

(F25, ti 18 apr 2006)

$(R, +, \times)$ är en **ring** om

- 1) $(R, +)$ är en **kommutativ grupp** med **identitets**element 0
- 2) $(R, \times)$ är **sluten** och **associativ**, med **identitets**element 1
- 3) $\times$ är **distributiv** m.a.p. $+$,
$$a(b + c) = ab + ac, (a + b)c = ac + bc \quad \text{för alla } a, b, c \in R$$

Exempel: $\mathbb{Z}$, $\mathbb{Z}_m$, $M_n(R)$, $R[x]$

$U(R)$: de **inverterbara** elementen i R

$(U(R), \times)$ är en **grupp**.

Exempel: $U(\mathbb{Z}) = \{1, -1\}$

$$U(\mathbb{Z}_m) = \{r \in \mathbb{Z}_m \mid \text{sgd}(r, m) = 1\}, \quad |U(\mathbb{Z}_m)| = \phi(m)$$

$(F, +, \times)$ är en **kropp** om

- 1) $(F, +, \times)$ är en **ring**
- 2) $(F \setminus \{0\}, \times)$ är en **kommutativ grupp**

Exempel: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$ (p primtal)