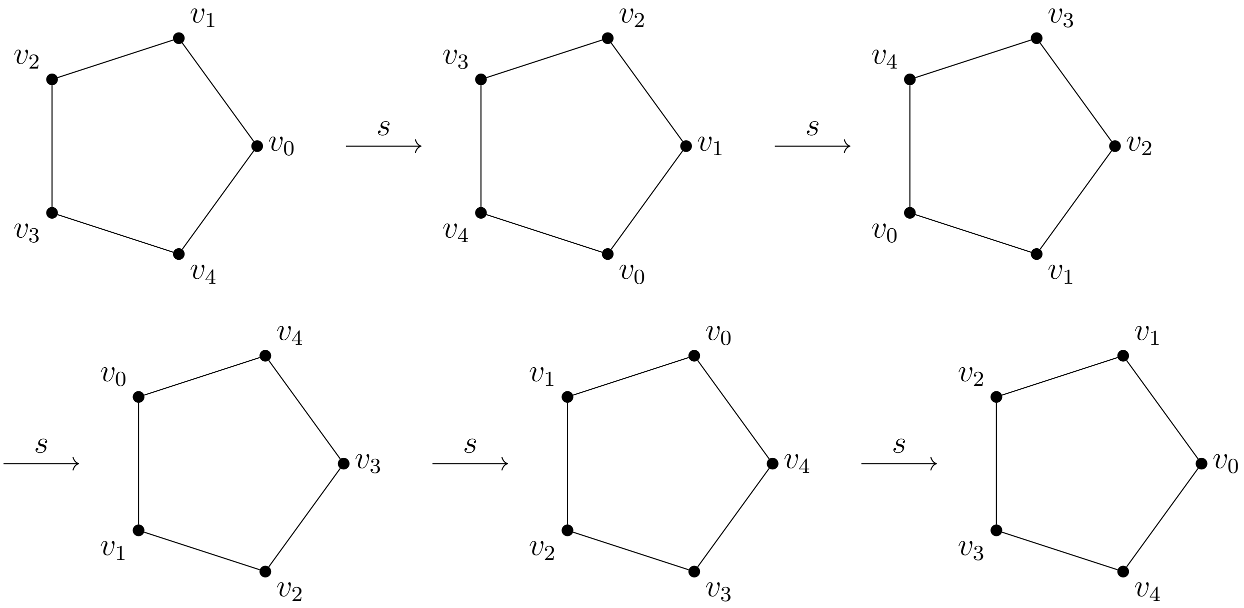
Proof.

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

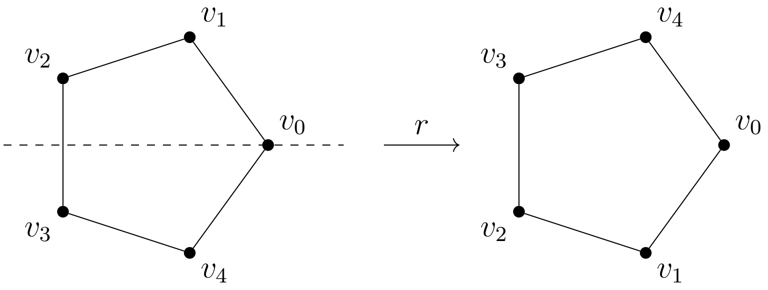
Intuitively, we can ask: for every pair of adjacent vertices (v_i, v_j), is there an element $T \in D_{2n}$ with $T(v_0) = v_i$ and $T(v_1) = v_j$? If yes, then $|D_{2n}| = 2n$.

Special elements of D_{2n}

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



Let r be reflection through the x-axis.



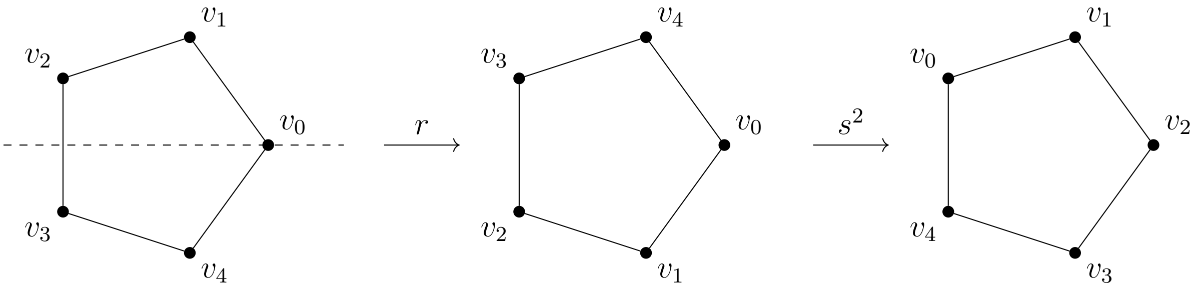
$|r| = 2$, that is, $r^2 = e$ and $r \neq e$.

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

Putting rotation and reflection together

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

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



Proposition

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

So what is rs?

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

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

Corollary

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

In summary:

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

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

What's group theory about?

Basic answer: sets with one binary operation.

Better answer: group theory is the study of symmetry.

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

Kleinian view of geometry:

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

Permutation groups

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

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

is an associative operation with an identity Id_X.

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

Proposition

S_X is a group under $\circ$.

Proof.

Homework. □

Definition — symmetric group

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

Elements of S_n are bijections $\pi \colon \{1,\dots,n\} \to \{1,\dots,n\}$.

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

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

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

Permutations

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

1. Two-line representation:
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}$$

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

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

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

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

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

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

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

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

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

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

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

Fixed points and support sets

Definition — fixed point, support set

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

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

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

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

Example

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

Some notes:

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

Commuting elements

Definition — commute

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

Lemma

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

Proof.

Suppose $1 \le i \le n$.

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

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

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

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

Cycles

Definition — cycle

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

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

Example

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

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

Example

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

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

Week 2: Subgroups and Homomorphisms

3: Subgroups

Subgroups

Definition — subgroup

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

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

Notation: $H \leq G$.

Example

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

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

Example

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

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

Proof.

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

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

Checking subgroup properties:

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

□

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

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

Example

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

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

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

Definition — trivial subgroup, proper subgroup

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

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

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

Example

Some non-subgroups:

- $\mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} : x \geq 0\}$ is not a subgroup of $\mathbb{Q}^{+}$.

  If $x, y \in \mathbb{Q}_{\geq 0}$, then $x + y \in \mathbb{Q}_{\geq 0}$. Also, $0 \in \mathbb{Q}_{\geq 0}$.

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

Proposition

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

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

Proof.

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

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

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

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

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

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

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

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

Example

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

Speeding up the subgroup check

Proposition

H is a subgroup of G if and only if

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

Proof.

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

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

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

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

□

Example

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

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

Check:

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

W is a subgroup by the proposition.

Finite subgroups

Proposition

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

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

Proof.

The forward direction is trivial.

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

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

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

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

Subgroups generated by a set

Proposition

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

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

is a subgroup of G.

Proof.

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

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

By proposition, K is a subgroup of G. □

Definition — subgroup generated by a set

Let S be a subset of a group G.

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

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

Notes:

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

Example

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

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

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

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

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

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

Proposition

If $S \subset G$, let

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

Then $\langle S \rangle = K$.

Proof.

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

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

Claim 2: K is a subgroup.

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

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

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

So K is a subgroup.

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

Thus $\langle S \rangle = K$. □

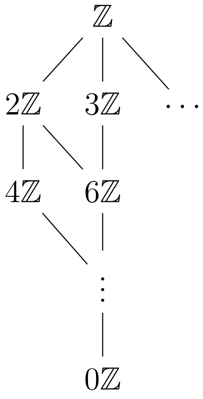
Lattice of subgroups

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

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

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

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



4: Cyclic groups

Generators and cyclic groups

Definition — generate, cyclic

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

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

Example

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

Lemma

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

Proof.

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

□

Questions:

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

Order of cyclic groups

Proposition

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

Proof.

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

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

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

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

Examples in closer detail

Example

For $G = \mathbb{Z}$:

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

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

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

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

Example

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

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

Questions:

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

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

Lemma

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

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

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

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

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

Lemma

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

Proof.

Homework. □

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

Lemma

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

Proof.

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

Lemma

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

Proof.

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

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

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

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

Proposition

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

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

Proof.

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

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

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

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

Corollary

Let $n \geq 1$.

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

Proof.

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

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

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

Example

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

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

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

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

Proofs later

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

5: Homomorphisms

Homomorphisms

Definition — homomorphism (morphism)

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

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

for all $g, h \in G$.

A homomorphism preserves the group operation from G to H.

Example

- For $\mathbb{K}$ a field, $\mathbb{K}^\times = \{a \in \mathbb{K} : a \neq 0\}$ is a group with operation $\cdot$.

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

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

- Additive notation: $\phi\colon (G, +) \to (H, +)$ is a homomorphism if $\phi(x+y) = \phi(x)+\phi(y)$ for all $x, y \in G$.

  $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ is a homomorphism for any $m \in \mathbb{Z}$ since $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{Z}$.

- If V, W are vector spaces and $T\colon V \to W$ 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 because $e^{x+y} \neq e^x + e^y$ in general (take $x = y = 0$).

Lemma

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

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

Proof.

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

□

Making new homomorphisms from old

Lemma

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

Proof.

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

Lemma

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

Proof.

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

Corollary

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

Proof.

$\phi|_K = \phi \circ i$, where $i\colon K \to G$ is the inclusion $x \mapsto x$. □

Images of homomorphisms

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

Proposition

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

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

Proof.

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

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

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

Definition — image

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

Example

- Let $\phi\colon \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$.

  $e^x > 0$ 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 $i\colon K \to G$ is inclusion, then $\operatorname{Im} i = K$.
- For $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$, $\phi(\mathbb{Z}) = m\mathbb{Z}$.

Properties of images

Lemma

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

Proof.

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

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

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

Lemma

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

Proof.
Obvious from definition. □

Corollary

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

Proposition

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

Proof.

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

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

□

Pulling back subgroups

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

Proposition

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

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

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

Proof.

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

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

The kernel of a homomorphism

Definition — kernel

If $\phi\colon G \to H$ 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 $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$, we have $\ker\det = \{A \in \mathrm{GL}_n(\mathbb{K}) : \det(A) = 1\}$.

  This subgroup of $\mathrm{GL}_n(\mathbb{K})$ is called the **special linear group**, denoted by $\mathrm{SL}_n(\mathbb{K})$.
- If $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$, 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 $\phi\colon \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$, then $e^x = 1$ if and only if $x = 0$, so $\ker\phi = \{0\}$.

Proposition

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

Proof.

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

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

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

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

□

Application: subgroups of cyclic groups

Proposition

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

Proof.

We need the following facts:

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

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

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

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

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

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

by (3).

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

Review on bijections

Definition — bijection

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

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

Proposition

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

Isomorphisms

Definition — isomorphism

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

Lemma

$\phi\colon G \to H$ 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 $\phi\colon G \to H$ is injective, then ϕ induces an isomorphism $G \to \operatorname{Im}\phi$.
- $\mathbb{Z} \to m\mathbb{Z} : k \mapsto mk$ is an isomorphism.

Proposition

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

Proof.

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

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

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

Corollary

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

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

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

Proof.

($\Longleftarrow$) If ψ exists, then ϕ is a bijection.

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

□

Definition — isomorphic

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

Notation: $G \cong H$.

Key facts:

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

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

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

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

- $G \cong G$ (reflexivity).

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

Isomorphism as a relation

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

If $\phi\colon G \to H$ 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.

Isomorphisms of cyclic groups

Proposition

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

Proof.

The forward implication is obvious.

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

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

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

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

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

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

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

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

Thus ϕ is an isomorphism. □

Corollary

Suppose G is a cyclic group.

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

Corollary

Cyclic groups are abelian.

Exercise

Prove the previous corollary without the corollary before it.

Multiplicative notation for cyclic groups

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

Definition

Let a be a formal indeterminate. Let

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

Of course, we have:

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

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

6: Cosets and Lagrange's Theorem

Affine spaces

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

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

Definition — coset

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

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

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

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

Example

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

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

Cosets in the dihedral group

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

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

The right cosets of H are:

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

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

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

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

The left cosets of H are:

- $eH = H$
- $s^iH = H$
- $s^irH = rs^{-i}H = rH$

Notice

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

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

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

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

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

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

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

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

Sets of cosets

Definition — set of cosets

If $H \leq G$, let

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

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

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

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

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

Example

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

Example

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

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

so

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

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

Cosets of a kernel

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

Lemma

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

Proof.

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

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

A similar argument using right cosets shows the set of solutions is also Hx_0. □

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

Proposition

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

Proof.

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

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

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

Example

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

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

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

Indexes and Lagrange's theorem

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

Definition — index

The **index** of H in G is

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

Theorem — Lagrange's theorem

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

Why use left cosets in the definition?

Proposition

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

Proof.

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

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

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

Finally, ψ is an inverse to ϕ. □

Corollary

If $H \leq G$ then

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

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

Example

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

Consequences of Lagrange's theorem

Corollary

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

Proof.

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

Proposition

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

Proof.

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

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

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

Corollary

If $\phi \colon G \to K$ 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 $|\operatorname{Im} \phi| = [G : \ker \phi]$ by definition. Lagrange's theorem then implies $|\operatorname{Im} \phi|$ divides $|G|$ (and $|K|$). □

Exercise

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

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

Beginning to prove Lagrange's theorem

Recall

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

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

Does this work in general?

Proposition

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

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

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

Proof.

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

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

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

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

Partitions

Definition — partition

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

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

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

We can show cosets partition G:

Corollary

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

Proof.

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

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

We can also show cosets have the same size:

Lemma

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

Proof.

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

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

Proof of Lagrange's theorem

Proof (Lagrange's theorem).

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

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

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

So $|G| = [G : H]|H|$. □

Equivalence relations

Definition — relation

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

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

Example

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

Definition — equivalence relation

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

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

Example

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

Equivalence classes

Definition — equivalence class

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

Proposition

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

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

Proof.

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

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

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

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

Equivalence relations yield partitions:

Corollary

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

Partitions yield equivalence relations:

Corollary

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

Proof.

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

Let's apply this to cosets:

Proposition

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

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

7: Normal subgroups

When is a left coset a right coset?

From before:

Proposition

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

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

By symmetry:

Proposition

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

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

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

Lemma

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

Proof.

$g \in Hg = hH$, so $gH = hH$. □

Definition — normal subgroup

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

Notation: $N \trianglelefteq G$.

Conjugation and set multiplication

Definition — conjugate

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

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

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

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

Equivalent characterizations of normal subgroups

Proposition

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

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

Proof.

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

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

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

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

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

(6) $\implies$ (1) is similar. □

Example

- $\langle s\rangle \leq D_{2n}$: we already saw $G/\langle s\rangle = \langle s\rangle\backslash G$. So $\langle s\rangle \trianglelefteq D_{2n}$. We can also check $s^i\langle s\rangle s^{-i} = \langle s\rangle$ and $r\langle s\rangle r^{-1} = \langle s\rangle$ (since $rs^ir^{-1} = s^{-i}$).
- $\langle r\rangle \leq D_{2n}$: $G/\langle r\rangle \neq \langle r\rangle\backslash G$, 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 $\phi\colon G \to K$ is a homomorphism, then $\ker\phi$ is normal.

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

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

Warning: normal subgroups are not transitive

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

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

Normalizers

Definition — normalizer

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

Lemma

$N_G(S) \leq G$.

Proof.

$eSe = S$, 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

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

Corollary

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

Proof.

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

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

Lemma

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

Proof.

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

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

Corollary

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

Centres

Definition — centre

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

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

Example

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

Proposition

$Z(G) \trianglelefteq G$.

Proof (exercise).

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

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

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

Thus $Z(G) \leq G$.

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

8: Product groups

Getting more groups

Proposition

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

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

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

Proof (homework).

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

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

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

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

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

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

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

Definition — product group

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

Example: Klein 4-group

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

The group's multiplication table is

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

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

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

Two subgroups of a product

Proposition

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

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

Proof (homework).

□

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

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

These subgroups commute.

Lemma

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

Proof (homework).

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

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

□

Corollary

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

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

Homomorphisms between products

Lemma

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

Proof.

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

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

□

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

Corollary

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

Proof.

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

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

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

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

Corollary

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

Proof.

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

Proposition

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

Proof.

See homework for equivalent proof. □

Groups of small order (revised)

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

Proposition

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

Proof (homework).

□

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

How do we know if a group is a product?

Recall:

Proposition

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

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

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

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

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

Unique factorizations

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

Lemma

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

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

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

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

Lemma

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

Proof.

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

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

Internal (direct) products

Definition — internal direct product

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

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

Example

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

Theorem

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

Proof.

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

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

A weaker condition

Lemma

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

Proof.

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

Similar for K. □

Proposition

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

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

Definition — commutator

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

Lemma

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

Proof (proposition).

We already saw the forward implication.

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

Week 4: Quotients and the Isomorphism Theorems

9: Quotient groups

Left cosets and functions

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

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

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

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

Definition — function

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

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

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

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

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

Lemma

The relation $\to$ 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).

Proof.

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

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

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

In the reverse direction, suppose H is normal.

> Then $h^{-1}Hh \subseteq H$ so $(h^{-1}Hh) \cdot H \subseteq H$. Since $e \in h^{-1}Hh$, we actually get $(h^{-1}Hh) \cdot H = H$. Hence $gH \cdot hH = gh(h^{-1}Hh) \cdot H = ghH$.
>
> Finally, say $(S, T) \to R$ and $(S, T) \to R'$ for $S, T, R, R' \in G/H$. Then $R = S \cdot T = R'$. So $\to$ is a function. □

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

Quotient groups

Theorem

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

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

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

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

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

Proof.

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

Then

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

so $\cdot$ is associative. Next,

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

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

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

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

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

Normal subgroups are kernels

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

Corollary

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

Proof.

Take $K = G/N$ and $q\colon G \to G/N$ the quotient homomorphism. Then $\ker q = N$. □

Examples of quotient groups

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

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

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

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

Multiplication table:

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

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

Example: N not normal

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

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

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

Homework.

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

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

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

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

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

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

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

In general, we can look at:

- $G/Z(G)$ for any group G
- $G/\ker\phi$ for any homomorphism $\phi\colon G \to K$

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

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

10: First isomorphism and correspondence theorems

Homomorphisms from quotients

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

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

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

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

Given ϕ, when can we fill in ψ so that the diagram **commutes** (the paths are equivalent)?

Theorem — Universal property of quotients

Suppose $\phi\colon G \to K$ is a homomorphism and $N \trianglelefteq G$. Let $q\colon G \to G/N$ be the quotient homomorphism. Then there is a homomorphism $\psi\colon G/N \to K$ 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, we can fill in ψ if and only if $N \subseteq \ker \phi$.

Definition — set of morphisms

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

Corollary

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

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

is a bijection.

Comparison to universal property of products

From before (but without the name):

Theorem — Universal property of products

Let $\alpha\colon H \to G$ and $\beta\colon K \to G$ be homomorphisms, and let $i_H\colon H \to H \times K$ and $i_K\colon K \to H \times K$ be the inclusions of H and K in $H \times K$. Then there is a homomorphism $\phi\colon H \times K \to G$ 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 $h \in H$ and $k \in K$.

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

Corollary

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

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

Proving the universal property of quotients

Lemma

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

Proof.

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

Restatement for reference:

Theorem — Universal property of quotients

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

Proof.

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

Suppose $N \subseteq \ker\phi$. Define $\psi\colon G/N \to K : [g] \mapsto \phi(g)$. 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 $\psi'\colon G/N \to K$ is another homomorphism with $\psi' \circ q = \phi$, then $\psi' \circ q = \psi \circ q$ which implies $\psi' = \psi$ by the lemma (q is surjective). So uniqueness holds. □

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

The first isomorphism theorem

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

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

This looks like what we just did!

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

Theorem — First isomorphism theorem

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

Proof.

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

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

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

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

Example

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

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

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

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

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

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

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

There are several more examples on the homework.

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

Images and pullbacks

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

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

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

From week 2:

Proposition

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

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

Proposition

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

The pullback of a subgroup is a subgroup.

Subgroup correspondence for isomorphisms

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

$$\begin{tikzcd}[column sep=huge] \text{Subgroups of } G \arrow[r, shift left, "K \mapsto \phi(K)"] & \text{Subgroups of } H \arrow[l, shift left, "\phi^{-1}(K') \mapsfrom K'"] \end{tikzcd}$$

Furthermore:

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

Set operation identities

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

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

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

One consequence of these identities is that order is preserved:

Lemma

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

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

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

Another consequence is that pullbacks preserve intersection:

Lemma

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

Set operation identities for surjections

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

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

Lemma

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

Definition — set of subgroups

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

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

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

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

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

Lemma

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

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

Proof.

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

□

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

Theorem — Correspondence theorem

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

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

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

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

Proof.

Since 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.

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

□

Correspondence theorem for quotient groups

If $N \trianglelefteq G$, then $q\colon G \to G/N$ is a surjection.

Theorem — Correspondence theorem for quotient groups

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

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

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

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

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

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

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

Identifying $q(K)$

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

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

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

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

Proposition

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

Because of this isomorphism, we use the following notation:

Definition — subgroup $q(K)$

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

Example

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

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

- $\operatorname{GL}_n \mathbb{K}/\operatorname{SL}_n \mathbb{K} \cong \mathbb{K}^\times$, 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 many).

11: Second and third isomorphism theorems

Third isomorphism theorem

What about quotients of quotients?

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

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

Theorem — Third isomorphism theorem (informal version)

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

Example

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

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

Theorem — Third isomorphism theorem

Let $N \trianglelefteq G$ and $N \leq K \trianglelefteq G$. Let
- q_1 be the quotient map $G \to G/N$,
- 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 $\psi \colon G/K \to (G/N)/(K/N)$ 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 $\ker q_2 \circ q_1 = (q_2 \circ q_1)^{-1}(\{e\}) = q_1^{-1}(q_2^{-1}(\{e\})) = q_1^{-1}(K/N) = K$.

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

By the first isomorphism theorem, there is an isomorphism $\psi \colon G/K \to (G/N)/(K/N)$ 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

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

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

Proposition

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

These are equivalent by the first isomorphism theorem.

Proof.

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

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 surjective.

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

Then f is a bijection, so the indices must be equal. □

Revisiting products

Recall this lemma:

Lemma

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

Which motivated this definition:

Definition — internal direct product

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

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

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

Lemma

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

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

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

Lemma

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

Proof.

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

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

Corollary

$H/(H \cap K) \to X\colon h(H \cap K) \to hK$ is a bijection.

Proof.

By the lemma, this is well-defined and injective. Surjectivity is obvious. □

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

Proposition

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

If H and K are finite, another way to think of this formula is $[H : H \cap K] = |X| = \frac{|HK|}{|K|}$. Is the fraction an index as well? Maybe–HK is not necessarily a group.

Proposition

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

Proof.

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

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

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

When is $KH \subseteq HK$?

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

Corollary

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

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

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

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

Second isomorphism theorem

Theorem — Second isomorphism theorem

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

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

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

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

By the first isomorphism theorem, there is an isomorphism ψ as desired. □

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

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

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

Since $K \trianglelefteq \mathrm{GL}_n \mathbb{C}$, $N_{\mathrm{GL}_n \mathbb{C}}(K) = \mathrm{GL}_n \mathbb{C}$.

Take $H = \mathrm{SL}_n \mathbb{C} = \{M \in \mathrm{GL}_n \mathbb{C} : \det M = 1\} \trianglelefteq \mathrm{GL}_n \mathbb{C} = N_{\mathrm{GL}_n \mathbb{C}}(K)$, so $HK \leq \mathrm{GL}_n \mathbb{C}$ by the second isomorphism theorem.

Suppose $M \in \mathrm{GL}_n \mathbb{C}$ and let $\lambda = \det M$. Then $\det \lambda^{-1/n} M = \lambda^{-1} \det M = 1$, so $\lambda^{-1/n} M \in H$ (for any choice of $\lambda^{-1/n}$).

We conclude $\mathrm{GL}_n \mathbb{C} = HK$.

Now define $C_n := H \cap K = \{\lambda 1 : \lambda^n = 1\} = \{e^{2\pi i k/n} : k = 0, \ldots, n-1\}$. (Note $C_n \cong \mathbb{Z}/n\mathbb{Z}$.)

By the second isomorphism theorem, $\mathrm{PGL}_n \mathbb{C} \cong \mathrm{SL}_n \mathbb{C}/C_n$.

Week 5: Group Actions

12: Group actions and Cayley's theorem

Group actions

Example

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

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

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

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

Example

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

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

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

Group actions can reveal a lot about a group.

Definition — (left) action

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

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

Example

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

Proposition

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

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

Lemma

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

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

Invariant subsets

Groups aren't tied to a particular action.

> **Example**
>
> D_{2n} was defined as a 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 sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i+1}$
> - $s^i r$ sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i-1}$

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

Definition — invariant under an action

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

Lemma

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

> **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 the trivial action.

Actions on functions

Proposition

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

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

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

Proof (homework).

□

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

Actions on subsets

Proposition

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

Proof.

Let $S \in 2^X$.

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

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

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

□

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

Left regular actions

Does every group act on some set?

Lemma

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

Proof.

Immediate from group definition. □

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

Lemma

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

Proof.

G/H is an invariant subset of 2^G. □

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

Right actions

Example

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

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

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

Can we fix this?

Definition — (right) action

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

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

Example

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

Can we reconcile right and left actions somehow?

Proposition

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

Proof.

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

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

□

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

Permutation representations

Lemma

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

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

Proof.

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

□

Corollary

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

Definition — permutation representation

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

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

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

Permutation representations of the dihedral group

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

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

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

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

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

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

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

Theorem

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

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

Proof.

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

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

□

Faithful actions

Definition — kernel, faithful

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

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

Lemma

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

Proof.

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

Example

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

Does every group act faithfully on some set?

Theorem — Cayley's theorem

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

Proof.

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

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

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

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

> **Example**
>
> Let $G = \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$.
>
> By Cayley's theorem, G is isomorphic to a subgroup of S_2.
>
> $[0] + [0] = [0]$ and $[0] + [1] = [1]$, so $[0] \mapsto e$ in S_2.
>
> $[1] + [0] = [1]$ and $[1] + [1] = [0]$, so $[1] \mapsto (12)$ in S_2.

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

> **Example**
>
> D_6 has order 6, so it is isomorphic to a subgroup of S_6.
>
> But D_6 acts faithfully on the vertices of the 3-gon, so there is an injective homomorphism $D_6 \to S_3$; since $|D_6| = |S_3| = 6$, this is an isomorphism.
>
> But $|S_6| = 6! \gg 6$, so the left regular representation may be much larger in terms of space.

13: Orbits and stabilizers

Orbits

Definition — orbit

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

Example

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

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

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

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

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

- If $1 \leq i \neq j \leq n$, then we can find $\pi \in S_n$ where $\pi(i) = j$. So $\mathcal{O}_i = \{1, \ldots, n\}$ for all i. We conclude the action of S_n on $\{1, \ldots, n\}$ is transitive and has one orbit.

- More generally, the action of S_X on X is transitive and has one orbit.

- Suppose $\sigma \in S_n$. What are the orbits of $\langle \sigma \rangle$ on $\{1, \ldots, n\}$?

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

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

Equivalence relation from a G-action

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

Definition

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

Lemma

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

Proof.

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

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

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

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

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

Proposition

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

Definition — set of representatives

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

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

Corollary

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

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

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

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

Stabilizers

Definition — stabilizer

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

Proposition

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

Proof.

First, $e \in G_x$.

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

Third, if $g \in G_x$, then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = e \cdot x = x \implies g^{-1} \in G_x$. □

Theorem — Orbit-stabilizer theorem

If G acts on X, and $x \in X$, then there is a bijection $G/G_x \to \mathcal{O}_x : gG_x \mapsto g \cdot x$.

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. □

Corollary

If G acts on X and $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

Example: S_n

Let $G = S_n$ and $X = \{1, \ldots, n\}$.

We know the action of G on X is transitive, so $\mathcal{O}_i = X$ for any i.

Then $n = |\mathcal{O}_i| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{n!}{|G_i|}$. Hence $|G_i| = (n-1)!$ for any i.

Thus the stabilizer of i is $G_i = \{\pi \in S_n : \pi(i) = i\}$.

For a concrete example, if $n = 4$, then $G_1 = \{e, (23), (24), (34), (234), (243)\}$.

In general, $G_i \cong S_{n-1}$ (add 1 to each number in S_{n-1} which is $\geq i$), so we see $|G_i| = (n-1)!$ directly.

Example: G/H

Recall that the action of G on G/H is $g \cdot kH = gkH$ (i.e. usual set multiplication).

Proposition

Suppose $H \leq G$. Then the left multiplication action of G on G/H is transitive, and $G_{eH} = H$.

Proof.

If $gH \in G/H$, then $gH = g \cdot eH$, so $\mathcal{O}_{eH} = G/H$.

Also, $g \cdot eH = eH \iff gH = H \iff g \in H$. □

In this case, the orbit-stabilizer theorem states that $\mathcal{O}_{eH} = G/H$ is in bijection with G/H (tautology).

Kernel versus stabilizer

If G acts on X, then the kernel of the action is $\{g \in G : g \cdot x = x \text{ for all } x\}$.

Meanwhile, the stabilizer $G_x = \{g \in G : g \cdot x = x\}$ has x fixed.

Consequently, if H is the kernel of the action, then $H \leq G_x$ for all $x \in X$.

Proposition

If G acts on X, then the kernel of the action is $\bigcap_{x \in X} G_x$, the intersection of the stabilizers.

Proof.

g is in the kernel if and only if $g \in G_x$ for all $x \in X$. □

An application:

Theorem

If G is finite and $H \leq G$ has index $[G : H] = p$ where p is the smallest prime dividing $|G|$, then $H \trianglelefteq G$.

Proof.

Let K be the kernel of the action of G on G/H (so K is normal).

By the proposition, $K \leq H = G_{eH}$. Then let $k = [H : K] = \frac{|H|}{|K|}$.

Now $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk$.

By the first isomorphism theorem, G/K is isomorphic to a subgroup of S_p. So $|G/K| = kp \mid p! = |S_p| \implies k \mid (p-1)!$.

But we also have $k \mid |G|$. Since p is the smallest prime dividing $|G|$, we must have $k = 1$. Hence $|H| = |K|$ so $H = K$. □

Conjugation actions

Recall left multiplication defines a left action of G on G. There is, however, another natural left action.

Lemma

$G \times G \to G : (g, k) \mapsto gkg^{-1}$ defines an action of G on G.

This action is called the **conjugation action** of G on G.

To avoid conjustion with the left multiplication action here, we'll denote it by $g \bullet k = gkg^{-1}$.

(In practice, there is no convention about $\cdot$ and $\bullet$; specify your choices when writing.)

Proof.

If $k \in G$, then $e \bullet k = eke = k$.

If $g, h, k \in G$, then $g \bullet (h \bullet k) = g \bullet hkh^{-1} = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = gh \bullet k$. □

Definition — conjugacy class, centralizer

The orbit of $k \in G$ under the conjugation action is called the **conjugacy class** of k, denoted by $\mathrm{Conj}_G(k)$.

The stabilizer of $k \in G$ is called the **centralizer** of k in G, denoted by $C_G(k)$.

By definition, $\mathrm{Conj}_G(k) = \{gkg^{-1} : g \in G\}$.

$C_G(k) = \{g \in G : gkg^{-1} = k\} = \{g \in G : gk = kg\}$, namely the centralizer is the set of elements in G which commute with k.

By the orbit-stabilizer theorem, $|\mathrm{Conj}_G(k)| = [G : C_G(k)]$.

For example: $\mathrm{Conj}(e) = \{geg^{-1} : g \in G\} = \{e\}$ and $C_G(e) = G$.

Note the conjugation action of G on G induces an action of G on 2^G. In particular, if $g \in G$ and $S \subseteq G$, then $g \bullet S = \{g \bullet h : h \in S\} = \{ghg^{-1} : h \in S\} = gSg^{-1} = N_G(S)$ (the normalizer of S in G).

Example: matrices

One important instance of the conjugation action is with $\mathrm{GL}_n \mathbb{K}$.

Actually, if A, B are $n \times n$ matrices and A is invertbile, then ABA^{-1} makes sense even if B is not invertible.

Exercise

Show $\mathrm{GL}_n \mathbb{K}$ acts on $M_n\mathbb{K}$ by conjugation, where $M_n\mathbb{K}$ is the set of $n \times n$ matrices over $\mathbb{K}$.

Recall matrices A and B are **similar** if there is $C \in \mathrm{GL}_n \mathbb{K}$ such that $CAC^{-1} = B$. This is the equivalence relation $\sim_{\mathrm{GL}_n \mathbb{K}}$.

The orbits of the conjugation action of $\mathrm{GL}_n \mathbb{K}$ on $M_n\mathbb{K}$ are called **similarity classes**.

A matrix A is **diagonalizable** if it is similar to a diagonal matrix.

When $\mathbb{K} = \mathbb{C}$, every similarity class contains exactly one matrix in Jordan normal form; matrices in Jordan normal form give a set of representatives for $\sim_{\mathrm{GL}_n \mathbb{K}}$.

Class equation and Cauchy's theorem

Using standard facts about orbits,

$$|G| = \sum_{g \in S} |\mathrm{Conj}(g)| = \sum_{g \in S} [G : C_G(g)]$$

where S is a set of representatives for conjugacy classes.

We could simplify this by pulling out conjugacy classes of size 1:

Lemma

$|\mathrm{Conj}(k)| = 1 \iff C_G(k) = G \iff k \in Z(G)$.

Proof.

$|\mathrm{Conj}(k)| = 1$ if and only if $gkg^{-1} = k$ for all $g \in G$ (since $k \in \mathrm{Conj}(k)$ always) if and only if $C_G(k) = G$ if and only if $k \in Z(G)$. □

Theorem — Class equation

If G is a finite group, then

$$|G| = |Z(G)| + \sum_{g \in T} |\mathrm{Conj}(g)|$$

where T is a set of representatives for conjugacy classes not contained in the center.

Theorem — Cauchy's theorem

If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof.

Let $|G| = pm$. Note the theorem is clear when G is cyclic.

First assume G is abelian; proof by induction on m.

Base case: if $m = 1$, then G is cyclic, so we are done.

Inductive step: pick $a \in G$, $a \neq e$. We can assume $|a| < |G|$ (otherwise G is cyclic). If $p \mid |a|$, then by induction we get $b \in \langle a \rangle$ with $|b| = p$. Otherwise, $N = \langle a \rangle \trianglelefteq G$ since G is abelian. Thus $|G/N| = \frac{|G|}{|N|} < |G|$. Since $p \mid |G|$ but $p \nmid |N|$, we get $p \mid |G/N|$. By induction, G/N has an element gN of order p. Let $n = |g|$. Since $g^n = 1$, $q(g)^n = 1$ where q is the quotient map, so $p \mid n$. If $G = \langle g \rangle$, we are done, otherwise apply induction to $\langle g \rangle$.

Now take a general G (possibly non-abelian); induction on $|G|$.

By the class equation, $|G| = |Z(G)| + \sum_{g \in T} |\mathrm{Conj}(g)|$.

If $p \nmid |\mathrm{Conj}(g)| = |G|/|C_G(g)|$ for some $g \in T$, then $p \mid |C_G(g)|$. Since $g \notin Z(G)$, $|\mathrm{Conj}(g)| > 1 \implies |C_G(g)| < |G|$. By induction, $C_G(g)$ contains an element of order p.

If $p \mid |\mathrm{Conj}(g)|$ for all $g \in T$, then $p \mid |Z(G)|$. $Z(G)$ is an abelian group, so by the abelian case, $Z(G)$ contains an element of order p. □

Center of p-groups

Definition — p-group

Let p be prime. A group G is a **p-group** if $|G| = p^k$ for some $k \geq 1$.

Theorem

If G is a p-group, then $Z(G) \neq \{e\}$.

Proof.

$|G| = |Z(G)| + \sum_{g \in T}[G : C_G(g)]$.

Note $[G : C_G(g)] \mid |G|$.

If $g \notin Z(G)$, then $[G : C_G(g)] > 1 \implies p \mid [G : C_G(g)]$.

So $p \mid |Z(G)|$. □

As shown in the proof, the order of $Z(G)$ is a non-zero power of p. Alternatively, get this from the theorem and Lagrange's theorem.

Week 6: Classification of Groups

14: Classification of groups

Classification problem: identify all groups up to isomorphism. (We could replace groups with any algebraic structure. Classification is one of the big questions in modern mathematics.)

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $D_6 = S_3$, ??
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, D_8, ??
9	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

Groups of order p^2

Proposition

Suppose p is prime and $|G| = p^2$. Then either G is cyclic, or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proof.

Suppose G is not cyclic, so choose $a \in G \setminus \{e\}$.

We know $\langle a \rangle \neq G$, so $|a| = p$ and we can find $b \in G \setminus \langle a \rangle$.

Since $\langle b \rangle \neq G$, we get $|b| = p$ as well. Let $H = \langle a \rangle$ and $K = \langle b \rangle$.

Since $H \cap K < K$, we see $|H \cap K| = 1$ so $H \cap K = \{e\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|} = p^2$ so $HK = G$.

Finally, $[G : H] = [G : K] = p$, the smallest prime dividing $|G|$. Hence $H, K \trianglelefteq G$ so $G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. □

Groups of order pq

Lemma

Suppose $H, K \trianglelefteq G$ where $\gcd(|H|, |K|) = 1$ and $|H||K| = |G|$. Then $G \cong H \times K$.

Proof.

Since $|H \cap K|$ divides both $|H|$ and $|K|$, we get $|H \cap K| = 1$ so $H \cap K = \{e\}$.

Also, $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$ so $HK = G$.

The result follows from the characterization of products. □

Suppose $|G| = pq$ for distinct primes $p < q$. What can we say about G?

By Cauchy's theorem, G has elements a, b with $|a| = p$ and $|b| = q$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Note $\gcd(|H|, |K|) = 1$ and $|H||K| = |G|$. Is it true that $H, K \trianglelefteq G$?

We know $[G : K] = p$, which is the smallest prime dividing $|G|$, so $K \trianglelefteq G$. But is $H \trianglelefteq G$? Not necessarily.

Counterexample: $G = D_6$, $H = \langle r \rangle$, $K = \langle s \rangle$.

What if we suppose $H, K \leq G$, $HK = G$, $H \cap K = \{e\}$, and $K \trianglelefteq G$? Is $G \cong H \times K$ here? Again, no!

In our counterexample, that would mean $D_6 \cong H \times K \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, but D_6 is non-abelian.

However, there is a set bijection $H \times K \to G : (h, k) \mapsto hk$, and we can say that $G \cong H \ltimes K$, the **semidirect product** of H and K (later, optional).

For $p = 2$ and $q = 3$, it turns out the only groups of order $pq = 6$ are $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_6$, and $D_6 \cong S_3$.

What can we say?

The difficulty in analyzing the pq case was that $H \leq G$ might not be normal. This concern is not present if G is abelian, so we will focus on finite abelian groups this week.

There are lots of other ways to approach classification. Notice that for small orders, we are essentially describing groups as being built out of other groups.

We say a group is **simple** if it contains no (non-trivial) normal subgroups. Simple groups are the minimal building blocks for other groups.

Finally, by looking at the isomorphism problem for **finitely-presented groups** (later, optional), we will see that the classification problem for infinite groups cannot be solved.

Decomposing finite abelian groups

From the earlier lemma, we can disregard the normality constraint when considering abelian groups. Then, how can we find groups of coprime order?

Lemma

Suppose G is an abelian group. Let $G^{(m)} = \{g \in G : g^m = e\}$. Then $G^{(m)} \leq G$ for all $m \geq 1$.

Proof.

Clearly $e \in G^{(m)}$ for all $m \geq 1$. If $g, h \in G^{(m)}$, then $(g^{-1}h)^m = g^{-m}h^m = e \in G^{(m)}$. □

$G^{(m)}$ is the **m-torsion subgroup**.

Proposition

Suppose $|G| = mn$ where $\gcd(m, n) = 1$. Then

1. $\phi\colon G \to G^{(m)} \times G^{(n)} : g \mapsto (g^n, g^m)$ is an isomorphism.
2. $|G^{(m)}| = m$ and $|G^{(n)}| = n$.

Proof.

1. If $g \in G$, then $g^{mn} = e$, so $g^n \in G^{(m)}$ and $g^m \in G^{(n)}$. Hence 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 $g = g^{an+bm} = g^{an}$ and similarly $h = h^{an+bm} = h^{bm}$, so $\phi(g^a h^b) = (g^{an}h^{bn}, g^{am}h^{bm}) = (g, h)$. Hence ϕ is also surjective.

   We also need to show ϕ is a homomorphism:

$$\phi(gh) = ((gh)^n, (gh)^m) = (g^n h^n, g^m h^m) = (g^n, g^m) \cdot (h^n, h^m) = \phi(g)\phi(h).$$

2. Since $G \cong G^{(m)} \times G^{(n)}$, $|G| = |G^{(m)}||G^{(n)}|$.

   Suppose $|G| = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of $|G|$. Since $|G| = mn$ and $\gcd(m, n) = 1$, we have $m = p_1^{b_1} \cdots p_k^{b_k}$ and $n = p_1^{c_1} \cdots p_k^{c_k}$ where for each i, $a_i = b_i + c_i$ and only one of b_i and c_i is non-zero.

   Suppose $b_i > 0$. If $p_i \mid |G^{(n)}|$, then $G^{(n)}$ has an element a of order p_i by Cauchy's theorem. Then $p_i \mid m \implies a \in G^{(m)} \implies a \in \ker\phi \implies a = e$, which is impossible. So $p_i \nmid |G^{(n)}| \implies p_i^{a_i} \mid |G^{(m)}|$.

Conclusion: $m \mid |G^{(m)}|$ and $n \mid |G^{(n)}|$. So $|G^{(m)}| = m$ and $|G^{(n)}| = n$.

□

Example

Suppose $\gcd(m, n) = 1$ and let $G = \mathbb{Z}/mn\mathbb{Z}$.

If $m[x] = 0$ for $0 \le x < mn$, 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 $m\mathbb{Z} \mapsto mn\mathbb{Z}$, $n\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$. Similarly, $G^{(n)} \cong m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

The proposition gives $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. (Chinese remainder theorem.)

Corollary

Let G be a finite abelian group and let $|G| = p_1^{a_1} \cdots p_k^{a_k}$ where $p_1, \ldots, p_k$ are distinct primes and $a_i > 0$ for all i. Then $G \cong G_1 \times G_2 \times \cdots \times G_k$ where $|G_i| = p_i^{a_i}$.

Proof.

Let $G_1 = G^{(p_1^{a_1})}$ and let $r = p_2^{a_2} \cdots p_k^{a_k}$.

Since $p_1^{a_1}$ and r are coprime and $p_1^{a_1} \cdot r = |G|$, the proposition implies $G \cong G_1 \times G^{(r)}$ and that $|G_1| = p_1^{a_1}$ and $|G^{(r)} = r|$.

We can continue to get $G^{(r)} = G_2 \times \cdots \times G_k$ as desired. □

We can go further, and decompose into cyclic groups.

Proposition

If G is a finite abelian group, then $G \cong C_{a_1} \times C_{a_2} \times \cdots \times C_{a_k}$ for some sequence $a_1, \ldots, a_k$ where every a_i is a prime power.

(Recall that C_n is the multiplicative form of $\mathbb{Z}/n\mathbb{Z}$.)

Proof.

By the previous corollary, we can assume G is a p-group, i.e. $|G| = p^n$ for some n. Proof by induction on n; for base case $n = 0$, take $k = 0$.

Choose an element $x \in G$ of maximal order, so say $|x| = p^r$. Since G is abelian, $N = \langle x \rangle \trianglelefteq G$.

Then $|G/N| < |G|$, so by induction, $G/N = C_{b_1} \times \cdots C_{b_\ell}$ for some sequence $b_1, \ldots, b_\ell$ of prime powers. By Lagrange's theorem, $b_i = p^{s_i}$ for all i.

For each i, let $\tilde{y}_i$ be the generator of C_{b_i}. Let $y_i N \in G/N$ be the element of G/N corresponding to $(e, \ldots, e, \tilde{y}_i, e, \ldots, e)$ (that is, $\tilde{y}_i$ in the i-th position). Say $|y_i| = p^{t_i}$; note $r \geq t_i \geq s_i$.

We know that $y_i^{b_i} \in N$, so $y_i^{b_i} = x^{c_i}$ for some c_i. Now $b_i = p^{s_i}$, so $|y_i^{b_i}| = p^{t_i}/p^{s_i} = p^{t_i - s_i}$. We conclude that $c_i = d_i p^{r-(t_i - s_i)} = d_i p^{r - t_i + s_i}$ for some d_i.

Let $z_i = y_i x^{-d_i p^{r-t_i}}$. Then $z_i N = y_i N$, and $z_i^{b_i} = y_i^{b_i} x^{-d_i p^{r-t_i+s_i}} = y_i^{b_i} x^{-c_i} = e$, so $|z_i| = b_i$.

Let $H = \langle z_1, \ldots, z_\ell \rangle \leq G$ and suppose $w \in H \cap N$. Then $w = z_1^{n_1} \cdots z_\ell^{n_\ell}$ where $0 \leq n_i < b_i$ for all i.

Let $q\colon G \to G/N$ 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 $w \in N = \ker q$, $q(w) = e$, so $n_1 = \cdots = n_\ell = 0$. We conclude $w = e$, or in other words $H \cap N = \{e\}$.

Suppose $g \in G$. Then $gN \cong (\tilde{y}_1^{n_1}, \ldots, \tilde{y}_\ell^{n_\ell})$ for some $n_1, \ldots, n_\ell$ which implies $gN = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (z_1^{n_1} \cdots z_\ell^{n_\ell})N$. In particular, $g \in HN$. We conclude $HN = G$.

Since G is abelian, $H, N \trianglelefteq G$. So $G = N \times H$

Now $N \cong C_{p^r}$ and $|H| < |G|$, so by induction, H is also a product of prime-power cyclic groups. □

Now, the main result.

Theorem — Classification of finite abelian groups

If G is a finite abelian group, then $G \cong C_{a_1} \times \cdots \times C_{a_k}$ where $a_1 \leq \cdots \leq a_k$ is a sequence of prime powers.
Furthermore, if $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$ where $b_1 \leq \cdots \leq b_\ell$ is another sequence of prime powers, then $k = \ell$ and $a_i = b_i$ for all $1 \leq i \leq k = \ell$.

Example

We saw earlier that $C_2 \times C_3 \cong C_6$ (or generally $C_m \times C_n \cong C_{mn}$ for coprime m and n), so the requirement that a_i be a prime power is required for uniqueness.

Proof.

We just need to prove uniqueness.

If $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$, then $G^{(m)} \cong C_{b_1}^{(m)} \times \cdots \times C_{b_\ell}^{(m)}$.

If p, q are distinct primes, then $C_{p^r}^{(q^s)} = \{e\}$. Otherwise if $p = q$, $|C_{p^r}^{(p^s)}| = p^{\min(r,s)}$.

Now

$$|G^{(p^r)}| = \prod_{s \geq 1} \prod_{i : b_i = p^s} |C_{b_i}^{(p^r)}| = \prod_{s \geq 1} \prod_{i : b_i = p^s} p^{\min(r,s)}$$

and hence

$$\frac{|G^{(p^r)}|}{|G^{(p^{r-1})}|} = \prod_{s \geq r} \prod_{i : b_i = p^s} p.$$

So $\log_p |G^{(p^r)}| - \log_p |G^{(p^{r-1})}| = |\{i : b_i = p^s \text{ for some } s \geq r\}|$.

Exercise: recover ℓ and $b_1, \ldots, b_\ell$ from these numbers. □

Week 7: Rings

15: Rings and fields

Rings

Rings abstract sets with operations addition $+$ and multiplication $\cdot$.

Definition — ring

A **ring** is a tuple $(R, +, \cdot)$, where

1. $(R, +)$ is an abelian group, and
2. $\cdot$ is an associative binary operation on R such that $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$ ((left/right) distributive property).

The operation $+$ is called **addition**, and $\cdot$ is called **multiplication**.

A ring is **commutative** if $\cdot$ is commutative.

Example

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all commutative rings.
- $(\mathbb{N}, +, \cdot)$ is not a ring, since $(\mathbb{N}, +)$ is not a group.
- $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.)
- If R is a ring and X is a set, then $\mathrm{Fun}(X, R)$ 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 (see later).
- If R is a ring and $n \geq 1$, the the set of $n \times n$ matrices $M_n R$ with coefficients in R is a ring under usual matrix operations.
- If $\circ \colon M_n\mathbb{C} \times M_n\mathbb{C} \to M_n\mathbb{C} : (A, B) \mapsto \frac{AB+BA}{2}$ then $(M_n\mathbb{C}, +, \circ)$ is not a ring since $\circ$ is not associative (homework #1).

Notation for rings:

- As with groups, we may refer to the ring $(R, +, \cdot)$ by R when the operations are clear.
- We always use additive notation for the group $(R, +)$, and almost always use $+$ as the symbol. (Sometimes $\oplus$ for $\mathbb{Z}/2\mathbb{Z}$, etc.)
- In particular, denote identity of $(R, +)$ by 0 and inverse of $x \in R$ with respect to $+$ by $-x$.
- Some variation in notation permitted for multiplication ($\cdot$, $\times$, $\otimes$, $\boxtimes$, etc.).

- Usually just use ab for multiplication of a and b.

Basic properties

Proposition

If R is ring, then:

1. $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ for all $a, b \in R$.
3. $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in R$.

Proof.

1. $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 \cdot a = 0$. Similarly, $a \cdot 0 = 0$.
2. $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \implies (-a) \cdot b = -(a \cdot b)$. Similarly, $a \cdot (-b) = -(a \cdot b)$.
3. $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$.

□

Multiplicative identities

Definition — ring with identity

A **ring with identity** is a ring $(R, +, \cdot)$ where $\cdot$ has an identity.

In this course, "ring" means "ring with identity" unless otherwise noted.

This is a common assumption outside of the course. If a ring doesn't have an identity, we can call it a "ring without an identity" or "ring not necessarily having an identity" (or a "rng", haha). (Will encounter these with subrings.)

All rings mentioned so far are rings with identities.

For $\mathrm{Fun}(X, R)$, $R[x]$, $M_n R$ to have identities, we need to assume that R has an identity.

Notation: use 1_R or 1 for identity of R.

Proposition

If R is a ring (with identity), then $-a = (-1) \cdot a$ for all $a \in R$.

Proof.

$0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a.$ □

Units

Definition — unit

Let R be a ring. An element $x \in R$ is a **unit** if x has an inverse with respect to multiplication $\cdot$ (*i.e.*, there is $y \in R$ where $xy = yx = 1$).

The set of units in R is denoted by $R^\times$.

If x is a unit, then the inverse of x is unique, and is denoted by x^{-1}.

From homework, the set of units $R^\times$ forms a group under multiplication, and thus is called the **group of units** of R.

Example

- $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.
- $\mathbb{Q}^\times = \{x \in \mathbb{Q} : x \neq 0\}$.

Rings with (without) identity are also called **unital (non-unital) rings**.

The trivial ring

The smallest possible ring is $R = \{0\}$, with multiplication $0 \cdot 0 = 0$. This is a ring with $1 = 0$. This ring is called the **trivial ring** or **zero ring**.

Unlike the trivial group, which is crucial in group theory, the trivial ring is often an annoyance, since there's a special property which holds only for the trivial ring.

Lemma

Let R be a ring. Then $1 = 0$ if and only if R is trivial.

Proof.

If $1 = 0$, then $x = 1 \cdot x = 0 \cdot x = 0$ for all $x \in R$. □

Fields and division rings

If R is a ring with $1 \neq 0$, then $0 \cdot y = 0 \neq 1$ for all $y \in R$ and hence $0 \notin R^\times$.

Definition — division ring

A **division ring** is a ring R with $1 \neq 0$, such that $R^\times = R \setminus \{0\}$.

A **field** is a commutative division ring.

Example

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields.

Reminder: if $\alpha = a + bi \in \mathbb{C}$, then $\alpha\overline{\alpha} = |\alpha|^2 = a^2 + b^2$, 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 multiplication $[x]\cdot[y] = [xy]$, making it a ring.

Lemma

$[x]$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(x, n) = 1$.

Proof.

If $\gcd(x, n) = 1$, then $ax + bn = 1$ for some $a, b \in \mathbb{Z}$. Since $n \mid ax - 1$, $[ax] = 1$ in $\mathbb{Z}/n\mathbb{Z}$.

Conversely, if $[ax] = 1$, then $ax - 1 = bn$ for some $b \in \mathbb{Z}$. Hence $\gcd(x, n) = 1$. □

Corollary: $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime (every non-zero element coprime to n).

In particular, there are fields $\mathbb{K}$ where $\mathbb{K}$ is finite.

Division rings

Theorem — Wedderburn

Any finite division ring is a field.

Definition — ring of quaternions

The **ring of quaternions** is the ring $Q = (\mathbb{R}^4, +, \cdot)$ where $+$ is vector addition, and for $\cdot$ we denote the standard basis vectors by $1, i, j, k$, and set $i^2 = j^2 = k^2 = -1$ and $ijk = -1$.

In this ring, we have $ij = k$ and $jk = i$ so $ji = -k$, and hence Q is non-commutative. Q is an example of a non-commutative division ring.

16: Subrings and homomorphisms

Subrings

Definition — subring

Let R be a ring. A subset $S \subseteq R$ is a **subring** of R if

1. S is a subgroup of $(R, +)$,
2. $ab \in S$ for all $a, b \in S$, and
3. $1 \in S$.

Lemma

If S is a subring of $(R, +, \cdot)$, then $(S, +, \cdot)$ is a ring.

Example

Subrings:

- $\mathbb{Z}$ is a subring of $\mathbb{Q}$ is a subring of $\mathbb{R}$ is a subring of $\mathbb{C}$ is a subring of the quaternions Q.
- The ring $\mathbb{R}[x]$ of polynomial functions with coefficients over $\mathbb{R}$ is a subring of $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$.
- $M_n\mathbb{Z}$ is a subring of $M_n\mathbb{R}$.

Not subrings:

- $\mathbb{Q}^\times$ is not a subring of $\mathbb{Q}$ (not a subgroup).
- $\mathrm{Span}\{1, x\}$ is not a subring of $\mathbb{R}[x]$ (not closed under multiplication).
- $2\mathbb{Z}$ is not a subring of $\mathbb{Z}$ ($1 \notin 2\mathbb{Z}$).
- $\{0\}$ is not a subring of any non-trivial ring R ($1_R \notin \{0\}$)!

Alternative approach: non-unital subrings

If we work with non-unital rings, then we might not care that subrings contain the identity.

Definition — subring (non-unital approach)

Let R be a not-necessarily-unital ring. A subset $S \subseteq R$ is a **subring** of R if

1. S is a subgroup of $(R, +, \cdot)$, and
2. $ab \in S$ for all $a, b \in S$.

If, in addition, R is a unital ring and

3. $1 \in S$,

then S is a **unital subring**.

In this course, "ring" = "unital ring" and "subring" = "unital subring". We'll call sets satisfying (1) and (2) "non-unital subrings".

One reason for interest in non-unital subrings is that many unital rings have interesting non-unital subrings.

Example

Let $R = \mathbb{R}[x]$, so R is unital.

Let $x\mathbb{R}[x] = \{f \in \mathbb{R}[x] : \text{constant term of } f \text{ is } 0\}$. (Alternatively, $f \in x\mathbb{R}[x] \iff f(0) = 0$.)

If $f, g \in x\mathbb{R}[x]$, then $f - g \in x\mathbb{R}[x]$ so $x\mathbb{R}[x]$ is a subgroup of $\mathbb{R}[x]$. Also, $f \cdot g \in x\mathbb{R}[x]$ since $(fg)(0) = f(0)g(0) = 0$. But $1 \notin x\mathbb{R}[x]$, so $x\mathbb{R}[x]$ is a non-unital subring of R.

Exercise: show $(x\mathbb{R}[x], +, \cdot)$ is a non-unital ring.

Example

Let $R = \text{Fun}(\mathbb{R}, \mathbb{R})$.

A function $f \colon \mathbb{R} \to \mathbb{R}$ is **compactly supported** if there is some interval $[a, b]$ with $a < b \in \mathbb{R}$ such that $f(x) = 0$ for all $x \notin [a, b]$.

Suppose $f, g \colon \mathbb{R} \to \mathbb{R}$ are compactly supported. We can choose $a < b$ such that $f(x) = g(x) = 0$ for all $x \notin [a, b]$. Then $(f - g)(x) = (fg)(x) = 0$ for $x \notin [a, b]$, so $f - g$ and $f \cdot g$ are compactly supported.

The identity in $\text{Fun}(\mathbb{R}, \mathbb{R})$ is the constant-1 function, which is not compactly supported.

So compactly supported functions are a non-unital subring.

Claim: compactly supported functions are a non-unital ring.

Proof: Suppose f is an identity element of the ring. There is some interval $[a, b]$ such that $f(x) = 0$ for all $x \notin [a, b]$. There is a compactly supported function g such that $g(x) \neq 0$ for some $x \notin [a, b]$. But then $fg(x) = f(x)g(x) = 0 \neq g(x)$ for this x, so f is not an identity.

Characteristics and prime subrings

Suppose $x \in R$ where R is a ring and $n \in \mathbb{Z}$. Since $(R, +)$ is an abelian group, nx is well-defined. We can think of n as the element $n1 \in R$, in the sense that if $x \in R$, we can talk about $n \cdot x$ or $x \cdot n$ or $x \pm n$. (For example, in $\mathbb{Z}/10\mathbb{Z}$, $10 \cdot 1 = 0$.)

Lemma

If R is a ring, $x \in R$, and $n, m \in \mathbb{Z}$, then

- $n1 \cdot x = x \cdot n1 = nx$, and
- $n(mx) = (nm)x$.

Proof.

Exercise. Idea: if $n \geq 0$, then $n1 \cdot x = (1 + \cdots + 1) \cdot x = x + \cdots + x = nx$. □

Lemma

Let R be a ring. The set $R_0 = \{n1 : n \in \mathbb{Z}\}$ is a subring of R and is contained in every other subring. Furthermore, as a group, $R_0 \cong \mathbb{Z}/k\mathbb{Z}$, where $k = \min\{m \in \mathbb{N} : m1 = 0\}$ (or $k = 0$ if this set is empty).

Definition — prime subring, characteristic

R_0 is called the **prime subring** of R, and k is called the **characteristic** of R, denoted $\mathrm{char}(R)$.

Example

- $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$.
- $\mathrm{char}(\mathbb{Z}/Z\mathbb{Z}) = 0$.
- $\mathrm{char}(R) = 1$ if and only if $R = \{0\}$.

Proof of lemma.

R_0 is the cyclic subgroup of $(R, +)$ generated by 1. As a cyclic group, $R_0 \cong \mathbb{Z}/k\mathbb{Z}$ where $k = \min\{m \in \mathbb{N} : m1 = 0\}$ or $k = 0$.

If $n, m \in \mathbb{Z}$, then $n1 \cdot m1 = nm1 \in R_0$.

Also $1 \in R_0$, so R_0 is a unital subring.

If S is a unital subring of R, then $1 \in S$, so S contains $\langle 1 \rangle = R_0$. $\square$

Centre of a ring

Definition — centre

If R is a ring, the **centre** of R is the set $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$.

Note this is different from the group centre of R (which is R since R is abelian).

Lemma

$Z(R)$ is a subring of R.

Proof.

Exercise. □

Corollary

If R is a non-zero ring, then $Z(R)$ is non-trivial.

Proof.

$Z(R)$ contains the prime subring R_0. □

Ring homomorphisms

Definition — homomorphism

Let R, S be rings. A function $\phi\colon R \to S$ is a **(unital) homomorphism** if

1. $\phi\colon (R,+) \to (S,+)$ 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) but not (3) are satisfied, then ϕ is a **non-unital homomorphism**.

In this course, "homomorphism" = "unital homomorphism".

Example

- If S is a subring of R, then $i\colon S \to R : x \mapsto x$ 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 $[xy] = [x] \cdot [y]$.

Definition — isomorphism

A homomorphism $\phi\colon R \to S$ is an **isomorphism** if ϕ is bijective.

Proposition

Let $R_0 = \mathbb{Z}1_R$ be the prime subring of a ring R, and let $n = \operatorname{char}(R)$. Then $\phi\colon \mathbb{Z}/n\mathbb{Z} \to R_0 : [x] \mapsto x1$ is a ring isomorphism.

Proof.

We already showed ϕ is a well-defined group isomorphism, so ϕ is bijective.

If $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, then

$$\phi([a] \cdot [b]) = \phi([ab]) = ab1 = a(b1) = (a1) \cdot (b1) = \phi([a])\phi([b]).$$

Since $\phi([1]) = 1$, ϕ is a homomorphism. □

Basic properties of ring homomorphisms

Proposition

Let $\phi\colon R \to S$ be a homomorphism.

1. If $a \in R$ and $n \geq 0$, then $\phi(a^n) = \phi(a)^n$.
2. If $u \in R^\times$, then $\phi(u) \in S^\times$ and $\phi(u^n) = \phi(u)^n$ for all $n \in \mathbb{Z}$.
3. If ϕ is an isomorphism, then ϕ^{-1} is a ring homomorphism.

Proof.

1. By induction.
2. $1 = \phi(1) = \phi(uu^{-1}) = \phi(u)\phi(u^{-1})$, so $\phi(u) \in S^\times$ and $\phi(u^{-1}) = \phi(u)^{-1}$. It follows from (1) that $\phi(u^n) = \phi(u)^n$ for all $n \in \mathbb{Z}$.
3. We already know ϕ^{-1} is a group homomorphism.

   Note $\phi(1_R) = 1_S$, so $\phi^{-1}(1_S) = 1_R$.

   If $a, b \in S$, then $a = \phi(\phi^{-1}(a))$ and $b = \phi(\phi^{-1}(b))$, so $ab = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = \phi(\phi^{-1}(a)\phi^{-1}(b))$ and hence $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$.

□

Proposition

Let $\phi\colon R \to S$ be a homomorphism where S is not zero.

1. $\operatorname{Im}\phi$ is a subring of S.
2. $\ker\phi$ is a non-unital subring of R.

Proof.

1. We already $\operatorname{Im}\phi$ 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 $a = \phi(x)$ and $b = \phi(y)$ for some $x, y \in R$ and $ab = \phi(x)\phi(y) = \phi(xy) \in \operatorname{Im}\phi$.
2. Revisit this when we study ideals.

□

Note about (2): if $1 \in \ker\phi$ and ϕ is unital, then $1_S = \phi(1_R) = 0_S$, so S is the zero ring.

17: Polynomials and group rings

Polynomials, formally

Let R be a ring.

The **ring of polynomials** in variable x with coefficients in R is the ring with elements $\sum_{i=0}^{n} a_i x^i$ for $n \geq 0$ and $a_0, \ldots, a_n \in R$.

Addition and multiplication are as usual:

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\sum_{i=0}^{k} a_i b_{k-i} x^k$$

where $a_i = b_j = 0$ when $i > n$ and $j > m$.

As usual, we can talk about degree, monomials, evaluation, etc., but how can we do it formally?

Definition

Given a ring R, let $R[x]$ be the set

$$\{(a_i)_{i=0}^{\infty} \subseteq R : \exists N \geq 0 \text{ such that } a_i = 0 \forall i \geq N\}.$$

We define binary operations $+$ and $\cdot$ on $R[x]$ by

$$(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} = (a_i + b_i)_{i=0}^{\infty}$$

and

$$(a_i)_{i=0}^{\infty} \cdot (b_i)_{i=0}^{\infty} = (c_k)_{k=0}^{\infty} \text{ where } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

The variable choice only matters in that we let $\sum_{i=0}^{n} a_i x^i$ denote $(a_0, \ldots, a_n, 0, 0, \ldots)$ (not unique representation). Changing the variable changes the notation.

Lemma

$(R[x], +, \cdot)$ is a ring.

Proof.

Need to show $+$ and $\cdot$ are well-defined for some sequences $(a_i)_{i=0}^{\infty}$ and $(b_i)_{i=0}^{\infty}$.

Let $N_1, N_2 \geq 0$ where $a_i = 0$ for all $i \geq N_1$ and $b_j = 0$ for all $b \geq N_2$. Then $a_i + b_j = 0$ for $i \geq \max(N_1, N_2)$, so $(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} \in R[x]$.

If $k \geq N_1 + N_2$ and $0 \leq i < N$, then $k - i > N_2$. So $\sum_{i=0}^{k} a_i b_{k-i} = 0$ if $k \geq N_1 + N_2$, so $(a_i)_{i=0}^{\infty} \cdot (b_i)_{i=0}^{\infty} \in R[x]$.

Exercise: $(R[x], +)$ is an abelian group with $0 = (0, 0, \ldots)$.

Next, suppose $(a_i)_{i=0}^{\infty}, (b_i)_{i=0}^{\infty}, (c_i)_{i=0}^{\infty} \in R[x]$.

(Lots of useless algebra...)

Exercise: $1 = (1, 0, 0, \ldots)$ is an identity for $\cdot$.

For distributivity, (more useless algebra...).

Conclusion: $R[x]$ is a ring. □

Terminology/notation for polynomial rings

- $R[x]$ is called the **ring of polynomials in variable x with coefficients in R**.
- x is the **variable** or **indeterminate**. Any variable works.
- We only use $(a_i)_{i=0}^{\infty}$ for elements of $R[x]$ for formal definitions or proofs.
- Use $\sum_{i=0}^{n} a_i x^i$ when working with $R[x]$. If coefficients not needed, denote elements by p or $p(x)$.
- Exercise: there is an isomorphism $R[x] \to R[y] : p(x) \mapsto p(y)$ for any variables x, y.

Degree and coefficients

Definition — degree

The **degree** of $p(x) \in R[x]$ is the smallest integer n such that $p(x) = \sum_{i=0}^{n} a_i x^i$ with $a_n \neq 0$, or $-\infty$ if no such n exists. Notation: $\deg(p)$.

Examples: $\deg(1) = 0$, $\deg(1 + x - x^3) = 3$, $\deg(0) = -\infty$.

Definition — coefficient, monomial, term

The **coefficient** of x^i in $(a_i)_{i=0}^{\infty} \in R[x]$ is a_i.

A **monomial** is a polynomial of the form x^i for some $i \geq 0$, and a polynomial of the form $a_i x^i$ is called a **term**.

If $p(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial of degree n, then the polynomials $a_i x^i$, $i = 0, \ldots, n$, are the **terms** of $p(x)$. $a_n x^n$ is the **leading term**, and a_n is the **leading coefficient**.

Constant polynomials

Polynomials of degree ≤ 0 are **constant polynomials**.

There is a constant polynomial $ax^0 \in R[x]$ for every $a \in R$. Usually just denote this by a.

Lemma

Let R be a ring. The set of constant polynomials in $R[x]$ is a subring of $R[x]$, and is isomorphic to R.

Because of this isomorphism, we think of R as a subring of $R[x]$.

Commutativity

Lemma

If R is commutative, then $R[x]$ is commutative.

Proof.

$$\begin{aligned}\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j} \\ &= \sum_{j=0}^{n}\sum_{i=0}^{n} b_j a_i x^{j+i} \\ &= \sum_{j=0}^{m} b_j x^j \cdot \sum_{i=0}^{n} a_i x^i.\end{aligned}$$

□

$R[x]$ makes sense even if R is not commutative, but note that $x \in Z(R[x])$, so it's not very natural.

Evaluation

Definition — evaluation

If $p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ and $c \in R$, then the **evaluation** of $p(x)$ at c is $p(c) := \sum_{i=0}^{n} a_i c^i$.

Proposition

If R is commutative and $c \in R$, then $R[x] \to R : p(x) \mapsto p(c)$ is a homomorphism.

This homomorphism is called **evaluation at c** or **substitution at c**. When necessary, refer to it by ev_c. Note ev_c begin 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 $p = \sum_i a_i x^i$ and $q = \sum_j b_j x^j$, then

$$(p+q)(c) = \sum_i (a_i + b_i)c^i = \sum_i a_i c^i + \sum_i b_i c^i = p(c) + q(c).$$

Also,

$$\begin{aligned}(p \cdot q)(c) &= \sum_k \sum_{i=0}^{k} a_i b_{k-i} c^k \\ &= \sum_i \sum_j (a_i c^i)(b_j c^j) \\ &= \left(\sum_i a_i c^i\right)\left(\sum_j b_j c^j\right) \\ &= p(c)q(c).\end{aligned}$$

Finally $1(c) = 1c^0 = 1$. □

Polynomials over fields

Most common type of polynomial rings are $\mathbb{K}[x]$ for $\mathbb{K}$ a field.

Proposition

Let $\mathbb{K}$ be a field. Then

1. $\deg(fg) = \deg(f) + \deg(g)$ for all $f, g \in \mathbb{K}[x]$.
2. $\mathbb{K}[x]^\times = \mathbb{K}^\times$.

Proof.

Homework. □

Example

$\deg(0 \cdot f) = -\infty = -\infty + \deg(f) = \deg(0) + \deg(f)$, which explains why we define $\deg(0) = -\infty$.

Example

Let $p(x) = 1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]$. Then $p(x)^2 = 1 + 4x + 4x^2 = 1$. So $p(x)$ is a unit.

Multivariable polynomials

Definition — multivariable polynomial ring

or any sequence of variables $x_1, \ldots, x_n$ 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 $x^i := x_1^{i_1} \cdots x_n^{i_n}$.

Example

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

Let R be a ring, $x_1, \ldots, x_n$ a sequence of variables, and $\sigma \in S_n$. Then there is an isomorphism $R[x_{\sigma(1)}, \ldots, x_{\sigma(n)}] \to R[x_1, \ldots, x_n]$ given by

$$\sum_{(i_1,\ldots,i_n)} a_i x_{\sigma(1)}^{i_1} \cdots x_{\sigma(n)}^{i_n} \mapsto \sum_{(i_1,\ldots,i_n)} a_i x_1^{i_{\sigma^{-1}(1)}} \cdots x_n^{i_{\sigma^{-1}(n)}}.$$

Example

Consider $3yx - 7y^2x^3 + 2y + 3x + 1 \in \mathbb{Z}[y, x]$.

The isomorphism above sends this to $3xy - 7x^3y^2 + 2y + 3x + 1 \in \mathbb{Z}[x, y]$.

The isomorphism in the lemma is not to be confused with the isomorphism (exercise) $\mathbb{Z}[y, x] \to \mathbb{Z}[x, y] : p(y, x) \mapsto p(x, y)$, which would instead send the above to $3xy - 7x^2y^3 + 2x + 3y + 1$.

Multivariate evaluation

Definition

If $p(x_1, \dots, x_n) = \sum_i a_i x^i \in R[x_1, \dots, x_n]$ and $c = (c_1, \dots, c_n) \in R^n$, then we define $p(c) = p(c_1, \dots, c_n) := \sum_i a_i c_1^{i_1} \cdots c_n^{i_n}$.

Lemma

Let $c = (c_1, \dots, c_n) \in R^n$. The function

$$\mathrm{ev}_c \colon R[x_1, \dots, x_n] \to R : p(x_1, \dots, x_n) \mapsto p(c_1, \dots, c_n)$$

is the composition

$$\mathrm{ev}_{c_1} \circ \cdots \circ \mathrm{ev}_{c_n} \colon R[x_1, \dots, x_{n-1}][x_n] \to R[x_1, \dots, x_{n-1}] \to \cdots \to R,$$

and hence is a homomorphism if R is commutative.

Proof.

Exercise. □

Group rings

Definition — group ring

Let G be a group and R be a ring. The **group ring** RG of G with coefficients in R is the set of formal sums

$$\left\{\sum_{g\in G} c_g \cdot g\right\}$$

where $(c_g)_{g\in G} \subseteq R$ is such that there is a finite subset $X \subset G$ with $c_g = 0$ for all $g \notin X$, with operations

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g$$

and

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h gh = \sum_{k\in G}\left(\sum_{g\in G} a_g b_{g^{-1}k}\right) k.$$

A formal sum $\sum_{g\in G} a_g g$ with coefficients in R is a fancy waya of writing a finitely support function $G \to R : g \mapsto a_g$. Recall a function is finitely support if it is 0 except at finitely many points of G.

The group elements $g \in G$ are "placeholders" in this formal sum.

Example

Let $R = \mathbb{Z}$ and $G = D_6 = \{e, r, s, sr, s^2, s^2r\}$. Some elements of $\mathbb{Z}D_6$ are:

- $1e + 7s - 2r + sr - s^2r$
- $2e + 2s + 2s^2$
- r
- e

A general element of RG is $a_e e + a_r r + a_s s + a_{sr} sr + a_{s^2} s^2 + a_{s^2r} s^2 r$ where $a_x \in R$ for each $x \in G$.

G versus RG

Group elements $g \in G$ can be regarded as elements of RG. For example, $g = 1 \cdot g + \sum_{h \neq g} 0 \cdot h$.

Technically speaking, though, $g \in G$ and $1 \cdot g \in RG$ are different.

Sometimes, write $\underline{g}$ for g considered as an element of RG.

Can also write $\sum_{g \in G} a_g g$ as $\sum_{g \in G} a_g \underline{g}$ if it's helpful.

> **Example**
>
> Consider $G = \mathbb{Z}^+$ and $R = \mathbb{Z}$. Elements of $RG = \mathbb{Z}\mathbb{Z}$ look like:
>
> - $3 \cdot \underline{0} - 2 \cdot \underline{1} + 5 \cdot \underline{10} - 6 \cdot \underline{-6}$
> - $\underline{1} + \underline{2} + \underline{3}$
> - $\underline{0}$ (in particular, not equal to $0_{RG} = 0 \cdot \underline{0} + 0 \cdot \underline{1} + \cdots$)

Ring operations of a group ring

Use component-wise addition:

Example

In $\mathbb{Z}D_6$, $(2\cdot e - s + 3\cdot s^2r) + (3\cdot e + s + r) = (5\cdot e + r + 3\cdot s^2r)$.

For multiplication, use principle that $\underline{g}\cdot\underline{h} = \underline{gh}$. Extend to RG so distributivity holds:

Example

In $\mathbb{Z}D_6$:

- $s\cdot(e + 2s + 3r + 4s^2r) = s + 2s^2 + 3sr + 4r$
- $(e+2s)(2e-3r) = 2e + 4s - 3r - 6sr$
- $(e-r)^2 = (e-r)(e-r) = e - r - r + r^2 = 2e - 2r = 2(e-r)$

Example

In $\mathbb{Z}\mathbb{Z}$, $(\underline{0} + 2\cdot\underline{-6})(3\cdot\underline{1} - 4\cdot\underline{2}) = 3\cdot\underline{1} - 4\cdot\underline{2} + 6\cdot\underline{-5} - 8\cdot\underline{-4}$.

Proposition

Let R be a ring and G be a group. Then RG is a ring with identity $\underline{e}$. If G is commutative, then RG is commutative.

Group rings are very important examples of not-necessarily-commutative rings.

However, we will focus on commutative rings in this course, so we won't prove this proposition.

Let's check that $\underline{e}$ is an identity:

$$\underline{e}\cdot\left(\sum_{g\in G} a_g\underline{g}\right) = \sum_{g\in G} a_g\underline{e\cdot g} = \sum_{g\in G} a_g\underline{g}$$

and similarly for right identity.

The remainder of the proof reduces to the fact that $\cdot$ is associative.

Group ring homomorphisms

Proposition

Let R be a ring and $\phi\colon G \to H$ be a group homomorphism. Then $\psi\colon RG \to RH$ 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.

Exercise: check well-definedness (two things: that $\sum_{g:\phi(g)=h} a_g$ is finite for $h \in H$, and $\psi(x)$ is finitely supported for all $x \in RG$).

$\psi(\underline{e_G}) = \underline{\phi(e)} = \underline{e_H}$, so ψ is unital.

Let $x = \sum_{g\in G} a_g \underline{g}$ and $y = \sum_{h\in G} b_h \underline{h}$. Then

$$\begin{aligned}\psi(x+y) &= \psi\left(\sum_{g\in G}(a_g+b_g)\underline{g}\right)\\ &= \sum_{g\in G}(a_g+b_g)\underline{\phi(g)}\\ &= \sum_{g\in G} a_g\underline{\phi(g)} + \sum_{g\in G} b_g\underline{\phi(g)}\\ &= \psi(x)+\psi(y).\end{aligned}$$

Also,

$$\begin{aligned}\psi(xy) &= \psi\left(\sum_{g,h\in G} a_g b_h \underline{gh}\right)\\ &= \sum_{g,h\in G} a_g b_h \underline{\phi(gh)}\\ &= \sum_{g,h\in G} a_g b_h \underline{\phi(g)\phi(h)}\\ &= \left(\sum_{g\in G} a_g\underline{\phi(g)}\right)\left(\sum_{h\in H} b_h\underline{\phi(h)}\right).\end{aligned}$$

□

Week 8: Ideals and Quotient Rings

18: Ideals

Recall:

Proposition

Let $\phi\colon R \to S$ be a homomorphism, where S is not zero.

1. $\operatorname{Im}\phi$ is a subring of S.
2. $\ker\phi$ is an ideal of R.

What's an ideal? But first, what's special about kernels?

Lemma

If $\phi\colon R \to S$ is a homomorphism, and $m \in \ker\phi$, then rm and mr are in $\ker\phi$ for all $r \in R$.

Proof.

$\phi(rm) = \phi(r)\phi(m) = \phi(r) \cdot 0_S = 0 = \cdots = \phi(mr)$. □

Definition — ideal

An **ideal** of a ring R is a subgroup $\mathcal{I}$ of $(R, +)$ such that if $m \in \mathcal{I}$ and $r \in R$, then $rm, mr \in \mathcal{I}$.

The lemma shows that the kernel of a homomorphism is an ideal (and so proves the proposition).

Note if R is commutative, we only need to check that $rm \in \mathcal{I}$ for all $m \in \mathcal{I}$ and $r \in R$.

Example: $m\mathbb{Z}$

Lemma

$m\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for every $m \in \mathbb{Z}$.

Proof.

We already know $m\mathbb{Z} \leq (\mathbb{Z}, +)$ (which is abelian).

If $r \in \mathbb{Z}$ and $km \in m\mathbb{Z}$, then $rkm \in m\mathbb{Z}$.

So $m\mathbb{Z}$ is an ideal. □

Intuition behind the ideal condition here: if $m \mid x$, then $m \mid rx$ for all $r \in \mathbb{Z}$. (Once we are inside the ideal, we can never move out of it.)

Special case: when $m = 0$, then $m\mathbb{Z} = \{0\}$.

Exercise: $\{0_R\}$ is an ideal of any ring R, called the **trivial ideal**, often denoted by (0) (notation later).

Simplifying conditions

To show that $\mathcal{I}$ is a subgroup of $(R, +)$, we need to check that

1. $0 \in \mathcal{I}$,
2. $\mathcal{I}$ is closed under addition, and
3. $\mathcal{I}$ is closed under negation (additive inverses).

Of course, we could speed this up by checking that

$1'$. $\mathcal{I}$ is non-empty, and

$2'$. $f, g \in \mathcal{I} \implies f - g \in \mathcal{I}$.

We can speed this up in a different way with the ideal condition:

Lemma

Let R be a ring and $\mathcal{I} \subseteq R$. Then $\mathcal{I}$ is an ideal if and only if

1. $\mathcal{I}$ is non-empty, and
2. if $r \in R$ and $f, g \in \mathcal{I}$, then $rf + g, fr + g \in \mathcal{I}$.

Proof.

If $f, g \in \mathcal{I}$, then $(-1) \cdot g + f = f - g \in \mathcal{I}$, so $(1')$ and $(2')$ are satisfied. So $\mathcal{I} \leq (R, +)$.

Hence $0 \in \mathcal{I}$. If $m \in \mathcal{I}$ and $r \in R$, then $rm = rm + 0 \in \mathcal{I}$. So $\mathcal{I}$ is an ideal. □

Example: evaluation

Let R be a commutative ring and pick $c \in R$.

The kernel of $\mathrm{ev}_c\colon R[x] \to R$ is $\mathcal{I} = \{f \in R[x] : f(c) = 0\}$.

By the previous lemma, this is an ideal, but let's check:

- $0 \in \mathcal{I}$, so $\mathcal{I}$ is non-empty.
- If $f, g \in \mathcal{I}$ and $r \in R[x]$, then $(rf + g)(c) = r(c)f(c) + g(c) = r(c) \cdot 0 + 0 = 0$ so $rf + g \in \mathcal{I}$.

Question: what do elements of this ideal look like?

First, consider $c = 0$.

Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$. Then $f(0) = \sum_i a_i 0^i = a_0$, so $f(0) = 0 \iff a_0 = 0$. (Note: in the context of polynomial evaluation, we use $0^0 := 1$.)

So elements of $\mathcal{I} = \ker \mathrm{ev}_0$ look like $a_1 x + a_2 x^2 + \cdots$. Because we can factor this as $a_1 x + a_2 x^2 \cdots = x(a_1 + a_2 x + \cdots)$, we sometimes denote $\mathcal{I}$ by $xR[x]$, or by (x).

Intuition behind $xR[x]$ being an ideal: if $f(x)$ has no constant term, then multiplying $f(x)$ by another polynomial can't add in a constant term.

Next, for general c.

Lemma

If $f(x) \in R[x]$ has degree $\leq n$ and $c \in R$, then there are $a_0, \ldots, a_n \in R$ 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 $f(x) - a_n(x - c)^n = a_n x^n +$ lower terms $- (a_n x^n) +$ lower terms is a polynomial of degree at most $n - 1$. By induction, $f(x) - a_n(x - c)^n = \sum_{i=0}^{n-1} a_i (x - c)^i$. Rearrange for $f(x)$. □

Because evaluation is homomorphism,

$$\mathrm{ev}_c((x - c)^i) = \mathrm{ev}_c(x - c)^i = \begin{cases} 0 & i > 0 \\ 1 & i = 0 \end{cases}.$$

So if $f(x) = \sum_{i=0}^{n} a_i (x - c)^i$, then $f(c) = a_0$. Conclusion: $\ker \mathrm{ev}_c = (x - c)R[x] = (x - c)$.

Caution: $2x = 2(x - 2) \in (\mathbb{Z}/4\mathbb{Z})[x]$, so $2x \in \ker \mathrm{ev}_2$.

Ideals containing 1

Note that $(x-c)R[x]$ doesn't contain 1 for any $c \in R$. That's because:

Lemma

If $\mathcal{I}$ is an ideal of a ring R, and $1 \in \mathcal{I}$, then $\mathcal{I} = R$.

Proof.

If $r \in R$ and $1 \in \mathcal{I}$, then $r = r \cdot 1 \in \mathcal{I}$. □

We typically consider **proper ideals**, that is, ideals $\mathcal{I} \subsetneq R$.

Ideals in fields

We can use the previous lemma to consider ideals in a field.

Corollary

The only ideals in a field $\mathbb{K}$ are (0) and $\mathbb{K}$.

Proof.

Suppose $\mathcal{I} \subseteq \mathbb{K}$ is an ideal. If $x \in \mathcal{I}$ and $x \neq 0$, then $x^{-1}x = 1 \in \mathcal{I}$. So $\mathcal{I} = \mathbb{K}$. □

Corollary

Let $\phi\colon \mathbb{K} \to R$ be a ring homomorphism, where $\mathbb{K}$ is a field and R is non-zero. Then ϕ is injective.

Proof.

$\ker\phi$ is an ideal of $\mathbb{K}$, so $\ker\phi$ is (0) or $\mathbb{K}$.

If $\ker\phi = \mathbb{K}$, then $0 = \phi(1_{\mathbb{K}}) = 1_R$, so R is zero. Since we are assuming R is non-zero, $\ker\phi = (0)$. Then we know from group theroy that ϕ is injective. □

Example

There are no homomorphisms from an infinite field to a finite field, since such a homomorphism would have to have a kernel (that is, be injective).

Example

$\mathbb{R}$ is uncountable, while $\mathbb{Q}$ is countable. So there is no injection $\mathbb{R} \to \mathbb{Q}$ as sets. Therefore there is no homomorphism $\mathbb{R} \to \mathbb{Q}$.

19: Quotient rings

Review on quotient groups

Recall in group theory:

- Kernels of homomorphisms are normal subgroups.
- Normal subgroups are kernels of homomorphisms, since if $N \trianglelefteq G$ then the quotient map $G \to G/N$ 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 $x - y \in N$.
- A group operation is $[x] + [y] = [x + y]$.
- The 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 homomorphism are ideals.
- Is it true that ideals are kernels of homomorphisms? If $\mathcal{I}$ is an ideal of R, is there a "quotient ring" $R/\mathcal{I}$?

Since $(R, +)$ is commutative, $\mathcal{I} \trianglelefteq R$, so the quotient group $R/\mathcal{I}$ exists. Can we put a ring structure on $R/\mathcal{I}$?

We want multiplication $\cdot$ such that the quotient map $q\colon R \to R/\mathcal{I}$ is a ring homomorphism. This means we want $[x] = q(xy) = q(x)q(y) = [x] \cdot [y]$, so we know what the multiplication should be (assuming this idea works).

Theorem

Let $\mathcal{I}$ be an ideal of a ring R, and define operations $+$ and $\cdot$ on $R/\mathcal{I}$ by $[x]+[y] = [x+y]$ and $[x] \cdot [y] = [xy]$ for $x, y \in R$. Then $(R/\mathcal{I}, +, \cdot)$ is a ring. Furthermore, the quotient map $q\colon R \to R/\mathcal{I} : x \mapsto [x]$ 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 a **quotient ring**.

Corollary

Every ideal is the kernel of some homomorphism.

Example

$\mathbb{Z}/m\mathbb{Z}$ is a ring with operations $[x] + [y] = [x + y]$ and $[x] \cdot [y] = [xy]$. We can use this as the definition of $\mathbb{Z}/m\mathbb{Z}$.

Proof of theorem.

We already know $(R/\mathcal{I}, +)$ is an abelian group.

First, we show $\cdot$ is **well-defined**.

Suppose $[x] = [x']$ and $[y] = [y']$ for $x, x', y, y' \in R$. We want to show that $[xy] = [x'y']$, or equivalent $xy - x'y' \in \mathcal{I}$. We see $xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y')$. Since $[x] = [x']$ and $[y] = [y']$, we know $x - x', y - y' \in \mathcal{I}$. By the ideal property, $(x - x')y, x'(y - y') \in \mathcal{I}$, so $xy - x'y' \in \mathcal{I}$.

Next, we show $\cdot$ is **associative**.

Suppose $x, y, z \in R$. Then $[x] \cdot ([y] \cdot [z]) = [x] \cdot [yz] = [xyz] = ([x] \cdot [y]) \cdot [z]$.

Next, we show $\cdot$ has an **identity**.

Note $[1] \cdot [x] = [1 \cdot x] = [x] = [x] \cdot [1]$, so $[1]$ is an identity for $\cdot$.

Next, we show **distributivity**.

If $x, y, z \in R$. Then

$$[x] \cdot ([y] + [z]) = [x] \cdot [y + z] = [x \cdot (y + z)] = [xy + xz] = [xy] + [xz] = [x] \cdot [y] + [x] \cdot [z],$$

and similarly $([y] + [z]) \cdot [x] = [y] \cdot [x] + [z] \cdot [x]$.

Since $(R/\mathcal{I}, +)$ is an abelian group, $\cdot$ is associative with identity, and $+$ and $\cdot$ satisfy distributivity, $R/\mathcal{I}$ is a ring.

Now, we show q is a **homomorphism**.

We already know q is a group homomorphism. Also, $q(xy) = [xy] = [x] \cdot [y] = q(x)q(y)$ and $q(1) = [1]$ is the identity for $R/\mathcal{I}$. So q is a ring homomorphism. □

Universal property of quotient groups, and quotient rings

Theorem — Universal property of quotient groups

Suppose $\phi\colon G \to K$ is a homomorphism and $N \trianglelefteq G$. Let $q\colon G \to G/N$ be the quotient homomorphism. Then there is a homomorphism $\psi\colon G/N \to K$ such that $\psi \circ q = \phi$ if and only if $N \subseteq \ker\phi$. Furthermore, if ψ exists then it is unique.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "q"'] & & K \\
& G/N \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

Can we extend this to rings?

Let $\phi\colon R \to S$ be a ring homomorphism and $\mathcal{I}$ an ideal of R. Suppose $\mathcal{I} \subseteq \ker\phi$. By the universal property of quotient groups, there is a unique group homomorphism $\psi\colon R/\mathcal{I} \to S$ 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

Let R, S, T be rings. Suppose that $\psi_1\colon R \to T$ is a ring homomorphism and $\psi_2\colon T \to S$ 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 $\psi_1(a) = x$ and $\psi_1(b) = y$. Then $\psi_2(xy) = \psi_2(\psi_1(a)\psi_1(b)) = \psi_2(\psi_1(ab)) = \phi(ab) = \phi(a)\phi(b) = \psi_2(\psi_1(a))\psi_2(\psi_1(b)) = \psi_2(x)\psi_2(y)$.

Also, $\psi_2(1_T) = \psi_2(\psi_1(1_R)) = \phi(1_R) = 1_S$.

So ψ_2 is a ring homomorphism. □

As a corollary of the lemma and the universal property of quotient groups:

Theorem — Universal property of quotient rings

Suppose $\phi\colon R \to S$ is a ring homomorphism and $\mathcal{I}$ is an ideal of R. Let $q\colon R \to R/\mathcal{I}$ be the quotient homomorphism. Then there is a ring homomorphism $\psi\colon R/\mathcal{I} \to S$ such that $\psi \circ q = \phi$ if and only if $\mathcal{I} \subseteq \ker\phi$. Furthermore, if ψ exists then it is unique.

Proof.

Existence: If $\mathcal{I} \subseteq \ker\phi$, then ψ exists as a group homomorphism. Applying the lemma with $\psi_1 = q$, $\psi_2 = \psi$, and $T = R/\mathcal{I}$ shows ψ is a ring homomorphism.

Uniqueness: Any ring homomorphism $\psi\colon R/\mathcal{I} \to S$ such that $\psi \circ q = \phi$ is equal to the unique group homomorphism with this property.

Necessity of $\mathcal{I} \in \ker\phi$: If ψ exists, then it is a group homomorphism, so apply the universal property of quotient groups. □

First isomorphism theorem for rings

Theorem — First isomorphism theorem for rings

If $\phi\colon R \to S$ is a ring homomorphism, then there is a ring isomorphism $\psi\colon R/\ker\phi \to \operatorname{Im}\phi$ such that $\phi = \psi \circ q$, where $q\colon R \to R/\ker\phi$ is the quotient homomorphism.

Proof.

By the universal property, we have a ring homomorphism $\psi\colon R/\ker\phi \to \operatorname{Im}\phi$ such that $\psi \circ q = \phi$. From the first isomorphism theorem for groups, there is a group isomorphism $\psi'\colon R/\ker\phi \to \operatorname{Im}\phi$ such that $\psi' \circ q = \phi$. ψ is also a group homomorphism. By the universal property of quotient groups, $\psi = \psi'$, so ψ is bijective.

(Or, apply the lemma to ψ'.) □

The first isomorphism theorem is very useful for finding quotient rings.

Proposition

Let R be a commutative ring and let $c \in R$. Then $R[x]/(x-c)R[x] \cong R$.

Proof.

$(x-c)R[x] = \ker \mathrm{ev}_c$, where $\mathrm{ev}_c\colon R[x] \to R$ is the evaluation map. If $r \in R$, then $\mathrm{ev}_c(r) = r$, so $\operatorname{Im}\mathrm{ev}_c = R$. By the first isomorphism theorem, $R[x]/(x-c)R[x] \cong R$. □

Example

Let $\mathcal{I} = (y - x^2)\mathbb{Z}[x,y] = \{(y-x^2)p(x,y) : p(x,y) \in \mathbb{Z}[x,y]\}$.

To see that $\mathcal{I}$ is an ideal, note that $\mathcal{I} = \ker \mathrm{ev}_{x^2}$, where $\mathrm{ev}_{x^2}\colon \mathbb{Z}[x,y] = \mathbb{Z}[x][y] \to \mathbb{Z}[x]$ is evaluation at x^2. (From the recursive definition and our previous investigation.)

By the proposition, $\mathbb{Z}[x,y]/\mathcal{I} \cong \mathbb{Z}[x]$.

20: Ideals generated by a subset

Ideal generated by a subset

Proposition

Let $\mathcal{F}$ be a family of ideals in a ring R. Then

$$\bigcap_{\mathcal{I}\in\mathcal{F}} \mathcal{I}$$

is an ideal of R.

Proof.

Homework. □

Definition — ideal generated by a subset

Let $X \subseteq R$. The **ideal generated by X** is

$$(X) := \bigcap_{\mathcal{I}\in\mathcal{F}} \mathcal{I},$$

where $\mathcal{F}$ is the set of ideals of R containing X.

Key properties:

- By proposition, (X) is an ideal.
- By definition, if $\mathcal{I}$ is an ideal containing X, then $X \subseteq (X) \subseteq \mathcal{I}$. Say that (X) is the smallest ideal containing X.
- Example: $(0) = (\varnothing) = \{0\}$.

Notation:

- Sometimes use $\langle X\rangle$ instead of (X).
- If $X = \{f_1, f_2, \ldots\}$, can replace $(X) = (\{f_1, f_2, \ldots\})$ by $(f_1, f_2, \ldots)$. Example: (0) instead of $(\{0\})$.

Proposition

If R is a ring and $X \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{k} s_i x_i t_i : k \geq 0,\ s_i, t_i \in R,\ x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

Corollary

If R is a commutative ring and $X \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{k} r_i x_i : k \geq 0,\ r_i \in R,\ x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

Proof.

$s_i x_i t_i = (s_i t_i) x_i$, so set $r_i = s_i t_i$. □

Proof of proposition.

Let $\mathcal{I}$ be the set in question.

First, show $\mathcal{I}$ is an ideal. Taking $k = 0$, we get $0_R \in \mathcal{I}$. Suppose $r \in R$ and $x, y \in \mathcal{I}$. Let $x = \sum_{i=1}^{k} s_i x_i t_i$ and $y = \sum_{i=1}^{\ell} s_i' y_i t_i'$ for $s_i, t_i, s_i', t_i' \in R$ and $x_i, y_i \in X$. Then $rx + y = \sum_{i=1}^{k} (rs_i) x_i t_i + \sum_{i=1}^{\ell} s_i' y_i t_i' \in \mathcal{I}$ and similarly $xr + y \in \mathcal{I}$, so $\mathcal{I}$ is an ideal.

Next, show $(X) \subseteq \mathcal{I}$. Taking $k = 1$ and $s_1 = t_1 = 1$, we get $X \subseteq \mathcal{I}$ so $(X) \subseteq \mathcal{I}$.

Finally, show $\mathcal{I} \subseteq (X)$. Suppose $k \geq 0$, $s_i, t_i \in R$, and $x_i \in X$ for $1 \leq i \leq k$. Since $X \subseteq (X)$, $x_i \in (X)$ means $s_i x_i t_i \in (X)$ for all $1 \leq i \leq k$. So $\sum_{i=1}^{k} s_i x_i t_i \in (X)$. Hence $\mathcal{I} \subseteq (X)$. □

The sum of ideals

Definition — ideal sum

If $\mathcal{I}, \mathcal{J} \subseteq R$ are ideals, then $\mathcal{I} + \mathcal{J} := \{x + y : x \in \mathcal{I},\ y \in \mathcal{J}\}$.

Corollary

$(\mathcal{I} \cup \mathcal{J}) = \mathcal{I} + \mathcal{J}$ is the smallest ideal containing both $\mathcal{I}$ and $\mathcal{J}$.

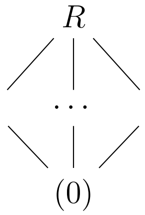
Proof.

By proposition, clearly $\mathcal{I} + \mathcal{J} \subseteq (\mathcal{I} \cup \mathcal{J})$.

For the reverse inclusion, suppose $s_i, t_i \in R$ and $x_i \in \mathcal{I} \cup \mathcal{J}$ for $1 \leq i \leq k$. Let $S = \{1 \leq i \leq k : x_i \in \mathcal{I}\}$, so if $i \in S$, then $s_i x_i t_i \in \mathcal{I}$. So $\sum_{i \in S} s_i x_i t_i \in \mathcal{I}$, and similarly $\sum_{i \notin S} s_i x_i t_i \in \mathcal{J}$. We conclude that $\sum_{i=1}^{k} s_i x_i t_i = \sum_{i \in S} s_i x_i t_i + \sum_{i \notin S} s_i x_i t_i \in \mathcal{I} + \mathcal{J}$. □

Lattice of ideals

Ideals of R are ordered by set inclusion $\subseteq$. The set of ideals of R with order $\subseteq$ is called the **lattice of ideals** of R.



The subgroup below $\mathcal{I}_1$ and $\mathcal{I}_2$ in the lattice is $\mathcal{I}_1 \cap \mathcal{I}_2$ (maximal subgroup contained in both).

The subgroup above $\mathcal{I}_1$ and $\mathcal{I}_2$ is $\mathcal{I}_1 + \mathcal{I}_2$ (minimal subgroup containing both).

Quotients by a subset

We get a new way of constructing rings: take $R/(X)$ for any subset X. We know $R/(X)$ is a unital ring, but when is it non-zero?

From group theory, we know that $R/\mathcal{I}$ is zero if and only if $\mathcal{I} = R$. We proved that $\mathcal{I} = R$ if and only if $1 \in \mathcal{I}$.

Corollary

Let R be a ring and $X \subseteq R$. Then $R/(X) = \{0\}$ if and only if there are $s_i, t_i \in R$ and $x_i \in X$ for $1 \leq i \leq k$ such that

$$\sum_{i=1}^{k} s_i x_i t_i = 1.$$

If R is commutative, we can instead just show $\sum_{i=1}^{k} r_i x_i = 1$ for $r_i \in R$ and $x_i \in X$.

Ideals generated by a finite subset

We often take ideals $(x_1, \ldots, x_n)$ generated by finite sets $\{x_1, \ldots, x_n\}$.

Corollary

If R is a commutative ring and $X \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{k} r_i x_i : k \geq 0,\ r_i \in R,\ x_i \in X \text{ for } 1 \leq i \leq k \right\}.$$

Corollary

If R is a commutative ring and $X = \{x_1, \ldots, x_n\} \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i : r_i \in R,\ 1 \leq i \leq n \right\}.$$

Proof.

RHS $\subseteq (X)$ is clear. For the other inclusion, note that $rx_i + r'x_i = (r + r')x_i$, so we can collect like terms; if x_i is unneeded, then set $r_i = 0$. □

Principal ideals

Definition — principal ideal

An ideal generated by a single element is called a **principal ideal**.

If R is a commutative ring, then $(x) = \{rx : r \in R\}$, so a principal ideal (x) is often denoted by xR or Rx.

Example

Let $R = \mathbb{Z}$ and $m \in \mathbb{Z}$. Then $(m) = m\mathbb{Z}$ is a principal ideal.

All subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$, so all subgroups of $\mathbb{Z}$ are principal ideals. In particular, all ideals of $\mathbb{Z}$ are principal ideals.

Example

If R is commutative and $p(x) \in R[x]$, then $(p) = pR[x]$ is an ideal.

Principal ideals in non-commutative rings

If R is non-commutative, then (x) is not necessarily equal to $\{rx : r \in R\}$ since $xr \in (x)$ for $r \in R$. But is $(x) = \{sxr : s, r \in R\}$? In general, no.

> **Example**
>
> Let $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2\mathbb{R}$.
>
> We know $AE_{11}B$ has rank ≤ 1 for every $A, B \in M_2\mathbb{R}$, hence $\{AE_{11}B : A, B \in M_2\mathbb{R}\} \subsetneq M_2\mathbb{R}$.
>
> Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $XE_{11}X = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
>
> So $E_{11} + XE_{11}X = I \in (E_{11})$, and we conclude that $(E_{11}) = M_2\mathbb{R}$.

More examples in polynomial rings

Principal ideals:

- We've already mentioned the principal ideals $(x-c)\mathbb{Z}[x]$ for $c \in \mathbb{Z}$. For example, $x\mathbb{Z}[x]$ is the ideal of polynomials with no constant term.
- Another good example is $m\mathbb{Z}[x]$ for $m \in \mathbb{Z}$. This is $m\mathbb{Z}[x] = \{\sum_{i=0}^n a_i x^i : n \geq 0,\ a_i \in m\mathbb{Z} \text{ for } 0 \leq i \leq n\}$.
- The previous example doesn't work in $\mathbb{Q}[x]$, though, since $2\mathbb{Q}[x] = \mathbb{Q}[x]$ $(2 \cdot \frac{1}{2} = 1)$. Also, $\mathbb{Z}[x]$ is not an ideal in $\mathbb{Q}[x]$ (in general, subrings are very different from ideals).

What about non-principal ideals?

In $\mathbb{Z}[x,y]$, $(x,y) = \{p(x,y)x + q(x,y)y : p, q \in \mathbb{Z}[x,y]\}$. So (x,y) contains x, y, xy, x^2, y^2, etc. Note p, q aren't unique: $xy = 0 + x \cdot y = y \cdot x + 0$. To see that (x,y) is a proper ideal of $\mathbb{Z}[x,y]$, observe that

$$(x,y) = \left\{ \sum_{i,j=0}^{n} a_{ij} x^i y^j : n \geq 0, a_{ij} \in \mathbb{Z} \text{ for } 0 \leq i,j \leq n,\ a_{00} = 0 \right\}.$$

Exercise

Suppose there are polynomials $f, p, q \in \mathbb{Z}[x,y]$ such that $p \cdot f = x$ and $q \cdot f = y$. Show $f \in \{\pm 1\}$.

Consequence: the only principal ideal containing (x,y) is $\mathbb{Z}[x,y]$. In particular, (x,y) is not principal.

All ideals of $\mathbb{Z}$ are principal, whereas $\mathbb{Z}[x,y]$ has non-principal ideals.

What about $\mathbb{Z}[x]$? Consider the ideal

$$\begin{aligned}(2,x) &= \{2p(x) + xq(x) : p, q \in \mathbb{Z}[x]\} \\ &= \left\{ \sum_{i=0}^{n} a_i x^i : n \geq 0,\ a_i \in \mathbb{Z} \text{ for } 0 \leq i \leq n,\ a_0 \in 2\mathbb{Z} \right\}.\end{aligned}$$

Can this ideal be principal?

Exercise

Show that if $p, f \in \mathbb{Z}[x]$ such that $p(x)f(x) = 2$, then $f \in \{\pm 1, \pm 2\}$.
Show that $x \notin \pm 2\mathbb{Z}[x]$.

Conclusion: the only principal ideal containing $(2,x)$ is $\mathbb{Z}[x]$.

21: Correspondence, second and third isomorphism theorems

Connecting ideals and homomorphisms (correspondence theorem)

Proposition

Let $\phi\colon R \to S$ be a ring homomorphism.

1. If $\mathcal{I}$ is an ideal of S, then $\phi^{-1}(\mathcal{I})$ is an ideal of R.
2. If $\mathcal{I}$ is an ideal of R and ϕ is surjective, then $\phi(\mathcal{I})$ is an ideal of S.

Proof.

Homework. (Also provide counterexample for (2) when ϕ is not surjective.) □

Recall from group theory:

Theorem — Correspondence theorem for groups

Let $\phi\colon G \to H$ be a surjective homomorphism. Then there is a bijection

$$\begin{tikzcd}
\begin{array}{c}\text{Subgroups}\\ K \text{ of } G \text{ with}\\ \ker\phi \le K\end{array} \arrow[r, shift left=2, "K \mapsto \phi(K)"] & \begin{array}{c}\text{Subgroups}\\ K' \text{ of } H\end{array} \arrow[l, shift left=2, "\phi^{-1}(K') \mapsfrom K'"]
\end{tikzcd}$$

Furthermore, if $\ker\phi \le K, K_1, K_2 \le G$ then

1. $K_1 \le K_2 \iff \phi(K_1) \le \phi(K_2)$,
2. $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$, and
3. K is normal $\iff$ $\phi(K)$ is normal.

We can get a version for rings immediately.

Theorem — Correspondence theorem for rings

Let $\phi\colon R \to S$ be a surjective ring homomorphism. Then there is a bijection

$$\begin{tikzcd}
\begin{array}{c}\text{Subgroups } K\\ \text{of } R^+ \text{ with}\\ \ker\phi \le K\end{array} \arrow[r, shift left=2, "K \mapsto \phi(K)"] & \begin{array}{c}\text{Subgroups}\\ K' \text{ of } S^+\end{array} \arrow[l, shift left=2, "\phi^{-1}(K') \mapsfrom K'"]
\end{tikzcd}$$

Furthermore, if $\ker\phi \le K, K_1, K_2 \le R^+$, then K is an ideal if and only if $\phi(K)$ is an ideal.

Proof.

Apply proposition and use the fact that $K = \phi^{-1}(\phi(K))$. □

In the special case of $q\colon R \to R/\mathcal{I}$, 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 $\mathrm{ev}_{x=0}\colon R[x] \to R$. So ideals of $R[x]$ containing (x) correspond to ideals $\mathcal{I}$ of R.

If $\mathcal{I}$ is an ideal of R, what is the corresponding ideal in $R[x]$?

Answer:

$$\begin{aligned}\mathrm{ev}_{x=0}^{-1}(\mathcal{I}) &= \{f \in R[x] : f(0) \in \mathcal{I}\} \\ &= \left\{\sum_{i=0}^{n} a_i x^i : n \geq 0,\ a_i \in R \text{ for } 0 \leq i \leq n,\ a_0 \in \mathcal{I}\right\}.\end{aligned}$$

Second isomorphism theorem

Recall from group theory:

Theorem — Second isomorphism theorem for groups

Suppose $H \subseteq N_G(K)$. Then $HK \leq G$, $K \trianglelefteq HK$, and $H \cap K \trianglelefteq H$. Furthermore, if $i_H \colon H \to HK$ is the inclusion and $q_1 \colon H \to H/(H \cap K)$ and $q_2 \colon HK \to HK/K$ are the quotient maps, then there is an isomorphism $\psi \colon H/(H \cap K) \to HK/K$ such that $\psi \circ q_1 = q_2 \circ i_H$.

$$\begin{tikzcd}
H \arrow[r, "i_H"] \arrow[d, "q_1"'] & HK \arrow[d, "q_2"] \\
H/H \cap K \arrow[r, "\psi"'] & HK/K
\end{tikzcd}$$

Let's restate this for abelian groups with additive notation.

Theorem — Second isomorphism theorem for abelian groups

Suppose $H, K \leq G$. Then $H + K \leq G$, and furthermore, if $i_H \colon H \to H + K$ is the inclusion, $q_1 \colon H \to H/H \cap K$ and $q_2 \colon H + K \to H + K/K$ are the quotient maps, then there is an isomorphism $\psi \colon H/H \cap K \to H + K/K$ such that $\psi \circ q_1 = q_2 \circ i_H$.

$$\begin{tikzcd}
H \arrow[r, "i_H"] \arrow[d, "q_1"'] & H + K \arrow[d, "q_2"] \\
H/H \cap K \arrow[r, "\psi"'] & H + K/K
\end{tikzcd}$$

Now we can extend this to rings.

Theorem — Second isomorphism theorem for rings

Let S be a subring of R and let $\mathcal{I}$ be an ideal of R. Then $S + \mathcal{I}$ is a subring of R and $S \cap \mathcal{I}$ is an ideal of S. Furthermore, if $i_S \colon S \to S + \mathcal{I}$ is the inclusion and $q_1 \colon S \to S/S \cap \mathcal{I}$ and $q_2 \colon S + \mathcal{I} \to S + \mathcal{I}/\mathcal{I}$ are the quotient maps, then there is a (ring) isomorphism $\psi \colon S/S \cap \mathcal{I} \to S + \mathcal{I}/\mathcal{I}$ 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 $S+\mathcal{I}$, note that $1 \in S+\mathcal{I}$. If $x, y \in S+\mathcal{I}$, then $x = s+a$ and $y = t+b$ for some $s, t \in S$ and $a, b \in \mathcal{I}$. So $xy = st + (st + at + ab) \in S+\mathcal{I}$ and hence $S+\mathcal{I}$ is a subring.

Exercise: show $S \cap \mathcal{I}$ is an ideal of S.

By second isomorphism theorem for groups, there is an isomorphism $\psi\colon S/S\cap\mathcal{I} \to S+\mathcal{I}/\mathcal{I}$ such that $\psi \circ q_1 = q_2 \circ i_S$.

By applying the lemma below, we see ψ is a ring isomorphism. □

Lemma — From universal property of quotient rings

Let R, S, T be rings. Suppose that $\psi_1\colon R \to T$ is a ring homomorphism and $\psi_2\colon T \to S$ 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.

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.

Third isomorphism theorem

From group theory:

Theorem — Third isomorphism theorem for groups

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 $\psi \colon G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$.

$$\begin{tikzcd}
G \arrow[r, "q_1"] \arrow[d, "q_3"'] & G/N \arrow[d, "q_2"] \\
G/K \arrow[r, "\psi"'] & (G/N)/(K/N)
\end{tikzcd}$$

Now for rings:

Theorem — Third isomorphism theorem for groups

Suppose $\mathcal{I} \subseteq \mathcal{K}$ are ideals of a ring R, and let

- q_1 be the quotient map $R \to R/\mathcal{I}$,
- 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 a (ring) isomorphism $\psi \colon R/\mathcal{K} \to (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$ such that $\psi \circ q_3 = q_2 \circ q_1$.

$$\begin{tikzcd}
R \arrow[r, "q_1"] \arrow[d, "q_3"'] & R/\mathcal{I} \arrow[d, "q_2"] \\
R/\mathcal{K} \arrow[r, "\psi"'] & (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})
\end{tikzcd}$$

Proof.

Apply the lemma from the universal property of quotient rings again. □

Example

$(\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ as groups, and also as rings.

Example

As in the previous example, let $\mathcal{J}$ be an ideal of R and $\mathcal{I} = \mathrm{ev}_0^{-1}(\mathcal{J}) \subseteq R[x]$.

Now $\mathcal{I}$ contains (x), so by the third isomorphism, $R[x]/\mathcal{I} \cong (R[x]/(x))/(\mathcal{I}/(x))$.

By first isomorphism theorem, $R[x]/(x) \cong R$ since $(x) = \ker \mathrm{ev}_0$. 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: $R[x]/\mathcal{I} \cong (R/(x))/(\mathcal{I}/(x)) \cong R/\mathcal{J}$.

Exercise: show that this isomorphism is the same as the isomorphism $R/\mathcal{J} \cong R[x]/\mathcal{I}$ from the second isomorphism theorem.

Week 9: Maximal and Prime Ideals

22: Maximal ideals and fields

Constructing complex numbers from real numbers

From last week: we can construct new rings $R/(X)$ by taking $X \subseteq R$. What sets X might we like to look at?

Suppose we didn't know about $\mathbb{C}$, and we want a square root of -1. We want to take $\mathbb{R}$ and add an element x such that $x^2 = -1$.

So let's look at $\mathbb{R}[x]/(x^2+1)$ (note $x^2 + 1 = 0 \iff x^2 = -1$). If we look at $\overline{x} = [x]$ 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

$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

If we didn't know about $\mathbb{C}$, we could use $\mathbb{R}[x]/(x^2+1)$ as the definition.

The complex numbers

Let's clarify what $\mathbb{C}$ is:

- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$
- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

How does $\mathbb{R}[x]/(x^2 + 1)$ correspond to $\mathbb{C}$? We know that $\overline{x}$ acts like i.

Lemma

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 the 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 $\sum_{i=0}^{n} a_i\overline{x}^i$. (Note the bar on a_i is dropped for brevity.)

If $n \geq 2$, then $a_n x^{n-2}(x^2 + 1) \in (x^2 + 1)$, so $a_n\overline{x}^n + a_n\overline{x}^{n-2} = 0$. Thus

$$\begin{aligned}\sum_{i=0}^{n} a_i\overline{x}^i &= \sum_{i=0}^{n} a_i\overline{x}^i - (a_n\overline{x}^n + a_n\overline{x}^{n-2}) \\ &= 0 \cdot \overline{x}^n + a_{n-1}\overline{x}^{n-1} + (a_{n-2} - a_n)\overline{x}^{n-2} + \cdots .\end{aligned}$$

We 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 $f \in (x^2 + 1)$ and $f \neq 0$, then $f = g(x^2 + 1)$ for $g \in \mathbb{R}[x]$ with $g \neq 0$. So $\deg(f) = \deg(g) + \deg(x^2 + 1) \geq 2$.

Hence every non-zero element of $(x^2 + 1)$ has degree ≥ 2. Then the only way $(a - c) + (b + d)x$ can be in $(x^2 + 1)$ is if it is zero, so $a = c$ and $b = d$. □

Now for the theorem:

Theorem

$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Proof.

Since $\mathbb{R}$ is a subring of $\mathbb{C}$, we can consider $\mathbb{R}[x]$ as a subring of $\mathbb{C}[x]$.

Let $j\colon \mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$ be the inclusion. Let $\phi = \mathrm{ev}_{x=i} \circ j\colon \mathbb{R}[x] \to \mathbb{C}[x] \to \mathbb{C}$. Then $\phi(x) = i$, so $\phi(x^2+1) = i^2+1 = 0$. So $x^2+1 \in \ker\phi$, so $(x^2+1) \subseteq \ker\phi$.

By the universal property of quotient rings, there is a homomorphism $\psi\colon \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ such that $\psi \circ q = \phi$. So $\psi(a+b\overline{x}) = \phi(a+bx) = a+bi$. By the lemma, ψ is a bijection. □

This is a common line of proof (see Homework #4 Q9).

Generalizations

We constructed $\mathbb{C}$ by asking for an element x such that $x^2+1=0$.

If we start from a field $\mathbb{K}$, can we ask for an element x satisfying any polynomial equation(s), and then just cosntruct a ring containing $\mathbb{K}$ with such an element?

Yes! But the ring might be zero if we ask for too much.

Example

- $1 \neq 0$ in $\mathbb{K}[x]/(x^2+1)$ as we've seen.
- If p is a polynomial of degree $n \geq 1$, then $\mathbb{K}[x]/(p)$ is a $\mathbb{K}$-vector space of dimension n (exercise similar to lemma). So $1 \neq 0$ in $\mathbb{K}[x]/(p)$.
- $1 = 0$ in $\mathbb{K}[x]/(x^2+1, x^3+x+1)$, since $x^3+x+1-x(x^2+1) = 1 \in (x^2+1, x^3+x+1)$.

Maximal ideals

Let $\mathcal{I}$ be an ideal of a commutative ring R. When is $R/\mathcal{I}$ a field?

We know that the only ideals in a field $\mathbb{K}$ are (0) and $\mathbb{K}$. Suppose $\mathbb{K} = R/\mathcal{I}$ is a field, and $q \colon R \to \mathbb{K}$ is the quotient map. By the correspondence theorem, the only ideals of R containing $\mathcal{I}$ are $q^{-1}((0)) = \ker q = \mathcal{I}$ and $q^{-1}(\mathbb{K}) = R$.

Definition — maximal ideal

An ideal $\mathcal{I}$ of a ring R is **maximal** if the only ideals containing $\mathcal{I}$ are $\mathcal{I}$ are R.

Intuition: a maximal ideal is a maximal proper ideal under $\subseteq$.

Lemma

If $R/\mathcal{I}$ is a field, then $\mathcal{I}$ is maximal.

Ideals in fields

Proposition

A commutative ring R is a field if and only if $1 \neq 0$, and the only ideals in R are (0) and R.

Requiring $1 \neq 0$ is the same as requiring $(0) \neq R$.

Proof.

We already saw the forward implication.

For the reverse, suppose $x \in R$ wher $x \neq 0$. Then $(x) = R$. Then $1 \in (x) = xR$, so there is $y \in R$ such that $xy = 1$. So x is a unit. Since all non-zero elements of R are units, R is a field. □

Maximal ideals and fields

Theorem

Let $\mathcal{I}$ be an ideal in a commutative ring R. Then $R/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is maximal.

Proof.

By correspondence theorem, the only ideals of $R/\mathcal{I}$ are (0) and $R/\mathcal{I}$ if and only if the only ideals of R containing $\mathcal{I}$ are $\mathcal{I}$ and R. So by the proposition, $R/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is maximal. □

Example

- $\mathbb{K}[x]/(x-c) \cong \mathbb{K}$ for all $c \in \mathbb{K}$, so $(x-c)$ is a maximal ideal of $\mathbb{K}[x]$ for any field $\mathbb{K}$.
- $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so (x^2+1) is a maximal ideal of $\mathbb{R}[x]$.

Example

$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field, so (x) is not a maximal ideal of $\mathbb{Z}[x]$.

Indeed, we know that $(x) \subsetneq (2,x) \subsetneq \mathbb{Z}[x]$. We also know that $(2,x) = \{f \in \mathbb{Z}[x] : f(0) \in (2)\} = \mathrm{ev}_{x=0}^{-1}((2))$ for ideal $(2) \subseteq \mathbb{Z}$. By the second isomorphism theorem, $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$, which is a field.

Exercise: $\mathbb{Z}[x]/(n,x) \cong \mathbb{Z}/n\mathbb{Z}$ and hence (n,x) is maximal for $n \in \mathbb{Z}$ if and only if n is prime.

Example

If R is commutative ring, we have

$$\mathrm{ev}_{(a,b)} = \mathrm{ev}_{x=a} \circ \mathrm{ev}_{y=b} \colon R[x,y] = R[x][y] \to R[x] \to R.$$

Then $\ker \mathrm{ev}_{(a,b)} = \mathrm{ev}_{(a,b)}^{-1}((0)) = \mathrm{ev}_{y=b}^{-1}((x-a)) = \{f \in R[x][y] : f(x,b) \in (x-a)R[x]\} = (x-a, y-b)$. By the first isomorphism theorem, $R[x,y]/(x-a,y-b) \cong R$. So $(x-a,y-b)$ is a maximal ideal of $R[x,y]$ if and only if R is a field.

For $(y-x^2) \subseteq R[x,y]$, we know $R[x,y]/(y-x^2) \cong R[x]$. $R[x]$ is not a field since x is not a unit. So $(y-x^2)$ is not maximal. (Indeed, $(y-x^2) \subsetneq (x,y)$.)

Example

Let $c \in \mathbb{R}$. In the homework, you'll show

$$\mathbb{R}[x]/(x^2 - c) \cong \begin{cases} \mathbb{C} & c < 0 \\ \mathbb{R} \times \mathbb{R} & c > 0 \\ \mathbb{R}[x]/(x^2) & c = 0 \end{cases}.$$

Exercise: $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}[x]/(x^2)$ are not fields. Hence $\mathbb{R}[x]/(x^2 - c)$ is a field if and only if $c < 0$. So $(x^2 - c)$ is maximal if and only if $c < 0$.

Exercise: find proper ideals properly containing $(x^2 - c)$ for $c \geq 0$.

Partially-ordered sets

Definition — partial order

A **partial order** on a set X is a relation $\leq$ on X such that for all $x, y, z \in X$:

1. $x \leq x$;
2. if $x \leq y$ and $y \leq x$, then $x = y$; and
3. if $x \leq y$ and $y \leq z$, then $x \leq z$.

We say that $x < y$ if $x \leq y$ and $x \neq y$.

A **maximal element of a subset** $S \subseteq X$ is an element $x \in S$ such that if $x \leq y$ for $y \in S$, then $x = y$.

An **upper bound of a subset** $S \subseteq X$ is an element $x \in X$ such that $y \leq x$ for all $y \in S$.

A **maximum element of a subset** $S \subseteq X$ is an element $x \in S$ which is an upper bound for S (unique if it exists).

A maximum element (if it exists) of a subset X is maximal. But a subset S can have maximal elements without having a maximum element.

Example

Consider $2^{\{1,2\}} = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$ 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 $\subseteq$.

Proper ideals ordered under inclusion

Let R be a non-zero ring, so the set of proper ideals is non-empty. Does the set of proper ideals of R have a maximum element? Once a set has more than one maximal element, it can't have a maximum.

> **Example**
>
> $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. So (n) is maximal if and only if n is prime. So (2) and (3) are both maximal.

Does the set of proper ideals always have a maximal element?

Maximal elements for the set of proper ideals?

Does the set of proper ideals always have a maximal element? Maybe we can construct one:

- Pick a proper ideal $\mathcal{I}_0$.
- If $\mathcal{I}_0$ is not maximal, find a proper ideal $\mathcal{I}_1$ with $\mathcal{I}_0 \subsetneq \mathcal{I}_1$.
- Continue until we get to a maximal element.

Of course, this might not work. We might be in a poset (partially ordered set) like $(\mathbb{N}, \leq)$, where we have infinitely long increasing sequences like $1 < 2 < 3 < \cdots$. In that case, we're only guaranteed to get a sequence $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$ of proper ideals.

Chains of ideals

If $x_0 \leq x_1 \leq x_2 \leq \cdots$ in a partially ordered set X, then the subset $S = \{x_0, x_1, x_2, \ldots\}$ is a chain.

Definition — chain

If $(X, \leq)$ is a partially ordered set, we say that a subset $S \subseteq X$ is a **chain** if for every $s, t \in S$, either $s \leq t$ or $t \leq s$ (or both).

Is the set of proper ideals like $\mathbb{N}$, a chain with no upper bound?

Lemma

Let R be a commutative ring, and let $\mathcal{F}$ be a chain of ideals. Then

$$\bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$$

is an ideal of R.

Proof.

Homework. □

Note that this doesn't work if $\mathcal{F}$ is not a chain, since the union of ideals is typically not closed under addition.

Example

$(2) \cup (3) \subseteq \mathbb{Z}$ doesn't contain $5 = 2 + 3$.

If $\mathcal{F}$ is a chain of proper ideals, then $1 \notin \mathcal{I}$ for all $\mathcal{I} \in \mathcal{F}$. So $1 \notin \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$.

Corollary

If $\mathcal{F}$ is a chain of proper ideals of R, then there is a proper ideal which is an upper bound for $\mathcal{F}$.

Suppose we try to construct a maximal ideal, and end up with a sequence $\mathcal{I}_0 \subsetneq \mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$ of proper ideals.

By the corollary, there is a proper ideal $\mathcal{J}_0$ which is an upper bound for $\{\mathcal{I}_0, \mathcal{I}_1, \ldots\}$, that is, $\mathcal{I}_k \subseteq \mathcal{J}_0$ for all k.

If $\mathcal{J}_0$ is maximal, then we are done. If not, we can find a proper ideal $\mathcal{J}_1$ with $\mathcal{J}_0 \subsetneq \mathcal{J}_1$, and our search continues.

Is this going to end? It looks like we face a never-ending (infinite) succession of choices. We need some help.

Zorn's lemma

Axiom — Axiom of choice

Let $X \subseteq 2^Y$ for some Y, such that if $A \in X$, then $A \neq \varnothing$. Then there is a function $f\colon X \to Y$ 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 formulation:

Axiom — Equivalent form of the axiom of choice #1

A function $f\colon X \to Y$ is surjective if and only if it has a right inverse.

(We called this a theorem earlier in the course because the axiom of choice is one of our standard axioms.)

Axiom — Equivalent form of the axiom of choice #2: Zorn's lemma

Let $(X, \leq)$ be a partially ordered set, such that if S is a chain in X, then there is an element $x \in X$ which is an upper bound for S. Then X contains a maximal element.

Maximal elements for the set of proper ideals, continued

Proposition

Suppose that $\mathcal{J}$ is a proper ideal in a commutative ring R. Then there is a maximal ideal $\mathcal{K}$ of R containing $\mathcal{J}$.

Proof.

Let $\mathcal{P} = \{\mathcal{I} \subsetneq R : \mathcal{I} \text{ is an ideal and } \mathcal{J} \subseteq \mathcal{I}\}$, ordered under $\subseteq$. Let $\mathcal{F}$ be a chain in $\mathcal{P}$.

By the lemma, $\mathcal{I}' = \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$ is an ideal of R. Clearly $\mathcal{J} \subseteq \mathcal{I}'$, and since $1 \notin \mathcal{I}'$ we have that $\mathcal{I}' \in \mathcal{P}$. So $\mathcal{I}'$ is an upper bound for $\mathcal{F}$ in $\mathcal{P}$.) By Zorn's lemma, $\mathcal{P}$ has a maximal element. □

Example

Take (0) in $\mathbb{Z}$. Then (0) is contained in (p) for any prime p, all of which are maximal. So the ideal $\mathcal{K}$ in the proposition isn't necessarily unique.

In particular, every non-zero commutative ring has a maximal ideal. Or equivalently:

Corollary

For every non-zero commutative ring R, there is a field $\mathbb{K}$ such that there is a homomorphism $\phi \colon R \to \mathbb{K}$.

Proof.

Take $\mathcal{I}$ to be a maximal ideal of R, and let $\phi \colon R \to R/\mathcal{I}$ be the quotient map. □

23: Prime ideals and integral domains

Zero divisors

If $\mathbb{K}$ is a field and $f, g \in \mathbb{K}[x]$, then $\deg(fg) = \deg(f) + \deg(g)$.

In contrast, in an arbitrary ring like $R = \mathbb{Z}/6\mathbb{Z}$, we can have things like $(1+2x)(1+3x) = 1 + 5x + 6x^2 = 1 - x$. This happens when there are elements $x, y \in R \setminus \{0\}$ with $xy = 0$.

Definition — zero divisor

Let R be a ring. A non-zero element $x \in R$ is a **zero divisor** if there is a non-zero element $y \in R$ such that $xy = 0$ or $yx = 0$.

That is, x (and y) divide 0.

Example

If n is not prime, then $n = ab$ for $2 \leq a, b < n$. So $[a], [b] \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$, but $[a] \cdot [b] = [ab] = 0$, so $[a], [b]$ are zero divisors.

Example

If R and S are non-zero rings and $a \neq 0$ in R and $b \neq 0$ in S, then $(a, 0)$ and $(0, b)$ are non-zero in the product ring $R \times S$.

But $(a, 0) \cdot (0, b) = (0, 0) = 0$ in $R \times S$, so $(a, 0)$ and $(0, b)$ are zero divisors.

Example

For any ring R, $\overline{x}$ is a zero divisor in $R[x]/(x^2)$ since $\overline{x}^2 = 0$.

Example

For any ring R, $\overline{x}$ and $\overline{y}$ are zero divisors in $R[x]/(xy)$.

For these examples, we still need to show $\overline{x}$ or $\overline{y}$ are non-zero; there are techniques for this later and on the homework.

Example

Suppose $\mathbb{K}$ is a field. Let $E_{ij} \in M_n\mathbb{K}$ be the matrix with a 1 in position ij and 0's elsewhere.

Then $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$, 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 less than

n (i.e., A is not invertible).

Example

Let G be a group, and let $g \in G \setminus \{e\}$ with $|g| = 2$.

Then $(e + g)(e - g) = e - g^2 = e - e = 0$ in $\mathbb{Z}G$.

Kaplansky zero divisor conjecture: if every element of $G \setminus \{e\}$ has infinite order, and $\mathbb{K}$ is a field, then $\mathbb{K}G$ has no zero divisors.

Units and zero divisors

Lemma

Let u be a unit in a ring R. Then u is not a zero divisor.

Proof.

$uv = 0 \implies v = u^{-1}uv = 0$ and $vu = 0 \implies v = vuu^{-1} = 0$. □

Every non-zero element of a field is a unit, so fields have no zero divisors.

In general, an element can be not a zero divisor but also not a unit:

- $\mathbb{Z}$ has no zero divisors, but the only units are ± 1.
- If $f \in \mathbb{K}[x]$ with $f \neq 0$ and $\mathbb{K}$ a field, then by the degree formula, $fg = 0$ if and only if $g = 0$.

  So $\mathbb{K}[x]$ has no zero divisors, but $\mathbb{K}[x]^\times = \mathbb{K}^\times$.

Cancellation laws

Proposition

Suppose a non-zero element x in a ring R is not a zero divisor. If $xa = xb$ or $ax = bx$ for some $a, b \in R$, then $a = b$.

Proof.

If $xa = xb$, then $x(a-b) = 0$. Since $x \neq 0$ and x is not a zero divisor, $a-b = 0 \implies a = b$. Similar if $ax = bx$. □

Corollary

Let R be a finite ring. If a non-zero element x is not a zero divisor, then x is a unit.

Proof.

Consider the function $\ell_x \colon R \to R : y \mapsto xy$. If $\ell_x(a) = \ell_x(b)$, then $xa = xb$ and so $a = b$. So ℓ_x is injective.

Since R is finite, by the pigeonhole principle ℓ_x is also surjective. Thus there is $y \in R$ such that $\ell_x(y) = xy = 1$, so x has a right inverse.

A similar argument with $y \mapsto yx$ shows x has a left inverse. Hence x is invertible. □

Integral domains

Definition — integral domain

An **integral domain** (or **domain**) is a commutative ring R such that $1 \neq 0$ and R has no zero divisors.

Example

- Every field is an integral domain.
- $\mathbb{Z}$ is an integral domain.
- All the examples of rings we've looked at with zero divisors are not domains ($\mathbb{Z}/n\mathbb{Z}$ for n not prime, $\mathbb{R} \times \mathbb{R}$, $\mathbb{R}[x]/(x^2)$).
- $\{0\}$ has no zero divisors, but is not a domain.

Since all non-zero divisors in finite rings are units:

Corollary

All finite integral domains are fields.

Proposition

If R is an integral domain, then:

1. If $f, g \in R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$.
2. $R[x]$ is an integral domain.

Proof.

1. True if f or g is zero, so suppose $f, g \neq 0$. Let $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ where $a_n, b_m \neq 0$. Then $fg = a_n b_m x^{n+m}$+lower degree terms. Since R is a domain, $a_n b_m \neq 0$, so $\deg(fg) = n + m = \deg(f) + \deg(g)$.
2. Suppose $f, g \neq 0$ and $fg = 0$. Then $\deg(fg) = -\infty$ so by part (a), we must have $\deg(f) = -\infty$ or $\deg(g) = -\infty$. So one of f, g is zero, so neither f nor g can be a zero divisor.

□

Interesting domains?

Proposition

If R is a subring of a field $\mathbb{K}$, then R is a domain.

Proof.

$\mathbb{K}$ is commutative with $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$. So R is commutative and $1_R \neq 0_R$.

If x is a non-zero element of R and $xy = 0$ for $y \in R$, then $y = x^{-1}xy = 0$ in $\mathbb{K}$, so $y = 0$ in R. So R has no zero divisors. □

Example

$\mathbb{Z}$ is a subring of $\mathbb{Q}$, and hence a domain.

Proposition

If $\alpha \in \mathbb{C}$ satisfies $\alpha^2 \in \mathbb{Z}$, then

$$\mathbb{Z}[a] = \{a + b\alpha : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$.

Proof.

Homework. □

This leads to interesting domains like the Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Prime ideals

Can we construct interesting domains of the form $R[x]/(p)$?

First, we need to answer: if $\mathcal{I}$ is an ideal of a commutative ring R, when is $R/\mathcal{I}$ an integral domain?

Suppose $R/\mathcal{I}$ is an integral domain. If $\overline{a} \cdot \overline{b} = 0$ 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, $\overline{r} = 0$ in $R/\mathcal{I}$ if and only if $r \in \mathcal{I}$. So $\overline{a} \cdot \overline{b} = 0$ in $R/\mathcal{I}$ if and only if $ab \in \mathcal{I}$, and one of $\overline{a}, \overline{b}$ is zero in $R/\mathcal{I}$ if and only if one of a, b is in $\mathcal{I}$.

Definition — prime ideal

Let R be a commutative ring. Then an ideal $\mathcal{I}$ is **prime** if $\mathcal{I} \subsetneq R$ and whenever $ab \in \mathcal{I}$ for $a, b \in R$, at least one of a, b is in $\mathcal{I}$.

Theorem

Let $\mathcal{I}$ be an ideal in a commutative ring R. Then $R/\mathcal{I}$ is an integral domain if and only if $\mathcal{I}$ is a prime ideal.

Example

- If $\mathcal{I}$ is a maximal ideal of a commutative ring R, then $R/\mathcal{I}$ is a field and hence a domain. So maximal ideals are prime.
- $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime. So $n\mathbb{Z}$ is a prime ideal if and only if n is prime.
- Previously we saw $\mathbb{K}[x, y]/(y - x^2) \cong \mathbb{K}[x]$, which is a domain but not a field. So $(y - x^2)$ is a prime ideal which is not maximal.

Proof.

Since R is commutative and $R \to R/\mathcal{I} : r \mapsto \overline{r}$ is surjective, $R/\mathcal{I}$ is commutative for any ideal $\mathcal{I}$, and $R/\mathcal{I}$ is zero if and only if $\mathcal{I} = R$.

Using surjectivity of $R \to R/\mathcal{I}$ again, $R/\mathcal{I}$ has no zero divisors if and only if for all $a, b \in R$, 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 $R/\mathcal{I}$ if and only if $r \in \mathcal{I}$, we have that $R/\mathcal{I}$ has no zero divisors if and only if $ab \in \mathcal{I}$ means one of a, b is in $\mathcal{I}$ for all $a, b \in \mathcal{I}$.

So $R/\mathcal{I}$ is an integral domain if and only if $\mathcal{I}$ is prime. □

Primality and factoring

We'll have more to say in a week about when an ideal is prime. For now, we consider one reason why an ideal might not be prime.

Lemma

If R is an integral domain and $f, g \in R[x]$ have 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 $f, g \notin fgR[x]$. □

Example

Since $(x^2 + 1)$ is maximal in $\mathbb{R}[x]$, we have $(x^2 + 1)$ is prime.

However, $(x^2 + 1)$ is not prime in $\mathbb{C}[x]$, since $x^2 + 1 = (x - i)(x + i)$ in $\mathbb{C}[x]$.

As the previous example shows, whether or not a polynomial factors can be subtle, since it depends on the coefficient ring.

Example

$(x^2 + 1)$ is not prime in $\mathbb{Z}_2[x]$ as $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$.

On the other hand, in $\mathbb{Z}_3[x]$, we can check that $(ax + b)(cx + d) \neq x^2 + 1$ for all $a, b, c, d \in \mathbb{Z}_3$, so $x^2 + 1$ does not factor. Later we will see $(x^2 + 1)$ is actually prime here.

A related idea

$\mathbb{C}[x]/(x^2+1)$ is a ring containing $\mathbb{C}$ and an additional element $x \notin \mathbb{C}$ such that $x^2 = -1$. However, $\mathbb{C}[x]/(x^2+1)$ is not a domain.

What if we wanted a domain containing $\mathbb{C}$ and an additional element $x \notin \mathbb{C}$ such that $x^2 = -1$?

Proposition

Suppose R is a subring of a domain S and x is an element of S such that $x^2 = t^2$ for some $t \in S$. Then $x = t$ or $x = -t$.

Proof.

If $x^2 = t^2$, then $x^2 - t^2 = 0$, so $(x-t)(x+t) = 0$. Since S is a domain, one of $x - t$ or $x + t$ must be 0. □

Since $i^2 = -1$ in $\mathbb{C}$, there is no domain containing $\mathbb{C}$ and an additional element $x \notin \mathbb{C}$ such that $x^2 = -1$.

Week 10: Fields of Fractions and the Chinese Remainder Theorem

24: Fields of fractions

Domains and subrings of fields

From last week, we had:

Proposition

If R is a subring of a field $\mathbb{K}$, then R is a domain.

This week, we'll show:

Theorem

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 $\mathbb{Q}$ (also of $\mathbb{R}$ and $\mathbb{C}$).
- $\mathbb{Q}[x]$ 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 proving the theorem: we've already done the reverse direction; for the forward direction, given R we 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

Let $\mathbb{K}$ be a field containing $\mathbb{Z}$ as a subring. Then $\mathbb{K}$ contains $\mathbb{Q}$ as a subfield.

Notes:

- Here, "$\mathbb{K}$ containing $\mathbb{Z}$ as a subring" means there is an isomorphism $\phi\colon \mathbb{Z} \to R$ where R is a subring of $\mathbb{K}$.
- By the first isomorphism theorem, this is equivalent to saying there is an injective homomorphism $\phi\colon \mathbb{Z} \to \mathbb{K}$.
- $\phi\colon \mathbb{Z} \to \mathbb{K}$ is called the **subgroup inclusion map**, since it's like the inclusion map $R \hookrightarrow \mathbb{K} : x \mapsto x$ for the actual subring.

Proof.

Let $\phi\colon \mathbb{Z} \to \mathbb{K}$ be the subgroup inclusion map. Define $\psi\colon \mathbb{Q} \to \mathbb{K}$ by $\frac{a}{b} \mapsto \phi(a)\phi(b)^{-1}$.

Is this 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 $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}$ and hence ψ is well-defined.

Exercise: show ψ is a ring homomorphism.

Any map from a field is injective, so ψ is an injective homomorphism. □

Constructing fractions

How do we get $\mathbb{Q}$ from $\mathbb{Z}$?

- Elements are $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$.
- $\frac{a}{c} = \frac{b}{d}$ if and only if $ad = bc$.
- 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 $a, b, a', b' \in \mathbb{Z}$.

We can do this for an arbitrary integral domain as well. The **field of fractions** Q of an integral domain R is defined as follows:

- Elements are $\frac{a}{b}$ where $a, b \in R$ and $b \neq 0$.
- $\frac{a}{c} = \frac{b}{d}$ if and only if $ad = bc$.
- 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 (i.e., why do we need an integral domain)? If $yz = 0$ and $y, z \neq 0$, 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 $a, b, a', b' \in \mathbb{Z}$.

Later, we'll see that we can take fractions over rings with zero divisors, we just can't put zero divisors in the denominator.

Constructing fractions of an arbitrary ring

Suppose we have a commutative ring R and we want to make a ring of fractions $\frac{a}{b}$ with $a, b \in R$.

The operations should be $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, with zero being $\frac{0}{1}$ and the identity being $\frac{1}{1}$.

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 an inverse, and for operations to be well-defined, we want S to be multiplicatively closed.

Definition — multiplicatively closed

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

1. every element of S is a unit in Q, and
2. 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.

That is, Q is the smallest commutative ring satisfying (1).

Theorem — (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 homomorphism $\phi\colon R \to Q$ such that

1. $\phi(a) \in Q^\times$ for all $a \in S$, and every element of Q is of the form $\phi(a)\phi(b)^{-1}$ for $a \in R$ and $b \in S$, and
2. if $\psi\colon R \to T$ is a homomorphism such that $\psi(x) \in T^\times$ for all $x \in S$, then there is a homomorphism $\tilde{\psi}\colon Q \to T$ 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 $\tilde{\psi}(\phi(a)^{-1}) = \tilde{\psi}(a)^{-1} = \psi(a)^{-1}$.

Definition — localization

The ring Q from the theorem is called the **localization** of R at S (or with respect to S), 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 $ad = bc$.

First we show $\sim$ is an equivalence relation:

- $(a,b) \sim (a,b)$ since $ab = ba$ by commutativity.
- If $(a,b) \sim (c,d)$ then commutativity again gives $cb = da$, 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 $d \in S$, we know d is neither zero nor a zero divisor, so $af = be$ by cancellation. So $(a,b) \sim (e,f)$.

Let $Q = Q_0/\sim$ be the set of equivalence classes of $\sim$.

Notation: If $a \in R$ and $b \in S$, let $\frac{a}{b} := [(a,b)] \in Q$.

Define operations $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

We show these are well-defined.

Because S is multiplicatively closed, if $a,c \in R$ and $b,d \in S$ then $[(ad+bc,bd)]$ and $[(ac,bd)]$ are well-defined elements of Q. So $([(a,b)],[(c,d)]) \sim_+ [(ad+bc,bd)]$ is a well-defined relation between $Q \times Q$ and Q; similar for $\cdot$.

Suppose $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$, so $ab' = ba'$ 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 $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ and $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ as desired.

Now we show $(Q,+)$ is an abelian group.

$\frac{a}{b} = \frac{0}{1}$ if and only if $a = 1 \cdot a = b \cdot 0 = 0$.

For all $a,c,e \in R$ and $b,d,f \in S$, we have associativity:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf + bcf + ebd}{bdf} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right);$$

commutativity:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{c}{d}+\frac{a}{b};$$

zero ($\frac{0}{1}$);

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b};$$

and additive inverse:

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b^2}=\frac{0}{b^2}=\frac{0}{1}.$$

$(Q,+)$ is an abelian group with zero $\frac{0}{1}$ and $-\frac{a}{b}=\frac{-a}{b}$.

Now we show $(Q,+,\cdot)$ is a commutative ring.

For all $a,c,e\in R$ and $b,d,f\in S$, we have

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ab}{cd}=\frac{ba}{dc}=\frac{c}{d}\cdot\frac{a}{b}$$

and

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)$$

so $\cdot$ is associative and commutative.

Since $\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{a}{b}$, we have that $\frac{1}{1}$ is an identity.
Also, if $a\in R$ and $b,c\in S$, then $\frac{ac}{bc}=\frac{a}{b}$ since $acb=bca$.

Finally for distributivity,

$$\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{cf+de}{df}=\frac{acf+ade}{bdf}=\frac{acfb+adeb}{b^2df}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}.$$

So $(Q,+,\cdot)$ is a commutative ring.

Now we can define $\phi\colon R\to Q : a\mapsto\frac{a}{1}$. To check this is a ring homomorphism, we have

$$\begin{aligned}\phi(1)&=\frac{1}{1}\\ \phi(a+b)&=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=\phi(a)+\phi(b)\\ \phi(ab)&=\frac{ab}{1}=\frac{a}{1}\cdot\frac{b}{1}=\phi(a)\phi(b)\end{aligned}$$

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 $a \in S$.

Lastly, since every element of Q has form $\frac{a}{b}$ for some $a \in R$ and $b \in S$, we see this is also $\phi(a)\phi(b)^{-1}$.

This proves part (1) of the theorem.

Suppose $\psi\colon R \to T$ is a homomorphism such that $\psi(a) \in T^\times$ for all $a \in S$. $\operatorname{Im}\psi \cong R/\ker\phi$ is commutative, so we can assume T is commutative. (Exercise: if $ab = ba$ for $a \in T^\times$ and $b \in T$, then $a^{-1}b = ba^{-1}$.)

Define $\tilde{\psi}\colon Q \to T : \frac{a}{b} \mapsto \psi(a)\psi(b)^{-1}$.

Since $\psi(b) \in T^\times$ if $b \in S$, we see $\psi(a)\psi(b)^{-1}$ 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 $\tilde{\psi} \circ \phi = \psi$.

Finally, we just need to show that $\tilde{\psi}$ is a ring homomorphism. We have that

$$\tilde{\psi}\left(\frac{1}{1}\right) = \psi(1)\psi(1)^{-1} = 1,$$

$$\begin{aligned}\tilde{\psi}\left(\frac{a}{b} + \frac{c}{d}\right) &= \tilde{\psi}\left(\frac{ad+bc}{bd}\right) \\ &= \psi(ad+bc)\psi(bd)^{-1} \\ &= \psi(a)\psi(b)^{-1} + \psi(c)\psi(d)^{-1} \\ &= \tilde{\psi}\left(\frac{a}{b}\right) + \tilde{\psi}\left(\frac{c}{d}\right),\end{aligned}$$

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 $a, c \in R$ and $b, d \in S$.

This proves part (2) of the theorem. □

Uniqueness of localization

Corollary

Let S be a multiplicatively closed subset of a ring R, where S does not contain 0 or any zero divisors. If Q_i and ϕ_i are a commutative ring and an injective homomorphism satisfying conditions (1) and (2) of the theorem for $i = 1, 2$, then there is an isomorphism $\alpha\colon Q_1 \to Q_2$ such that $\alpha \circ \phi_1 = \phi_2$.

$$\begin{tikzcd}
& R \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\
Q_1 \arrow[rr, dashed, "\alpha"'] & & Q_2
\end{tikzcd}$$

Intuitively, α preserves the subring structure of R between Q_1 and Q_2.

Proof.

Since $\phi_i(a) \in Q_i^\times$ for all $a \in S$ and $i = 1, 2$, we can apply part (2) of the theorem to get homomorphisms $\alpha\colon Q_1 \to Q_2$ and $\beta\colon Q_2 \to Q_1$ with $\alpha \circ \phi_1 = \phi_2$ and $\beta \circ \phi_2 = \phi_1$.

$$\begin{tikzcd}
& R \arrow[dl, "\phi_1"'] \arrow[dr, "\phi_2"] & \\
Q_1 \arrow[rr, dashed, bend left, "\alpha"] & & Q_2 \arrow[ll, dashed, bend left, "\beta"]
\end{tikzcd}$$

Suppose $x \in Q_1$. By part (1) of the theorem, $x = \phi_1(a)\phi_1(b)^{-1}$ for some $a \in R$ and $b \in S$. Since $\alpha(\phi_1(b)) = \phi_2(b)$, we get $\alpha(x) = \phi_2(a)\phi_2(b)^{-1}$. So $\beta(\alpha(x)) = \phi_1(a)\phi_1(b)^{-1} = x$. So β is a left inverse to α.

Symmetrically, α is a left inverse to β, so α and β are inverses. So α is an isomorphism. □

Hence the localization $S^{-1}R$ is unique up to isomorphism. Usually, we just take $S^{-1}R$ to be the ring from the proof of the theorem.

Exercise

Show that if we leave out the requirement from that every element of Q is of the form $\phi(a)\phi(b)^{-1}$ for some $a \in R$ and $b \in S$, then there can be non-isomorphic rings satisfying conditions (1) and (2).
(Hint: show that you can replace Q with $Q[x]$ and still satisfy parts (1) and (2).)

Fields of fractions

Lemma

Let R be an integral domain. Then $S = R \setminus \{0\}$ is multiplicatively closed and does not contain 0 or any zero divisors. Furthermore, $S^{-1}R$ is a field.

Proof.

Because R is a subring of S^-1R (in the homomorphic sense), $S^{-1}R$ 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 $\frac{b}{a}$. (Thus $S^{-1}R$ is a non-zero commutative ring where every non-zero element is a unit.) □

Definition — field of fractions

If R is an integral domain and $S = R\setminus\{0\}$, then $S^{-1}R$ is called the **field of fractions** of R.

Now we can prove the main theorem from this week:

Theorem

A ring R is an integral domain if and only if it is (isomorphic to) a subring of a field.

Proof.

We've already seen that every subring of a field is an integral domain.

Conversely, every domain is a subring of its field of fractions. □

Examples of fields of fractions

Lemma

The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

Proof.

It is clear from the construction of $S^{-1}R$ here that we get $\mathbb{Q}$.

Alternatively, we can show $\mathbb{Q}$ satisfies conditions (1) and (2) of the localization theorem. □

Definition — 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

Let Q be the field of fractions of a domain R. Then $Q(x) = R(x)$.

Proof.

Since $R[x]$ is a subring of $Q[x]$, there is an injective homomorphism $\phi\colon R[x] \to Q(x)$.

By part (2) of the localization theorem, there is an inclusion homomorphism $R(x) \to Q(x)$. Since $R(x)$ is a field, this homomorphism is injective.

But $R(x)$ contains $\frac{a}{b}$ for any $a, b \in R$ with $b \neq 0$, this homomorphism $R(x) \to Q(x)$ is surjective. □

So for rational functions, we can assume the coefficients form a field.

Rational functions

Suppose $\mathbb{K}$ is a field. Why do we call fractions $\frac{f(x)}{g(x)} \in \mathbb{K}(x)$ rational *functions*?

Suppose we have $c \in \mathbb{K}$. If $g(c) \neq 0$, then $\frac{f(c)}{g(c)} \in \mathbb{K}$.

Definition — domain

The **domain** $D(F)$ of $F \in \mathbb{K}(x)$ is the set of points $c \in \mathbb{K}$ such that $F = \frac{f(x)}{g(x)}$ for some $f, g \in \mathbb{K}[x]$ with $g(c) \neq 0$.

Homework: give an example of $f, g \in \mathbb{K}[x]$ such that $g(c) = 0$ but $c \in D(f/g)$.

Lemma

$F \in \mathbb{K}(x)$ defines a function $D(F) \to \mathbb{K} : c \mapsto \frac{f(c)}{g(c)}$, where $f, g \in \mathbb{K}[x]$ are chosen such that $F = f/g$ and $g(c) \neq 0$.

Proof (exercise).

Suppose $F = f/g = f'/g'$ for some $f, g, f', g' \in \mathbb{K}[x]$ with $g(c), g'(c) \neq 0$. Then $fg' = f'g$, so $f(c)g'(c) = f'(c)g(c)$. Since $g(c), g'(c) \neq 0$, we get $f(c)g(c)^{-1} = f'(c)g'(c)^{-1}$ or equivalently $\frac{f(c)}{g(c)} = \frac{f'(c)}{g'(c)}$. □

Example

Let $F = \frac{1}{x(x-1)(x+1)} \in \mathbb{C}(x)$. If $F = f/g$, then $g(x) = x(x-1)(x+1)f(x)$, so $g(c) = 0$ for $c \in \{0, 1, -1\}$. We conclude $D(F) = \mathbb{C} \setminus \{0, 1, -1\}$. 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 later this week).

Intuition: functions defined on all $\mathbb{C}$ are polynomials.

The **localization** of $\mathbb{C}[x]$ at $c \in \mathbb{C}$ is the set of rational functions $F \in \mathbb{C}(x)$ with $c \in D(F)$. (Intuition: focus in on c, expand $\mathbb{C}[x]$.)

Lemma

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 $\mathbb{K}(x)$.

Proof.

Homework. □

Localization at a prime ideal

If R is a domain, then $R \setminus \{0\}$ is multiplicatively closed.

Lemma

Let $\mathcal{P}$ be an ideal of a commutative ring R. Then $R \setminus \mathcal{P}$ is multiplicatively closed if and only if $\mathcal{P}$ is prime.

Proof.

Homework. □

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.

Definition — localization (at a prime ideal)

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.

Localization and local rings

Lemma

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 $R(x) \subseteq \mathbb{K}(x)$ of rational functions with c in the domain.

Proof.

Homework. □

This chain of examples is why $S^{-1}R$ is called a "localization".

Proposition

Let $\mathcal{P}$ be a prime ideal in a domain R. Then $R_{\mathcal{P}}$ has a unique maximal ideal.

Recall a commutative ring R is **local** if it has a unique maximal ideal, so equivalently $R_{\mathcal{P}}$ is local.

Localization at a prime ideal, continued

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 $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \notin (p)\} \subseteq \mathbb{Q}$. In particular, this set has a unique maximal ideal.

25: The Chinese remainder theorem

Products of ideals

Definition — product ideal

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. The **product ideal** $\mathcal{I}\mathcal{J}$ is the ideal

$$(\{ab : a \in \mathcal{I},\ b \in \mathcal{J}\}),$$

that is, 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 neither x nor 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 $\mathcal{J}$.

Basic properties of product ideals

Lemma

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. Then:

1. $\mathcal{I}\mathcal{J} = \{\sum_{i=1}^{k} a_i b_i : k \geq 0,\ a_i \in \mathcal{I},\ b_i \in \mathcal{J}\}$.
2. If R is commutative, $\mathcal{I} = (S)$, and $\mathcal{J} = (T)$, then $\mathcal{I}\mathcal{J} = (\{ab : a \in S,\ b \in T\})$.

Notes:

- Another way to say (1) is that $\mathcal{I}\mathcal{J}$ 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 $rxs = \sum_{i=1}^{k}(ra_i)(b_i s) \in K$ since $ra_i \in \mathcal{I}$ and $b_i s \in \mathcal{J}$.

   So K is an ideal. Since K contains the generating set for $\mathcal{I}\mathcal{J}$ (take $k = 1$) and is contained in $\mathcal{I}\mathcal{J}$, we must have $\mathcal{I}\mathcal{J} = K$.

2. Clearly RHS $\subseteq \mathcal{J}$, so we need to show the other inclusion.

   Suppose $x \in \mathcal{I}$ and $y \in \mathcal{J}$. Then $x = \sum a_i s_i$ for $a_i \in R$ and $s_i \in S$, and $y = \sum b_i t_i$ for $b_i \in R$ and $t_i \in T$. So $xy = \sum_{i,j} a_i b_j s_i t_j \in$ RHS. Since RHS contains generators for $\mathcal{I}\mathcal{J}$, it contains $\mathcal{I}\mathcal{J}$.

□

Products and intersections

Lemma

Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in a ring R. Then $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.

Proof.

If $a \in \mathcal{I}$ and $b \in \mathcal{J}$, then $ab \in \mathcal{I} \cap \mathcal{J}$, so $\mathcal{I} \cap \mathcal{J}$ contains a generating set for $\mathcal{I}\mathcal{J}$. Since $\mathcal{I} \cap \mathcal{J}$ is an ideal, $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$. □

Example

Consider $\mathcal{I} = (xy)$ and $\mathcal{J} = (yz)$ in $R[x, y, z]$ where R is commutative. Then $\mathcal{I}\mathcal{J} = (xy^2z)$, but $xyz \in \mathcal{I} \cap \mathcal{J}$. So here, $\mathcal{I}\mathcal{J} \neq \mathcal{I} \cap \mathcal{J}$.

Example

Suppose $\mathcal{I} = (x)$ and $\mathcal{J} = (y)$ in $\mathbb{Z}[x, y]$.

$f \in \mathcal{I}$ (respectively $\mathcal{J}$) if and only if every monomial of f contains a positive power of x (respectively 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 $\mathcal{I} \cap \mathcal{J} = (xy) = \mathcal{I}\mathcal{J}$.

Soon, we'll see a sufficient condition for $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$.

From group theory: Chinese remainder theorem

If $m, n \geq 0$ and $\gcd(m,n) = 1$, 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 $0 \leq a < m$ and $0 \leq b < n$, there is a unique $0 \leq x < mn$ such that x is the solution to

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

Is there a connection to ring theory?

Connections with rings?

Group theory: if $\gcd(m,n) = 1$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

What about ring theory?

Well, $\gcd(m,n) = 1$ if and only if $\operatorname{lcm}(m,n) = mn$, where $\operatorname{lcm}(m,n)$ is the **least common multiple** of m and n: the smallest integer $k \geq 0$ where $k = xm = yn$ for some $x, y \in \mathbb{Z}$.

Lemma

$\operatorname{lcm}(m,n) = k$, where $k \geq 0$ and $(m) \cap (n) = (k)$.

Proof.

$k = xm = yn$ 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 $\mathcal{I}$. □

We can restate the CRT: if $(m)(n) = (m) \cap (n)$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Generalizing the Chinese remainder theorem

Lemma

If R, S, T are rings and $\phi\colon R \to S$ and $\psi\colon R \to T$ are homomorphisms, then

$$\phi \times \psi\colon R \to S \times T : r \mapsto (\phi(r), \psi(r))$$

is a homomorphism.

Proof.

Exercise. □

Notice $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : x \mapsto (x, x)$ is the product $q_1 \times q_2$, where $q_1\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and $q_2\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ are the quotient maps. So this is a ring isomorphism as well.

Now let $\mathcal{I}, \mathcal{J}$ be ideals in some ring 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

If $\mathcal{I}, \mathcal{J}$ are ideals in a ring R, and $\phi = q_1 \times q_2\colon R \to R/\mathcal{I} \times R/\mathcal{J}$ where $q_1\colon R \to R/\mathcal{I}$ and $q_2\colon R \to R/\mathcal{J}$ are the quotient maps, then $\ker \phi = \mathcal{I} \cap \mathcal{J}$.
As a result, there is a homomorphism $\psi\colon R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ such that $\psi(\overline{x}) = (q_1(x), q_2(x))$ and $\ker \psi = \mathcal{I} \cap \mathcal{J}/\mathcal{I}\mathcal{J}$.

Proof.

First, $x \in \ker \phi \iff (q_1(x), q_2(x)) = (0, 0) \iff x \in \ker q_1 \cap \ker q_2 = \mathcal{I} \cap \mathcal{J}$.

Next, note $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J} = \ker \phi$. By the universal property of quotient rings, there is a homomorphism $\psi\colon R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ 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 $\psi(\overline{x}) = 0 \iff \phi(x) = 0$. □

Let $\mathcal{I}, \mathcal{J}$ be ideals in R. Is $\phi\colon R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J} : \overline{r} \mapsto (\overline{r}, \overline{r})$ a ring isomorphism?

By the lemma, ϕ is injective if and only if $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$. Is injectivity sufficient to prove surjectivity?

Example

Let $R = \mathbb{Z}$, $\mathcal{I} = (m)$, and $\mathcal{J} = (n)$.

Then $|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$.

By the pigeonhole principle, ϕ is surjective if and only if ϕ is injective. We can conclude the following are equivalent:

1. ϕ is a group isomorphism.
2. ϕ is a ring isomorphism.
3. $(m) \cap (n) = (mn)$, i.e., $\operatorname{lcm}(m, n) = mn$, i.e., $\gcd(m, n) = 1$.

Note this is actually slightly stronger than the stated CRT.

Example

Consider $(2), (x)$ in $\mathbb{Z}[x]$. Exercise: $(2) \cap (x) = (2x)$.

Is $\phi\colon \mathbb{Z}[x]/(2x) \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x) : \overline{p} \mapsto (\overline{p}, \overline{p})$ 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.

We need some more work to fully generalize CRT.

Comaximal ideals

Recall $\gcd(m, n) = 1 \iff xm + yn = 1$ for some $x, y \in \mathbb{Z}$.

(We used this fact to prove the group theory version of the CRT.)

Can we build off of this idea, rather than the connection with lcm?

Note $a = xm$ for $x \in \mathbb{Z}$ if and only if $a \in (m)$, and similarly $b = yn$ for $y \in \mathbb{Z}$ if and only if $b \in (n)$.

Lemma

$\gcd(m, n) = 1$ if and only if $(m) + (n) = \mathbb{Z}$.

Proof.

We know $(m) + (n)$ is an ideal, so $(m) + (n) = \mathbb{Z}$ if and only if $1 \in (m) + (n)$, which happens if and only if $1 = xm + yn$ for some $x, y \in \mathbb{Z}$. □

Definition — comaximal ideals

Two ideals $\mathcal{I}$ and $\mathcal{J}$ in a ring R are **comaximal** (or **coprime**) if $\mathcal{I} + \mathcal{J} = R$, or equivalently if $1 \in \mathcal{I} + \mathcal{J}$.

This is actually enough to generalize the CRT.

Theorem — Generalized Chinese remainder theorem

If $\mathcal{I}, \mathcal{J}$ are comaximal in a commutative ring R, then $\phi\colon R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ is an isomorphism.

Proof.

Suppose $a \in \mathcal{I}$ and $b \in \mathcal{J}$ such that $a + b = 1$.

ϕ is surjective: If $r \in R$, then $ra + rb = r$, so $r - rb = ra \in \mathcal{I}$ and $r - ra = rb \in \mathcal{J}$. So $\overline{r} = \overline{rb}$ in $R/\mathcal{I}$ and $\overline{r} = \overline{ra}$ in $R/\mathcal{J}$. But $\overline{rb} = 0$ in $R/\mathcal{J}$ and $\overline{ra} = 0$ in $R/\mathcal{I}$. So for all $r_1, r_2 \in R$, we see $\phi(\overline{r_1 b + r_2 a}) = (\overline{r_1}, \overline{r_2})$ in $R/\mathcal{I} \times R/\mathcal{J}$.

ϕ is injective: Need to show $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$. Suppose $x \in \mathcal{I} \cap \mathcal{J}$. Then $x = xa + xb \in \mathcal{I}\mathcal{J}$. So $\mathcal{I} \cap \mathcal{J} \subseteq \mathcal{I}\mathcal{J}$. We already know $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$, so $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$. □

Continuing the decomposition

If $n = p_1^{a_1} \cdots p_k^{a_k}$ where $p_1, \ldots, p_k$ are distinct primes, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \mathbb{Z}/p_2^{a_2} \cdots p_k^{a_k}\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$.

Why? Because $p_1^{a_1}$ is coprime to $p_2^{a_2} \cdots p_k^{a_k}$.

In $\mathbb{Z}$, if a is coprime to b and coprime to c, then a is coprime to bc.

Lemma

If $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{K}$ are ideals of R such that $\mathcal{I}, \mathcal{J}$ and $\mathcal{I}, \mathcal{K}$ are comaximal, then $\mathcal{I}$ and $\mathcal{J}\mathcal{K}$ are comaximal.

Proof.

Suppose $a + b = 1 = a' + c$ where $a, a' \in \mathcal{I}$, $b \in \mathcal{J}$, and $c \in \mathcal{K}$. Then $b = ba' + bc$, so $1 = a + b = (a + ba') + bc \in \mathcal{I} + \mathcal{J}\mathcal{K}$. □

We can generalize the CRT even further.

Theorem — Generalized CRT, extended version

Suppose $\mathcal{I}_1, \ldots, \mathcal{I}_k$ are pairwise comaximal ideals of a commutative ring R for $k \geq 2$. Then there is an isomorphism $\phi\colon R/\mathcal{I}_1 \cdots \mathcal{I}_k \to R/\mathcal{I}_1 \times \cdots \times R/\mathcal{I}_k$ defined by $\phi(\overline{r}) = (\overline{r}, \ldots, \overline{r})$.

Proof.

By induction on k. We've already done the base case $k = 2$.

If $k > 2$, by induction be get an isomorphism $R/\mathcal{I}_2 \cdots \mathcal{I}_k \to R/\mathcal{I}_2 \times \cdots \times R/\mathcal{I}_k : \overline{r} \mapsto (\overline{r}, \ldots, \overline{r})$. By lemma, $\mathcal{I}_1$ and $\mathcal{I}_2 \cdots \mathcal{I}_k$ are comaximal. So $R/\mathcal{I}_1 \cdots \mathcal{I}_k \to R/\mathcal{I}_1 \times R/\mathcal{I}_2 \cdots R/\mathcal{I}_k : \overline{r} \mapsto (\overline{r}, \overline{r})$ is an isomorphism.

Exercise: compose these steps to get the desired isomorphism. □

End notes

Question: Why not go straight from CRT to generalized CRT? (That is, why did we bother looking at the other ring-theoretic approaches that didn't work?)

Answer: There are some applications of generalized CRT (especially to polynomials), but the generalized CRT doesn't come up as much as we might expect in ring theory.

The important takeaway from this section is that it's interesting to look for "decompositions" of a ring R.

Week 11: PIDs and UFDs

26: Principal ideal domains (PIDs)

Division in a ring

Definition — division

Let x and y be elements of a commutative ring R. We say that x **divides** y if $y = xr$ for some $r \in R$, or equivalent if $y \in Rx$. Notation: $x \mid y$.

Example

- In $\mathbb{Z}$, $12 = 3 \cdot 4$, so $3 \mid 12$; meanwhile $5 \nmid 12$.
- $12 = (-3) \cdot (-4)$, so also $-3 \mid 12$.
- $x - 1$ divides $x^2 - 1$ in $\mathbb{Z}[x]$, since $x^2 - 1 = (x-1)(x+1)$.

Basic properties:

- If $x \mid y$, then $x \mid yz$ for all $z \in R$.
- Every $x \in R$ divides 0, since $x \cdot 0 = 0$. Caution: "divides 0" is not the same as "zero divisor".
- $u \mid 1$ if and only if $u \in R^\times$. More generally, if $u \in R^\times$, then $x = u(u^{-1}x)$, so $u \mid x$ for all $x \in R$.
- $x = x \cdot 1$, so $x \mid x$ for all $x \in R$.
- Suppose $x, y \in R$ and $u \in R^\times$. If $x \mid y$, then $y = rx = ru^{-1}(ux)$, so $ux \mid y$. In particular, $ux \mid x$ and $x = u^{-1}(ux) \mid ux$ for all units $u \in R^\times$.

Definition — associates

Two elements x and y of a commutative ring R are **associates** if $y = ux$ for some $u \in R^\times$. We write $x \sim y$.

Lemma

Suppose R is a commutative ring. Then:

1. $\sim$ is an equivalence relation.
2. If $x_1 \sim x_2$ and $y_1 \sim y_2$, then $x_1 \mid y_1 \iff x_2 \mid y_2$.
3. If $x \sim y$, then $x \mid y$ and $y \mid x$.

Proof.

1. (Exercise) Key idea: if $y = ux$, then $x = u^{-1}y$.
2. (Exercise) Key idea: $x_1 \mid y_1 \implies x_2 \mid y_2$ from earlier observations.
3. (Exercise) From previous observations.

□

When do x and y mutual divide?

Lemma

If R is a commutative ring, then $x \mid y$ and $y \mid x$ if and only if $(x) = (y)$.

Proof.

Follows from the fact that $x \mid y \iff y \in (x) \iff (y) \subseteq (x)$. □

Lemma

If R is a domain, then for all $x, y \in R$, $x \sim y$ if and only if $x \mid y$ and $y \mid x$.

Proof.

We already know that if $x \sim y$, then $x \mid y$ and $y \mid x$.

Suppose $y = xr$ and $x = yt$ for $r, t \in R$. If $y = 0$, then $x = 0$, so $x \sim y$. Then suppose $y \neq 0$. We have $y = xr = yrt$ so $(1-rt)y = 0$, but $y \neq 0$ and R is a domain, so $1-rt = 0$ and hence $r, t \in R^\times$. □

Common divisors

Definition — common divisor, greatest common divisor

Let R be a commutative ring and $a, b \in R$. An element $d \in R$ is a **common divisor** of a and b if $d \mid a$ and $d \mid b$.

A common divisor d is a **greatest common divisor** if for all common divisors $d' \in R$ of a and b, we have $d' \mid d$.

We write $d = \gcd(x, y)$ to say d is a greatest common divisor of x and y. (Caution: this definition does not say $\gcd(x, y)$ exists, is computable, or even unique.)

Lemma

Let $d, a, b \in R$ where R is a commutative ring. Then the following are equivalent:

1. $d \mid a$ and $d \mid b$.
2. $d \mid xa + yb$ for all $x, y \in R$.
3. $(a, b) \subseteq (d)$.

Proof.

(1) $\implies$ (2): if $a = dr$ and $b = dt$, then $xa + yb = (xr + yt)d$.

(2) $\implies$ (1): set $x = 1$ and $y = 0$, and vice versa.

(3) $\iff$ (2): every element of (a, b) is of the form $xa + yb$, and $d \mid xa + yb$ if and only if $xa + yb \in (d)$. □

Basic properties of greatest common divisors:

- If a and b have 0 as a common divisor, then $a = b = 0$, so $0 = \gcd(a, b)$ if and only if $a = b = 0$.
- Every common divisor of $x \in R$ and $u \in R^\times$ is a unit. Since units divide every element, $v = \gcd(x, u)$ for all $v \in R^\times$.
- If d, d' are both greatest common divisors of $x, y \in R$, then $d \mid d'$ and $d' \mid d$. Hence if R is a domain, $d \sim d'$.

  Meanwhile, in any ring R: if $d = \gcd(x, y)$ and $d \sim d'$, then $d' = \gcd(x, y)$.

  We say that greatest common divisors in integral domains are **unique up to units**. For example: $3 = \gcd(12, 9)$ and $-3 = \gcd(12, 9)$.

Existence of greatest common divisors

Proposition

Let $a, b \in R$ where R is a commutative ring. Then a and b have a greatest common divisor if and only if there is a principal ideal $\mathcal{I}$ such that

1. $(a, b) \subseteq \mathcal{I}$, and
2. if $\mathcal{J} \subseteq R$ is a principal ideal containing (a, b), then $\mathcal{I} \subseteq \mathcal{J}$.

If $\mathcal{I}$ exists then it is unique, and $\mathcal{I} = (d) \iff d = \gcd(a, b)$.

Proof.

Since d' is a common divisor of a and b if and only if $(a, b) \subseteq (d')$, and $d = \gcd(a, b)$ if and only if $\mathcal{I} := (d)$ satisfies (1) and (2).

If $\mathcal{I}$ and $\mathcal{I}'$ are principal ideals satisfying (1) and (2), then $\mathcal{I} \subseteq \mathcal{I}'$ and $\mathcal{I}' \subseteq \mathcal{I}$, so $\mathcal{I} = \mathcal{I}'$. Combining uniqueness with the first observation, we see $\mathcal{I} = (d) \iff d = \gcd(a, b)$. □

Corollary

Let $a, b \in R$ where R is a commutative ring. If (a, b) is a principal ideal, then a greatest common divisor of a and b exists. As a result, if d is a common divisor of a and b such that $d = xa + yb$ for some $x, y \in R$, then $d = \gcd(a, b)$.

Proof.

If $(a, b) = (d)$, then $\mathcal{I} = (d)$ satisfies (1) and (2) of the proposition. If d is a common divisor of a and b, then $(a, b) \subseteq (d)$, and if $d = xa + yb$, then $d \in (a, b)$, so $(d) = (a, b)$. □

In $\mathbb{Z}$, every ideal is principal, so greatest common divisors always exist.

Corollary

Let $a, b \in R$ where R is a commutative ring, and suppose (a) and (b) are comaximal. Then $1 = \gcd(a, b)$.

Proof.

$(a) + (b) = (1)$. □

Example

In $\mathbb{Z}$, $d = \gcd(a,b) \iff (d) = (a,b)$.

For instance, $(9,12) = (3)$.

Example

In $\mathbb{Z}[x]$, (x^2+1) and (x^2) are comaximal, so $1 = \gcd(x^2, x^2+1)$.

On the other hand, $(2,x)$ is not principal in $\mathbb{Z}[x]$, so we can't use this method to find $\gcd(2,x)$. Does $\gcd(2,x)$ exist?

We showed that the only principal ideal containing $(2,x)$ is (1), so $1 = \gcd(2,x)$, even though (2) and (x) are not comaximal.

Different argument: 2 and x don't factor, so we should treat the like distinct primes. That is, they should be "coprime".

We'll explore this argument in this week and the next.

Principal ideal domains

Recall: since all ideals of $\mathbb{Z}$ are principal, there is a greatest common divisor of every $a, b \in \mathbb{Z}$.

Definition — principal ideal domain (PID)

A ring R is a **principal ideal domain (PID)** if

- R is an integral domain, and
- every ideal of R is principal.

Example

- $\mathbb{Z}$ is a principal ideal domain.
- Later: if $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is a principal ideal domain.
- $\mathbb{Z}[x]$ is not a PID, since $(2, x)$ is not principal.
- $\mathbb{K}[x, y]$ is not a principal ideal domain even if $\mathbb{K}$ is a field, since (x, y) is not principal.

Proposition

If R is a PID, then every pair of elements $a, b \in R$ has a greatest common divisor. Also, $d = \gcd(a, b)$ if and only if d is a common divisor of a and b and $d = xa + yb$ for some $x, y \in R$.

Proof.

Easy application of last corollary. □

Recall that maximal ideals are prime. In $\mathbb{Z}$, an ideal $n\mathbb{Z}$ is maximal if and only if n is prime. ~~Since $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime, $n\mathbb{Z}$ is prime if and only if n is prime.~~

Correction!
$\mathbb{Z}/n\mathbb{Z}$ is also an integral domain if $n = 0$. So $n\mathbb{Z}$ is prime if and only if n is prime or zero.

Proposition

If R is a PID, then every non-zero prime ideal of R is maximal.

Proof.

Suppose $\mathcal{I}$ is a non-zero prime ideal in R. Let $\mathcal{J}$ be a proper ideal of R containing $\mathcal{I}$.

Because R is a PID, $\mathcal{I} = (a)$ and $\mathcal{J} = (b)$ for some $a, b \in R$. Since $\mathcal{I} \subseteq \mathcal{J}$, $a = br$ for some $r \in R$.

Since $\mathcal{I}$ is prime and $br \in \mathcal{I}$, one of b or r is in $\mathcal{I}$. Suppose for contradiction $b \notin \mathcal{I}$, so $r \in \mathcal{I}$.

Then $(r) \subseteq (a)$, and since $a = br \in (r)$, we have $(a) = (r)$. Since R is a domain, a and r are associates. This means $a = ur$ for some $u \in R^{\times}$. So $br = a = ur \implies (b - u)r = 0$. Since $\mathcal{I} = (r)$ is non-zero, $r \neq 0$, so $b = u$. But then $1 \in \mathcal{J}$, a contradiction.

So $b \in \mathcal{I}$ and hence $\mathcal{J} \subseteq \mathcal{I}$. So $\mathcal{I}$ is maximal. □

Later, we'll see that if $\mathbb{K}$ is a field then $\mathbb{K}[x]$ is a PID. The converse is also true:

Corollary

Suppose R is a commutative ring such that $R[x]$ is a PID. Then R is a field.

Proof.

If $R[x]$ is a PID, then it is a domain. As a subring of $R[x]$, R must also be a domain. Since $R \cong R[x]/(x)$, (x) is prime. But then (x) is maximal, so R is a field. □

Euclidean domains

Why is every ideal of $\mathbb{Z}$ principal?

Streamlined (ring theory) answer:

- Suppose $\mathcal{I}$ is a non-zero ideal of $\mathbb{Z}$.
- Let n be the smallest positive integer of $\mathcal{I}$ (so $n\mathbb{Z} \subseteq \mathcal{I}$).
- If $x \in \mathcal{I}$, then $x = qn + r$ where $0 \leq r < n$.
- $r = x - qn \in \mathcal{I}$, so $r = 0$ by assumption on n.
- Therefore $x \in n\mathbb{Z}$ for all $x \in \mathcal{I}$, so $\mathcal{I} \subseteq n\mathbb{Z}$.

This argument relies on being able to divide in $\mathbb{Z}$ (writing $x = qn + r$).

What would it mean to do division in an arbitrary ring? Given $n, x \in R$, maybe we can find $q, r \in R$ such that $x = qn + r$, but then taking $q = 0$ and $r = x$ gives a trivial result.

We want to somehow have $|r| < |n|$, but we don't necessarily have an order on R.

Definition — Euclidean domain

A domain R is a **Euclidean domain** if there is a function $N \colon R \to \mathbb{N} \cup \{0\}$ such that

- $N(0) = 0$, and
- for all $x, y \in R$ with $x \neq 0$, there are $q, r \in R$ where $y = qx + r$ with $r = 0$ or $N(r) < N(x)$.

N is called a **norm**.

Sometimes a Euclidean domain is called a **domain with a division algorithm** (cf. Euclidean algorithm).

Example

$\mathbb{Z}$ is a Euclidean domain with norm $N(x) = |x|$. (If $x < 0$, then $y = q|x| + r = (-q)x + r$ where $0 \leq r < |x|$.)

We'll see it's possible to have norms with $N(x) = 0$, but $x \neq 0$. However, if $N(x) = 0$, then $1 = qx + r$ with $r = 0$ ~~or $N(r) < N(x)$~~. So $x \mid 1$ and hence x is a unit.

Proposition

Any Euclidean domain R is a PID.

Proof.

Suppose $\mathcal{I}$ is an ideal in R.

If $\mathcal{I}$ is zero, then it is principal, so suppose $\mathcal{I} \neq (0)$.

Let $k = \min\{N(x) : x \in \mathcal{I},\ x \neq 0\}$. Let $x \in \mathcal{I}$ such that $N(x) = k$. Suppose $y \in \mathcal{I}$. Then $y = qx + r$ for $q, r \in R$ with $r = 0$ or $N(r) < N(x)$.

Since $r = y - qx \in \mathcal{I}$, we can't have $N(r) < N(x)$, so $r = 0$. Thus $y \in (x)$, so $\mathcal{I} \subseteq (x)$. We see readily $(x) \subseteq \mathcal{I}$ as well. □

Now for polynomial rings.

Proposition

If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is a Euclidean domain.

Proof.

Define $N\colon \mathbb{K}[x] \to \mathbb{N} \cup \{0\}$ by $N(p) = \deg(p)$ if $p \neq 0$, and $N(0) = 0$. Suppose $y, p \in \mathbb{K}[x]$ with $p \neq 0$. If $\deg(p) = 0$, then p is a unit, so $y = qp + 0$ for some $q \in \mathbb{K}[x]$. If $\deg(p) > 0$, then we can divide y by p to get $y = qp + r$ for $q, r \in \mathbb{K}[x]$ with $\deg(r) < \deg(p)$. In both cases, we can get $y = qp + r$ with $q, r \in \mathbb{K}[x]$ such that $r = 0$ or $N(r) < N(p)$. □

Corollary

If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is a PID.

Polynomial division over a field

Suppose $y, p \in \mathbb{K}[x]$ with $\deg(p) \geq 1$.

Let $p = \sum_{i=0}^{n} a_i x^i$ with $a_n \neq 0$ and let $y = \sum_{j=0}^{m} b_j x^j$. We can divide y by p with the following procedure:

- Keep track of q, starting with $q = 0$.
- If $m < n$, return q and $r = y$.
- If $m \geq n$, then

$$y - \frac{b_m}{a_n} x^{m-n} p = 0x^m + \frac{a_n b_{m-1} - b_m a_{n-1}}{a_n} x^{m-1} + \cdots .$$

So replace q by $q + \frac{b_m}{a_n} x^{m-n}$ and y by $y - \frac{b_m}{a_n} x^{m-n} p$, and repeat.

Eventually we'll finish with q and r such that $y - qp = r$ and $\deg(r) < \deg(p)$.

Euclidean domains vs. PIDs

Every Euclidean domain is a PID.

Are there PIDs which are not Euclidean?

- Yes: famously $\mathbb{Z}[(1+\sqrt{-19})/2]$ (we won't prove this).

How do Euclidean domains functionally differ from PIDs?

- In PIDs, greatest common divisors always exist (but may not be easy to find).
- In Euclidean domains, we have an algorithm (the Euclidean algorithm) for computing greatest common divisors. This algorithm is nice because it is fast as long as division is fast.

27: Unique factorization domains (UFDs)

Primes and irreducibles

Prime numbers in $\mathbb{Z}$ have two equivalent definitions:

1. p is prime if $p \neq \pm 1, 0$ and whenever $p \mid ab$, one of $p \mid a$ or $p \mid b$ holds.
2. p is prime if $p \neq \pm 1$ and whenever $p = ab$, one of a or b is a unit.

In an arbitrary ring, prime ideals generalize definition (1).

But what if we want prime elements, rather than prime ideals? What about definition (2)?

Definition — prime, irreducible, reducible

Let R be a domain and let $p \in R$ with $p \neq 0$ and $p \notin R^\times$.

- p is **prime** if for all $a, b \in R$, if $p \mid ab$, then $p \mid a$ or $p \mid b$.
- p is **irreducible** if for all $a, b \in R$, if $p = ab$ then one of a or b is a unit.
- p is **reducible** if it is not irreducible.

Some basic properties:

Proposition

Let R be a domain.

1. $p \in R$ is prime if and only if $p \neq 0$ and (p) is a prime ideal.
2. If p_1 and p_2 are associates, then p_1 is prime (resp. irreducible) if and only if p_2 is prime (resp. irreducible).
3. If p is prime, then p is irreducible.

Proof.

1. Use fact that $p \mid m \iff m \in (p)$.
2. Exercise.
3. Suppose p is prime and let $p = ab$. Then $p \mid ab$ so $p \mid a$ or $p \mid b$. Suppose $p \mid a$. Then $a = up$, and $0 = p - ab = p(1 - ub)$. Since R is a domain and $p \neq 0$, then $ub = 1$ so $b \in R^\times$.

□

Primes are irreducibles, but is the converse true? Yes, in PIDs.

Proposition

Let p be an irreducible in a PID R. Then p is prime.

Proof.

Suppose $\mathcal{I}$ is an ideal of R containing (p). Since R is a PID, $\mathcal{I} = (q)$ for some $q \in R$. Since $p \in \mathcal{I}$, $p = kq$ for some $k \in R$. Since p is irreducible, either k or q is a unit. If q is a unit, then $\mathcal{I} = R$. If k is a unit, then p and q are associates, so $(p) = (q)$. Thus (p) is maximal and hence prime. Since $p \neq 0$ by definition, p is prime. □

What about general domains? We'll get there later.

Complete factorizations

Let's consider another question first. In $\mathbb{Z}$, every number is a product of primes.

Is every element of a domain R a product of irreducibles?

Definition — complete factorization

Let R be a domain. Say that $r \in R$ has a **complete factorization into irreducibles** if and only if $r = r_1 \cdots r_k$ where $k \geq 1$ and $r_1, \ldots, r_k$ are irreducible.

Say that R has **complete factorizations (into irreducibles)** if every $r \in R \backslash (R^\times \cup \{0\})$ has a complete factorization into irreducibles.

Side question: should we use irreducibles or primes in this definition? We define **complete factorizations into primes** similarly.

If R has complete factorizations into primes, then R has complete factorizations into irreducibles (since primes are irreducible).

So having complete factorizations into primes is (potentially) stronger than having complete factorizations into irreducibles. Could these be equivalent?

Lemma

If $r \in R$ is irreducible and a product of primes, then r is prime.

Proof.

Suppose $r = p_1 \cdots p_k$ is irreducible and $p_1, \ldots, p_k$ are prime. If r is irreducible and $k \geq 2$, then either $p_1 \cdots p_{k-1}$ or p_k is a unit. If $p_1 \cdots p_{k-1}$ is a unit, then p_i divides 1 for all i, so p_i is a unit. Since primes can't be units, this is a contradiction. So $k = 1$ and hence r is prime. □

Corollary

If R has complete factorizations into irreducibles, then R has complete factorizations into primes if and only if every irreducible in R is prime.

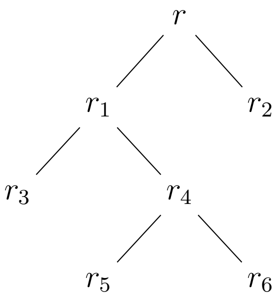
Since we don't know whether irreducibles are always prime yet, we'll use the weaker condition (into irreducibles).

A procedure for factoring

Let $r \in R$ where R is a domain, $r \neq 0$, and $r \notin R^\times$. Let's try to show that r factors into a product of irreducibles.

1. If r is irreducible, we're done.
2. Otherwise $r = r_1 r_2$ where r_1, r_2 are not units.
3. Start over at step 1 and try to write r_1 and r_2 as products of irreducibles.
4. If this is possible, we can write r as a product of irreducibles.

In this example, $r = r_3 r_5 r_6 r_2$.



Does this always terminate? If even one branch keeps growing, the process won't terminate.

Lemma

Let $r = r_1 r_2 \in R$ where R is a domain, so $(r) \subseteq (r_2)$. If $r \neq 0$, then $(r) = (r_2)$ if and only if r_1 is a unit.

Proof.

$(r) = (r_2)$ if and only if r and r_2 are associates. So if r_1 is a unit then $(r) = (r_2)$.

Conversely, if $(r) = (r_2)$, then $r = ur_2$ for u a unit, so $(r_1 - u)r_2 = 0$. Since $r \neq 0$, we have $r_2 \neq 0$, hence $r_1 = u$ is a unit. □

So if r is reducible, then $r = r_1 r_2$ where $(r) \subsetneq (r_1)$ and $(r) \subsetneq (r_2)$. If the procedure continues infinitely, we get an infinite strictly increasing sequence of principal ideals $\mathcal{I}_1 = (r_1) \subsetneq \mathcal{I}_2 = (r_2) \subsetneq \mathcal{I}_3 \subsetneq \cdots$ in R.

Definition — acending chain condition for principal ideals

A ring R satisfies the **ascending chain condition for principal ideals** if there is no infinite strictly increasing sequence $\mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \cdots$ of principal ideals in R.

Equivalently, if $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots$ is an infinite chain of principal ideals, eventually there is k such that $\mathcal{I}_n = \mathcal{I}_k$ for all $n \geq k$.

R satisfies the ascending chain condition for principal ideals if and only if the procedure always terminates. This proves:

Proposition

If R satisfies the ascending chain condition for principal ideals, then R has complete factorizations into irreducibles.

Note: there is an "ascending chain condition for ideals" that is also very important in commutative ring theory.

Proposition

If R is a PID, then R satisfies the ascending chain condition for principal ideals.

Proof.

Suppose $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots$ is an increasing sequence of ideals. Then $\mathcal{I} := \bigcup \mathcal{I}_i$ is an ideal. Since R is a PID, $\mathcal{I} = (x)$ for some $x \in R$. Since $x \in \mathcal{I}$, $x \in \mathcal{I}_k$ for some k. But then $\mathcal{I}_k \subseteq \mathcal{I}_n \subseteq \mathcal{I} = (x) \subseteq \mathcal{I}_k$ for all $n \geq k$, so $\mathcal{I}_n = \mathcal{I}_k$ for all $n \geq k$. □

What about rings which do not satisfy the ascending chain condition for principal ideals?

Example

Let $\mathbb{K}$ be a field, and let $R = \mathbb{K}[x_1, x_2, \ldots]$ denote the infinite polynomial ring in variables $x_1, x_2, \ldots$.

Elements of this ring belong to $R_n := \mathbb{K}[x_1, \ldots, x_n]$ for some n, so we can think of R as $\bigcup_{n\geq 1} R_n$. (Technically, we say R is the direct limit of rings R_n.)

Let $\mathcal{I} = (x_1 - x_2^2, x_2 - x_3^2, x_3 - x_4^2, \ldots)$. Then in $R/\mathcal{I}$, we have $x_1 = x_2^2$, $x_2 = x_3^2$, and so on, so $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ (details omitted).

Thus $R/\mathcal{I}$ does not satisfy the ascending chain condition.

In the homework, you'll do a more elementary example.

Unique factorizations

In $\mathbb{Z}$, not only can we write every element as a product of irreducibles, but factorizations are unique.

We'll explore the question of uniqueness before considering complete factorizations.

Definition — uniqueness of complete factorizations

Let R be a domain. We say **complete factorizations are unique when they exist** if for every pair of sequences of irreducibles $f_1, \dots, f_n$ and $g_1, \dots, g_m$ in R where $n, m \geq 1$ and $f_1 \cdots f_n = g_1 \cdots g_m$, we have that

1. $n = m$, and
2. there is $\sigma \in S_n$ such that $f_i \sim g_{\sigma(i)}$ for all $1 \leq i \leq n$.

Example

Complete factorizations in $\mathbb{Z}$ are unique when they exist. For example, $12 = 2 \cdot 3 \cdot 2 = (-2) \cdot 2 \cdot (-3)$.

Note: we don't say anything about when $n = 0$ or $m = 0$, because:

Lemma

If $f_1, \dots, f_n$ are irreducibles in a domain R with $n \geq 1$, then $f_1 \cdots f_n \notin R^\times$.

Proof.

If $f_1 \cdots f_n = u \in R^\times$, then $u^{-1} f_1 \cdots f_n = 1$ so $f_i \mid 1$ so $f_i \in R^\times$, a contradiction. □

What domains satisfy this condition?

Proposition

Let R be a domain such that every irreducible in R is prime. Then complete factorizations are unique when they exist.

In particular, PIDs have unique factorizations.

Proof.

Similar to uniqueness of prime factorizations in $\mathbb{Z}$.

Exercise: if p is prime and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$ (use induction).

Proposition follows from this claim: if $1 \leq n \leq m$ and $f_1, \ldots, f_n, g_1, \ldots, g_m \in R$ are irreducibles such that $f_1 \cdots f_n = g_1 \cdots g_m$, then

- $n = m$, and
- there is $\sigma \in S_n$ such that $f_i \sim g_{\sigma(i)}$ for all $1 \leq i \leq n$.

Proof of claim is by induction on n.

Base case ($n = 1$): since $f_1 = g_1 \cdots g_m$, we know $f_1 \mid g_i$ for some $1 \leq i \leq m$. So $g_i = uf_1$. Since f_1 is not a unit and g_i is irreducible, u is a unit.

Now let $r = g_1 \cdots g_{i-1} g_{i+1} \cdots g_m$, so $f_1 = f_1 ur$. Then $f_1(1 - ur) = 0$, so $r \in R^\times$. Hence $m = 1 = n$ by the lemma, so $r = u = 1$ and $f_1 = g_1$.

Inductive case: suppose we have $f_1, \ldots, f_n, g_1, \ldots, g_m$ as in the claim, where $n \geq 2$ and the claim holds for smaller n.

Since $f_1 \cdots f_n = g_1 \cdots g_m$, we have $f_1 \mid g_1 \cdots g_m$ and hence $f_1 \mid g_i$ for some $1 \leq i \leq m$. Then $g_i = uf_1$ where u is a unit.

Since $m \geq n \geq 2$, pick $1 \leq j \leq m$ such that $j \neq i$. Define $\tilde{g}_j := ug_j$ and $\tilde{g}_k := g_k$ for $k \neq j$, so that $f_1 \cdots f_n = f_1 \tilde{g}_1 \cdots \tilde{g}_{i-1} \tilde{g}_{i+1} \cdots \tilde{g}_m$.

Since R is a domain, $f_2 \cdots f_n = \tilde{g}_1 \cdots \tilde{g}_{i-1} \tilde{g}_{i+1} \cdots \tilde{g}_m$ by cancellation. Since the $f_k, \tilde{g}_\ell$ are irreducibles, by induction we get $n - 1 = m = 1$ and a bijection $\tilde{\sigma} \colon \{2, \ldots, n\} \to \{1, \ldots, n\} \setminus \{i\}$ such that $f_k \sim \tilde{g}_{\tilde{\sigma}(k)}$ for $2 \leq k \leq n$.

Finally define $\sigma \in S_n$ by $\sigma(1) = i$ and $\sigma(k) = \tilde{\sigma}(k)$ for $2 \leq k \leq n$. Then $n = m$ and $f_k \sim g_{\sigma(k)}$ for all $1 \leq k \leq n$. □

Can we find domains which don't have unique factorizations?

Example

$R = \mathbb{Z}[x, y, z, w]/(xy - zw)$ is a domain (see why later).

Exercise (not easy): x, y, z, w are non-associated irreducibles in R.

But $xy = zw$ in R, so R does not have unique factorizations. Since factorizations in R are not unique when they exist, there are irreducibles in R which are not prime.

Indeed, we can show that x, y, z, w are not prime, since $R/(x) \cong \mathbb{Z}[x, y, z, w]/(xy - zw, x) \cong \mathbb{Z}[x, y, z, w]/(zw, x) \cong \mathbb{Z}[y, z, w]/(zw)$ which is not a domain.

Example

In $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$, we have $6 = 2 \cdot 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$. In the homework, you'll show $2, 3, (1 - i\sqrt{5}), (1 + i\sqrt{5})$ are irreducibles.

Unique factorization domains

Definition — unique factorization domain (UFD)

domain R is a **unique factorization domain (UFD)** if R has complete factorizations into irreducibles, and complete factorizations are unique when they exist.

In other words, R is a UFD if

- every $r \in R \setminus (R^\times \cup \{0\})$ is a product of irreducibles in R, and
- if $f_1, \ldots, f_n, g_1, \ldots, g_m$ for $n, m \geq 1$ are irreducibles in R such that $f_1 \cdots f_n = g_1 \cdots g_m$, then
  1. $n = m$, and
  2. there is $\sigma \in S_n$ such that $f_i \sim g_{\sigma(i)}$.

Idea: every non-zero non-unit element in R has a unique factorization into irreducibles (where unique is qualified as above).

Example: $\mathbb{Z}$ is a UFD (no surprise).

Examples of UFDs

We've shown:

- A domain with the ascending chain condition for principal ideals has complete factorizations.
- A domain where all irreducibles are prime has unique complete factorizations when they exist.
- Irreducibles in PIDs are prime, and all PIDs satisfy the ascending chain condition for principal ideals.

Corollary

PIDs are UFDs. In particular, Euclidean domains are UFDs.

Example

If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is a UFD.

For instance, $\mathbb{Q}(y)[x]$.

Domains which aren't UFDs

- We sketched out a proof that $R = \mathbb{Z}[x, y, z, w]/(xy - zw)$ does not have unique factorizations. So R is not a UFD.
- In the homework, you'll show $\mathbb{Z}[i\sqrt{5}]$ is not a UFD.
- The question of whether $\mathbb{Z}[i\sqrt{n}]$ is a UFD is interesting.

  For example, in the textbook it is shown that $\mathbb{Z}[i]$ is a Euclidean domain and hence a UFD. Homework: modify this proof to show that $\mathbb{Z}[i\sqrt{2}]$ is also a Euclidean domain.
- We also sketched a proof that $R = \mathbb{K}[x_1, x_2, \ldots]/(x_1 - x_2^2, x_2 - x_3^2, \ldots)$ does not satisfy the ascending chain condition for principal ideals.

  Is R a UFD? We need to clarify the relationship between UFDs, the ascending chain condition, and the condition that primes be irreducibles.

UFDs and the other conditions

Theorem

A domain R is a UFD if and only if R satisfies the ascending chain condition for principal ideals and every irreducible in R is prime.

So irreducibles in a UFD are prime.

Hence if R is a UFD and $x \notin R^\times \cup \{0\}$, we refer to the factorization of x into irreducibles as the **prime factorization** of x.

Example

$R = \mathbb{K}[x_1, x_2, \ldots]/(x_1 - x_2^2, x_2 - x_3^2, \ldots)$ does not satisfy the ascending chain condition for principal ideals.

Hence R is not a UFD.

Proof later.

What about multivariate polynomial rings like $\mathbb{Q}[x, y]$? Are these UFDs? In week 12, we'll see:

Theorem

If R is a UFD, then $R[x]$ is a UFD.

Note this property is shared by domains, but not PIDs: $\mathbb{Q}[x]$ is a PID (since $\mathbb{Q}$ is a field), but $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ is not a PID ((x, y) is not principal).

The theorem implies that rings like $\mathbb{Q}[x, y]$ and $\mathbb{Z}[x, y, z, w]$ are UFDs.

Example

Let $p = xy - zw \in \mathbb{Z}[x, y, z, w]$. Exercise: show p is irreducible (show highest x (or y or z or w) degree in any factor is 1, then use brute force).

Since $\mathbb{Z}[x, y, z, w]$ is a UFD, p is prime. So $\mathbb{Z}[x, y, z, w]/(p)$ is a domain.

Proving the main UFD theorem

Recall:

Theorem

A domain R is a UFD if and only if R satisfies the ascending chain condition for principal ideals and every irreducible in R is prime.

Recall that if R is a UFD and $x \in R^\times \cup \{0\}$, we refer to the factorization of x into irreducibles as the **prime factorization** of x.

We'll need this lemma to prove the theorem:

Lemma

Suppose R is a UFD and $a, b \in R$ are non-zero non-units. If $a \mid b$, then the number of factors in the prime factorization of a is at most the number of factors in the prime factorization of b, and equality holds if and only if $(a) = (b)$.

Proof.

If $ca = b$, we can write $a = p_1 \cdots p_m$, $b = q_1 \cdots q_n$, and $c = ug_1 \cdots g_\ell$ where p_i, q_j, g_k are irreducibles, $u \in R^\times$, and $m, n \geq 1$ and $\ell \geq 0$. (Letting $\ell \geq 0$ allows c to be a unit.)

Then $g_1 \cdots g_\ell (up_1) \cdots p_m = q_1 \cdots q_n$, so $m \leq m + \ell = n$ (since the factorization is unique). We previously showed that $(a) = (b)$ if and only if c is a unit. But c is a unit if and only if $\ell = 0$, which happens if and only if $m = n$. □

Proof of theorem.

We've already shown the reverse direction (satisfying the ascending chain condition for principal ideals implies complete factorizations into irreducibles, and if every irreducible is prime then factorizations are unique when they exist).

So assume R is a UFD.

Irreducibles in R are prime: Let $r \in R$ be irreducible and suppose $r \mid ab$, so $kr = ab$ for some $k, a, b \in R$. We want to show $r \mid a$ or $r \mid b$.

If $a = 0$, then $r \mid a$, so we can assume $a, b \neq 0$.

If $a \in R^\times$, then $a^{-1}kr = b$ so $r \mid b$; similar for if $b \in R^\times$. So we can assume $a, b \notin R^\times$.

Then $a = p_1 \cdots p_m$ and $b = q_1 \cdots q_n$ where $p_1, \ldots, p_m, q_1, \ldots, q_n$ are irreducibles. Let $k = ug_1 \cdots g_\ell$ where $\ell \geq 0$ and $g_1, \ldots, g_\ell$ are irreducibles, and $u \in R^\times$ (to include the case when $k \in R^\times$). Then $ug_1 \cdots g_\ell r = p_1 \cdots p_m q_1 \cdots q_n$. By uniqueness of factorizations,

ur (and hence r) is associated with some p_i or q_j.

So r divides some p_i or q_j, hence r divides a or b.

R satisfies the ascending chain condition for principal ideals: Suppose $(x_1) \subseteq (x_2) \subseteq \cdots \subseteq (x_i) \subseteq \cdots$ is an increasing chain of principal ideals. We want to show there is n such that $(x_k) = (x_n)$ for all $k \geq n$.

If $x_i = 0$ for all i, then we are done. If $x_n \neq 0$, then $x_k \neq 0$ for all $k \geq n$, so assume WLOG that $x_i \neq 0$ for all $i \geq 1$.

If $x_n \in R^\times$ for some n, then $R = (x_n)$ and hence $(x_k) = R = (x_n)$ for all $k \geq n$. So assume that $x_i \notin R^\times$ for all $i \geq 1$.

Let f_i be the number of factors in the prime factorization of x_i. Since $x_{i+1} \mid x_i$, the lemma implies that $f_i \geq f_{i+1}$. Since the sequence of integers $f_1, f_2, \ldots$ is bounded below by 1, there must be some n such that $f_k = f_n$ for all $k \geq n$. Again by the lemma, we get $(x_k) = (x_n)$ for all $k \geq n$. □

GCDs in UFDs

Suppose $p_1, \dots, p_n$ are distinct primes in $\mathbb{Z}$, and $x = p_1^{a_1} \cdots p_n^{a_n}$ and $y = p_1^{b_1} \cdots p_n^{b_n}$ for some $a_1, \dots, a_n, b_1, \dots, b_n \geq 0$. Then we know that $\gcd(x, y) = p_1^{c_1} \cdots p_n^{c_n}$ where $c_i = \min(a_i, b_i)$.

This works in a general UFD. To show this, we need to consider "formatting" prime factorizations.

So far, if R is a UFD and $x \in R \setminus \{0\}$, then we've written $x = ug_1 \cdots g_n$ where $u \in R^\times$, $n \geq 0$, and $g_1, \dots, g_n \in R$ are irreducibles.

What if $g_n \sim g_i$? Then $g_n = u' g_i$ for some $u' \in R^\times$, so we can instead write $x = (uu')g_1 \cdots g_{i-1} g_i^2 g_{i+1} \cdots g_{n-1}$. Repeating this, we can eventually write

$$x = ug_1^{a_1} \cdots g_n^{a_n}$$

where $u \in R^\times$, $a_1, \dots, a_n$ are positive integers, and (*) $g_1, \dots, g_n$ are irreducibles, $n \geq 0$, where $g_i \not\sim g_j$ for all $1 \leq i \neq j \leq n$.

Proposition

Let R be a UFD.

1. (Compact representation) If $0 \neq x \in R$, there are $u \in R^\times$, $g_1, \dots, g_n$ as in (*), and positive integers $a_1, \dots, a_n$ where $x = ug_1^{a_1} \cdots g_n^{a_n}$.
2. (Unique compact representation) If $u, v \in R^\times$, $a_1, \dots, a_n, b_1, \dots, b_n \geq 0$, and $g_1, \dots, g_n$ are as in (*) such that $ug_1^{a_1} \cdots g_n^{a_n} = vg_1^{b_1} \cdots g_n^{b_n}$, then $u = v$ and $a_i = b_i$.
3. (Division) If $x = ug_1^{a_1} \cdots g_n^{a_n}$ where $u \in R^\times$, $g_1, \dots, g_n$ are as in (*), and $a_1, \dots, a_n \geq 0$, then $y \mid x$ if and only if $y = vg_1^{b_1} \cdots g_n^{b_n}$ for $v \in R^\times$ and $0 \leq b_i \leq a_i$.
4. (Common primes) If $x, y \in R$ are non-zero, then there are $u, v \in R^\times$, $g_1, \dots, g_n$ as in (*), and $a_1, \dots, a_n, b_1, \dots, b_n \geq 0$ such that $x = ug_1^{a_1} \cdots g_n^{a_n}$ and $y = vg_1^{b_1} \cdots g_n^{b_n}$.

Proof.

1. Already done.
2. If $a_i > 0$, then g_i divides the RHS, so $b_i > 0$. Divide out g_i on both sides and repeat until $a_i \leq b_i$. By symmetry, $b_i \leq a_i$ so $a_i = b_i$. Hence $u = v$.

   Division in a domain: If R is a domain, and $a = kb = k'b$ for $b \neq 0$, then $(k - k')b = 0$ so $k = k'$. So if $b \mid a$ and $b \neq 0$, let $\frac{b}{a}$ denote the unique element $k \in R$ such that $a = kb$.

3. The reverse direction is clear, so suppose $y \mid x$. Write $y = vf_1 \cdots f_k$ where $v \in R^\times$,

$k \geq 0$, and $f_1, \ldots, f_k$ are irreducibles. Since $f_k \mid x$, we see $f_k \sim g_i$ for some i with $a_i > 0$. Let $f_k = v'g_i$ for some $v' \in R^\times$. Now $(vv')y/g_i \mid x/g_i$. Repeating this gives y as desired.

4. Exercise.

□

Now for the generalized formula for GCDs in a UFD.

Proposition

Suppose R is a UFD, $u, v \in R^\times$, $g_1, \ldots, g_n$ are primes in R such that $g_i \not\sim g_j$ for all $1 \leq i \neq j \leq n$, and $a_1, \ldots, a_n, b_1, \ldots, b_n$ are non-negative integers. Let $c_i = \min(a_i, b_i)$ for each i. Then

$$g_1^{c_1} \cdots g_n^{c_n} = \gcd(ug_1^{a_1} \cdots g_n^{a_n}, vg_1^{b_1} \ldots g_n^{b_n}).$$

Proof.

Let $d = g_1^{c_1} \cdots g_n^{c_n}$, $x = ug_1^{a_1} \cdots g_n^{a_n}$, and $y = vg_1^{b_1} \cdots g_n^{b_n}$. Clearly $d \mid x$ and $d \mid y$. Suppose $d' \mid x$ and $d' \mid y$ as well.

By part (3) of the proposition, $d' = wg_1^{d_1} \cdots g_n^{d_n}$ with $w \in R^\times$ and $d_i \leq a_i$ and $d' = w'g_1^{d_1'} \cdots g_n^{d_n'}$ with $w' \in R^\times$ and $d_i' \leq b_i$.

By part (2) of the proposition, $w = w'$ and $d_i = d_i'$ for all i, so $d_i \leq c_i$. Hence $d' \mid d$. So d is a greatest common divisor. □

In a UFD, greatest common divisors always exist.

Summary of greatest common divisors

- Euclidean domain:
  - $\gcd(a, b)$ always exists.
  - Can calculate $\gcd(a, b)$ from prime factorization.
  - There are $x, y \in R$ such that $\gcd(a, b) = xa + yb$.
  - Can calculate $\gcd(a, b)$ by Euclidean algorithm.

  Examples: $\mathbb{Z}$, $\mathbb{K}[x]$ for $\mathbb{K}$ a field.
- Principal ideal domain (PID):
  - $\gcd(a, b)$ always exists.
  - Can calculate $\gcd(a, b)$ from prime factorization.
  - There are $x, y \in R$ such that $\gcd(a, b) = xa + yb$.
- Unique factorization domain (UFD):
  - $\gcd(a, b)$ always exists.
  - Can calculate $\gcd(a, b)$ from prime factorization.

  Example: $\gcd(2, x) = 1$, but $1 \notin (2, x) \subseteq \mathbb{Z}[x]$.

What about domains where $\gcd(a, b)$ doesn't exist?

Domains where GCDs don't exist

In the homework, you'll show:

- If R is a domain with complete factorizations, then R is a UFD if and only if every pair of elements has a greatest common divisor.
- $\mathbb{Z}[i\sqrt{5}]$ is a domain with complete factorizations, but is not a UFD.

So $\gcd(a, b)$ does not always exist for $a, b \in \mathbb{Z}[i\sqrt{5}]$.

For a specific counterexample, take $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. We can show 2, 3, $(1 + i\sqrt{5})$, $(1 - i\sqrt{5})$ are irreducibles (homework).

Suppose $d = \gcd(6, 2(1 + i\sqrt{5}))$. Then $2 \mid d$, so $d = 2d'$, and $2 \cdot 3 = kd = 2kd'$. So $3 = kd'$. Since 3 is irreducible, k or d' is a unit. If k is a unit, then $d' \sim 3$, but $d \sim 6 \nmid 2(1 + i\sqrt{5})$. If d' is a unit, then $d \sim 2$, but $(1 + i\sqrt{5}) \nmid d$. Contradiction in both cases.