5F

Setning 15 $G = \mathbb{Z}_n$

(a) $\langle \bar{s} \rangle \subseteq \mathbb{Z}_n$. La $\gcd(s,n) = d$. Da er

$$\langle \bar{s} \rangle = \{\bar{0}, \bar{d}, 2\cdot\bar{d}, \dots, (\tfrac{n}{d}-1)\bar{d}\} = \langle \bar{d} \rangle$$

Spesielt, $|\langle \bar{s} \rangle| = \frac{n}{d}$.

(b) $\langle \bar{s} \rangle = \langle \bar{t} \rangle \iff \gcd(s,n) = \gcd(t,n)$.

Bevis: (a) La $d = \gcd(s,n)$.

(1) $\langle \bar{s} \rangle = \langle \bar{d} \rangle$: $d \mid s$ slik at $s = dq$ og $\bar{s} \in \langle \bar{d} \rangle$.

dvs. $\langle \bar{s} \rangle \subseteq \langle \bar{d} \rangle$. Motsatt inklusjon: Har at $d = sx + ny$ for for $x, y \in \mathbb{Z}$. Dette gir

$$\bar{d} = \overline{sx} = x \cdot \bar{s} \text{ og } \bar{d} \in \langle \bar{s} \rangle.$$

dvs. $\langle \bar{d} \rangle \subseteq \langle \bar{s} \rangle$ og $\langle \bar{s} \rangle = \langle \bar{d} \rangle$.

Spesielt er

$$|\bar{s}| = |\bar{d}|$$

Har at $\frac{n}{d} \cdot \bar{d} = \overline{\frac{n}{d} \cdot d} = \bar{n} = \bar{0}$, slik at $|\bar{d}| \leq \frac{n}{d}$ (Lemma 13). Anta at $m \cdot \bar{d} = \bar{0}$ med $m > 0$. Da er $md = n \cdot q$ for en $q \in \mathbb{Z}$. dvs. $m = \frac{n}{d} \cdot q$ og $\frac{n}{d} \mid m \Rightarrow m \geq \frac{n}{d}$

$$\Rightarrow |\bar{d}| \geq \frac{n}{d} \text{ og } |\bar{d}| = |\bar{s}| = \frac{n}{d}.$$

Lemma 13 $\Rightarrow \langle \bar{s} \rangle = \{\bar{0}, \bar{d}, 2\bar{d}, \dots, (\frac{n}{d}-1)\bar{d}\}$.

(b) Anta at $\langle \bar{s} \rangle = \langle \bar{t} \rangle$. Fra (a)

$$\Downarrow$$

$$\frac{n}{\gcd(s,n)} = |\langle \bar{s} \rangle| = |\langle \bar{t} \rangle| = \frac{n}{\gcd(t,n)}$$

$$\Longrightarrow \gcd(s,n) = \gcd(t,n).$$

<u>Motsatt</u>: Anta at $\gcd(s,n) = \gcd(t,n)$

Fra (a) har vi

$$\langle \bar{s} \rangle = \langle \overline{\gcd(s,n)} \rangle = \langle \overline{\gcd(t,n)} \rangle = \langle \bar{t} \rangle. \quad \square$$

<u>Merk</u>: Får alle undergruppene av $\mathbb{Z}_n$ ved å se på $\langle \bar{d} \rangle$, der $d \mid n$.