Primijetimo da ako su A i B ideali prstena R, onda je i $A \cap B \trianglelefteq R$.

Uopšte, ako su $A_i \trianglelefteq R$, $i \in I$, onda je $\bigcap_{i \in I} A_i \trianglelefteq R$ (sami)

Ali, $A \cup B \ntrianglelefteq R$ (može a ne mora).

Međutim, $\langle A \cup B \rangle \trianglelefteq R$.

Ako je $A \subseteq R$, onda $\langle A \rangle$ - ideal generisan skupom A.

$$\langle A \rangle = \bigcap_{B \trianglelefteq R,\ B \supseteq A} B$$ - najmanji ideal prstena R, koji sadrži podskup A.

Specijalno, ako je $A = \{a\}$, onda $\langle a \rangle$ - ideal generisan elementom a, naziva se glavni ideal prstena R.

$\langle A \cup B \rangle \overset{?}{=} A + B$.

$\langle A \cup B \rangle$ → najmanji ideal prstena R koji sadrži uniju

---

$A + B = \{x \mid x = a + b,\ a \in A,\ b \in B\} \trianglelefteq R$

A → ideal, B → ideal = (suma ideala)

→ ideal prstena R (sami)

$A \ni a = a + 0 \in A + B$

$B \ni b = 0 + b \in A + B$

$A \cup B \subseteq A + B$.

$A \cup B \subseteq \langle A \cup B \rangle$ ↳ najmanji ideal koji sadrži uniju

$\Rightarrow \langle A \cup B \rangle \subseteq A + B$.

Očigledno, $A + B \subseteq \langle A \cup B \rangle$

$$\begin{array}{cc} A & B \\ \Downarrow & \Downarrow \\ a & b \\ \cap & \cap \\ A \cup B & A \cup B \end{array}$$

$A \oplus B$ → direktna suma ideala

$= A + B$, $A \cap B = \{0\}$

$R = A \oplus B$ - dekompozicija prstena R u obliku direktne sume ideala

Uopšte, $A_1 \oplus \dots \oplus A_n = A_1 + \dots + A_n$, $\quad A_i \cap (A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_n) = \{0\}$

$R = A_1 \oplus \dots \oplus A_n$

$A \cdot B = \{ \sum_i a_i b_i \mid a_i \in A, b_i \in B \}$

proizvod dva ideala

$A : B = \{ x \in R \mid xB \subseteq A \} = X$

količnik dva ideala

$X \trianglelefteq R \rightarrow$ najveći ideal takav da je $XB \subseteq A$.

Neka je $A \trianglelefteq R$. Na prstenu R se definiše binarna relacija $\sim$ na sledeći način:

$$(\forall x, y \in R),\ x \sim y \iff x - y \in A$$

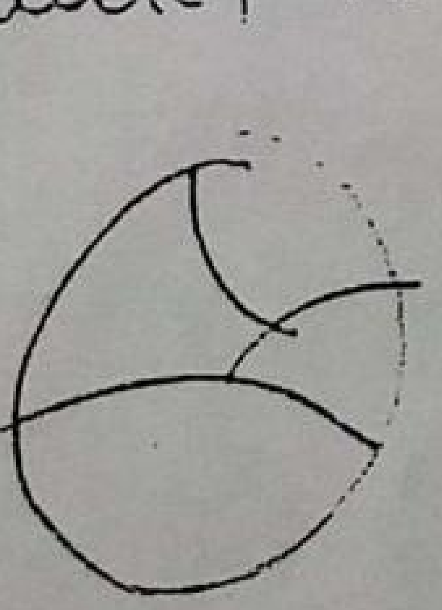
Lako se provjerava da je relacija $\sim$ relacija ekvivalencije (R, S, T)-sami. Ova relacija je saglasna sa binarnom operacijom u prstenu R t.d. važi:

$$\left.\begin{matrix} x \sim x' \\ y \sim y' \end{matrix}\right\} \Rightarrow \left.\begin{matrix} x + y \sim x' + y' \\ xy \sim x'y' \end{matrix}\right\}$$

$$\left\ulcorner \left.\begin{matrix} x - x' \in A \\ y - y' \in A \end{matrix}\right\} \Rightarrow \begin{matrix} (x+y) - (x'+y') \in A \\ \underbrace{(x - x')}_{\in A} + \underbrace{(y - y')}_{\in A} \in A \end{matrix} \right\lrcorner$$

$$xy - x'y' = xy - xy' + xy' - x'y' = \underbrace{x\underbrace{(y - y')}_{\in A}}_{\in A} + \underbrace{\underbrace{(x - x')}_{\in A}y'}_{\in A} \in A.$$

Dakle, relacija ekvivalencije $\sim$ je kongruencija na prstenu R.



$R/_\sim = \{ C_x \mid x \in R \}$

$C_x = \{ y \in R \mid y \sim x \} = \{ y \in R \mid y - x \in A \}$

$= \{ y \in R \mid y \in x + A \} = x + A$

klasa ekvivalencije

x-reprezent

$C_x = x + A = \{ x + a \mid a \in A \}$

$R/\sim \quad R/A$

$R/A = \{x + A \mid x \in R\}$

Na faktor skupu R/A se definišu linearne operacije $\oplus$ i $\odot$ na sledeći način:

$$\left.\begin{aligned}(x+A)\oplus(y+A) &= x+y+A\\ (x+A)\odot(y+A) &= x\cdot y+A\end{aligned}\right\}$$ One su korektno definisane jer je relacija $\sim$ kongruencija na prstenu R.

$(R/A, \oplus, \odot)$ – prsten koji se naziva faktor prstenom prstena R po idealu A

Neutralni element je A.

Distributivnost operacije $\odot$ u odnosu na $\oplus$

$((x+A)\oplus(y+A))\odot(z+A) = (x+y+A)\odot(z+A) = (x+y)\cdot z + A =$

$xz + yz + A = (xz + A)\oplus(yz + A) = (x+A)\odot(z+A)\oplus(y+A)\odot(z+A)$

~~Primetimo da, ako je prsten R komutativan, asocijativan ili~~ sa jedinicom, odgovarajuća svojstva ima i R/A (sam) ($1+A$ - jed.)

Def. Preslikavanje $f: R \to R'$ se naziva **homomorfizam prstena** ako važi $(\forall x, y \in R)$
$$f(x+y) = f(x) + f(y)$$
$$f(x\cdot y) = f(x)\cdot f(y)$$

Ako je uz to f i „1-1" – monomorfizam

Ako je uz to f i „na" – epimorfizam

Ako je uz to f bijekcija – izomorfizam ($R \cong R'$)

Specijalno, ako je $R' = R$, onda homomorfizam $f: R \to R$ se naziva endomorfizam. Izomorfizam f se naziva automorfizam.

$\mathrm{Ker} f = \{x \in R \mid f(x) = 0\}$ → neutralni element u R'.

$\mathrm{Im} f = \{f(x) \mid x \in R\} = f(R) \leq R'$ → homomorfna slika prstena

Lema: Epimorfna slika prstena je prsten.

$$\ulcorner f : R \xrightarrow{\text{epimorf.}} R'$$

R-prsten $\qquad R'$ – struktura sa 2 binarne operacije

$$f(R) = R'$$

Lema. Neka je $f: R \to R'$ homomorfizam prstenova. Onda:

a) $A \leq R \Rightarrow f(A) = \{ f(a) \mid a \in A \} \leq R'$

b) $A' \leq R' \Rightarrow f^{-1}(A') = \{ x \in R \mid f(x) \in A' \} \leq R$

c) Ako je R komutativan, onda je $f(R)$ također komutativan

d) Ako prsten R ima 1, onda $f(1)$ je jedinični element u $f(R)$ ili je $f(R) = \{0\}$

e) Ako je R integralni domen i f injekcija, onda je $f(R)$ također integralni domen.

Dokaz. a) $\Rightarrow$ d) $\to$ znam

e) Neka je prsten R integralni domen. Onda $f(R)$ je komutativan, asocijativan i sa jedinicom $f(1)$.

Kako u integralnom domenu R nema djelitelja nula to

$(\forall x, y \in R)$, $x \neq 0$, $y \neq 0 \Rightarrow x \cdot y \neq 0$

Pretpostavimo da je

$$f(x) \neq 0 \ \text{ i } \ f(y) \neq 0$$

$$x \neq 0 \quad f(x) = 0, \text{ ovo je nemoguće jer je } f \text{ injekcija.}$$

Onda: $f(xy) \neq 0$, tj. $f(x) f(y) \neq 0$

Dakle, za $\forall f(x), f(y) \in f(R)$ (koji su $\neq 0$) slijedi $f(x) \cdot f(y) \neq 0$,

tj. $f(R)$ nema djelitelja nula.

Dakle, homomorfna slika integralnog domena je integralni domen.

Teorema (Osnovna teorema o homomorfizmu prstena)

Neka je $f: R \to R'$ homomorfizam prstena. Onda je $\ker f \trianglelefteq R$. Važi i obratno, ako je $A \trianglelefteq R$ onda $\exists R/A$ i prirodni (kanonski) homomorfizam $\pi: R \to R/A$ takav da je $\ker \pi = A$. Takođe $R/\ker f \cong \operatorname{Im} f$

Dokaz. $\ker f = \{x \in R \mid f(x) = 0\}$. Prvo, $\ker f \neq \emptyset$, jer $0 \in \ker f$, zbog $f(0) = 0$.

1) $\forall a_1, a_2 \in \ker f: a_1 - a_2 \in \ker f$,

$$f(a_1 - a_2) = \underbrace{f(a_1)}_{0} - \underbrace{f(a_2)}_{0} = 0 - 0 = 0$$

$\ulcorner f(a_1 - a_2) = f(a_1) + f(-a_2) = f(a_1) - f(a_2) \lrcorner$

2) $\forall a \in \ker f$, $\forall r \in R$: $ra, ar \in \ker f$

$$f(ra) = f(r) \cdot \underbrace{f(a)}_{0} = f(r) \cdot 0 = 0$$

$$f(ar) = 0$$

Iz 1) i 2) $\Rightarrow \ker f \trianglelefteq R$.

Neka je $A \trianglelefteq R$. Onda $\exists R/A$ i prirodni homomorfizam $\pi: R \to R/A$ definisan sa $(\forall x \in R)\ x \longmapsto x + A$. Zaista, $\forall x, y \in R$

$$\pi(x+y) = x + y + A = (x+A) \oplus (y+A) = \pi(x) \oplus \pi(y).$$

$$\pi(xy) = xy + A = (x+A) \odot (y+A) = \pi(x) \odot \pi(y).$$

Još jače, π je epimorfizam

$\ulcorner$ Zaista, $\forall x + A \in R/A$, $\exists x \in R$, $\pi(x) = x + A \lrcorner$

$$\ker \pi = \{x \in R \mid \pi(x) = x + A = A\}$$

Jasno, $A \subseteq \ker \pi$.

Obratno, neka je $x \in \ker \pi$. Onda, $\pi(x) = x + A = A$, tj. postoje $\exists a, a' \in A$ td. $x + a = a'$. $\Rightarrow x = a' - a \in A$. $\Rightarrow \ker \pi \subseteq A$

$\Rightarrow \ker \pi = A$.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & R' \\ R/A \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

Neka je $\ker f = A$. Onda postoji $\exists R/A$ - faktor prsten i prirodni homomorfizam $\pi : R \to R/A$. Definišemo preslikavanje $h : R/A \to R'$ na sledeći način: $(\forall x \in R)\ h(x+A) = f(x)$

<u>Korektnost</u>. Neka je $x+A = y+A$ za neke $x, y \in R$. Onda, $x \sim y$ odnosno $x - y \in A = \ker f$ tj. $f(x) = f(y)$ odnosno $h(x+A) = h(y+A)$.

<u>Homomorfizam</u>. $(\forall x, y \in R) : h((x+A) \oplus (y+A)) = h(x+y+A) = f(x+y) = f(x) + f(y) = h(x+A) + h(y+A)$.

$h((x+A) \odot (y+A)) = h(xy+A) = f(xy) = f(x) \cdot f(y) = h(x+A) \cdot h(y+A)$.

<u>"$1 \to 1$"</u>. Neka je $h(x+A) = h(y+A)$, za neke $x, y \in R$.

Onda, $f(x) = f(y)$.

$f(x) - f(y) = 0$

$f(x-y) = 0$

$x - y \in \ker f = A$

$x \sim y$ tj. $x + A = y + A$

Dakle, preslikavanje $h : R/A \to R'$ je monomorfizam, odnosno $h : R/A \xrightarrow[\text{"na"}]{} h(R/A) = \underbrace{f(R)}_{\text{homomorfna slika prstena}} \leq R$. tj. $h : R/A \to f(R) \leq R'$ jeste izomorfizam.

Pišemo, $R/A \cong f(R)$, odnosno $R/\ker f \cong \operatorname{Im} f$.