18MAA242 Lecture 15

Subgroups, Order, Cyclic Groups

A subgroup of a group G is a subset which is itself a group (with the same operation).

More precisely:

Definition: A subset $H \subset G$ of a group G is a subgroup of G if:

1) $x, y \in H \Rightarrow xy \in H$ ("H is closed under the operation on G")
2) $e \in H$ where e = identity element of G
3) $x \in H \Rightarrow x^{-1} \in H$ where x^{-1} = inverse of x in G.

Examples: The following are all subgroups:

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (all with operation $+$)
- Even numbers $\underset{\{2n \mid n \in \mathbb{Z}\}}{\overset{}{2\mathbb{Z}}} \subset \mathbb{Z}$ with $+$

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$$

- $SL(2,\mathbb{Z}) \subset SL(2,\mathbb{R}) \subset GL(2,\mathbb{R})$

$SL(2,\mathbb{Z})$ " = det = 1, entries in $\mathbb{Z}$; $SL(2,\mathbb{R})$ " = det = 1; $GL(2,\mathbb{R})$ " = det $\neq 0$.

- Alternating group $A_n \subset S_n$.

A special kind of subgroup:

Definition: For an element $g \in G$, the set

$\langle g \rangle =: \{ g^n , n \in \mathbb{Z} \} \subset G$ (where $g^0 = e$, $g^{-n} = (g^{-1})^n$)

is called the cyclic subgroup of G generated by the element g.

If there is an element $g \in G$ such that $G = \langle g \rangle$, then we say G is cyclic, and g is a generator of G.

Example: $\mathbb{Z}$ is cyclic with generator 1:

- if $n > 0$ then $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$
- if $n < 0$ then $n = \underbrace{(-1) + \cdots + (-1)}_{-n \text{ times}}$

(and -1 is the inverse of 1).

Order

For a finite group G, the order of G means the number of elements in G. We write it $|G|$.

There is another meaning of "order" that applies to elements of a group:

Definition: The order $\mathrm{ord}(g)$ of $g \in G$ is the smallest natural number k such that $g^k = e$.
If no such k exists, we say g has infinite order.

Example: $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$, multiplication mod 5.

Orders of elements:
- $1^1 = 1 = e \Rightarrow \mathrm{ord}(1) = 1$
- $2^2 = 4$, $2^3 = 8 \overset{\text{mod } 5}{=} 3$, $2^4 = 3 \cdot 2 = 6 \overset{\text{mod } 5}{=} 1$

$$\Rightarrow \mathrm{ord}(2) = 4$$

- $3^2 = 9 = 4$, $3^3 = 3 \cdot 4 = 2$, $3^4 = 3 \cdot 2 = 1$

$$\Rightarrow \mathrm{ord}(3) = 4.$$

- $4^2 = 1 \Rightarrow \mathrm{ord}(4) = 2$.

We can say:
$$\langle 1 \rangle = \{1\}$$
$$\langle 2 \rangle = \langle 3 \rangle = \{1, 2, 3, 4\} = \mathbb{Z}_5^\times$$
$$\langle 4 \rangle = \{1, 4\}.$$

So $\mathbb{Z}_5^\times$ is cyclic, generated by either 2 or 3.

Remarks:

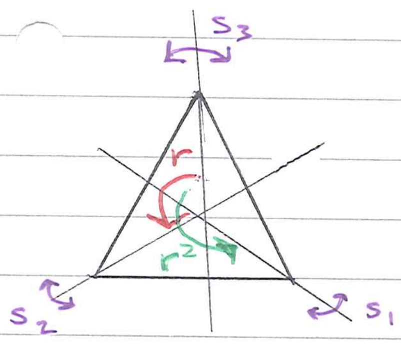
a) Another way to describe order of an element: the order of $g \in G$ is the order of the cyclic subgroup it generates: $\mathrm{ord}(g) = |\langle g \rangle|$.

b) G is cyclic $\Leftrightarrow \exists\, g \in G$ such that $\langle g \rangle = G$

By a) this is $\Leftrightarrow \exists\, g \in G$ such that $\mathrm{ord}(g) = |G|$ (for finite groups G).

Example: Dihedral group D_3

$$D_3 = \{e, \underbrace{r}_{\text{rotation by } 2\pi/3}, \underbrace{r^2}_{\text{rotation by } 4\pi/3}, \underbrace{s_1, s_2, s_3}_{\text{reflections}}\}$$



Orders of elements:

- $\mathrm{ord}(e) = 1$ (always true)
- $\mathrm{ord}(r) = \mathrm{ord}(r^2) = 3$
- $\mathrm{ord}(s_1) = \mathrm{ord}(s_2) = \mathrm{ord}(s_3) = 2$.

Cyclic subgroups:
- $\langle e \rangle = \{e\}$ (always true)
- $\langle r \rangle = \{e, r, r^2\} = \langle r^2 \rangle$

- $\langle s_i \rangle = \{e, s_i\}$ for $i = 1, 2, 3$.

Notice: D_3 is not cyclic, since there are no elements of order 6 $(= |D_3|)$.

Example: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
(with addition mod 6).

Orders of elements: note identity is 0, so we are looking for smallest k such that

$$g^k := \underbrace{g + \cdots + g}_{k \text{ times}} \pmod 6 = 0.$$

- $\operatorname{ord}(0) = 1$ as always

- $1^2 = 1+1 = 2$, $1^3 = 1+1+1 = 3$, $1^4 = 4$,
  $1^5 = 5$, $1^6 = 0$ $\Rightarrow$ $\operatorname{ord}(1) = 6$.

- $2^2 \overset{= 2+2}{=} 4$, $2^3 = 4+2 = 0$ $\Rightarrow$ $\operatorname{ord}(2) = 3$

- $3^2 = 3+3 = 0$ $\Rightarrow$ $\operatorname{ord}(3) = 2$

- $4^2 = 4+4 = 2$, $4^3 = 2+4 = 0 \Rightarrow ord(4) = \underline{3}$

- $5^2 = 5+5 = 4$, $5^3 = 4+5 = 3$,

  $5^4 = 3+5 = 2$, $5^5 = 2+5 = 1$, $5^6 = 1+5 = 0$

  $\Rightarrow ord(5) = \underline{6}$.

Cyclic subgroups:

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \langle 5 \rangle = \underline{\mathbb{Z}_6}$

$\langle 2 \rangle = \langle 4 \rangle = \underline{\{0, 2, 4\}}$

$\langle 3 \rangle = \underline{\{0, 3\}}$

So $\mathbb{Z}_6$ is cyclic, generated by

$\underline{1}$ or $\underline{5}$

Remark: In all cases, $ord(g)$ divides $|G|$.

Do you think this is a coincidence?