Lecture 14: cyclic subgroups and order of elements.

Wednesday, November 05, 2014
10:04 AM

In the previous lecture we showed:

- $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$

Def. . order of $a = o(a) := \min\{i \in \mathbb{Z}^+ \mid a^i = e\}$

if $a^i \neq e$ for $i \in \mathbb{Z}^+$, then $o(a) = \infty$.

. a is called torsion if $o(a) < \infty$.

Proposition. Let $a \in G$ be a torsion element. Then

① $K_a := \{n \in \mathbb{Z} \mid a^n = e\}$ is a subgroup of $\mathbb{Z}$.

② $K_a = o(a)\mathbb{Z}$.

Pf ① $0 \in K_a$. So by Subgroup Criteria it is enough to show: $n, m \in K_a \overset{?}{\Rightarrow} n - m \in K_a$

$$\left.\begin{array}{l} a^n = e \\ a^m = e \end{array}\right\} \Rightarrow a^{n-m} = (a^n)(a^m)^{-1} = (e)(e)^{-1} = e.$$

② We proved that a non-zero subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$ where d is the smallest non-zero element of the subgp. So $K_a = o(a)\mathbb{Z}$. ∎

Lemma. $a^m = a^n \iff m \equiv n \pmod{o(a)}$

Pf. $a^m = a^n \iff a^{m-n} = e$

$$\iff m-n \in K_a$$

$$\iff o(a) \mid m-n$$

$$\iff m \equiv n \pmod{o(a)}.$$ ∎

Proposition. Let $a \in G$ be a torsion element. Then

$$\theta : \mathbb{Z}_{o(a)} \longrightarrow \langle a \rangle,$$

$$\theta([n]_{o(a)}) := a^n$$

is a (well-defined) bijection.

Pf. well-defined and 1-1: $[n_1]_{o(a)} = [n_2]_{o(a)} \iff n_1 \overset{o(a)}{\equiv} n_2$

$$\iff a^{n_1} = a^{n_2}$$

Onto since $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$. ∎

Remark. $\theta([n]_{o(a)} + [m]_{o(a)}) = \theta([n+m]_{o(a)}) = a^{n+m}$

$$= a^n \cdot a^m$$

$$= \Theta([n]_{o(a)}) \cdot \Theta([m]_{o(a)}).$$

Cor. $|\langle a\rangle| = o(a)$. And $\langle a\rangle = \{e, a, a^2, \dots, a^{o(a)-1}\}$.

Proposition. Let $a \in G$ be torsion. Then

$$o(a^m) = \frac{o(a)}{\gcd(m, o(a))}.$$

Pf. Let $o(a) = d$ and $o(a^m) = d'$.

$$a^{mk} = e \iff d \mid mk$$

$$\iff \frac{d}{\gcd(m,d)} \,\Big|\, \frac{m}{\gcd(m,d)} k$$

$$\iff \frac{d}{\gcd(m,d)} \,\Big|\, k.$$

So $d' = \dfrac{d}{\gcd(m,d)}$. ∎

Cor. ① $\langle a^m\rangle = \langle a\rangle \iff \gcd(m, o(a)) = 1$.

So there are $\varphi(o(a))$ many of them.

② $d \mid o(a) \Rightarrow \exists\, a' \in \langle a\rangle$ s.t. $o(a') = d$.

(notice. $o(a^{o(a)/d}) = \dfrac{o(a)}{\gcd(o(a), o(a)/d)} = \dfrac{o(a)}{o(a)/d} = d.$)

Problem. $\left.\begin{array}{l} a,b\in G \text{ torsion, } ab=ba \\ \gcd(o(a),o(b))=1 \end{array}\right\} \Rightarrow o(ab)=o(a)\,o(b)$

Solution. Let $o(a)=n$, $o(b)=m$, and $o(ab)=\ell$.

$\Rightarrow (ab)^{\ell}=e \Rightarrow a^{\ell}=b^{-\ell}$

$\Rightarrow o(a^{\ell})=o(b^{-\ell})$

$$\left.\begin{array}{l} \Rightarrow \dfrac{n}{\gcd(n,\ell)}=\dfrac{m}{\gcd(m,\ell)} \\ \gcd(n,m)=1 \\ \dfrac{n}{\gcd(n,\ell)}\,\Big|\, n \text{ and } \dfrac{m}{\gcd(m,\ell)}\,\Big|\, m \end{array}\right\} \Rightarrow \begin{cases} n=\gcd(n,\ell) \\ m=\gcd(m,\ell) \end{cases}$$

$$\Rightarrow \left.\begin{array}{l} n\mid \ell \\ m\mid \ell \end{array}\right\} \Rightarrow \left.\begin{array}{l} \operatorname{lcm}(m,n)\mid \ell \\ \gcd(m,n)=1 \end{array}\right\} \Rightarrow mn\mid \ell. \quad \text{I}$$

$$(ab)^{mn}=a^{mn}b^{mn}=(a^{n})^{m}\cdot(b^{m})^{n}=e \Rightarrow \ell\mid mn \quad \text{II}$$

So by I, II we have $mn=\ell$. ∎

Question. Is there a group s.t. $o(a), o(b)<\infty$,

but $o(ab)=\infty$?

Answer. Yes, consider symmetries of $\mathbb{Z}$:

Let $f_0 : \mathbb{Z} \to \mathbb{Z}$ be $f_0(x) = -x$ (reflection about 0)

$f_1 : \mathbb{Z} \to \mathbb{Z}$ be $f_1(x) = -(x-1)+1$ (reflection about 1)

$$(f_1 \circ f_0)(x) = f_1(-x) = -(-x-1)+1$$

$$= x+2. \quad \text{translation by } 2$$

$\Longrightarrow o(f_0) = o(f_1) = 2$ and $o(f_1 \circ f_0) = \infty$. $\blacksquare$