CS201

Mathematics for Computer Science I

Lecture 20

GROUPS

- Groups were originally defined to capture symmetries.
- They capture a structure present in wide varieties of objects, including numbers, permutations etc.
- We study them using the notions of subgroups, quotienting, and homomorphism.

Subgroups

Group $(H, \cdot)$ is a subgroup of group $(G, \cdot)$ if $H \subseteq G$. It is a proper subgroup if $H \subset G$.

- $(2\mathbb{Z}, +)$ is a proper subgroup of $(\mathbb{Z}, +)$.
- Set of $n \times n$ invertible matrices over $\mathbb{Z}/\mathbb{Q}/\mathbb{R}/\mathbb{C}$ with determinant 1 is a proper subgroup of set of $n \times n$ invertible matrices.
- $(\{2^n \mid n \in \mathbb{Z}\}, *)$ is a proper subgroup of $(\mathbb{Q}, *)$.

Subgroup Induced Equivalence Relation

- Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$.
- Define relation R_H on G as: aR_Hb if there exists $h \in H$ such that $a \cdot h = b$.

Theorem

R_H is an equivalence relation on G.

Subgroup Induced Equivalence Relation

- R_H is reflexive: aR_Ha for all a with $a \cdot e = a$, $e \in H$.
- R_H is symmetric:
  - Suppose aR_Hb.
  - This means there exists $h \in H$ with $a \cdot h = b$.
  - Then $b \cdot h^{-1} = a$ and $h^{-1} \in H$ since H is a group.
  - Hence, bR_Ha.
- R_H is transitive:
  - Suppose aR_Hb and bR_Hc.
  - This means there exist $h, h' \in H$ with $a \cdot h = b$ and $b \cdot h' = c$.
  - Then $a \cdot (h \cdot h') = (a \cdot h) \cdot h' = b \cdot h' = c$ and $h \cdot h' \in H$.
  - Hence, aR_Hc.

Quotient Group

- Relation R_H divides G into equivalence classes.
- For any $a \in G$, let $[a]$ represent the equivalence class to which a belongs.
- Consider two equivalence classes $[a]$ and $[b]$.
- Let $a' \in [a]$ and $b' \in [b]$.
- Then $a' \cdot b' \in [a \cdot b]$:
  - We have $a \cdot h = a'$ and $b \cdot h' = b'$ for $h, h' \in H$.
  - So $a' \cdot b' = a \cdot h \cdot b \cdot h' = a \cdot b \cdot (h \cdot h')$.
- Conversely, any element of $[a \cdot b]$ can be written as a product of elements of $[a]$ and $[b]$: $a \cdot b \cdot h = a \cdot (b \cdot h)$.
- Define operation $\circ$ on equivalence classes as:

$$[a] \circ [b] = [a \cdot b].$$

Quotient Group

- Let $[G]$ denote the set equivalence classes of G.
- For $([G], \circ)$, closure clearly holds.
- Associativity holds since

$$([a] \circ [b]) \circ [c] = [a \cdot b] \circ [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \circ ([b] \circ [c]).$$

- Commutativity holds since

$$[a] \circ [b] = [a \cdot b] = [b \cdot a] = [b] \circ [a].$$

- Identity is $[e]$ since $[a] \cdot [e] = [a]$.
- Inverse holds since

$$[a] \circ [a^{-1}] = [a \cdot a^{-1}] = [e].$$

Quotient Group

- Therefore, $([G], \circ)$ is a group.
- It is called quotient group of G.
- It can be viewed as "dividing" G by H since elements of H become identity of $[G]$.
- It is denoted as G/H.

Examples of Quotient Groups

- $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$ with group operation $\oplus$.
  - $[0]$ is the identity.
  - $[1] \oplus [1] = [2] = [0]$.
- $\mathbb{R}/\mathbb{Z}$ represents $[0, 1)$:
  - $[a]$ can be viewed as fractional part of a.
- $\mathbb{R}/\mathbb{Q} \setminus [0]$ can be viewed as the set of all irrational numbers unrelated by rational numbers.

Homomorphisms

- There is a clear equivalence between
  - $\mathbb{Z}/2\mathbb{Z}$ and addition modulo two,
  - $\mathbb{R}/\mathbb{Z}$ and interval $[0, 1)$ with addition limited to fractional parts
- It is formalized through the notion of homomorphism and isomorphism.

Let $(G, \cdot)$ and $(H, \circ)$ be two groups and $\phi : G \mapsto H$ such that for all $a, b \in G$:

$$\phi(a \cdot b) = \phi(a) \circ \phi(b).$$

Function ϕ is called a homomorphism from G to H. If ϕ is also a bijection, then it is called an isomorphism.

Examples

- $\phi : \mathbb{Z}/2\mathbb{Z} \mapsto \{0, 1\}$ is an isomorphism with $\phi([a] \circ [b]) = a + b \pmod 2$.
- $\phi : \mathbb{R}/\mathbb{Z} \mapsto [0, 1)$ is an isomorphism with $\phi([a] \circ [b]) = a + b \pmod 1$.
- Quotienting can also be defined through homomorphisms as follows.
- Let ϕ be a homomorphism from group $(G, \cdot)$ to group $(G', \circ)$, define

  $$H = \{a \mid a \in G, \phi(a) = e'\},$$

  where e is identify of G and e' identity of G'.
- Set H is called kernel of ϕ.

Homomorphism and Quotienting

- H is a subgroup of G:
  - If $a, b \in H$ then $\phi(a \cdot b) = \phi(a) \circ \phi(b) = e_{G'}$.
  - $\phi(e) = \phi(e \cdot e) = \phi(e) \circ \phi(e)$ implying $\phi(e) = e'$.
  - If $a \in H$ then $e' = \phi(e) = \phi(a \cdot a^{-1}) = \phi(a) \circ \phi(a^{-1})$ implying $\phi(a^{-1}) = e'$.
- $\phi(G)$ is a subgroup of G':
  - If $a', b' \in \phi(G)$ with $\phi(a) = a'$ and $\phi(b) = b'$ then $a' \circ b' = \phi(a) \circ \phi(b) = \phi(a \cdot b) \in \phi(G)$.
  - $e' \in \phi(G)$ as shown above.
  - If $a' \in \phi(G)$ with $\phi(a) = a'$ then $e' = \phi(e) = \phi(a \cdot a^{-1}) = a' \circ \phi(a^{-1})$.
  - Therefore, $\phi(a^{-1}) = a'^{-1} \in \phi(G)$.

Homomorphism and Quotienting

- Therefore, ϕ is an onto homomorphism from G to $\phi(G)$.
- If $\phi(a) = a'$ then

$$[a] = \{b \mid b \in G, \phi(b) = a'\}.$$

  - $b \in [a]$ implies $b = a \cdot h$ for some $h \in H$. Therefore, $\phi(b) = \phi(a) \circ \phi(h) = a'$.
  - $\phi(b) = a' = \phi(a)$ implies $e' = \phi(b) \circ \phi(a^{-1}) = \phi(b \cdot a^{-1})$. Therefore, $b \cdot a^{-1} \in H$.
- Therefore, ϕ is an isomorphism between G/H and $\phi(G)$.

Examples Revisited

- Let $\psi : \mathbb{Z} \mapsto \{0, 1\}$ be defined as: $\psi(a) = a \pmod 2$.
  - ψ is a homomorphism with $2\mathbb{Z}$ as its kernel.
  - Hence it is an isomorphism between $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}_2 = \{0, 1\}$ with addition modulo 2.
- Let $\psi : \mathbb{R} \mapsto [0, 1)$ be defined as: $\psi(a) = a \pmod 1$.
- It is easily seen that ψ is an isomorphism between $\mathbb{R}/\mathbb{Z}$ and $[0, 1)$ with addition modulo 1.

Groups via Kernels

A homomorphism $\phi : G \mapsto G'$ gives rise to four groups: its kernel is a subgroup of G, its range is a subgroup of G', quotient of G by kernel and quotient of G' by range of ϕ are two quotient groups.