Second lecture

[Home][PDF]

Topics: Cyclic Groups, Finite Groups, Caylay Tables, Subgroups

Cyclic Groups

A multiplicative group G is called a cyclic group if $\exists a \in G$ s.t $G = \{ a^i : i \in \mathbb{Z} \}$ Then a is called a generator of G And we denote this $G = \langle a \rangle$

All cyclic groups are commutative: $ab = ba$

For a cyclic group the following holds: $a^i \cdot a^j = a^{i+j} = a^{j+i} = a^j \cdot a^i$

Equivelence relation

Let S be a set and $R \subseteq S \times S$

Then R is calles the equivelance relation if the followig holds:

i) Reflexivity:

$$\forall s \in S, (s, s) \in R$$

ii) Symmetry:

$\forall s, t \in S$ if there is a pair $(s, t) \in R$ then there must also be an pair $(t, s) \in R$

iii) Transivity

$\forall s, t, p \in S$ if there exist $(s, t) \in R$ and $(t, p) \in R$ then there exist an $(s, p) \in R$

Equiv Examples

Reflexivity: Property i) $a = a$

Symmetry: Property ii) $a = b \Rightarrow b = a$

Transivity: Property iii) $a = b, b = c \Rightarrow a = c$

Partition of a Set

When we can represent S as a union of subsets

$S = \bigcup_{i \in T} S_{ij}$ where $S_j \neq \emptyset$ and $S_i \subseteq S$ we have that $S_i \cap S_j = \emptyset$ when $i \neq j$

[s] = { $t \in S$: $(s, t) \in R$ } is an equivelence class.

$t \in$ [s] $\Rightarrow$ [t] = [s]

Different equivelence classes gives a partition of S.

Congruent

On the set $\mathbb{Z}$, $\forall a, b \in \mathbb{Z}$,$n \in \mathbb{N}$

a is congruent to b modulo n if $a - b$ is divisible/mutiple by/of n.

That is, $a = b + k \cdot n$ for some $k \in \mathbb{Z}$.

Congruent is an equvilence relation.

i) Reflexitivity: $a \equiv a \bmod n$

ii) Symetry:

$$a, b, k, k' \in \mathbb{Z}$$

$$a \equiv b \bmod n \Rightarrow a = b + k \cdot n$$

$$\Rightarrow b = a + k' \cdot n$$

$$\Rightarrow b = a \bmod n$$

iii) Transivity

$$a, b, c, k, k' \in \mathbb{Z}$$

$$a \equiv b \bmod n, b \equiv c \bmod n$$

$$\Rightarrow a = b + k \cdot n, b = c + k' \cdot n$$

$$\Rightarrow a = (c + k' \cdot n) + k \cdot n$$

$$\Rightarrow a = c + (k' + k) \cdot n$$

$$a = c \bmod n$$

Classes

Considewr the equivalance classes into which the relation of congruence modulo n partitions the set $\mathbb{Z}. These will be the sets:

[0] = $\{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

[1] = $\{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \ldots\}$

[$n - 1$] = $\{\ldots, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\}$

[0] gives 0 for all integers [1] gives 1 for all integers [$n - 1$] gives $n - 1$ for all integers

The generator $\langle a \rangle = \langle n \cdot a; n \in \mathbb{Z}$

$\mathbb{Z}$ = $\langle \cdot$ [i] : $n \in \mathbb{Z} \rangle$

$|\mathbb{Z}| = n$, where n is ther order of $\mathbb{Z}$

Example of a group

$\langle$ [1], [2], ... , [$n-1$] , $+\rangle$

Does this form a group?

We may define the sets of equvelance classes a binary operation $+$:

[$a+b$] = [a] + [b]

Where a and b are any element in their respective sets [a] and [b].

[a'] = [a]

[b'] = [b]

Is this true: [a] + [b] = [a'] + [b']

We wanna know if the are congruent:

$$a' = a + k \cdot n, k \in \mathbb{Z}$$

$$b' = b + k' \cdot n, k' \in \mathbb{Z}$$

Proof:

$$[a] + [a] = [a'] + [b']$$

$$RHS = [a' + b']$$

$$= [(a + k \cdot n) + (b + k' \cdot n)]$$

$$= [a + b + (k + k') \cdot n]$$

$$= [a + b]$$

$$[a] + [b] = [a] + [b]$$

OK it is a congruent.

Assisiative property

$$([a] + [b]) + [c] = [a] + ([b] + [c])$$

$$([a] + [b]) + [c] = [a + b] + [c]$$

$$= [(a + b) + c]$$

$$= [a + (b + c)]$$

$$= [a] + [b + c]$$

$$= [a] + ([b] + [c])$$

$$\square \text{ OK}$$

i) Identity element: [0] + [a] = [$0+a$] = [a]

ii) [a] the inverse is [$-a$]

$$[a] + [-a] = [-a] + [a] = 0$$

Yeas, $\langle$ [1], [2], ... , [$n-1$] , $+\rangle$ and it forms the group:

$\mathbb{Z}$ = $\langle$ { [0], [1], [2], ... , [$n-1$], $+\rangle$ } and is calles the group of integers modulo n.

Finite groups

In general G is finite if it contains a finite number of elements.

Then this number is called the order of $G \to |G|$

Otherwise a group is galles infinite.

G-group has finite numbers $|G| = n$

Caylay tables

For the group $\langle G, * \rangle = \{ a_1, a_2, \ldots, a_n \}$

Caylay table for multiplication

$\cdot$	a_1	a_2	...	a_n
a_1	$a_1 \cdot a_1$	$a_1 \cdot a_2$	...	$a_1 \cdot a_n$
a_2	$a_2 \cdot a_1$	$a_2 \cdot a_2$	...	$a_2 \cdot a_n$
...	...	...		...
a_n	$a_n \cdot a_1$	$a_n \cdot a_2$	...	$a_n \cdot a_n$

Caylay table for addition

$+$	a_1	a_2	...	a_n
a_1	$a_1 + a_1$	$a_1 + a_2$	...	$a_1 + a_n$
a_2	$a_2 + a_1$	$a_2 + a_2$	...	$a_2 + a_n$
...	...	...		...
a_n	$a_n + a_1$	$a_n + a_2$	...	$a_n + a_n$

Example

The Caylay table for the group $\langle \mathbb{Z}, + \rangle$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0

$+$	0	1	2	3	4	5
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Subgroups

Let G be a group and $H \subseteq G$, then H is a subgroup of G.

$\langle H, * \rangle$ is a group, if it has the same operations.

$H \subseteq G$ then the following holds:

i) $\forall a, b \in H \Rightarrow a \cdot b \in H$ ii) $e \in H$ iii) $\forall a \in H$, there is a $a^{-1} \in H$

$\{ e \}$ is a subgroup containg only e and is called the trivial group

$\{ G \}$ is a subgroup of itself.

If H is a subgroup of G, s.t $H \neq \{ e \}$, $H \neq G$ then H is called a non trivial group.

Subgroups are necessarily cyclic.

$\forall a \in G \langle a \rangle = \{ a^i : i \in \mathbb{Z}\}$ is called a subgroup generated by a

$$a^i \cdot a^j = a^{i+j}$$

$$a^0 = e$$

$$a^i = a^{-i}$$

The properties above leads to:

$$\rightarrow a^i \cdot a^{-i} = a^{i+(-i)} = a^0 = e$$

If $|\langle a \rangle| = n$ is finite and , $n \in \mathbb{N} \Rightarrow n$ is the order of element a

How to find the order

The smallest positive integer d s.t $a^d = e$ is the order of a.

$\langle a \rangle = \{ a^0, a^1, a^2, \ldots, a^{d-1} \} \rightarrow$ All elements are different

$a^i = a^j$ where $0 \leq i < j \leq d-1$ we have that

$a^{j-i} = a^0 = e$