(F22, to 20 feb)

$(R, +, \times)$ är en **ring** om

1) $(R, +)$ är en **kommutativ grupp** med **identitetselement** 0

2) $(R, \times)$ är **sluten** och **associativ**, med **identitetselement** 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: $U(\mathbb{Z}) = \{1, -1\}$

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

$(F, +, \times)$ 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)

$R[x]$, mängden av **polynom** över en ring R,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad a_i \in R$$

$f(x) + g(x)$, $f(x)g(x)$ definieras ”som vanligt”