# L10: Subgroups of finite cyclic groups

**Prop** Let $G = \langle x \rangle$ be a cyclic group of order $n$ ($|G| = n$). Then

i) $\langle x^\ell \rangle = \langle x^{(\ell,n)} \rangle$

ii) $|\langle x^\ell \rangle| = \frac{n}{(\ell,n)}$

In particular, there is a one-to-one correspondence

$$\{\text{positive divisors of } n\} \leftrightarrow \{\text{subgroups of } G\}$$
$$\begin{matrix} \Psi \\ d \end{matrix} \quad \longmapsto \quad \langle x^d \rangle$$

**Pf** i) "$\subseteq$" write $d = (\ell,n)$. In part $\exists k$ $\ell = d \cdot k$ and thus $x^\ell = x^{d \cdot k} \in \langle x^d \rangle$. Hence $\langle x^\ell \rangle \subseteq \langle x^d \rangle$

"$\supseteq$" By Euclidean algorithm $d = a\ell + bn$ and we have
$x^d = x^{a\ell + bn} = (x^\ell)^a \cdot \underbrace{(x^n)^b}_{= e} = (x^\ell)^a \in \langle x^\ell \rangle$ and thus $\langle x^d \rangle \subseteq \langle x^\ell \rangle$.

ii) By i) we can assume $\ell = d \mid n$. We find the smallest $k$ s.t. $(x^d)^k = e$ i.e. the smallest $k$ s.t. $dk = mn = m d \underbrace{\frac{n}{d}}_{\in \mathbb{Z}}$ for some $m \in \mathbb{Z}$

$\Leftrightarrow k = m \cdot \frac{n}{d}$

$\Rightarrow k = \frac{n}{d}$.

Define $\varphi : \{\text{divisors of } n\} \to \{\text{subgroups of } G\}$
$$d \longmapsto \langle x^d \rangle$$

We have seen every subgroup is cyclic i.e. of the form $\langle x^\ell \rangle$ for some $\ell$ and by i) $\langle x^\ell \rangle = \langle x^{(\ell,n)} \rangle$ and $(\ell,n) \mid n$. Hence $\varphi$ is surj.

Suppose $\varphi(d_1) = \varphi(d_2)$. But then by ii) we have
$\frac{n}{d_1} = \frac{n}{d_2} \Rightarrow d_1 = d_2$. Thus $\varphi$ is inj.

$\square$

**Rmk** We have also shown that $G$ has a unique subgroup of order $d$ for any pos divisor of $n$.

**Cor** $x \in G$ and $\langle x^k \rangle = \langle x \rangle$, then $(k, |x|) = 1$.

**Pf** $|\langle x^k \rangle| = \frac{|x|}{(k,|x|)} \stackrel{!}{=} |\langle x \rangle| \Rightarrow (k,|x|) = 1$

**Def** Let $G$ be a group. We define the group of automorphisms of $G$ to be $\mathrm{Aut}(G) = \{ \varphi : G \to G \mid \varphi \text{ a group isom} \}$

**Lemma** $\mathrm{Aut}(G) \leq S_G$, in part $\mathrm{Aut}(G)$ is a group wrt composition.

**Pf** Exercise

"multiplicative group of integers mod $n$"

**Prop** $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^\times := \{ k \in \mathbb{Z}/n\mathbb{Z} \mid (k,n) = 1 \}$

with group multiplication $\bar{k}_1 \cdot \bar{k}_2 = \overline{k_1 \cdot k_2}$ and unit $\bar{1}$

**Pf** Define $\Psi : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}^\times$

$\varphi \longmapsto \varphi(\bar{1})$

- $\Psi$ is well-defined: $\langle 1 \rangle = \mathbb{Z}/n\mathbb{Z} \Rightarrow \langle \varphi(1) \rangle = \mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$

  $\Rightarrow (\varphi(1), n) = 1$.

- $\Psi$ inj: suppose $\varphi$ is st. $\varphi(\bar{1}) = \bar{1}$ but then $\varphi(\bar{k}) = \varphi(k \cdot \bar{1}) = k \cdot \varphi(\bar{1})$

  $= k \cdot \bar{1} = \bar{k}$.

- $\Psi$ surj: Let $\ell \in \mathbb{Z}/n\mathbb{Z}^\times$ then $\langle \bar{\ell} \rangle = \langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ and thus $\ell$ has order $n$,

  hence $\varphi_\ell(k) := \overline{k\ell}$ defines a group isom $\mathbb{Z}/n\mathbb{Z} \to \langle \bar{\ell} \rangle$

  st. $\varphi_\ell(1) = \ell$.

Since $\Psi$ is a bijection we have endowed $\mathbb{Z}/n\mathbb{Z}^\times$ with the structure of a group. It remains to check the claimed formula for the group multiplication.

I.e. $\Psi(\Psi^{-1}(\ell_1) \circ \Psi^{-1}(\ell_2)) = \Psi^{-1}(\ell_1)(\Psi^{-1}(\ell_2)(\bar{1}))$

$= \Psi^{-1}(\ell_1)(\bar{\ell}_2) = \overline{\ell_1 \ell_2}$. $\square$

**Rmk** We have also shown that if $(k,n) = 1$ then $\exists\, k'$ st. $kk' = 1 \bmod n$.

this is the result of Euclidean algorithm $\exists\, a, b$ st. $ak + bn = 1$

$k' = k$.