Lemma 59 R ring med $1 \neq 0$.
R er en divisjonsring $\iff (R \setminus \{0\}, \cdot)$ er en gruppe.

Bevis: $\Leftarrow$: Direkte.

$\Rightarrow$: Anta at R er en divisjonsring. La $G = R \setminus \{0\}$

1) $G \neq \emptyset$: Siden $1 \in G$, så er $G \neq \emptyset$

2) $1 \in G$.

3) G lukket under mult.: La $a, b \in G$. Anta at $ab \notin G$. dvs. $ab = 0$. Pr. antakelse har a en invers a^{-1}

$\Rightarrow a^{-1}(ab) \overset{\text{ass}}{=} (a^{-1}a)b = 1 \cdot b = b$
$a^{-1} \cdot 0 = 0$
$\Rightarrow b = 0$ ⚡

4) $a \in G \Rightarrow a^{-1} \in G$: Direkte fra def. av div. ring.

$\Rightarrow (G, \cdot)$ er en gruppe. □

Setning 60 $n \geq 1$
$\mathbb{Z}_n$ er en kropp $\iff$ n er et primtall.

Bevis: $\Rightarrow$: Anta at $\mathbb{Z}_n$ er en kropp. For alle $\bar{r} \in \mathbb{Z}_n \setminus \{\bar{0}\}$, så $\exists\, \bar{s} \in \mathbb{Z}_n$ slik at $\bar{s} \cdot \bar{r} = \bar{1}$. Dvs. for alle $1 \leq r < n$, så $\exists s$ med $1 \leq s < n$ slik at

$$\bar{1} = \bar{s} \cdot \bar{r} = \overline{s \cdot r} = \underbrace{r + r + \cdots + r}_{s \text{ ganger}} = \underbrace{\bar{r} + \bar{r} + \cdots + \bar{r}}_{s \text{ ganger}} = s \cdot \bar{r}$$

$\Rightarrow \bar{1} \in \langle \bar{r} \rangle \leq (\mathbb{Z}_n, +) \Rightarrow \langle \bar{r} \rangle = \mathbb{Z}_n \; (= \langle \bar{1} \rangle)$.

Setning 15 (b) $\Rightarrow \gcd(r, n) = 1, \; \forall\, 1 \leq r < n$.
$\Rightarrow r \nmid n, \; \forall\, 1 < r < n$
$\Rightarrow n$ primtall. ← Merk: Feil i forelesning!

$\Leftarrow$: Anta at $n = p$ er et primtall. For $r \in \{1, 2, \ldots, p\}$ så er $\gcd(r, p) = 1$, dvs. $\exists\, s, t \in \mathbb{Z}$ slik at

$rs + pt = 1$

modulo p $\Rightarrow$ $\bar{r}\bar{s} = \bar{1}$ i $\mathbb{Z}_p$ $\Rightarrow$ $\bar{r}$ har en invers i $\mathbb{Z}_p$.

$\Rightarrow$ $\mathbb{Z}_p$ er en divisjonsring og en kropp. $\square$