Cyclic Groups

Tuesday, September 21, 2021 1:32 PM

Group Theory

- Building crypto on prime order cyclic groups.

- Def'n: A Group is a set G, and a binary operation $\cdot$

  $\cdot : G \times G \to G$

Satisfying:

- Identity:

  $\exists e, \ \forall g \in G, \ e \cdot g = g \cdot e = g$

- Inverses:

  $\forall g \in G \ \exists g^{-1}$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$

- Associative:

  $\forall g, h, j \in G, \ g \cdot (h \cdot j) = (g \cdot h) \cdot j$

Examples:

- $\mathbb{Z}^{+}$ integers under addition.

  $+$ closed integers

  0 id.

  $(-X) + X = 0$

- $\times \ \mathbb{N}^{+}$?

  closed ✓

  assoc ✓

  identity ✓ 0

  inverses $\quad x \in \mathbb{N}$? $\quad 5 + (x) = 0$

- $\mathbb{Z}_n^{+}$ integers mod n $\quad n \in \mathbb{N}$

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

  Inverse: $a + (n-a) = 0 \mod n$.

Q. next time:

$\{1, 2, 3, 4, 5\}$ under $\times$ mod 6.

? integers from 1 to (6-1) under multiplication 6.

- 2 doesn't have an inverse? ~

closure: $2 \times 3 = 6 = 0 \bmod 6 \notin \{1, \ldots 5\}$

— [illegible]

Six with $\{0, \dots 5\}$ under mult.?

— $\mathbb{Z}_n^{\times}$ = integers relatively prime to n under mult.

$\mathbb{Z}_6^{\times}$

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

~~probably~~ an even number

— $|\mathbb{Z}_p^{\times}|$ where p is prime? $p-1$.

$\mathbb{Z}_7^{\times} = \{1, 2, 3, 4, 5, 6\}$ $\quad 4 \cdot 4^{-1} = 4 \cdot 2 = 8 = 1 \bmod 7$

— Subgroups.

Defn: $(G, \cdot)$ is a subgroup of $(H, \cdot)$ (same op) iff $G \subseteq H$ and G is a group.

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

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

$\{0\}$ $\quad \mathbb{Z}_4^{+}$? addition mod 4

✗ $\{0, 1, 2, 3\}$ $\quad 2+3 \notin \mathbb{Z}_4$

$\{0, 1, 5\} \Rightarrow 1+1 = 2 \notin \{0, 1, 5\}$

$\{0, 2, 4\}$ ✓ $\qquad \{0, 3\}$ ✓

— LaGrange's Theorem.

G subgroup of H, (both finite) then $|G|$ divides $|H|$.

— Cauchy's Theorem:

If prime p divides $|H|$, then $|H|$ has a subgroup G, $|G| = p$.

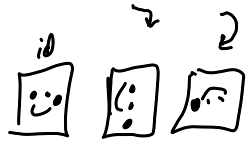
Ex. $|H| = 2 \cdot q$ where q is a prime.

By Cauchy, $\exists\, G$, $|G| = q$ [illegible]

By Lagrange, if G subgroup of $|H|$, Then $|G| \in \{1, 2, q, 2q\}$

- If G is a finite group,
  $a \in G$, is there an m s.t.

  ✓ $a^{m} = e$?

$D_4 =$ 

$\{a, aa, aaa, \ldots\}$
have to have a repeat since G is finite and closed.

So, $a^j = a^k$ for some $j < k$

$\overbrace{a \cdots a}^{j}$ $\qquad a^j = a^j a^{(k-j)}$

$\overbrace{a}^{j} \overbrace{\wedge a}^{(k-j)}$ $\qquad (a^j)^{-1} a^j = (a^j)^{-1} a^j a^{(k-j)}$

$$1 = a^{\underline{(k-j)}}$$

Generators and cyclic groups. $g \in G$, G is finite

$\langle g \rangle$ means $\{ g^n \mid n \in \mathbb{N} \}$

$\langle g \rangle = \{ \underline{1}, g, g^2, \ldots \}$ "the cyclic group generated by g."

- Claim: $\langle g \rangle$ is a subgroup for finite G.

Prove:
- closure g^m and g^n

  $(g^m)(g^n) = g^{m+n}$

- inverses... by above $\boxed{g^m}$, $(g^m)^{-1} = (g^m)^n$ for some n.

  let $a = g^m$
  above says $a^n = 1$ for some n.

  Given g^n, $\underline{g^{|G|-m} \text{ is an inverse.}}$

$\boxed{\text{— Claim! } a^{\underline{|G|}} = 1 \text{ for any } a}$

- Safe Primes.

Let $p = 2q + 1$ where p, q both prime

safe prime

Take $g \in \mathbb{Z}_p^{\times}$. $\leftarrow$ p is 2 bits.

How can we determine $|\langle g \rangle|$?

$|\langle g \rangle| \in \{1, 2, \underline{q, 2q}\}$ by Lagrange.

Since $g^{|\langle g\rangle|}=1$, check $g^2=1$? If so $\{1,g\}=\langle g\rangle$

check $g^q=1$? If so $|\langle g\rangle|=q$.

If not, still $g^{2q}=1$, $|\langle g^2\rangle|=q$.

- $QR_p^\times = \{y\in\mathbb{Z}_p \mid \exists x\in\mathbb{Z}_p\ x^2=y\}$

ex. $\mathbb{Z}_7^\times = \{1,2,3,4,5,6\}$ has a subgroup of size 3? $\quad 7=2\cdot\underline{3}+1$

$2^2 \quad 3^2 \quad 3^2 \quad (-3)\bmod 7^{\,2} \quad 4^2=16=2 \bmod 7$

$\{1,2,4\} \quad \downarrow \quad \downarrow 4^2$

$QR_p^\times=\{1,4,2\}$

For next time: 14.6 Prove for $x,y\in G$

$x^n=y^n$ for $n=|G|$