# Lecture 16: Cosets; Lagrange theorem; orbits;

Friday, November 07, 2014
12:18 PM

**Exp.** • $H \curvearrowright G$ left multiplication. Then

$$O(g) = \{hg \mid h \in H\} =: Hg$$ (a right coset of $H$.)

• $G \curvearrowleft H$ right multiplication. Then

$$O(g) = \{gh \mid h \in H\} = gH$$ (a left coset of $H$ in $G$.)

$H\backslash G :=$ the set of all right cosets.

## Basic Properties of Orbits

Let $G \curvearrowright X$. The following properties are equivalent:

① $O(x_1) \cap O(x_2) \neq \emptyset$.

② $x_1 \in O(x_2)$ ②′ $x_2 \in O(x_1)$.

③ $O(x_1) = O(x_2)$

**Pf.** ① $\Rightarrow$ ② $x_0 \in O(x_1) \cap O(x_2) \Rightarrow \exists g_1, g_2 \in G$,

$$x_0 = g_1 \cdot x_1 = g_2 \cdot x_2$$

$$\Rightarrow (g_1^{-1} g_2) \cdot x_2 = x_1$$

$(g_1^{-1}) \cdot (g_1 \cdot x_1) = (g_1^{-1}) \cdot g_2 \cdot x_2$

$\Rightarrow (g_1^{-1} g_1) \cdot x_1 = (g_1^{-1} g_1) \cdot x_2$

$$\Rightarrow (g_1^{-1}g_1)\cdot x_1 = (g_1^{-1}g_2)\cdot x_2$$

$$\Rightarrow e\cdot x_1 = (g_1^{-1}g_2)\cdot x_2$$

$$\Rightarrow x_1 = (g_1^{-1}g_2)\cdot x_2$$

$$\Rightarrow x_1 \in O(x_2).$$

② $\Rightarrow$ ③ $x_1 \in O(x_2) \Rightarrow x_1 = g_0 \cdot x_2$

$x \in O(x_1) \Longrightarrow x = g\cdot x_1 \Rightarrow x = g\cdot(g_0\cdot x_2)$

$= (gg_0)\cdot x_2 \in O(x_2).$

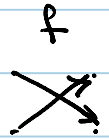
So $O(x_1) \subseteq O(x_2)$.

$x_2 = g_0^{-1}\cdot x_1 \Rightarrow x_2 \in O(x_1) \Rightarrow O(x_2) \subseteq O(x_1)$ $\Rightarrow$ ✓

③ $\Rightarrow$ ① $x_1 \in O(x_1) = O(x_2) \Rightarrow x_1 \in O(x_1)\cap O(x_2)$. ∎

**Cor.** $G\backslash X = \{O(x) \mid x \in X\}$ is a partition of $X$.

**Exp.** $G = \langle f \rangle \curvearrowright \{1,2,3,4,5\}$




$O(1) = \{1,2\}$

$O(2) = O(1)$

$O(3) = \{3,5,4\}$

$O(4) = O(5)$

$$G\backslash X = \{\{1,2\},\{3,4,5\}\}$$

**Cor.** Let $G \curvearrowright X$. Set $x_1 \sim x_2 \iff \exists\, g \in G,\ x_1 = g \cdot x_2$

Then ① $\sim$ is an equivalent relation, i.e.

1a $x \sim x$.

1b $x_1 \sim x_2 \Rightarrow x_2 \sim x_1$

1c $x_1 \sim x_2$ and $x_2 \sim x_3 \Rightarrow x_1 \sim x_3$

② The equivalency class $[x]_\sim := \{x' \in X \mid x \sim x'\}$

$= O(x)$.

③ $G\backslash X = \{[x]_\sim \mid x \in X\}$.

**Pf.** From the definition of $\sim$ we have

$$x_1 \sim x_2 \iff x_1 \in O(x_2) \iff O(x_1) = O(x_2).$$

Now all the claims can be easily verified. ∎

**Cor.** Let $G \curvearrowright X$ and $X$ be a finite set.

$$\Rightarrow |X| = \sum_{O \text{one} \in G\backslash X} |O(x)|.$$

**Thm** Let $G$ be a finite group and $H \leq G$. Then

$$|G| = |H| \, |H \backslash G| \text{ ; in particular } |H| \mid |G|.$$

**Pf.** Consider $H \curvearrowright G$ by left multiplication.

We prove that any orbit $O(g) = Hg$ has exactly $|H|$- many elements. And so by the previous corollary we get: $|G| = \sum_{O(g) \in H \backslash G} |O(g)| = |H| \, |H \backslash G|$.

**Claim** $H \longrightarrow Hg$, $h \longmapsto hg$ is a bijection. And so $|H| = |Hg|$.

**Pf of the claim.** By the definition of $Hg$, it is onto. So it is enough to show it is 1-1:

$$h_1 g = h_2 g \Rightarrow (h_1 g) g^{-1} = (h_2 g) g^{-1}$$

$$\Rightarrow h_1 (g g^{-1}) = h_2 (g g^{-1})$$

$$\Rightarrow h_1 = h_2. \quad \blacksquare$$

**Cor.** Let $G$ be a finite group. Then $\forall g \in G$ we

$|G|$

Cor. Let $G$ be a finite group. Then $\forall g \in G$ we have $g^{|G|} = e$.

Pf. $|\langle g \rangle| \mid |G| \Rightarrow o(g) \mid |G|$

$\Rightarrow g^{|G|} = e$. ∎

Cor. $\forall a, n \in \mathbb{Z}^+$, $\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Pf. $\gcd(a,n) = 1 \Rightarrow [a]_n \in \mathbb{Z}_n^\times$

$\Rightarrow [a]_n^{|\mathbb{Z}_n^\times|} = [1]_n$

$\Rightarrow [a^{\varphi(n)}]_n = [1]_n$

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$. ∎

Def. $[G:H] := |{}_H\backslash G|$ is called the index of $H$ in $G$.

Proposition. Let $G \curvearrowright X$, and $x_0 \in X$.

(a) $G_{x_0} := \{g \in G \mid g \cdot x_0 = x_0\}$

(Stabalizer of $x_0$ in $G$) is a subgroup of $G$.

(b) $G/G_{x_0} \xrightarrow{\theta} O(x_0)$,

$\theta(g G_{x_0}) := g \cdot x_0$ is a well-defined bijection.

In particular, $|O(x_0)| = [G : G_{x_0}]$.

Pf. (a) $e \in G_{x_0} \neq \emptyset$. Subgp Criteria

$$g_1, g_2 \in G_{x_0} \Rightarrow g_1 \cdot x_0 = g_2 \cdot x_0 = x_0$$

$$\Rightarrow (g_2^{-1} g_1) \cdot x_0 = x_0$$

$$\Rightarrow g_2^{-1} g_1 \in G_{x_0}.$$

(b) well-defined. $g_1 G_{x_0} = g_2 G_{x_0} \Rightarrow$

$g_1 = g_2 g_0$ for some $g_0 \in G_{x_0} \Rightarrow$

$$g_1 \cdot x_0 = (g_2 g_0) \cdot x_0 = g_2 \cdot (g_0 \cdot x_0) = g_2 \cdot x_0.$$

1-1. $g_1 \cdot x_0 = g_2 \cdot x_0 \Rightarrow (g_1^{-1} g_2) \cdot x_0 = x_0$

$$\Rightarrow g_0 = g_1^{-1} g_2 \in G_{x_0}$$

$$\Rightarrow g_1 g_0 = g_2$$

$$\Rightarrow g_2 \in g_1 G_{x_0}$$

$$\Rightarrow g_1 G_{x_0} = g_2 G_{x_0}.$$

$\Rightarrow g_1 G_{x_0} = g_2 G_{x_0}$.

Onto. It is clear from the definition of $O(x_0)$. ∎

**Def.** $X^G := \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$

The set of fixed points.

**Cor.** $|X| = |X^G| + \sum_{\substack{O(x) \in \frac{X}{G} \\ x \notin X^G}} [G : G_x]$.