

Sætning 6.2 (19.3)
Nulldivisorene i $\mathbb{Z}_n = \{\bar{r} \in \mathbb{Z}_n \mid \gcd(r, n) > 1\}$

Bevis: Har sett: $\gcd(r, n) = 1 \Rightarrow \bar{r}$ enhet i $\mathbb{Z}_n \Rightarrow \bar{r}$ ikke nulldiv.
 $\Rightarrow \{\bar{r} \text{ nulldivisor} \Rightarrow \gcd(r, n) > 1\}$, dvs. har vist " \subseteq "

Anta at $\gcd(r, n) = d > 1$ med $0 < r < n$.

Har: $r = ds$ for $s \in \mathbb{Z}$, $0 < s < r$

La $m = \frac{n}{d} \in \mathbb{Z}$. Da er $1 < m < n$ og $\bar{m} \neq \bar{0}$ i \mathbb{Z}_n .

Har da at

$$\bar{r} \cdot \bar{m} = \overline{ds} \cdot \overline{\frac{n}{d}} = \overline{ds \frac{n}{d}} = \overline{sn} = \bar{0} \text{ i } \mathbb{Z}_n.$$

$\Rightarrow \bar{r}$ er en nulldivisor i \mathbb{Z}_n og vi har vist " \supseteq ". Detek gir likhet. \square

DEF: R kommutativ ring med 1. Ringen R kalles et integritetsområde hvis R ikke har noen nulldivisorer, dvs. $ab = 0 \Rightarrow a = 0$ eller $b = 0$.

Eksempler

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ integritetsområder.

Direkte produkt av ringer

R_1, R_2 ringe. Dann

$$R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$$

Addisjon: $(r_1, r_2) + (r'_1, r'_2) \stackrel{\text{def}}{=} (r_1 + r'_1, r_2 + r'_2)$

Multiplikasjon

$$(r_1, r_2) \cdot (r'_1, r'_2) = (r_1 r'_1, r_2 r'_2)$$

$$1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$$

Spjeldk: $R_1 \times R_2$ er en ring med 1

Merk: R_1, R_2 kommutative ringe
 $\implies R_1 \times R_2$ kommutativ.

Eksempel

$\mathbb{Z} \times \mathbb{Z}$ Komm. ring, ikke integritetsområde for:

$$a = (1, 0), b = (0, 1) \in \mathbb{Z} \times \mathbb{Z}, \text{ begge } \neq 0.$$

$$a \cdot b = (1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0 \text{ i } \mathbb{Z} \times \mathbb{Z}.$$

$\implies \mathbb{Z} \times \mathbb{Z}$ ikke et integritetsområde.