Def. Neprazan podskup $S \subseteq R$ (R- prsten) naziva se <u>podprsten</u> prstena R ako je S sam za sebe prsten tj. 1) $(S,+) \leq (R,+)$ → podgrupa

2) $(S,\cdot) \leq (R,\cdot)$ → podgrupoid

Očigledno: 1) $\forall x,y \in S \quad x-y \in S$

2) $\forall x,y \in S \quad x \cdot y \in S$

Pišemo: $S \leq R$ → podprsten.

Trivijalni podprsten su: $\{0\}, R$

Prsten R uvijek ima najmanje elemente 1, ali podprsten S ne mora da ga sadrži.

Npr. $(\mathbb{Z},+,\cdot)$ - prsten celih brojeva koji ima jedinični element 1.

a $(2\mathbb{Z},+,\cdot) \leq (\mathbb{Z},+,\cdot)$
↓ prsten parnih brojeva; → podprsten

Def. Neprazan skup F, na kome su definisane dvije binarne operacije $+$ i $\cdot$ za:

I) $(F,+)$ Abelova grupa

II) $(F^*,\cdot)$ Abelova grupa, gdje je $F^* = F \setminus \{0\}$

III) Distributivnost operacije $\cdot$ u odnosu na $+$,

naziva se <u>polje</u>.

Pišemo: polje F, polje $(F,+,\cdot)$

polje $(F, \underline{+}, \underline{-}, \underline{^{-1}}, \underline{0}, \underline{1})$
↓ nosač polja; binarne unarne nularne

Primjeri: $(\mathbb{Q},+,\cdot), (\mathbb{R},+,\cdot), (\mathbb{C},+,\cdot)$ → beskonačna polja.

Def: Neprazan skup $S \subseteq F$ naziva se **podpolje** polja F ako je S samo za sebe polje (u odnosu na restrikcije operacija definisanih na S)

$(+|_S, \cdot|_S)$, $S \subseteq F$ ⌄ podpolje

1) $\forall x,y \in S : x-y \in S$
2) $\forall x,y \in S, y \neq 0 : xy^{-1} \in S.$

$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Def. Neprazan skup K na kome su definisane dve binarne operacije $+$ i $\cdot$ naziva se:

I $(K,+)$ Abelova grupa

II $(K^*,+)$ grupa , $K^* = K \setminus \{0\}$

III Distributivnost operacije $\cdot$ u odnosu na $+$

naziva se **telo**. U telu sem komutativnu telo je polje.

Telo - Kosopolje.

Primeri: 1) Skup svih invertibilnih elemenata u prstenu $M(n,\mathbb{R})$ - kvadratnih matrica sa elementima iz $\mathbb{R}$ oznaćen sa $GL(n,\mathbb{R})$ je telo.

2) $(G,+)$ - aditivna Abelova grupa

$(\text{hut } G,+,\cdot)$ - telo

Def. Nenula element $a \in R$, R-prsten, naziva se levi (desni) delilac nule, ako $\exists b \in R$, $b \neq 0$ takvo da je $ab = 0$ ($ba = 0$)

Element a je delilac nule (obostrani) ako je on i levi i desni delilac nule.

Def. Komutativan asocijativan prsten sa jedinicom, bez delilaca nule se naziva **integralni domen**.

Primeri: a) $(\mathbb{Z},+,\cdot)$ - prsten celih brojeva - beskonačan, integralni domen

b) $(\mathbb{Z}_n,+,\cdot)$ - integralni domen ako je n prost broj.

$(\mathbb{Z}_p, +, \cdot)$ - polje (integrali domen) $GF(p)$ → polje Galoa od p elemenata

c) R/p - integralni domen akko je p prost ideal

Primjetimo da svako polje je integralni domen, ali obratno ne vrijedi u opštem slučaju. Međutim, konačni integralni domen je polje. (sami!)

Γ F - polje

$\amalg$ F^* - grupa (Multiplikativna)

$a, b \in F^*$ $(a, b \neq 0) \Rightarrow ab \in F^*$ tj. $ab \neq 0$ $\rfloor$

Def. Najmanji prirodan broj n za koji vrijedi da je $n \cdot x = 0, \forall x \in R$, R - prsten, nazivamo **karakteristika prstena** (ako takav postoji).

Prsten Prstenu $\mathrm{char} R = n$.

Ako takav broj ne postoji kažemo da je prsten R karakteristike nula.

Lema. Neka je R prsten sa jedinicom. Onda:

a) $\mathrm{char} R = n$ akko je jedinični element 1 konačnog aditivnog reda

b) $\mathrm{char} R = 0$ akko je jedinični element 1 beskonačnog aditivnog reda

Dokaz a) $\Rightarrow$ Neka je $\mathrm{char} R = n$. To znači $(\exists n$ pozitivan broj) td. $n \cdot x = 0, \forall x \in R$ (najmanji takav), pa i za $x = 1$ tj. $n \cdot 1 = 0$

Ako n nije najmanji takav, onda $\exists m < n$, td. $m \cdot 1 = 0$. Tada,

$(m \cdot 1) \cdot x = 0 \cdot x$

$m \cdot (1 \cdot x) = 0$

$m \cdot x = 0$ $/\forall x \in R$, što je u kontradikciji sa pretpostavkom

Dakle, n je najmanji prirodan broj takav da je $n \cdot 1 = 0$, tj. n je aditivni red jedinice (konačan)

$\Leftarrow$ Neka je jedinični element 1 konačnog aditivnog reda, tj. $\exists n$ (prirodan broj) $n \cdot 1 = 0$ (najmanji takav). Onda, $(\forall x \in R)$: $(n \cdot 1) \cdot x = 0 \cdot x$

$w(1-x) = 0$

$w \cdot x = 0$, $\forall x \in R$.

Dokažimo da je w najmanji takav za $\forall x$. Ako nije onda, $\exists n < w$: $nx = 0$, $\forall x \in R$ pa tada $x = 1$: $n \cdot 1 = 0$ što je u kontradikciji sa pretpostavkom. Dakle, $w = charR$.

b) $(\Rightarrow)$ Neka je $charR = 0$. Pretpostavimo suprotno tj. da je jedinični element 1 konačnog aditivnog reda n. $\exists n$ (pozitivan) $n \cdot 1 = 0$ najmanji takav. Onda, $\forall x \in R$ $(n \cdot 1) \cdot x = 0 \cdot x$

$n \cdot (1 \cdot x) = 0$

$0 \cdot x = 0$, $\forall x \in R$.

$\Rightarrow$ $n = charR$. (konačno) što je suprotno pretpostavci n je prost. Dakle, jedinični element 1 je beskonačnog reda.

$(\Leftarrow)$ Neka je jedinični element 1 beskonačnog reda. Pretpostavimo suprotno tj. da je $charR = n$ (prost broj). To znači da je $n \cdot x = 0$, $\forall x \in R$ (n-najmanji takav), to tada $x = 1$ $n \cdot 1 = 0$ što je u kontradikciji sa pretpostavkom. Dakle, $charR = 0$.

Teorema Neka je R prsten bez djelitelja nule i konačne karakteristike. Onda:

a) $charR$ - prost broj

b) svaki nenula element prstena R je konačnog aditivnog reda.

Dokaz: a) $charR = n$, R - bez djelitelja nule.

Pretpostavimo suprotno tj. da n nije prost broj. Onda $\exists r, s < n$, $n = r \cdot s$. Onda $(\forall x \in R)$ $(r \cdot x)(s \cdot x) = r(x(s \cdot x)) =$

$= r(s(x \cdot x)) = r(s \cdot x^2) = (r \cdot s)x^2 = nx^2 = (nx)x = 0 \cdot x = 0$

Kako je R prsten bez djelioca nule to je $rx=0 \vee sx=0$. Ako je $rx=0$, $\forall x \in R$, onda $r=charR$, $r<n$ a to je nemoguće. Ako je $sx=0$, $\forall x \in R$, $\Rightarrow s=charR$, $s<n$, što je nemoguće. Dakle, n je prost broj.

b) Neka je $a \in R$, $a \neq 0$ i njegov aditivni red m. Tada $ma=0$ i m najmanji takav. $\forall x \in R$ $a(mx)=m(ax)=(ma)x=0 \cdot x=0$

Kako je R prsten bez djelitelja nule i $a \neq 0$ to je $mx=0$. Dvo vrijedi za $\forall x \in R$, i m je najmanji takav.

Ako m nije najmanji takav, onda bi $\exists n<m$ $nx=0$, $\forall x \in R$, a to bi značilo da i za $x=a$ $na=0$, $n<m$ što je nemoguće.

Preostaje element $x \in R$ je istog aditivnog reda kao i nenula. □

Primjetimo sličnost između prstena ideala i tijela prstena (mogli smo govoriti o normalnim podgrupama i teoriji grupa).

Def. Neprazan podskup $A \subseteq R$ zvat će se **idealom** prstena ako vrijedi
1) $(A,+) \leq (R,+)$
2) $RA \subseteq A$, $AR \subseteq A$, tj. ekvivalentno:
1) $a_1 - a_2 \in A$, $\forall a_1, a_2 \in A$
2) $ra \in A$, $ar \in A$, $\forall a \in A, r \in R$

Uvjet (1) i $ra \in A \rightarrow$ lijevi ideal
Uvjet (1) i $ar \in A \rightarrow$ desni ideal
} obje - obostrani ideali

Pišemo: $A \trianglelefteq R$.

Primjer. $(\mathbb{Z},+,\cdot)$ - prsten cijelih brojeva
Svi ideali su oblika $n\mathbb{Z}$, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$
$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$

Teorema. Asocijativan prsten K sa jedinicom je tijelo akko K nema pravih netrivijalnih lijevih, odnosno desnih ideala.

Dokaz. $\Rightarrow$ Neka je asocijativan prsten K sa jedinicom tijelo. Dokazimo da nema pravih netrivijalnih lijevih ideala. Pretpostavimo suprotno, tj. da postoji pravi netrivijalni lijevi ideal A prstena K.

$A \trianglelefteq K$, $A \neq \{0\}$

$\exists a \in A,\ a \neq 0 \ \wedge\ K \cdot A \subseteq A$

$\Downarrow$

$\exists a^{-1} \in K$ jer je K tijelo $\qquad a^{-1} \cdot a = 1 \in A$

Tada, $\forall k \in K$ vrijedi da je $k = \underset{K}{k} \cdot \underset{A}{1} \in A \quad \Rightarrow K \subseteq A$

a kako je $A \subseteq K$, to je $A = K$, što je u kontradikciji sa pretpostavkom.

$\Leftarrow$ Dokazujemo da je K tijelo, tj. da svaki netrivijalni element a ima svoj lijevi inverzni element. Razmotrimo skup $\{xa \mid x \in K\}$ koji se pokazuje da je ono lijevi ideal u prstenu K.

$\lceil K(xa) = (kx)a \rfloor$ (asocijativnost)

Ono je netrivijalni ideal, jer $a = 1 \cdot a$. Po pretpostavci, ovaj skup $\{xa \mid x \in K\} = K$. Kako je $1 \in K$ to je $1 \in \{xa \mid x \in K\}$ pa je oblika $1 = a'a$, i a' je lijevi inverzni element za element a. Dokažimo da je to ujedno i desni inverzni element za element a. Razmotrimo skup $B = \{x \mid x(aa'-1) = 0\}$. Kako se pokazuje da je $B \trianglelefteq K$.

$\lceil \forall x \in B,\ k(x(aa'-1)) = k(\underbrace{x(aa'-1)}_{0}) = k \cdot 0 = 0 \rfloor$ ($k \in K$)

$B \neq \{0\}$ jer sadrži bar element $a' \neq a$

$\lceil a'(aa'-1) = a'aa' - a' = (a'a)a' - a' = 1 \cdot a' - a' = a' - a' = 0 \rfloor$

Po pretpostavci $B = K$, pa je $1 \in B$, tj. $1 \cdot (aa'-1) = 0$ odnosno

$aa' - 1 = 0 \Rightarrow aa' = 1 \Rightarrow a'$ – desni inverzni.