Algebraic structures

common data types

- $\mathbb{Z}$ set of integers $\{\ldots, -1, 0, 1, \ldots\}$
- $\mathbb{Q}$ set of rational numbers $\{1/2, 2, \ldots\}$
- set of rationals on $\mathbb{R}$
- set of reals (or $\mathbb{R}$) on $\mathbb{C}$
- set of complex numbers (no $\mathbb{O}$)

sometimes called:

- set
- domain

$$\mathbb{Z}_4 \equiv \mathbb{Z}/4\mathbb{Z} \equiv \{0, 1, 2, \ldots, q-1\}$$

Groups

	Total	Associative	Identity	Divisible	Commutative
Group	Yes	Yes	Yes	Yes	optional

(define) group G

an underlying (non-empty) set (ex: $\mathbb{Z}$)

with some binary operator $\cdot$ (often $+$ or $*$)

(that is)

1. associative

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

2. has an identity (e) $\in G$

$$\exists e, \text{ s.t. } \forall a \quad \begin{array}{l} a \cdot e = a \\ e \cdot a = a \end{array}$$

3. has an inverses for each element in the set (all elements are units)

$$\forall a, \ \exists a^{-1} \in G \quad \text{s.t. } a \cdot a^{-1} = e$$

common groups:

- addition group — ex: $\mathbb{Z}, \mathbb{Z}^+$
- multiplication group — ex: $\mathbb{Z}, \mathbb{Z}^+$

(define) order of a group

the # of unique elements inside it

(define) cyclic group C_n

a group whose elements are all the powers of a generator g

(define) generator (primitive root) — (often denoted ζg)

the element that generates the cyclic group

$$\text{ex: } g^1, g^2, g^3, \ldots, g^{n-1}, \quad \underbrace{g^1, g^2, g^3, \ldots, g^{n-1}}_{\text{loops back around}}, \ldots$$

$\Rightarrow$ group of order n $\{1, \ldots, n-1\}$

(define) subgroup

H is a subgroup of G (denoted $H \leq G$)

$\hookrightarrow$ (denoted $H < G$ if no doubts $H \neq G$)

1. H's underlying set is a subset of G
2. H and G use the same binary operator

(note) cyclic subgroup are common

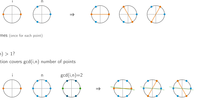
given a cyclic group G of order n

For additive groups, given $i, g \in G$ — notation is mostly a formality: *last g is always just 1*

$$\text{ord}(\langle i, g \rangle) = \frac{n}{\text{gcd}(n, i)}$$

Proof: how many times do we have to embed i inside a to cover all points?

(Σ how many times do we have to rotate to make a full circle



ex: $n = 3$, $i = 2$

Answer: 3 times (since for each point)

what if $\text{gcd}(n, i) > 1$?

each rotation covers $\text{gcd}(i, n)$ number of points

ex: $n = 6$, $i = 2$

Answer: 3 times (since each rotation covers 2 points (if pattern repeats after half the points)

$\therefore$ cycle is $\frac{n}{\text{gcd}(n, i)}$ — notably, it's a representative point from each rotation starting at the 0 point

$\therefore$ i is a generator iff $\text{gcd}(n, i) = 1$

$\text{gcd}(n, i) = 1 \quad \uparrow$ (prefer 1)

For multiplicative groups, given $g' \in G$

$\text{ord}(\langle g' \rangle) \Rightarrow$ smallest x s.t. $(g')^x \equiv 1$ *(mod n)*

$$\Rightarrow \frac{\varphi(n)}{\text{gcd}(\varphi(n), i)}$$

Proof: given a group with n points,

how many times do we have to embed i inside a to cover all points?

(Σ how many times do we have to rotate to make a full circle

ex: $n = 3$, $i = 2$

Answer: 3 times (since for each point)

what if $\text{gcd}(n, i) > 1$?

each rotation covers $\text{gcd}(i, n)$ number of points

ex: $n = 6$, $i = 2$

Answer: 3 times (since each rotation covers 2 points (if pattern repeats after half the points)

$\therefore$ cycle is $\frac{n}{\text{gcd}(n, i)}$ — notably, it's a representative point from each rotation starting at the 0 point

(recall) by Euler's theorem,

$\mathbb{Z}^+$ has $\varphi(n)$ points

so $k = \varphi(n)$

$$\therefore \text{ cycle is } \frac{\varphi(n)}{\text{gcd}(\varphi(n), i)}$$

$\therefore$ g' is a generator iff $\text{ord}(\langle g' \rangle) = \varphi(n)$

g' is a generator $\text{gcd}(\varphi(n), i) = 1 \quad \uparrow$ (prefer 1)

(define) Lagrange's Theorem

order(subgroup) divides order(original group)

$\hookrightarrow$ (through divisors from definition for cyclic groups from previous proof)
Lagrange's Theorem holds for all groups

Claim: For $\mathbb{Z}_n^+$, point k has a multiplicative inverse iff $\text{gcd}(k, n) = 1$

Proof: (recall) group generated by k has order $\frac{\varphi(n)}{\text{gcd}(k, \varphi(n))}$

$\hookrightarrow$ $\mathbb{Z}$, s.t. $0 \neq 1$

let point be g'

(claim) if cycle generated by k (call it C_k) is a proper subgroup ($C_k \subset C_n$), $\Rightarrow$ $\exists$ g s.t. $\text{gcd}(k, n) = 2$

so g' generates a proper subgroup

so k must skip g'

(proof) Show $g' \in C_k$ implies $C_n \subset C_k$

group contains both g' (by definition) and g' (by assumption)

since group is closed,

group contains $\underbrace{g', g', g', \ldots, g'}_{\text{this is every element}}$

$\therefore C_n \subset C_k \quad \rightarrow \quad g' \in C_k$

(implication) $\mathbb{Z}_n^+$ is a group iff q is prime — only way to guarantee all elements have inverses — i.e. $\forall k$, $\text{gcd}(k, q) = 1$

(note) for every prime p

- $\mathbb{Z}_p$ is a additive cyclic group of order p
- $\mathbb{Z}_p$ is a multiplicative cyclic subgroup of order $p-1$

$\hookrightarrow \{1, \ldots, p-1\}$

$\hookrightarrow$ 0 is omitted, as it has no inverse

$\hookrightarrow \mathbb{Z}$, s.t. $0 \neq 1$

$\therefore$ $g \in \mathbb{Z}_p^+$ is a generator iff $\text{gcd}(g, p-1) = 1$

g' is a primitive root

$\{g^1, (g^1)^2, (g^1)^3, \ldots, (g^1)^{p-1}\}$

$\hookrightarrow$ $n \geq 1$ because we rescaled n of -1

(note) there will always be some g' that is a generator

$\hookrightarrow$ ex: $n = 5$

however no known formula finds these generators better than just trying all i

TODO

- cosets
- abelian group

Fields & Rings

	Ring	Commutative Ring	Field
Closed (addition, multiplication)	Yes	Yes	Yes
Addition (existence 1 identity 1 inverse)	Yes	Yes	Yes
Multiplication (closed)	Yes	Yes	Yes
Multiplication (assoc)	Maybe	Maybe	Yes
Multiplication (commutative)	No	Yes	Yes
Multiplication (inverse)	No	No	Yes

Field: "usual" numbers $\mathbb{Q}, \mathbb{R}$ — add, multiplication: w/ identity & inverse & closed

$\mathbb{F}_q$ *denote finite field mod q*

Ring: field, but $\mathbb{Z}$ — NO multiplicative inverse $\rightarrow$ ex: 3 has inverse $\mathbb{R}$, but $\mathbb{R} \not\in \mathbb{Z}$; NO multiplicative identity (only additive identity); NO multiplicative commutativity (unless commutative ring)

$\hookrightarrow$ $\mathbb{Z}$, s.t. $0 \neq 1$

Ex: $\mathbb{Z}_4$ is a field

Ex: $\mathbb{Z}_4$ is NOT a field but $\mathbb{O}_4$ is a ring — ex: 2 has no multiplicative inverse

$\hookrightarrow$ $\mathbb{Z}$, s.t. $0 \neq 1$

$$2 \cdot 0 = 0$$
$$2 \cdot 1 = 2$$
$$2 \cdot 2 = 0$$
$$2 \cdot 3 = 2$$

Two separate concepts:

1. What values are *allowed* (2, $\mathbb{R}$, ...)
2. What operation are *allowed* (ring, field, ...)

Common structures:

$\mathbb{Z}_p$ is a field for every prime p: $\mathbb{F}_p \equiv \mathbb{Z}_p$ is called a *prime field*

p is called the characteristic of the field

$|\mathbb{F}| = p$ *elements*

$\hookrightarrow$ Need a larger field? What to do?

Field extensions: build a new field from an existing field

- Adding single elements: $\mathbb{Q}(\sqrt{2}) \quad \rightarrow \quad \mathbb{Q}$ with $\sqrt{2}$ as an element

(recall) $\mathbb{Q}(\sqrt{2})$ is closed under addition under multiplication $\rightarrow$ $a + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ $b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$$\therefore \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$\hookrightarrow$ Note: $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[2$

call this a *k-degree extension*

$\mathbb{Q}(\sqrt{2})$ is a *2-degree extension*

- Adding multiple elements: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad \leftarrow$ equivalent to adding more dimensions

Careful: Minimal model check

the number of dimensions $\neq$ the number of elements added (ex: $\dim(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \neq 3$)

recall: fields are closed under multiplication.

$\therefore \mathbb{Q} = \{r \times \sqrt{2} \mid r \in \mathbb{Q}(\sqrt{2}, \sqrt{3})\}$

recall: vectors are a graph can linear combinations of elements

ex: $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

note: $\underbrace{\{1, a, b, c\}}_{\text{4 elements}}$, $\underbrace{\{a, a\sqrt{2}, b, c\}}_{\text{4 elements}} \Rightarrow 3$

(it is also a dimension (as max 3 = $3(1) + 3(3) + 3(9) = 39$)

$\therefore \dim(\mathbb{Q}(\sqrt{2})) = 4$

note: 3 vectors with dimension 3

ex: $\mathbb{Q}(\sqrt{2})$ — $\mathbb{Z}_2$ — 2nd dimension; $\mathbb{Z}_2 \times \mathbb{Z}_2$ — 3rd dimension; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ≥ 2 — multiplication results in an existing element

(question) how do we make this more generic?

Instead of picking a specific value (ex: $\sqrt{2}$), use a generic variable x

(recall) closed under addition under multiplication $\rightarrow$ $\begin{array}{l} a + x \in \mathbb{Z}(x) \\ ax \in \mathbb{Z}(x) \\ a + x^2 \in \mathbb{Z}(x) \\ x^2 \in \mathbb{Z}(x) \end{array}$ *(this is just all polynomials)*

(define) $\mathbb{Z}[x]$ set of polynomials $\in$ with integer coefficients ex: $x^2 - 2$

Careful: Minimal model check

Think of x as a constructor argument, and not a dynamic variable!

i.e. $\mathbb{Q}(x)$ is not a field per se,
it's a template you use to create fields

$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ are not fields of the same field!
they are two totally separate fields created by the same template

Often, a specific value (ex: $\sqrt{2}$) is not picked
rather, just say "for x to be some element with some desirable properties"

(problem) this has infinite dimensions! — $x \in \mathbb{Z}(x)$; $x^2 \in \mathbb{Z}(x)$; $x^n \in \mathbb{Z}(x)$

(solution) re-introduce the concept of modulo

recall: $\mathbb{Z}_n \equiv \underbrace{\{0, 1, \ldots, n-1\}}_{\text{finite set}}$

note: $\mathbb{Z}[x]$ mod x^n is $\underbrace{\{1, x, x^2, \ldots, x^{n-1}\}}_{\text{finite set}}$ $\leftarrow$ limits the number of dimensions to 4

$\hookrightarrow$ (n) called the *reduction polynomial*

$\hookrightarrow$ $\mathbb{Z}[x](n)$ called the *polynomial ring*

(note) want $\mathbb{Z}(x)$ to have a leading coefficient of 1 (be a ***monic polynomial***) ex: $x^2 - 2$

so modulo triggers an integer coordinate

(intuition) for same reason, (mod 13/5) is awkward and causes issues

ex: it helps make polynomial division work regardless of the ring

want to divide: $g(x) = 3x^2 - 3$

	monic case	non-monic case
(define f)	$f(x) = x + 1$	$f(x) = 2x + 1$
(first step in division)	$3x \cdot f(x) = 3x^2 + 3x$	$\frac{1}{2}x \cdot f(x) = 3x^2 + \frac{1}{2}x$
	$\hookrightarrow$ can always clearly multiple	$\hookrightarrow$ a problem as $\frac{1}{2}$, $\notin \mathbb{Z}$

(note) polynomial rings are closed under polynomial multiplication $g(x)h(x)$

$$\begin{array}{lll} \text{proof} & \text{degree}(\ g(x)h(x)\ ) & \text{mod degree}(\ f(x)\ ) \\ \Rightarrow & 0 - 2(n-1) & \text{mod } n \\ \Rightarrow & 0 & \text{mod } n-1 \end{array}$$

$\hookrightarrow$ dimensions $\forall i, j \leq n$, $i \bmod n = j \leq$

(question) how to model exactly the properties of $\sqrt{2}$ that you want

ex: x^2 is almost what we want to model $\sqrt{2}$ (has 2 dimensions)

(solution) model the extension you want (ex: $\sqrt{2}$) as the roots of the polynomial

ex: $R = \mathbb{Z}[x] / (x^2 - 2)$ $\leftarrow$ (solution) $\sqrt{2} \in \mathbb{R}$

$$\begin{array}{l} \text{ex: } x^2 - 2 = 0 \\ \quad x^2 = 2 \\ \quad x = \pm\sqrt{2} \end{array}$$

$\hookrightarrow$ note: it is fine because things are closed under addition anyway
$\rightarrow f \notin \mathbb{Q}(\sqrt{2}) \quad \rightarrow x^2 - x^2 - x^2 \rightarrow x^2 \notin \mathbb{Q}(\sqrt{2})$

ex: $R = \mathbb{Z}[x] / (x^2 + 1)$ $\leftarrow$ (solution) $x \in \mathbb{C}$

$$\begin{array}{l} \text{ex: } x^2 + 1 = 0 \\ \quad x^2 = -1 \\ \quad x = \pm i \Rightarrow x = \{\sqrt{1}^{\,0}, \text{ ex: } x^{\frac{1}{2}}\} \end{array}$$

$\hookrightarrow$ recall: euler's identity
$e^{i\pi} + 1 = 0$
$e^{i\pi} = -1$
$e^{i\frac{\pi}{2}} = \pm i$

ex: $R = \mathbb{Z}[x] / (x^n - 1)$ $\leftarrow$ (solution) **nth roots of unity**

(why this works) remember, $\sqrt{2}$ only has 2 dimensions because $\sqrt{2} \cdot \sqrt{2} = 2$ $\leftarrow$ multiplication results in an existing element

i.e. it avoids $x^3, x^4, \ldots$ giving infinity many dimensions

note: avoiding this property of blowing up to infinite dimensions
is exactly the property we encode with the modulo!

(define) **Galois Field** binary fields $GF(2^n)$ $\leftarrow$ binary strings of length n

ex: $GF(2^3)$ contains

$$\begin{array}{lll} 0 & 1 & 000 \ 001 \\ x \in 0 & x \in 1 & 010 \ 011 \\ x^2 + 0x + 0 & x^2 + 0x + 1 & x^2 + 1x + 0 \quad x^2 + 1x + 1 \quad 100 \ 101 \ 110 \ 110 \end{array}$$

(define) **Ideal**: subset of a structure (but still closed under operations) ex: even numbers in $\mathbb{Z}$

An *ideal* of R is a subset $I \subseteq R$ such that:

1) $0 \in R$
2) if $a, b \in I$ then $a + b \in I$ *(closed under addition when a,b $\in I$)*
3) if $a \in I$ and $r \in R$ then $ar \in I$ *(closed under multiplication when $a \in I$ even when $r \notin R$)*

(define) **Principle ideal** subset of a structure

created by $I(x) = \{ \text{ ax } \mid \begin{array}{l} a \in R \text{ (ring)} \\ x \in R \text{ (ring)} \end{array} \}$

$\hookrightarrow$ Note: ring not always commutative for multiplication
so this is a right principal ideal (left principal $\rightarrow$ ca instead)

TODO

- Gaussian integers