Group Theory

Monday, August 26, 2019 12:36 PM

Groups!

Def'n: A group is a set G and a closed binary operation $\cdot : G \times G \to G$ satisfying the following:

- Identity

  $\exists e \in G, \quad \forall g \in G$

  $$e \cdot g = g = g \cdot e$$

- Inverses:

  $\forall g \in G, \quad \exists g^{-1}. \quad g \cdot (g^{-1}) = e = (g^{-1}) \cdot g$

- Associativity:

  $\forall g, h, j \in G$

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

Examples of groups:

- $\mathbb{Z}^{+}$ is a group. (Integers under addition)

  $+$ is closed in $\mathbb{Z}$ ✓

  Identity: $0 \qquad 0 + x = x$

  Inverse: [illegible] $\qquad -x + x = 0$

  Associative: ✓

- the natural numbers

- Is $\mathbb{N}^+$ ↙ The natural numbers a group? $0, 1, \ldots$
  - closed? ✓
  - identity: 0 ✓
  - inverse: ✗

- $\mathbb{Z}_n^+$: integers modulo n (n is a natural number)

  $\{0, 1, \ldots\ n-1\}$

  operation $a + b \mod n$

  Ex: $\mathbb{Z}_5 = \{0, 1, \ldots 4\}$

  $2 + 3 = 0 \mod 5$

  $(n - x)$ is inverse of x

  $x + (n-x) = n = 0 \mod n$

- $\mathbb{Z}_n^*$: numbers mod n under mult...?

  $\{\cancel{0}, 1, \ldots\ n-1\}$

  operation: mult mod n

  id: 1 ✓

  closed: ✓

  $\mathbb{Z}_5^*$ inverses: inverse of 3

  $3 \cdot 2 = 6 = 1 \mod 5$ ✓

- $\mathbb{Z}^*$: $\{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, \ldots\ 5\}$

$\mathbb{Z}_6$ ...

id: 1 $\quad 2 \cdot 3 = 0 \bmod 6 \notin \mathbb{Z}_6$ (without 0)

inverse:

- $\mathbb{Z}_n^*$: numbers mod n, relatively prime to n and also 1

- $\mathbb{Z}_p^*$ where p is prime

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

  $|\mathbb{Z}_p^*| = p-1$ ← size of group

- We mostly use finite groups.

- Algebra hierarchy:
  there are names for objects w/ subset of these properties and add'l properties.

Subgroups:

$(G, \cdot)$ is subgroup of $(H, \cdot)$ — "$\cdot$": operator (mult); "of group"

iff $G \subseteq H$ and

$(G, \cdot)$ is a group.

Ex. $\mathbb{Z}_6^+$ Does this have any subgroups?

$\{0,1,2,3,4,5\}$

- $\{0, 1, \ldots 5\}$ $\quad \mathbb{Z}_6^+$ is a subgroup of itself

- $\{0\}$ ← trivial subgroup
- $\{\}$ no ∵ must exist identity
- $\{0, 1\}$ no: not closed
- $\{0, 3\}$: ✓
- $\{0, 2, 4\}$ ✓

- La Grange's Theorem:

  If G is a subgroup of H then $|G|$ divides $|H|$

- Cyclic groups generated by g

$$\langle g \rangle = \{ g^x \mid x \in \mathbb{N} \}$$

$$= \{ g^0, g^1, g^2 \ldots \ldots \}$$

$$g^x = \underbrace{g \cdot g \cdot g \cdots g}_{x \text{ times}}$$

$$g^0 = e$$

Claim $\langle g \rangle$ is a subgroup if G is finite and $g \in G$

- closed $g^a \cdot g^b = g^{a+b}$

$$\underbrace{g \cdot g \cdots g}_{a \text{ times}} \cdot \underbrace{g \cdots\cdots g}_{b \text{ times}} \quad ✓$$

$$(\quad)^{-1} \qquad {}^{-a}$$

— inverses $(g^a) = g$

Subclaim:

$\exists\, n \in \mathbb{N} > 0,\ g^n = e$

$g^0, \dots g^a \quad g^1 \mid g^{a+n}$

$g^{a+n} = \underline{g^a}$

1) — $\underline{(g^a)^{-1}}\ \overline{(g^a)\, g^n} = (g^a)\ \underline{(g^a)^{-1}}$

2) — $g^n = e$

$\overbrace{g \cdots g}^{n \text{ times}} = e$

3) — $g^{(n-a)} \cdot g^a = e$

$\underbrace{g \cdots}_{a}\ \underbrace{\cdots g}_{n-a}$

$-a \bmod n$, where $n = |\langle g \rangle|$ ✓

— Cosets:

Def'n: Let G be a subgroup

and let $h \in H$,

Then h-cosets, written h

are $\{ hg \mid g \in G \}$

Ex: $\mathbb{Z}_6^+ = H = \{0, 1, \dots 5\}$

$G = \{0, 2, 4\}$

The 1-coset of G is $\{1+$

$\{0, 2, 4\}$ $\quad$ 0 1 2

$\{1, 3, 5\}$ $\quad$ 3 4 5

$\vdots$

2-cosets

$\{1, \ldots$

$2+0$

$\{2, \ldots$

Claim: all cosets of G are the same size

Bijection between any two cosets

Let aG and bG be two c...

$\phi_{a,b} : a \cdot G \to b \cdot G$ ✓ $\qquad \phi_{a,b}^{-1} :$

goal $\phi_{a,b}(\phi_{a,b}^{-1}(x)) = x$ ✓

$\phi_{a,b}(x) = b \cdot ((a^{-1}) \cdot x)$ $\qquad \phi$

$\phi_{a,b}(\phi_{a,b}^{-1}(y)) = b\,\underbrace{(a^{-1})a}(b^{-1})y$

$x \in aG$

$\Rightarrow x = ax'$ for some $x' \in G$

$a^{-1}(ax') \in G$

$b(a^{-1}(ax'))\in bG$

So, all cosets of G have the s

So $|G| = |aG| = |bG| \ldots$

$|H| = |G| \cdot (\#$ of cosets) of

- Missing claim:
either $aG = bG$ or $a b$ disj

- Claim: $h \in H \Rightarrow h \in h$

$e \in G$

$h \cdot e \in$

Corollaries relevant to crypto:

1. If $|G|$ is prime,

no nontrivial subgroups

Every element is a generator

$g \in G,\ g \neq e,\ \langle g \rangle = G$

2. Safe primes and schnorr gr

defn: p is a safe prime if $p = 2q +$

Let's look at $\mathbb{Z}_p^*$ for p

$$|\mathbb{Z}_p^*| = p-1 = 2\underline{q}$$

G is nontrivial subgroup of

Suppose $g \in \mathbb{Z}_p^*$,

Case 0: $g = e$ Can we check $|\langle g \rangle| =$

Case 1 $|\langle g \rangle| = \underline{2},$ look at $g^2 = e$

Case 2: $|\langle g \rangle| = 2q$ no

Case 3: $|\langle g \rangle| = q$ $g^q = e$ yes

$p = 7 = 2 \cdot 3 + 1$

$\mathbb{Z}_p$ $\{1, 2, 3, 4, 5, 6\}$

$(\{1, 2, 4\})$ 1, 5, 4, 6, 5

$\{3 \quad 5 \cdot 6\}$

$\langle 3 \rangle = \cancel{a} \langle 1, 3, 2, 6, 4, 5 \rangle = ($

$\langle 6 \rangle = \{1, 6\}$

$\langle 4 \rangle = \{1, 4, 2\}$