




Lecture 24

Modular Arithmetic, Groups and Cryptography

CS105: Discrete Structures

Instructor: S. Akshay, Guest Lecturer: Sruthi Sekar

Visual example of Groups



Suppose I give you a solved Rubik's Cube. Imagine every possible way you can scramble it just by turning the faces — no peeling off stickers! What is the mathematical object that consists of all these possible moves?

Set: all possible moves

Operation: Composition of different moves

Defining Groups

- Group $(\mathbb{G},*)$ consists of set $\mathbb{G}$ and operation $* : \mathbb{G}\times\mathbb{G} \longrightarrow \mathbb{G}$ that satisfies:
  1. **Closure Property**: For all $a, b \in \mathbb{G}$, $a * b \in \mathbb{G}$ (denote $*(a, b)$ as $a * b$)
  2. **Associativity**: For all $a, b, c \in \mathbb{G}$, $a * (b * c) = (a * b) * c$
  3. **Identity**: There exists an $e \in \mathbb{G}$ such that $a * e = a = e * a, \forall\, a \in \mathbb{G}$
  4. **Inverse**: For every $a \in \mathbb{G}$, there exists $a^{-1} \in \mathbb{G}$ such that $a * a^{-1} = e = a^{-1} * a$
  5. **Commutativity (additional property)**: For all $a, b \in \mathbb{G}$, $a * b = b * a$
- **Order** of a group $|\mathbb{G}|$: number of elements in $\mathbb{G}$.

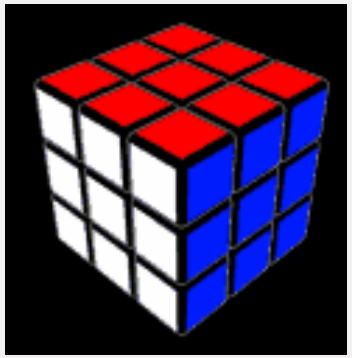
Abelian groups

IS THIS A GROUP? WHAT IS THE ORDER?

✓ $\mathbb{Z}$ =(Integers, +)

✗ $\mathbb{R}$ =(Real Numbers, ×)

See the Group: Rubik's Cube



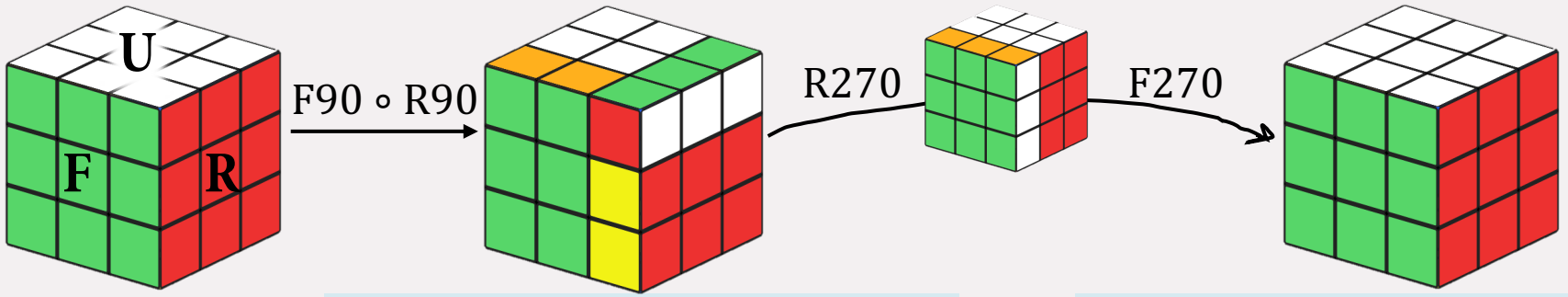
(Set) $\mathcal{R}$: all possible legal moves
(Operation) $\circ$: Composition of different moves

Each move is a combination of base moves:
R,L,U,D,F,B (phases) moved 0°, 90°, 180°, or 270°

Example move: (F90°) ∘ (R90°) (Front90 followed by up Right90)

What you see: Move corresponds to configuration of the cube

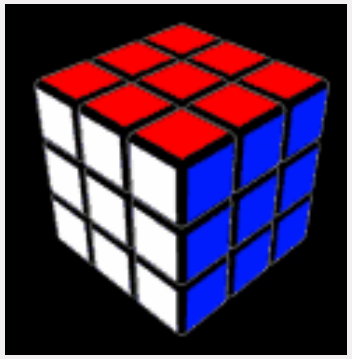
- **Closure**: clearly composition of valid moves results in a valid move in $\mathcal{R}$ each time.
- **Identity**: I = R0 ∘ F0 ∘ U0 ∘ L0 ∘ B0 ∘ D0 (no phase is turned) clearly is the identity!
- **Inverse**: take example of F90 ∘ R90, inverse is R270 ∘ F270 (similarly all moves invertible)



$I \circ (F90 \circ R90) = F90 \circ R90$

$(F90 \circ R90) \circ R270 \circ F270 = I$

See the Group: Rubik's Cube



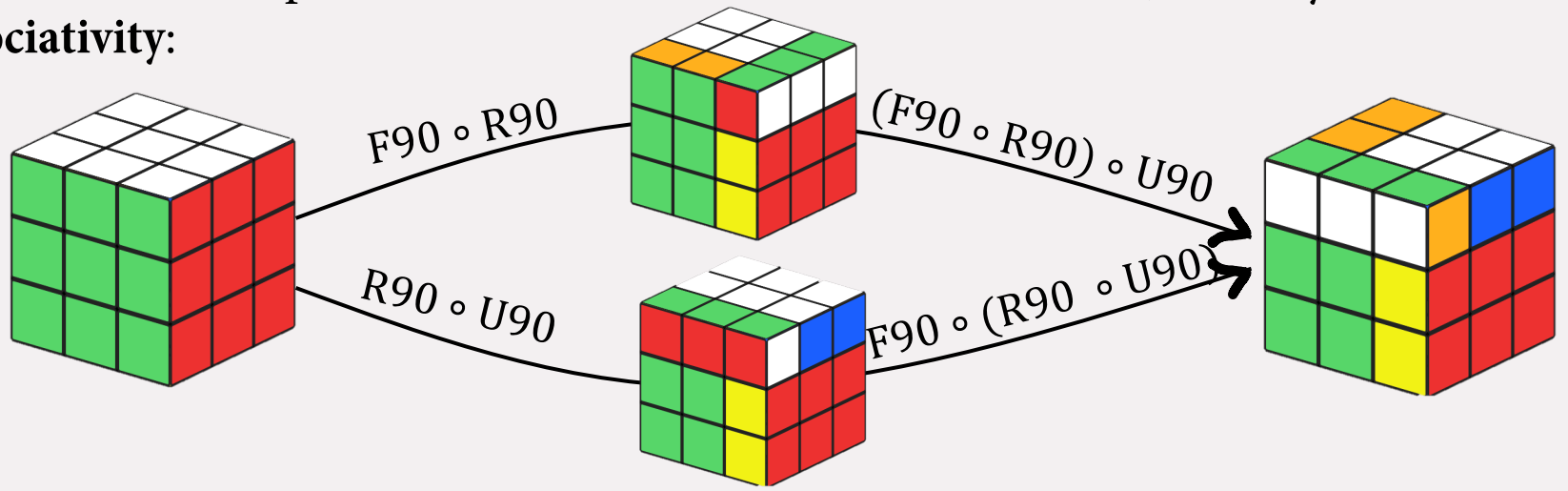
(Set) $\mathcal{R}$: all possible legal moves
(Operation) $\circ$: Composition of different moves

Each move is a combination of base moves:
R,L,U,D,F,B (phases) moved 0°, 90°, 180°, or 270°

Example move: (F90°) ∘ (R90°) (Front90 followed by up Right90)

What you see: Move corresponds to configuration of the cube

- **Closure**: clearly composition of valid moves results in a valid move in $\mathcal{R}$ each time.
- **Identity**: I = R0 ∘ F0 ∘ U0 ∘ L0 ∘ B0 ∘ D0 (no phase is turned) clearly is the identity!
- **Inverse**: take example of F90 ∘ R90, inverse is R270 ∘ F270 (similarly all moves invertible)
- **Associativity**:



Modular Arithmetic

Quotient Remainder Theorem

For any two integers m, n, $m \neq 0$, there is a unique quotient q and remainder r (integers), s.t.

$$n = q \cdot m + r, \qquad 0 \leq r < |m|$$

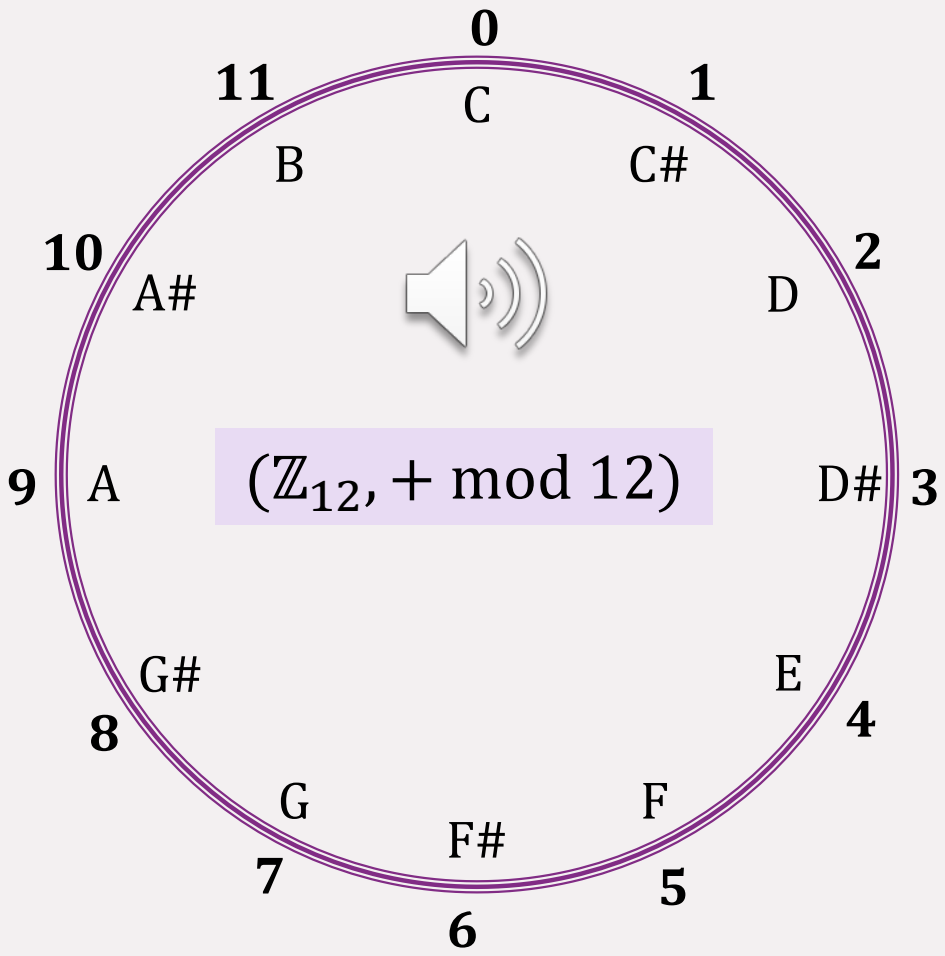
Modulus operation For integers a, n define $a \pmod{n} :=$ the remainder r on dividing a by n

Congruence

For a ***modulus*** n and two integers a, b we say that $a \equiv b \pmod{n}$ if $n|(a - b)$ (n divides $(a - b)$)

Example:

Hear the Group: Semitones

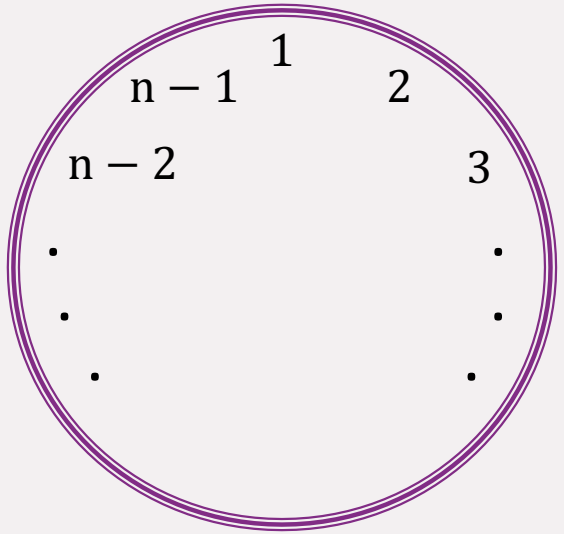


12 SEMITONES

Additive Group $(\mathbb{Z}_n, +\bmod n)$

$\mathbb{Z}_n = \{0,1, \dots, n-1\}$ (all integers modulo n)
For integers a, b: $(a \pmod n + b \pmod n) \pmod n = (a+b) \pmod n$

- **Closure**: easy to see and prove!
- **Associativity**: easy to see and prove!
- **Identity**: 0 (why?)
- **Inverse**: For any $a \in \mathbb{Z}_n$, $(-a) \pmod n = (n-a) \pmod n$
- **Commutativity** : $(a+b) \pmod n = (b+a) \pmod n$
- **Order of the group (denoted by $|\mathbb{Z}_n|$)** : n

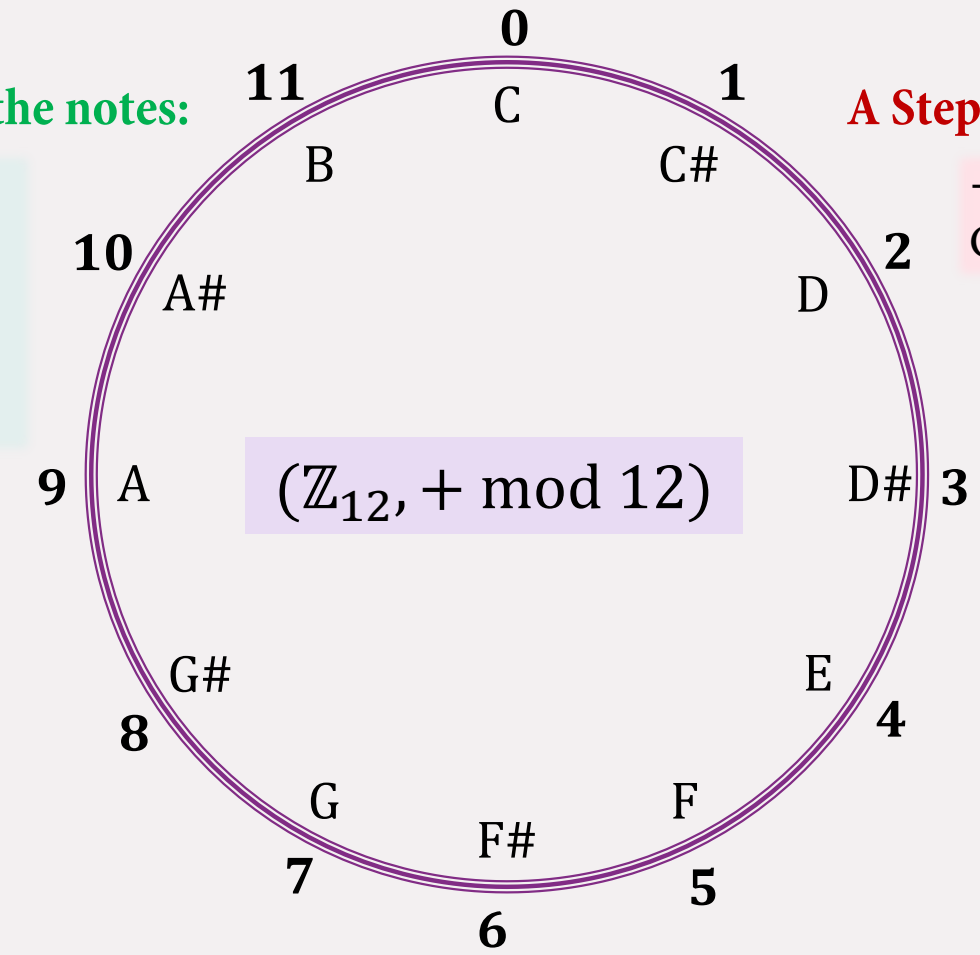


Hear the Group: Semitones

Example of steps which give all the notes:

+1 semitone (move +1 note up)
CC#DD#EFF#GG#AA#BC

+7 semitone (move +7 note up)
CGDAEBF#C#G#D#A#FC



12 SEMITONES

A Step which doesn't give all the notes:

+2 note up each time gives
CDEF#G#A#C

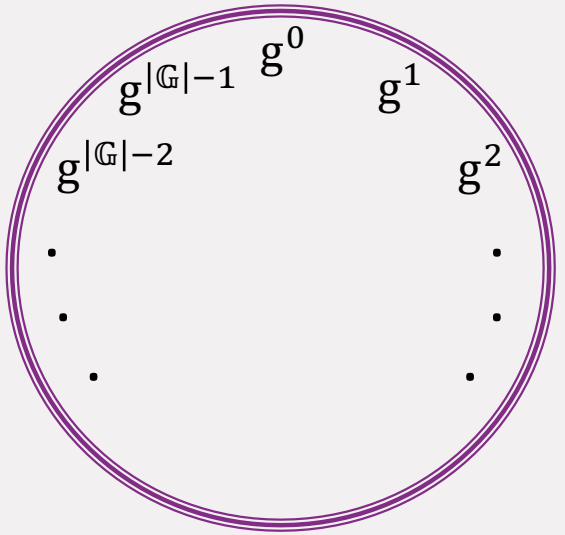
Properties of Groups

Lagrange's Theorem For any $g \in \mathbb{G}, g^{|\mathbb{G}|} = g * g * \cdots * g$ ($|\mathbb{G}|$ times) = identity, i.e., $|g|$ divides $|\mathbb{G}|$

Notation: g^i is used to denote $g * g * \cdots * g$ (i times), $|g|$, the order of $g \in \mathbb{G}$ is $\min_i(g^i = \text{identity})$

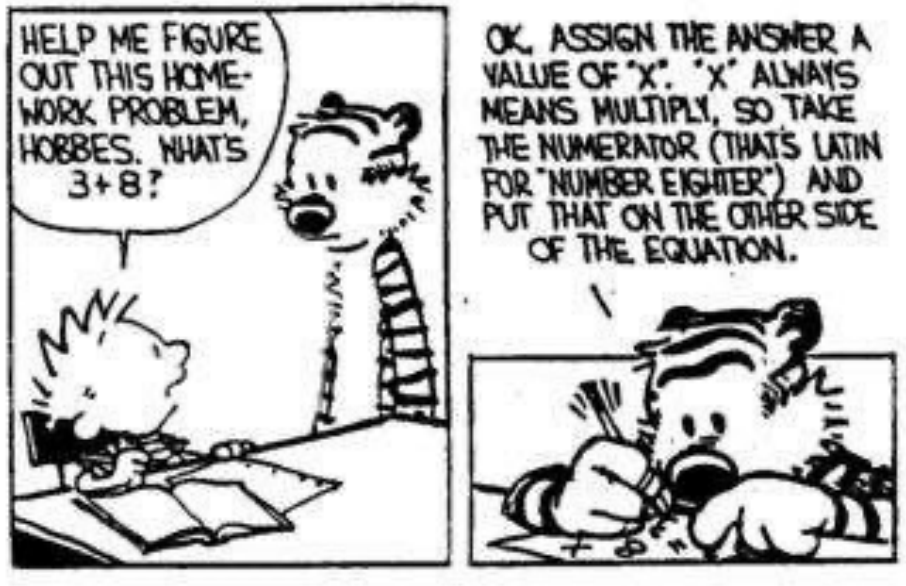
Finite Cyclic Group $\exists\, g \in \mathbb{G}$ such that $\mathbb{G} = \{g^0, g^1, \ldots, g^{|\mathbb{G}|-1}\}$. g is called generator of the cyclic group.

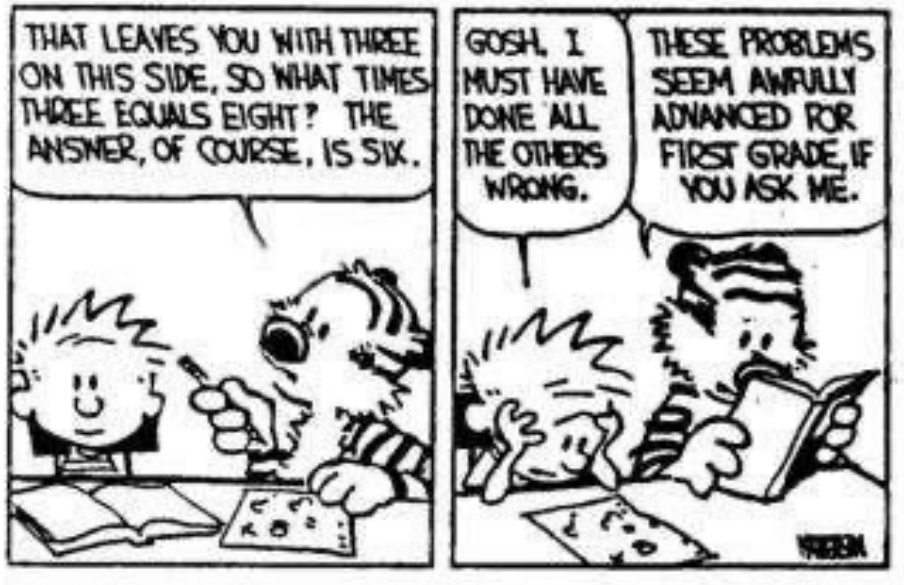
EXAMPLE: $\mathbb{Z}_n$, +mod n : generator?



Theorem: Prime order groups are cyclic

Every group $\mathbb{G}$ with $|\mathbb{G}| = p$, where p is a prime, is cyclic.
Every element other than the identity is a generator of $\mathbb{G}$.





THANK YOU

HW: Spot natural groups around you!