Abstract Algebra Part 3

Disclaimer: Work in progress. Portions of these written materials are incomplete.

Group homomorphisms

Homomorphisms

Main idea: symmetries of symmetries – we can learn about groups by studying their structure preserving transformations

What does it mean for a transformation to preserve the structure of a group? The function needs to respect the group operation.

Defn: A function $f: G \to H$ is a **homomorphism** if

- (multiplicative) $f(a *_G b) = f(a) *_H f(b)$
- (additive) $f(a +_G b) = f(a) +_H f(b)$

Homomorphisms

What about the other group structure, like identity and inverses? Those follow from $f(a * b) = f(a) * f(b)$

- A homomorphism always **preserves the identity.**
- A homomorphism always **preserves inverses.**

Homomorphism Examples

- $f: \mathbb{Z} \to \mathbb{Z}$, $f(a) = ma$
  - $f(a + b) = m(a+b) = ma + mb = f(a) + f(b)$

- $f: \mathbb{Z} \to \mathbb{Z}_p$, $f(a) = a \bmod (p)$

- Exp and log
  - exp: $(\mathbb{R}, +) \to (\mathbb{R}^+, *)$ $e^{a+b} = e^a e^b$
  - log: $(\mathbb{R}^+, *) \to (\mathbb{R}, +)$ $\log(ab) = \log(a) + \log(b)$

- Determinant: Invertible NxN matrices to non-zero (multiplicative) reals
  - $\det(AB) = \det(A) \det(B)$, also implies that $\det(A^{-1}) = \det(A)^{-1} = 1 / \det(A)$

- Identity map: $f(g) = e$
  - $f(ab) = e = e * e = f(a) f(b)$

Homomorphism Non-Examples

$f: \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(a) = a + k$ (where $k \neq 0$)

- Doesn't respect group operation (integer addition)
- $f(a + b) = a + b + k \neq (a + k) + (b + k) = f(a) + f(b)$

$f: \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(a) = a^2$

- Also doesn't respect group operation (integer addition)
- $f(a + b) = (a + b)^2 = a^2 + 2ab + b^2 \neq a^2 + b^2 = f(a) + f(b)$

$f: D_n \longrightarrow D_n$, $f(r) = s$ and $f(s) = r$

- Doesn't preserve order (unless $n = 2$)
- Doesn't respect the relation $rs = sr^{-1}$

Image of a Homomorphism

The **image of a homomorphism** is defined just like the image of a function:

$f(G) = \{f(g) \text{ for } g \text{ in } G\}$

- The image $f(G)$ is a subgroup of H
  - If $a_1 = f(g_1)$ and $a_2 = f(g_2)$ then $a_1a_2 = f(g_1)f(g_2) = f(g_1g_2)$ is also in the image
  - Lagrange's theorem implies that $|f(G)|$ divides $|G|$ and $|H|$
- More generally, homomorphisms carry subgroups to subgroups
  - If $G' \leqslant G$ then $f(G') \leqslant H$, so subgroup lattices are "preserved" (or collapsed)
- It's also true that $|f(g)|$ divides $|g|$
  - If $|g| = n$ then $(f(g))^n = f(g^n) = e$, so $|g|$ is a multiple of $|f(g)|$
  - The order of an element can only get smaller

Isomorphisms

An isomorphism is a homomorphism that is also bijective. This means that the two groups are in some sense “the same” abstractly

Examples:

- $\exp(x) = e^x$ and (natural) Log are inverse functions (so bijective) and homomorphisms, so they are isomorphisms between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, *)$

- $f(x) = x^3$ and $g(x) = x^{1/3}$ are isomorphisms from $\mathbb{R}$ to $\mathbb{R}$
  - Multiplicatively but not additively

- The cyclic groups $C_n = \langle r \rangle$ and modular integers $\mathbb{Z}_n$ (additively) are iso
  - $f(r) = 1 \bmod (p)$
  - $f(r^m r^n) = m + n \pmod{p} = f(r^m) + f(r^n) \pmod{p}$

Kernel of a homomorphism

The kernel of a homomorphism is all the elements that get mapped to the identity: ker(f) = {g in G | f(g) = e_H}

- ker(f) is a subgroup of G
  - Contains identity: f(e_G) = e_H
  - Closure: If f(a) = e_H = f(b) then f(ab) = f(a)f(b) = $e_H e_H$ = e_H

- [Lagrange’s Theorem] |ker G| divides |G|

- Cosets of Ker f partition G and we’ll see that
  - |G| = |ker f| |f(G)|
  - So |f(G)| also divides |G|

Kernels and Injectivity

A homomorphism f: G →H is injective if and only if ker(f) = {e}

- Injective → ker(f) = {e} since f(e) = e
- Suppose ker(f) = {e} and f(g) = f(h)
  - Then $f(gh^{-1}) = f(g)f(h)^{-1} = f(g)f(g)^{-1} = e$, so gh^{-1} is in the kernel
  - So $gh^{-1} = e$ and g = h → injective

More generally, f is a |ker(f)| to one mapping

- k in ker(f) → f(g) = f(g) + f(k) = f(g + k)

Example: f: $\mathbb{Z}_{16} \to \mathbb{Z}_4$ given by f(x) = 4x is a 4 : 1 mapping

- ker(f) = {0, 4, 8, 12} ← any kernel element times 4 is 0 mod (16)

Example: Roots of Unity and the Circle Group

Recall the circle group C: rotation by any angle

$$r_\theta = e^{i\theta}$$

Roots of unity are described by

$$x = e^{\frac{2\pi i}{n}}$$

Example: Roots of Unity and the Circle Group

Recall the circle group C: rotation by any angle

$$r_\theta = e^{i\theta}$$

Roots of unity are described by

$$x = e^{\frac{2\pi i}{n}}$$

Define a homomorphism by f: C → C with f(x) = x^n

- ker(f): need $x^n = e^{2\pi i}$ so the kernel consists of the n-th roots of unity
- Shows that n-th roots are a subgroup of C

General Isomorphism Examples

If G abelian, $f: G \to G$ given by $f(g) = g^{-1}$ is a homomorphism

- Recall if G abelian then: $(ab)^{-1} = b^{-1} a^{-1} = a^{-1}b^{-1}$
  - Shows f is a homomorphism $f(ab) = (ab)^{-1} = a^{-1}b^{-1} = f(a)f(b)$
- It's an isomorphism
  - $\mathrm{Ker}(f) = \{e\}$ since $g^{-1} = e \Rightarrow g = e$, so it's injective
  - Onto since every element has a unique inverse

For any group G, $f_h{:}G \to G$ given by $f_h(g) = hgh^{-1}$ is an isomorphism from G to G

- These are called "inner automorphisms" by conjugation

Homomorphisms Summary

- Homomorphisms preserve group structure
- Image and kernel are subgroups of the domain and codomain
- If bijective, we call it a isomorphism

Cayley’s Theorem

Subgroups of the Symmetric group

- Symmetric groups (permutations) have many subgroups

- $S_k \leqslant S_n$ for all $k \leqslant n$

- [Cayley's theorem] Every finite group of order n is realizable as a subgroup of S_n

Subgroup lattice of S_4 (wikipedia)

Cayley’s Theorem

Main idea: Represent any group as a subgroup of permutations (of the symmetric group)

This gives a “concrete” way to represent and multiply elements of a group

We need to construct an injective homomorphism from G to the symmetric group S_n

First let’s talk a bit more about permutations

Cayley’s Theorem

For a group G, consider the action of an element g on G as a set:

$$f_g : X \to X$$
$$f_g(x) = g\, x$$

This is a permutation of the elements of G, so a member of the symmetric group S on |X| elements.

Why is it invertible? Notice that

$$f_{gh}(x) = (gh)\, x = g\, (gx) = f_g(f_h(x)) = (f_g \circ f_h)(x)$$

So if e = gh then f_g and f_h are inverse permutations (on the set of G)

Cayley's Theorem

Now we can define a homomorphism c: $G \to S_n$ by mapping each element to the permutation that it induces:

$$c(g) = f_g$$

It's a homomorphism because we had the following

$$f_{gh}(x) = (gh)\ x = g\ (gx) = f_g(f_h(x)) = (f_g \circ f_h)(x)$$

It's injective because the kernel = {e}:

$$f_g = id_G \text{ iff } f_g(x) = gx = x \text{ for all } x\text{, so } g{=}e$$

It's not generally surjective, so it's an embedding rather than a full isomorphism

Examples of Cayley's Theorem

- The cyclic group on n-elements C_n can be represented by an order n permutation
  - For example, C_6 is given by <(234561)> or any order 6 permutation
  - Just need to map the generator to an order 6 permutation

Examples of Cayley's Theorem

- The elements of Klein four-group K={e, a, b, ab} correspond to {e, (12)(34), (13)(24), (14)(23)} $\leqslant S_4$

Label the elements of K and look at the functions actions f_g

e	a	b	ab
1	2	3	4

For example, let g = a. Then we have that that $f_a \rightarrow (12)(34)$

a*e = a	a * a = e	a * b = ab	a *ab = b
1 → 2	2 → 1	3 –> 4	4 → 3

Examples of Cayley's Theorem

- Note that our labeling was arbitrary, so an alternative labeling could product a different embedding
  - In other words, the representation is not unique
- Can get a new embedding by composing our first embedding with a permutation of G (as a set), or an automorphism of S_n
  - If we have an injective homomorphism $f: G \to S_n$
  - and an automorphism of $p: S_n \to S_n$
  - then $p \circ f$ is also an injective homomorphism $G \to S_n$
- Groups can also be represented as subgroups of matrix groups, where the operation becomes matrix multiplication
  - Representation theory

Normal Subgroups and Quotients

Normal subgroups

The kernel of a homomorphism has a special property: it's fixed by conjugation

If g in ker(f) and h in G, then hgh^{-1} is also in the kernel:

$$f(hgh^{-1}) = f(h)f(g)f(h)^{-1} = f(h)\ e\ f(h)^{-1} = f(h)\ f(h)^{-1} = e$$

A subgroup H is called normal if $gHg^{-1} = H$ for all g in G

$$gHg^{-1} = \{ghg^{-1} \text{ for all } g \text{ in } G \text{ and } h \text{ in } H\}$$

Notation: $N \triangleleft G$ means that N is a normal subgroup of G

Normal subgroups are nice because their cosets $\{gH\}$ also form a group, called a quotient group.

Normal subgroups

Some facts about normal subgroups:

- All subgroups of an abelian group are normal:
  - ghg^{-1} = h in an abelian group
- {e} and G are normal subgroups
- Center of a group: elements that commute with all others
  - The center is defined as Z(G) = {h | gh=hg for all g in G}
  - If G abelian, Z(G) = G
  - $Z(S_n)$= {e} for n>= 3
- Commutator subgroup: [G, G] = {$g^{-1}h^{-1}gh$ for all g,h in G}
  - For an abelian group, [G, G] = e
  - Otherwise [G, G] measures how non-abelian a group is

Quotients from Normal Subgroups

The set of left cosets of a group {gN for g in G} is a group with the operation from G, if and only if N is a normal subgroup:

(gN)(hN) = (gh)N

When N is normal, we define the quotient group G/N to be the left cosets of N:

G/N = {gN for all g in N}

We have to show that the choice of representative of the coset doesn’t matter (well-defined)

Example: Cyclic groups

Intuition: For G/N, everything in N is the identity

For cyclic groups, you can imagine starting with an infinite cycle group $\langle a \rangle$, looking at the subgroup generated by $\langle a^n \rangle$ which imposes $a^n=1$, so the infinite cycle is wrapped around the cyclic group C_n

So $C_n = \langle a \rangle / \langle a^n \rangle$

Example: modular integers

Intuition: For G/N, everything in N is the identity

$n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, with cosets:

- $n\mathbb{Z}$, $n\mathbb{Z} + 1$, ..., $n\mathbb{Z} + (n-1)$
- The operation is $(n\mathbb{Z} + a) + (n\mathbb{Z} + b) = (n\mathbb{Z} + (a+b \bmod n))$

These cosets are the same as the integers mod n, which is written as $\mathbb{Z}/n\mathbb{Z}$.

Example: Abelianization

Idea: Replace a group G with the “best” abelian group
Intuition: make all of the elements g,h where gh != hg equal to the identity:
$ghg^{-1}h^{-1} = e$ would guarantee that $gh = hg$

So we “mod out” by all elements of the form $ghg^{-1}h^{-1}$ which is the commutator subgroup [G, G]. Then the quotient group is abelian, since we’ve forced $ghg^{-1}h^{-1} = e$

$Ab(G) := G/[G, G]$

Noether's First Isomorphism Theorem

First Isomorphism Theorem

Let f: G → H be a group homomorphism. Then

$G \,/\, \ker(f) \cong \text{image}(f) = f(G)$

Example: $f: \mathbb{Z} \to \mathbb{Z}_n$ by $f(x) = x \bmod n$. Then we have:

- $\ker(f) = n\mathbb{Z}$
- $\text{im}(f) = \mathbb{Z}_n$

So by the theorem, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

First Isomorphism Theorem

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

$G / \ker(f) \cong \text{image}(f) = f(G)$

Example: $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $f(x) = x \bmod n$. Then we have:

- $\ker(f) = n\mathbb{Z}$
- $\text{im}(f) = \mathbb{Z}_n$

So by the theorem, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

Example: Circle group

$f: \mathbb{R} \longrightarrow C \quad f(x) = e^{2\pi i x}$

$\ker(f) = \mathbb{Z}$

$\mathrm{im}(g) = C$

So $C \cong \mathbb{R}/\mathbb{Z}$

Groups act on themselves

G acts on itself by conjugation. For h in G, define $f_h : G \to G$ by:

$$f_h(g) = hgh^{-1}$$

We say before that these functions are inner automorphisms, which form a subgroup Inn(G) of the automorphism group Aut(G).

If G is abelian, these are all trivial, since $hgh^{-1} = g$ and so f_h would be the identity function.

We can now define a homomorphism from $G \to \mathrm{Aut}(G)$ by $g \to f_g$

The kernel of this map is the center of G, so by the first isomorphism theorem

$$G / Z(G) \cong \mathrm{Inn}(G)$$

Summary so far

We’ve got groups, which are collections of symmetries

We can get new groups by looking for subgroups or quotients

Both subgroups and quotients are closely related to homomorphisms, structure preserving functions between groups

We’ve seen that every group is a subgroup of a Symmetric group, and that many familiar groups come from quotients

Is every group a quotient somehow?

Free Groups

Free Group

- Definition
- Natural group on n elements
- Free abelian group
- F2 contains Fn for all n
- Every group is the quotient of a free group
    - Example: Dihedral group
    - Integers mod n

Direct Products and FTFGAB

Direct Products of Groups

Given two groups G and H, we form the direct product $G \times H$ as:

- Elements of $G \times H$ are ordered pairs of elements (g, h)
- The group operation is pairwise
  - $(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$

The order of the direct product is given by: $|G \times H| = |G|\,|H|$

We can take the direct product of several groups by iteration

$$G_1 \times G_2 \times \cdots \times G_n$$

In general we have that $G \times H \cong H \times G$

Direct Product Examples

Klein four group $K = \{e, a, b, ab \text{ where } a^2 = b^2 = (ab)^2 = e\}$

$K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

iso $f: K \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by $f(a) = (1, 0)$ and $f(b) = (0, 1)$

*	(1,1)	(a,1)	(1,b)	(a,b)
(1,1)	(1,1)	(a,1)	(1,b)	(a,b)
(a,1)	(a,1)	(1,1)	(a,b)	(1,b)
(1,b)	(1,b)	(a,b)	(1,1)	(a,1)
(a,b)	(a,b)	(1,b)	(a,1)	(1,1)

Direct Product Examples

Klein four group $K = \{e, a, b, ab$ where $a^2 = b^2 = (ab)^2 = e\}$

$K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

iso $f: K \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by $f(a) = (1, 0)$ and $f(b) = (0, 1)$

*	(1,1)	(a,1)	(1,b)	(a,b)
(1,1)	(1,1)	(a,1)	(1,b)	(a,b)
(a,1)	(a,1)	(1,1)	(a,b)	(1,b)
(1,b)	(1,b)	(a,b)	(1,1)	(a,1)
(a,b)	(a,b)	(1,b)	(a,1)	(1,1)

Euclidean space: $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$

Direct Products of Cyclic Groups

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$ (no common factors)

- In the direct product $(a, b) = (a, 1)(1, b)$ for generators a and b
  - If $\gcd(m, n) = 1$, then $|(a, b)| = |(a, 1)| \cdot |(1, b)| = |a| \cdot |b| = mn$, so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic
- If $\gcd(m, n) > 1$ then $|(a, b)| < mn$, so not cyclic

This in turn implies that any finite cyclic group can be written as a product of cyclic groups of prime power order:

Direct Products of Cyclic Groups

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$ (no common factors)

- In the direct product $(a, b) = (a, 1)(1, b)$ for generators a and b
  - If $\gcd(m, n) = 1$, then $|(a, b)| = |(a, 1)| \cdot |(1, b)| = |a| \cdot |b| = mn$, so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic
- If $\gcd(m, n) > 1$ then $|(a, b)| < mn$, so not cyclic

This in turn implies that any finite cyclic group can be written as a product of cyclic groups of prime power order:

$$n = p_1^{a_1} \cdots p_k^{a_k} \to \mathbb{Z}_n = \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

Finitely Generated Abelian Groups

A group is **finitely generated** if it can be described by a finite set of generators

$G = \langle g_1, g_2, \ldots, g_k \rangle$

Examples:

- $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ has n generators $\{(1, 0, \ldots), (0, 1, \ldots), \ldots, (0, \ldots, 0, 1)\}$
- $\mathbb{Z}_n$ has 1 generator: $\{1 \pmod{n}\}$
- Klein four group K has 2 generators $\{a, b\}$
- Any **finite group** is **finitely generated** by its underlying set

Non-examples (all infinitely generated):

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Fundamental Theorem of FG Abelian Groups

Theorem: Every finitely generated abelian group is of the form

$$G \cong \mathbb{Z}^k \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_k}$$

Example: If G is abelian and of order $|G| = 200 = 2^3 5^2$, then G is one of the following six groups:

Fundamental Theorem of FG Abelian Groups

Theorem: Every finitely generated abelian group is of the form

$$G \cong \mathbb{Z}^k \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_k}$$

Example: If G is abelian and of order |G| = 200 = $2^3 5^2$, then G is one of the following six groups:

- $\mathbb{Z}_{200}$
- $\mathbb{Z}_{100} \times \mathbb{Z}_2$
- $\mathbb{Z}_{50} \times \mathbb{Z}_4$
- $\mathbb{Z}_5 \times \mathbb{Z}_{40}$
- $\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
- $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

⟷

- $\mathbb{Z}_{25} \times \mathbb{Z}_8$
- $\mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_{25} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_8$
- $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Algebraic Structures

Algebraic Structures

In abstract algebra, we study many structures that are typically similar to groups. Often we

- relax some condition such as invertibility (monoids)

- add some structure such as having both multiplication and addition (rings)

Monoids

Monoids are groups without guaranteed inverses

The integers ℤ (multiplicatively) are a monoid, with only 1 and −1 having inverses

Square (n x n) matrices are a monoid multiplicatively, only matrices with determinant != 0 are invertible

Every group is a monoid

Monoids

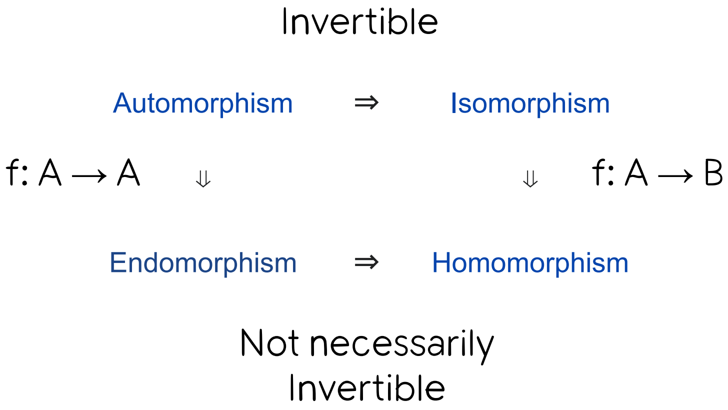
Just as groups occur as sets of automorphisms (isomorphisms from an object to itself)

Monoids occur as sets of **endomorphisms** (just functions from an object to itself)

- Not all functions are invertible, but
- Functions are still composable
- Associative but not necessarily commutative

For example, non-invertible matrices are (linear) endomorphisms of $\mathbb{R}^n$

Types of morphisms



Invertible

Automorphism ⇒ Isomorphism

f: A → A ⇓ ⇓ f: A → B

Endomorphism ⇒ Homomorphism

Not necessarily Invertible

Monoid Examples:

Additively, The natural numbers $\mathbb{N}$ = {0, 1, 2, 3, ...} are the free monoid on one generator: 1

Multiplicatively $\mathbb{N}$ is **freely generated** by the infinite set of **prime numbers**

In formal language theory, the set of all strings is the free monoid on the associated alphabet

- Operation is string concatenation (not invertible)

In functional programming, Lists of a given type T form a similar monoid

- Operation is list concatenation

Recall: Additively $\mathbb{Z}$ is the free group on one generator

Rings

Often we have both **addition** and **multiplication** on the same set:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ all have both addition and multiplication as operations

These are all groups under addition, but have some non-invertible elements multiplicatively:

- 0 is not invertible in all of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$
- For $\mathbb{Z}$: only 1 and -1 have multiplicative inverses (themselves)
- For $\mathbb{Z}_n$: only elements k that are relatively prime to n (no common factors) have multiplicative inverses

Rings

A **ring** is an algebraic structure **R** such that:

- R is an **abelian group** (additively) with identity element 0
- R is a **monoid** (multiplicatively) with identity element 1
- R has a **distributive property** for addition and multiplication:
  - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity)
  - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity)

From the definitions, it follows that:

- $0 \cdot x = 0 = x \cdot 0$
- $(-1) \cdot x = -x$, so $(-1)(-1) = 1$

Rings: Examples

Commutative rings ($xy = yx$ always).

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ and their direct products such as $\mathbb{R}^n$
- Gaussian integers $\mathbb{Z}[i] = \{a + bi$ for a, b in $\mathbb{Z}\}$ where $i = \sqrt{-1}$

$\mathbb{Z}[i]$: lattice points in the complex plane

Rings: Examples

Commutative rings ($xy = yx$ always).

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ and their direct products such as $\mathbb{R}^n$
- Gaussian integers $\mathbb{Z}[i] = \{a + bi \text{ for } a, b \text{ in } \mathbb{Z}\}$ where $i = \sqrt{-1}$

Non-commutative rings:

- Rings of $n \times n$ matrices
- Quaternions: $\{a + bi + cj + dk\}$ where $i^2 = j^2 = k^2 = ijk = -1$ and a, b, c, and d are real numbers
  - $ij = k$ but $ji = -k$

$\mathbb{Z}[i]$: lattice points in the complex plane

Polynomial rings and ideals

Given a ring **R**, we can form the polynomial ring **R[x]** of all the polynomials in one variable **x** with coefficients in **R**: $p(x) = r_0 + r_1x + r_2x^2 + \cdots + r_kx^k$

This is a ring because we can add and multiply such polynomials using the same operations from **R**

We can create quotients with subsets of **R** called **ideals**: these are subgroups of **R** additively that are closed multiplicatively (by any element of **R**).

We can generate ideals (just like subgroups) from one or more elements.
For $R = \mathbb{Z}$:

$$(x^2 + 1) = \{x^2 + 1, (x^2 + 1)^2, 2(x^2 + 1), 3(x^2 + 1), -(x^2 + 1), \ldots\}$$

Polynomial rings

Given an ideal like $(x^2 + 1)$, we can form a quotient ring: $R[x] / (x^2 + 1)$

As with groups we can think of this as forcing $x^2 + 1 = 0$, so we've essentially added an element x to R that solves $x^2 + 1 = 0$. For example:

$$\mathbb{C} \cong \mathbb{R}[x] / (x^2 + 1) \qquad \text{and} \qquad \mathbb{Z}[i] \cong \mathbb{Z}[x] / (x^2 + 1)$$

Ring Homomorphisms

I've claimed that $\mathbb{C} \cong \mathbb{R}[x] / (x^2 + 1)$ but I didn't tell you how to define a ring homomorphism!

Like with groups we want to preserve the structure of the ring, which means:

- Additive group structure: $f(a + b) = f(a) + f(b)$
  - Additive identity: $f(0) = 0$
- Multiplicative monoid structure: $f(ab) = f(a)f(b)$
  - Multiplicative identity: $f(1) = 1$

$f: \mathbb{R}[x] / (x^2+1) \to \mathbb{C}$ is defined by plugging $i = \sqrt{-1}$ into the polynomials of $\mathbb{R}[x]$

- $f(p \pmod{x^2+1}) = p(i)$

Ring Homomorphisms

We could also rephrase this in terms of the **first isomorphism theorem** for rings

$f: \mathbb{R}[x] \to \mathbb{C}$ is defined by plugging $i = \sqrt{-1}$ into the polynomials of $\mathbb{R}[x]$

- $f(p) = p(i)$

The **kernel** of f is the ideal (x^2+1), since such polynomials are zero when we plug in $i = \sqrt{-1}$

Then the first isomorphism theorem (for rings) says that

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

Algebraic structures: universal algebra

Hopefully you see a pattern! Given some algebraic structure like a group or a ring formed from some collection of operations, we can:

- Form subobjects (subgroups, ideals)
- Define structure preserving homomorphisms and kernels
- Form quotients
- Formulate standard theorems like the first isomorphism theorem
- Define free objects, direct products, …

The study of algebraic objects at this level of generality is called **Universal Algebra**

- It's the study of algebraic theories rather than algebraic models

Fields

Fields

A field is a commutative ring where everything except zero is multiplicatively invertible

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ (for prime p) are all fields
- The algebraic numbers (solutions to all finite polynomial equations) form a field
- $\mathbb{Z}$ and $\mathbb{Z}_n$ (for composite n) are not fields

Finite fields are widely used in number theory and cryptography.

Finite Fields

In addition to $\mathbb{Z}_p$ (p prime) there are also fields for $\mathbb{Z}_n$ where $n = p^k$ is a prime power

- Addition is just as in $\mathbb{Z}_n$ (ordinary modular addition)
- But multiplication is different.
  - Why? If $n=p^2$, $p*p = 0 \pmod{p^2}$ then p would not be invertible with the usual multiplication

So how does the multiplication work?

Given any irreducible polynomial (can't be factored into smaller polynomials) $p(x)$ we can form a finite field via the quotient $\mathbb{Z}_p[x] / (p(x))$. All arithmetic works out modulo $p(x)$.

Finite Field of 4 elements

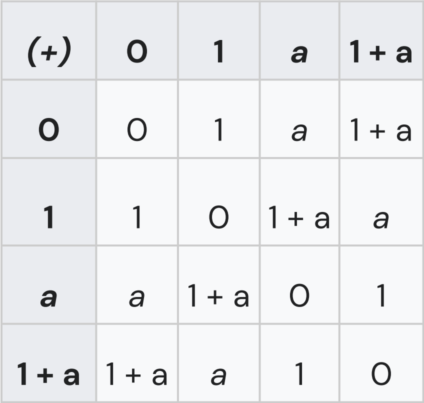
To define a finite field on four elements, we can take a polynomial like $p(x) = x^2 + x + 1$ over $\mathbb{Z}_2$. Operating modulo p is asserting that $p(x) = 0$.

Let a be a root of $p(x)$, then $a^2 = a + 1$ and we extend $\mathbb{Z}_2$ with a and $a+1$.

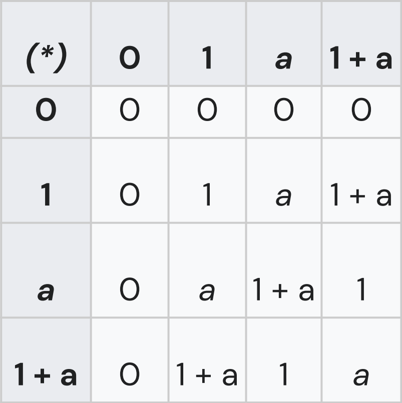
Finite Fields

To define a finite field on four elements, we can take a polynomial like $p(x) = x^2 + x + 1$ over $\mathbb{Z}_2$. Operating modulo p is asserting that $p(x) = 0$.

Let a be a root of $p(x)$, then $a^2 = a + 1$ and we extend $\mathbb{Z}_2$ with a and a+1



(+)	**0**	**1**	***a***	**1 + a**
0	0	1	*a*	1 + a
1	1	0	1 + a	*a*
a	*a*	1 + a	0	1
1 + a	1 + a	*a*	1	0

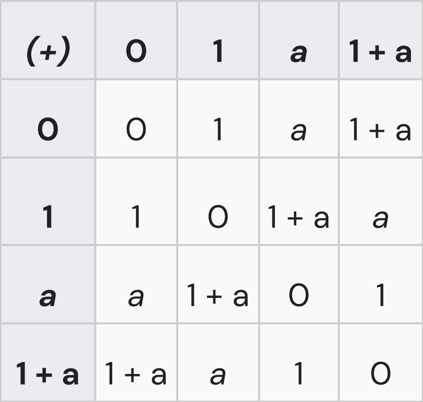


(*)	**0**	**1**	***a***	**1 + a**
0	0	0	0	0
1	0	1	*a*	1 + a
a	0	*a*	1 + a	1
1 + a	0	1 + a	1	*a*

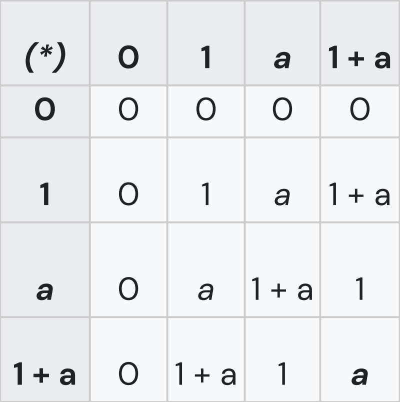
Finite Fields

To define a finite field on four elements, we can take a polynomial like $p(x) = x^2 + x + 1$ over $\mathbb{Z}_2$. Operating modulo p is asserting that $p(x) = 0$.

Let a be a root of $p(x)$, then $a^2 = a + 1$ and we extend $\mathbb{Z}_2$ with a and a+1



(+)	**0**	**1**	***a***	**1 + a**
0	0	1	*a*	1 + a
1	1	0	1 + a	*a*
a	*a*	1 + a	0	1
1 + a	1 + a	*a*	1	0



(*)	**0**	**1**	***a***	**1 + a**
0	0	0	0	0
1	0	1	*a*	1 + a
a	0	*a*	1 + a	1
1 + a	0	1 + a	1	***a***

$$(1 + a)(1 + a) = 1 + 2a + a^2 = 1 + a^2 = a + 2 = a \pmod 2$$

Galois Groups of Polynomials

Fields are fundamental to Galois theory, where to each polynomial we assign a group based on how the roots of the polynomial can be permuted.

If this group is **solvable**, the associated polynomial can be **solved by radicals**, multiplication, and addition.

For example, the polynomial $\mathbf{x^2 + 1}$ has two roots, $\mathbf{a = i}$ and $\mathbf{b = -i}$, which satisfy two equations: $\mathbf{a + b = 0}$ and $\mathbf{ab = 1}$.

These equations are still satisfied if we interchange the roots, so the Galois group is $\mathbb{Z}_2$ defined by the permutation (ab) of order 2.

Galois Groups of Polynomials

The Galois group of a degree n polynomial is a subgroup of the symmetric group S_n

It turns out that the smallest non-solvable group is a subgroup (A_5) of the symmetric group S_5 so the smallest possible degree polynomial not solvable by radicals is a quintic.

For example, the polynomial $p(x) = x^5 - x - 1$ is not solvable.

Note that some quintics **are** solvable. For example $x^5 - 1$ is solvable (5th roots of unity) and has Galois group $\mathbb{Z}_4$ (solvable because it's abelian).

Algebra Across Mathematics

Linear Algebra

Linear algebra is widely used across mathematics, science, machine learning, etc.

- central object of study are vector spaces over fields
- and their homomorphisms (matrices)

Despite being well-understood, linear algebra has found new applications recently, such as singular value decomposition in machine learning.

Algebra applied to other fields

Abstract algebra has been central to many advances in mathematics in the last century:

- Algebraic topology
- Algebraic number theory
- Algebraic geometry
- Modern physics

This has led to solutions to many important mathematical problems such as the Poincaré conjecture and Fermat's last theorem.

Algebraic Topology

A common technique in modern mathematics is to reduce a complex problem to an algebraic problem, which is typically easier to resolve

For example, to each topological space we can associate a group called the fundamental group

Fundamental Group

Main ideas:

- (Closed) loops inside our space can be combined (concatenated)
- Loops are equivalent if they can be smoothly deformed into each other
- Taking the inverse is reversing the orientation of the loop

Fundamental Group: Circle (S^1)

For a circle, a loop is characterized by how many times it winds around. Two loops are equivalent if they wind around the same number of times

The fundamental group of a circle is $\mathbb{Z}$

Fundamental Group: Figure 8

For a figure eight, a loop is determined by how many times, and in what order and orientation, it traverses each loop

The fundamental group is the Free group on two generators F[a, b]

Fundamental Group: Sphere (S^2)

On a sphere, we have an extra dimension to move in and every loop can be smoothly deformed to a point.

The fundamental group of a sphere is the one element group $\{e\}$

For the same reason, the fundamental group of the plane $\mathbb{R}^2$ is $\{e\}$

Fundamental Group: Torus

For a torus, a loop can go around longitudinally or latitudinally multiple times.

The fundamental group of a torus is $\mathbb{Z} \times \mathbb{Z}$

Algebraic Invariants

The fundamental group construction translates **homeomorphisms** (functions that preserve topology) into **isomorphisms** of the respective fundamental groups

So if the fundamental groups are **different**, the spaces **cannot** be homeomorphic (but different spaces can have the same group)

It’s typically much easier to compute and compare algebraic invariants like the fundamental group than it is prove that there is no homeomorphism between two topological spaces

Algebraic Invariants

In fact we can often associate infinitely many groups to an object via (co)homology theories. We study these groups to learn more about the original object.

For example, we can define higher order homotopy groups by replacing loops with n-dimensional spheres

Algebraic Invariants

In fact we can often associate infinitely many groups to an object via (co)homology theories. We study these groups to learn more about the original object.

For example, we can define higher order homotopy groups by replacing loops with n-dimensional spheres

Some surprising features emerge. For example it's possible to smoothly map a 3-sphere onto a 2-sphere (Hopf Fibration)

Hopf Fibration $S^3 \longrightarrow S^2$

Algebraic Number Theory

Rings and other algebraic objects are commonly used to study equations in algebraic number theory.

For example, to find integer solutions to a Diophantine equation such as $x^3 = y^2 + 1$ we study the property of associated rings such as $\mathbb{Z}[i]$. This is because

$$x^3 = y^2 + 1 \longrightarrow x^3 = (y + i)(y - i)$$

Whether a ring has unique factorization is often important. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are unique factorization domains, but $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-19}]$ are not.

- In $\mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- Since elements don't factor uniquely, there can be more solutions to equations like $6 = xy$ or $36 = (a^2+1)b^2$

Algebraic Geometry

Elliptic curve
$y^2 = x^2(x + 1)$

In algebraic geometry, we study the geometric properties of objects like $y^2 = x^2(x + 1)$ via rings and other algebraic techniques.

The solutions of $y^2 = x^2(x + 1)$ are zeros of the equation $y^2 - x^2(x + 1) = 0$, which correspond to certain ideals of the quotient ring:

$$R[x, y] / (y^2 - x^2(x + 1))$$

where $R[x, y]$ is a polynomial ring on two variables

Algebraic Geometry

$$y^3 = x^2(x + 1)$$

Algebraic geometry can also be applied to number theoretic problems. These techniques helped solve Fermat's Last Theorem and many other important problems.

Algebraic invariants (cohomology theories) can also be assigned to curves (like the one on the right).

Intersections between algebraic topology and algebraic geometry are active areas of research.

Computational algebraic geometry

Computational algebraic geometry studies algorithms to solve, for example, systems of polynomial equations

Such solutions are often equivalent to finding a finite set of generators for a collection of ideals

This is a generalization of linear algebra (systems of linear equations) and has many interesting algorithmic questions

How to solve a nonlinear system?

$$y^3 = x^2(x + 1)$$
$$x^4 + x^3 = 3$$
$$xy = 6$$

Exercises

Agenda

- The Fermat-Euler Theorem
  - Review: Fermat’s Little Theorem
  - The Euler totient function
  - The Fermat-Euler Theorem
- The Euclidean algorithm: how to rapidly compute a GCD

The Fermat–Euler Theorem

Review: Fermat's Little Theorem

Recall from Tuesday's lecture:

> **Fermat's Little Theorem**: Let p be a prime, and let a be an integer not divisible by p. Then $a^{p-1} \equiv 1 \bmod p$.

Sketch of proof: apply Lagrange's Theorem to the subgroup <a> sitting inside $\mathbb{Z}_p{}^*$.

The multiplicative group $\mathbb{Z}_n$*.

Recall from the first week the exercise about how to make $\mathbb{Z}_n$* a group: remove all elements $[a]_n$ where gcd(a, n) > 1.

Examples:

- $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$
- $\mathbb{Z}_9^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$

The Euler totient function

What is the size of $\mathbb{Z}_n$*? Evidently it is the number of integers in {1, 2, ..., n} coprime (that is, gcd(a, n) = 1) to n. We call this number **φ**(n), and **φ** is called the ***Euler totient function***.

How do we compute **φ**(n) without actually going through every integer 1, 2, .., n and checking if they are co-prime to n?

Exercises: Values of the Euler totient function

Exercise: Show that, if p is a prime and n a positive integer, then $\boldsymbol{\varphi}(p^n) = p^n - p^{n-1}$.

Exercise: Now suppose n and m are positive integers with gcd(n, m) = 1. What can you say about the relationship between $\boldsymbol{\varphi}(nm)$ and $\boldsymbol{\varphi}(n)$, $\boldsymbol{\varphi}(m)$? (Try working this out explicitly for small values of n and m, like n = 3, m = 2, or n =3, m = 4, etc.).

Exercise: Compute $\boldsymbol{\varphi}(900)$. More generally, how would you compute $\boldsymbol{\varphi}(n)$ for arbitrary n?

The Fermat-Euler Theorem

Fermat's Little Theorem is generalizable to $(\mathbb{Z}/n\mathbb{Z})^*$. The major changes are:

- $(\mathbb{Z}/n\mathbb{Z})^*$ has size $\boldsymbol{\varphi}(n)$.
- a has to be coprime to n.

Then:

Fermat-Euler Theorem: If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.

(Notice, if $n = p$, we get exactly Fermat's Little Theorem).