Buď R, S okruhy.

<u>def</u>: $\varphi: R \to S$ je <u>HOMOMORFISMUS</u> pokud $\forall a, b \in R$ $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$\varphi(-a) = -\varphi(a)$, $\varphi(0) = 0$, $\varphi(1) = 1$.

$Im(\varphi) = \{\varphi(a) : a \in R\}$, $Ker(\varphi) = \{a \in R : \varphi(a) = 0\}$

<u>Tvrzení</u>: $\varphi: R \to S$ hom. okruhů $\Rightarrow$
(1) $Im(\varphi)$ je podokruh S
(2) $Ker(\varphi)$ je <u>ideál</u> v R
(3) φ prostý $\Leftrightarrow$ $Ker(\varphi) = \{0\}$

<u>Tvrzení</u>: $\varphi: R \to S$, $\psi: S \to T$ hom. okruhů $\Rightarrow$
(1) $\psi \circ \varphi : R \to T$ je hom.
(2) φ bijektivní $\to$ $\varphi^{-1}: S \to R$ je hom.

<u>Př.</u>: <u>modulární</u> hom. $\mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto a \bmod m$ $T[x] \to T[x]/(m)$, $f \mapsto f \bmod m$

<u>dosazovací</u> hom. $R \leq S \ni a$ .... $R[x] \to S$, $f \mapsto f(a)$

<u>def</u>: <u>Frobeniův endomorfismus</u>: R komut. okruh charakteristiky p (prvočíslo)

$\rightsquigarrow$ $\varphi: R \to R$, $a \mapsto a^p$

<u>Tvrzení</u>: (1) φ je hom.
(2) R obor $\Rightarrow$ φ je prosté
(3) R konečné těleso $\Rightarrow$ φ je <u>na</u> (říkáme <u>Frobeniův automorfismus</u>)

Konstrukce <u>FAKTOROKRUHU</u> R/I, kde I je ideál v R:

def. $a \sim b \iff a - b \in I$

$\ddot{\odot}$ je to ekvivalence, bloky jsou $[a] = a + I$

def. operace
$$[a] + [b] := [a+b]$$
$$[a] \cdot [b] := [a \cdot b]$$
$$-[a] := [-a]$$

$$\rightsquigarrow \quad R/I := \left(\{[a] : a \in R\}, +, -, \cdot, [0], [1]\right)$$

<u>Tvrzení</u>: Operace jsou dobře definovány, R/I je okruh.

<u>Věta o homomorfismu</u>: Buď $\varphi: R \to S$ hom. okruhů.

(1) Je-li $I \subseteq Ker(\varphi)$ ideál, pak $\psi: R/I \to S$, $[a] \mapsto \varphi(a)$ je dobře def. hom.

(2) $\boxed{R/Ker(\varphi) \simeq Im(\varphi)}$ (1. věta o izomorfismu)

<u>2. věta o izomorfismu</u>: Buď R okruh, I ideál v R.

(1) $I \subseteq J$ ideály $\Rightarrow$ $J/I = \{[a] : a \in J\}$ je ideál v R/I

(2) K ideál v R/I $\Rightarrow$ $K = J/I$ pro nějaký ideál J v R

(3) $\boxed{\dfrac{R/I}{J/I} \simeq R/J}$

def: Buď R ~~komut~~. okruh, I ideál v R. I nazveme

- *prvoideálem*, pokud $\forall a,b \in R$ $\boxed{a \cdot b \in I \Rightarrow a \in I \text{ nebo } b \in I}$
- *maximálním ideálem*, pokud $\boxed{\text{neexistuje ideál } J \text{ t.ž. } I \subsetneq J \subsetneq R}$

Věta: Buď R komut. okruh, I ideál v R. Pak

(1) R/I je obor $\Leftrightarrow$ I je prvoideál

(2) R/I je těleso $\Leftrightarrow$ I je maximální ideál

Připomenutí: S komut. okruh $\Rightarrow$ $[S$ je těleso $\Leftrightarrow$ S nemá žádné vlastní ideály$]$