

Algebarske strukture

prof.dr.sc. Saša Krešić-Jurić

PMF–Split

Definicija

Prsten je neprazan skup R s dvije binarne operacije $+$ i $\cdot$ koje nazivamo zbrajanje i množenje, i koje za svaki $a, b, c \in R$ zadovoljavaju sljedeća svojstva:

1 $(R, +)$ je Abelova grupa,

2 množenje je asocijativno:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

3 množenje je distributivno u odnosu na zbrajanje slijeva i zdesna:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Definicija

Ako je množenje u prstenu R komutativno, tada R nazivamo komutativni prsten.

Kažemo da je R prsten s jedinicom ako postoji element $1 \in R$ takav da je

$$1a = a1 = a \quad \text{za svaki } a \in R.$$

Definicija

Prsten je neprazan skup R s dvije binarne operacije $+$ i $\cdot$ koje nazivamo zbrajanje i množenje, i koje za svaki $a, b, c \in R$ zadovoljavaju sljedeća svojstva:

1 $(R, +)$ je Abelova grupa,

2 množenje je asocijativno:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

3 množenje je distributivno u odnosu na zbrajanje slijeva i zdesna:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Definicija

Ako je množenje u prstenu R komutativno, tada R nazivamo komutativni prsten. Kažemo da je R prsten s jedinicom ako postoji element $1 \in R$ takav da je

$$1a = a1 = a \quad \text{za svaki } a \in R.$$

Definicija

Prsten je neprazan skup R s dvije binarne operacije $+$ i $\cdot$ koje nazivamo zbrajanje i množenje, i koje za svaki $a, b, c \in R$ zadovoljavaju sljedeća svojstva:

1 $(R, +)$ je Abelova grupa,

2 množenje je asocijativno:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

3 množenje je distributivno u odnosu na zbrajanje slijeva i zdesna:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Definicija

Ako je množenje u prstenu R komutativno, tada R nazivamo komutativni prsten. Kažemo da je R prsten s jedinicom ako postoji element $1 \in R$ takav da je

$$1a = a1 = a \quad \text{za svaki } a \in R.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Primjedbe

- Prsten ne mora imati jedinicu.
- Zbrajanje u prstenu mora biti komutativno da bi bilo kompatibilno s uvjetom distributivnosti.

Primjeri

- 1 Neka je $(R, +)$ Abelova grupa. R je trivijalni prsten ako definiramo $ab = 0$ za sve $a, b \in R$. Prsten R nema jedinicu.
- 2 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ su komutativni prsteni s jedinicom.
- 3 $M(n, \mathbb{R})$ i $M(n, \mathbb{C})$ sa standardnim zbrajanjem i množenjem matrica.
 - Nula u $M(n, \mathbb{F})$ je nul matrica $\mathbf{0}$ reda n .
 - Jedinica u $M(n, \mathbb{F})$ je jedinična matrica I reda n .
- 4 $\mathbb{R}[x] = \{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{R} \}$ je prsten polinoma u varijabli x sa standardnim zbrajanjem i množenjem polinoma.
- 5 Abelova grupa $(\mathbb{Z}_n, +)$ postaje komutativni prsten s jedinicom ako množenje definiramo sa

$$\bar{x}\bar{y} = \overline{xy}, \quad \bar{x}, \bar{y} \in \mathbb{Z}_n.$$

Sumu i umnožak više elemenata označavamo sa

$$\sum_{k=1}^n a_k = a_1 + a_2 + \cdots + a_n,$$

$$\prod_{k=1}^n a_k = a_1 a_2 \dots a_n.$$

Zbog distributivnosti zbrajanja, u prstenu vrijedi

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

Definicija

Ako je R prsten s jedinicom $1_R \in R$, onda kažemo da je $b \in R$ multiplikativni inverz elementa $a \in R$ ako je

$$ab = ba = 1_R.$$

Sumu i umnožak više elemenata označavamo sa

$$\sum_{k=1}^n a_k = a_1 + a_2 + \cdots + a_n,$$

$$\prod_{k=1}^n a_k = a_1 a_2 \dots a_n.$$

Zbog distributivnosti zbrajanja, u prstenu vrijedi

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

Definicija

Ako je R prsten s jedinicom $1_R \in R$, onda kažemo da je $b \in R$ multiplikativni inverz elementa $a \in R$ ako je

$$ab = ba = 1_R.$$

Sumu i umnožak više elemenata označavamo sa

$$\sum_{k=1}^n a_k = a_1 + a_2 + \cdots + a_n,$$

$$\prod_{k=1}^n a_k = a_1 a_2 \dots a_n.$$

Zbog distributivnosti zbrajanja, u prstenu vrijedi

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

Definicija

Ako je R prsten s jedinicom $1_R \in R$, onda kažemo da je $b \in R$ multiplikativni inverz elementa $a \in R$ ako je

$$ab = ba = 1_R.$$

U prstenu koristimo sljedeće standardne oznake:

$$a^m = a \cdot a \cdot \dots \cdot a \quad (m \text{ puta}),$$

$$a^{-m} = a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1} \quad (m \text{ puta ako } a^{-1} \text{ postoji}),$$

$$a^0 = 1 \quad (\text{ako je } 1 \in R),$$

$$ma = a + a + \dots + a \quad (m \text{ puta}),$$

$$(-m)a = -a + (-a) + \dots + (-a) \quad (m \text{ puta}).$$

Teorem

Neka je R prsten. Onda za svaki $a, b, c \in R$ vrijedi

1 $a0 = 0a = 0,$

2 $a(-b) = -(ab) = (-a)b,$

3 $a(b - c) = ab - ac, \quad (a - b)c = ac - bc.$

U prstenu koristimo sljedeće standardne oznake:

$$a^m = a \cdot a \cdot \dots \cdot a \quad (m \text{ puta}),$$

$$a^{-m} = a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1} \quad (m \text{ puta ako } a^{-1} \text{ postoji}),$$

$$a^0 = 1 \quad (\text{ako je } 1 \in R),$$

$$ma = a + a + \dots + a \quad (m \text{ puta}),$$

$$(-m)a = -a + (-a) + \dots + (-a) \quad (m \text{ puta}).$$

Teorem

Neka je R prsten. Onda za svaki $a, b, c \in R$ vrijedi

1 $a0 = 0a = 0,$

2 $a(-b) = -(ab) = (-a)b,$

3 $a(b - c) = ab - ac, \quad (a - b)c = ac - bc.$

Teorem

Neka je R prsten, i neka su $a, b \in R$. Tada za svaki $n, m \in \mathbb{N}$ vrijedi

$$\mathbf{1} \quad a^m a^n = a^{m+n},$$

$$\mathbf{2} \quad (a^m)^n = a^{mn}.$$

Također, za svaki $n, m \in \mathbb{Z}$ imamo

$$\mathbf{1} \quad (m+n)a = ma + na,$$

$$\mathbf{2} \quad (mn)a = m(na),$$

$$\mathbf{3} \quad (mn)(ab) = (ma)(nb) = (na)(mb).$$

Definicija

Neka je R prsten s jedinicom.

- 1 Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz $a^{-1} \in R$, onda R nazivamo prsten s dijeljenjem.
- 2 Ako je R prsten s dijeljenjem i množenje u R je komutativno, onda R nazivamo polje.

Primjeri

- 1 $\mathbb{Q}$ je prsten s dijeljenjem. $\mathbb{Z}$ nije prsten s dijeljenjem.
- 2 Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja.

Ako je R prsten s dijeljenjem, onda je

$$R^* = \{a \in R \mid a \neq 0\}$$

grupa s obzirom na množenje.

Definicija

Neka je R prsten s jedinicom.

- 1 Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz $a^{-1} \in R$, onda R nazivamo prsten s dijeljenjem.
- 2 Ako je R prsten s dijeljenjem i množenje u R je komutativno, onda R nazivamo polje.

Primjeri

- 1 $\mathbb{Q}$ je prsten s dijeljenjem. $\mathbb{Z}$ nije prsten s dijeljenjem.
- 2 Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja.

Ako je R prsten s dijeljenjem, onda je

$$R^* = \{a \in R \mid a \neq 0\}$$

grupa s obzirom na množenje.

Definicija

Neka je R prsten s jedinicom.

- 1 Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz $a^{-1} \in R$, onda R nazivamo prsten s dijeljenjem.
- 2 Ako je R prsten s dijeljenjem i množenje u R je komutativno, onda R nazivamo polje.

Primjeri

- 1 $\mathbb{Q}$ je prsten s dijeljenjem. $\mathbb{Z}$ nije prsten s dijeljenjem.
- 2 Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja.

Ako je R prsten s dijeljenjem, onda je

$$R^* = \{a \in R \mid a \neq 0\}$$

grupa s obzirom na množenje.

Definicija

Neka je R prsten s jedinicom.

- 1 Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz $a^{-1} \in R$, onda R nazivamo prsten s dijeljenjem.
- 2 Ako je R prsten s dijeljenjem i množenje u R je komutativno, onda R nazivamo polje.

Primjeri

- 1 $\mathbb{Q}$ je prsten s dijeljenjem. $\mathbb{Z}$ nije prsten s dijeljenjem.
- 2 Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja.

Ako je R prsten s dijeljenjem, onda je

$$R^* = \{a \in R \mid a \neq 0\}$$

grupa s obzirom na množenje.

Definicija

Neka je R prsten s jedinicom.

- 1 Ako svaki element $a \in R$, $a \neq 0$, ima multiplikativni inverz $a^{-1} \in R$, onda R nazivamo prsten s dijeljenjem.
- 2 Ako je R prsten s dijeljenjem i množenje u R je komutativno, onda R nazivamo polje.

Primjeri

- 1 $\mathbb{Q}$ je prsten s dijeljenjem. $\mathbb{Z}$ nije prsten s dijeljenjem.
- 2 Prsteni $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja.

Ako je R prsten s dijeljenjem, onda je

$$R^* = \{a \in R \mid a \neq 0\}$$

grupa s obzirom na množenje.

Definicija

Kažemo da je prsten R integralna domena ako $xy = 0$, $x, y \in R$, implicira $x = 0$ ili $y = 0$.

Primjeri

- 1 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su integralne domene.
- 2 $\mathbb{Z}_n$ nije integralna domena ako je n složeni broj.
- 3 Prsten Gaussovih cijelih brojeva

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1}\}$$

je integralna domena.

Propozicija

Ako je F polje, onda je F integralna domena.

Definicija

Kažemo da je prsten R integralna domena ako $xy = 0$, $x, y \in R$, implicira $x = 0$ ili $y = 0$.

Primjeri

- 1 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su integralne domene.
- 2 $\mathbb{Z}_n$ nije integralna domena ako je n složeni broj.
- 3 Prsten Gaussovih cijelih brojeva

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1}\}$$

je integralna domena.

Propozicija

Ako je F polje, onda je F integralna domena.

Definicija

Kažemo da je prsten R integralna domena ako $xy = 0$, $x, y \in R$, implicira $x = 0$ ili $y = 0$.

Primjeri

- 1 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su integralne domene.
- 2 $\mathbb{Z}_n$ nije integralna domena ako je n složeni broj.
- 3 Prsten Gaussovih cijelih brojeva

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1}\}$$

je integralna domena.

Propozicija

Ako je F polje, onda je F integralna domena.

Definicija

Kažemo da je prsten R integralna domena ako $xy = 0$, $x, y \in R$, implicira $x = 0$ ili $y = 0$.

Primjeri

- 1 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su integralne domene.
- 2 $\mathbb{Z}_n$ nije integralna domena ako je n složeni broj.
- 3 Prsten Gaussovih cijelih brojeva

$$\mathbb{Z}[i] = \left\{ m + in \mid m, n \in \mathbb{Z}, i = \sqrt{-1} \right\}$$

je integralna domena.

Propozicija

Ako je F polje, onda je F integralna domena.

Propozicija

Neka je R komutativna integralna domena s jedinicom. Ako je R konačan skup, onda je R polje.

Primjer

Ako je p prosti broj, onda je $\mathbb{Z}_p$ polje.

Definicija

Neka je R prsten. Element $x \in R$ se naziva

- 1 lijevi djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $xy = 0$,
- 2 desni djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $yx = 0$.
- 3 Ako je x lijevi i desni djelitelj nule, onda se x naziva djelitelj nule.

Primjedba

- 1 $0 \in R$ je trivijalni djelitelj nule.
- 2 R je integralna domena ako i samo ako je $0 \in R$ jedini djelitelj nule u R .

Propozicija

Neka je R komutativna integralna domena s jedinicom. Ako je R konačan skup, onda je R polje.

Primjer

Ako je p prosti broj, onda je $\mathbb{Z}_p$ polje.

Definicija

Neka je R prsten. Element $x \in R$ se naziva

- 1 lijevi djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $xy = 0$,
- 2 desni djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $yx = 0$.
- 3 Ako je x lijevi i desni djelitelj nule, onda se x naziva djelitelj nule.

Primjedba

- 1 $0 \in R$ je trivijalni djelitelj nule.
- 2 R je integralna domena ako i samo ako je $0 \in R$ jedini djelitelj nule u R .

Propozicija

Neka je R komutativna integralna domena s jedinicom. Ako je R konačan skup, onda je R polje.

Primjer

Ako je p prosti broj, onda je $\mathbb{Z}_p$ polje.

Definicija

Neka je R prsten. Element $x \in R$ se naziva

- 1 lijevi djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $xy = 0$,
- 2 desni djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $yx = 0$.
- 3 Ako je x lijevi i desni djelitelj nule, onda se x naziva djelitelj nule.

Primjedba

- 1 $0 \in R$ je trivijalni djelitelj nule.
- 2 R je integralna domena ako i samo ako je $0 \in R$ jedini djelitelj nule u R .

Propozicija

Neka je R komutativna integralna domena s jedinicom. Ako je R konačan skup, onda je R polje.

Primjer

Ako je p prosti broj, onda je $\mathbb{Z}_p$ polje.

Definicija

Neka je R prsten. Element $x \in R$ se naziva

- 1 lijevi djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $xy = 0$,
- 2 desni djelitelj nule ako postoji $y \in R$, $y \neq 0$, takav da je $yx = 0$.
- 3 Ako je x lijevi i desni djelitelj nule, onda se x naziva djelitelj nule.

Primjedba

- 1 $0 \in R$ je trivijalni djelitelj nule.
- 2 R je integralna domena ako i samo ako je $0 \in R$ jedini djelitelj nule u R .

Definicija

Neka je R prsten.

- 1 Kažemo da je $a \in R$ nilpotentan ako postoji $n \in \mathbb{N}$ takav da je $a^n = 0$.
- 2 Kažemo da je $a \in R$ idempotentan ako je $a^2 = a$.

Podprsten i karakteristika prstena

Definicija

Neka je $(R, +, \cdot)$ prsten, i neka je $S \subseteq R$ neprazni podskup. Ako je $(S, +, \cdot)$ prsten, tada S nazivamo podprsten od R .

- 1 S je aditivna podgrupa od R ,
- 2 S je zatvoren na množenje.

Propozicija

Neka je R prsten. Neprazni podskup $S \subseteq R$ je podprsten od R ako za svaki $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Definicija

Neka je R prsten. Skup

$$Z(R) = \{a \in R \mid xa = ax \text{ za svaki } x \in R\}$$

se naziva centar prstena R .

Podprsten i karakteristika prstena

Definicija

Neka je $(R, +, \cdot)$ prsten, i neka je $S \subseteq R$ neprazni podskup. Ako je $(S, +, \cdot)$ prsten, tada S nazivamo podprsten od R .

- 1 S je aditivna podgrupa od R ,
- 2 S je zatvoren na množenje.

Propozicija

Neka je R prsten. Neprazni podskup $S \subseteq R$ je podprsten od R ako za svaki $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Definicija

Neka je R prsten. Skup

$$Z(R) = \{a \in R \mid xa = ax \text{ za svaki } x \in R\}$$

se naziva centar prstena R .

Podprsten i karakteristika prstena

Definicija

Neka je $(R, +, \cdot)$ prsten, i neka je $S \subseteq R$ neprazni podskup. Ako je $(S, +, \cdot)$ prsten, tada S nazivamo podprsten od R .

- 1 S je aditivna podgrupa od R ,
- 2 S je zatvoren na množenje.

Propozicija

Neka je R prsten. Neprazni podskup $S \subseteq R$ je podprsten od R ako za svaki $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Definicija

Neka je R prsten. Skup

$$Z(R) = \{a \in R \mid xa = ax \text{ za svaki } x \in R\}$$

se naziva centar prstena R .

Podprsten i karakteristika prstena

Definicija

Neka je $(R, +, \cdot)$ prsten, i neka je $S \subseteq R$ neprazni podskup. Ako je $(S, +, \cdot)$ prsten, tada S nazivamo podprsten od R .

- 1 S je aditivna podgrupa od R ,
- 2 S je zatvoren na množenje.

Propozicija

Neka je R prsten. Neprazni podskup $S \subseteq R$ je podprsten od R ako za svaki $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Definicija

Neka je R prsten. Skup

$$Z(R) = \{a \in R \mid xa = ax \text{ za svaki } x \in R\}$$

se naziva centar prstena R .

Propozicija

Centar prstena R je podprsten od R .

Definicija

Neka je R prsten. Pretpostavimo da postoji prirodni broj n takav da je $na = 0$ za svaki element $a \in R$. Najmanji takav prirodni broj naziva se karakteristika prstena R . Ako takav broj ne postoji, onda kažemo da R ima karakteristiku nula.

$\text{char}(R)$ karakteristika prstena R

Teorem

Ako je F polje, onda je $\text{char}(F)$ nula ili prosti broj.

Propozicija

Centar prstena R je podprsten od R .

Definicija

Neka je R prsten. Pretpostavimo da postoji prirodni broj n takav da je $na = 0$ za svaki element $a \in R$. Najmanji takav prirodni broj naziva se karakteristika prstena R . Ako takav broj ne postoji, onda kažemo da R ima karakteristiku nula.

$\text{char}(R)$ karakteristika prstena R

Teorem

Ako je F polje, onda je $\text{char}(F)$ nula ili prosti broj.

Propozicija

Centar prstena R je podprsten od R .

Definicija

Neka je R prsten. Pretpostavimo da postoji prirodni broj n takav da je $na = 0$ za svaki element $a \in R$. Najmanji takav prirodni broj naziva se karakteristika prstena R . Ako takav broj ne postoji, onda kažemo da R ima karakteristiku nula.

$\text{char}(R)$ karakteristika prstena R

Teorem

Ako je F polje, onda je $\text{char}(F)$ nula ili prosti broj.

Prsten kvaterniona

- Prsten kvaterniona je proširenje prstena kompleksnih brojeva

$$z = a + bi, \quad i^2 = -1, \quad a, b \in \mathbb{R}.$$

- Kvaternioni su prvi primjer nekomutativnog prstena s dijeljenjem (R. Hamilton 1843.).
- Kvaternioni su brojevi oblika

$$x = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R},$$

gdje i, j i k zadovoljavaju tablicu množenja

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Prsten kvaterniona

- Prsten kvaterniona je proširenje prstena kompleksnih brojeva

$$z = a + bi, \quad i^2 = -1, \quad a, b \in \mathbb{R}.$$

- Kvaternioni su prvi primjer nekomutativnog prstena s dijeljenjem (R. Hamilton 1843.).
- Kvaternioni su brojevi oblika

$$x = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R},$$

gdje i, j i k zadovoljavaju tablicu množenja

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Prsten kvaterniona

- Prsten kvaterniona je proširenje prstena kompleksnih brojeva

$$z = a + bi, \quad i^2 = -1, \quad a, b \in \mathbb{R}.$$

- Kvaternioni su prvi primjer nekomutativnog prstena s dijeljenjem (R. Hamilton 1843.).
- Kvaternioni su brojevi oblika

$$x = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R},$$

gdje i, j i k zadovoljavaju tablicu množenja

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Prsten kvaterniona

- Prsten kvaterniona je proširenje prstena kompleksnih brojeva

$$z = a + bi, \quad i^2 = -1, \quad a, b \in \mathbb{R}.$$

- Kvaternioni su prvi primjer nekomutativnog prstena s dijeljenjem (R. Hamilton 1843.).
- Kvaternioni su brojevi oblika

$$x = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R},$$

gdje i, j i k zadovoljavaju tablicu množenja

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Prsten kvaterniona

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

Nula u $\mathbb{H}$: $0 \equiv 0 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Jedinica u $\mathbb{H}$: $1 \equiv 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Ako je $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$, onda je

$$x^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

Prsten kvaterniona

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

Nula u $\mathbb{H}$: $0 \equiv 0 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Jedinica u $\mathbb{H}$: $1 \equiv 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Ako je $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$, onda je

$$x^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

Prsten kvaterniona

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

Nula u $\mathbb{H}$: $0 \equiv 0 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Jedinica u $\mathbb{H}$: $1 \equiv 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$

Ako je $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$, onda je

$$x^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

Prsten matrica

Neka je R prsten. Matricu reda n nad prstenom R definiramo na standardni način kao

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \quad a_{ij} \in R, \quad 1 \leq i, j \leq n.$$

Zbrajanje i množenje matrica definiramo sa

$$A + B = (a_{ij} + b_{ij}),$$

$$AB = \left(\sum_{k=1}^n a_{ik} b_{kj} \right).$$

$M(n, R)$ prsten matrica reda n nad R

Prsten matrica

Neka je R prsten. Matricu reda n nad prstenom R definiramo na standardni način kao

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \quad a_{ij} \in R, \quad 1 \leq i, j \leq n.$$

Zbrajanje i množenje matrica definiramo sa

$$A + B = (a_{ij} + b_{ij}),$$

$$AB = \left(\sum_{k=1}^n a_{ik} b_{kj} \right).$$

$M(n, R)$ prsten matrica reda n nad R

Ako R ima jedinicu $1 \in R$, onda je jedinica u $M(n, R)$ jedinična matrica

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Ako je R komutativni prsten s jedinicom, onda možemo definirati determinantu matrice $A \in M(n, R)$ na standardni način kao

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

Ako R ima jedinicu $1 \in R$, onda je jedinica u $M(n, R)$ jedinična matrica

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Ako je R komutativni prsten s jedinicom, onda možemo definirati determinantu matrice $A \in M(n, R)$ na standardni način kao

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Binet-Caucheyev teorem

Neka je R komutativni prsten s jedinicom i neka su $A, B \in M(n, R)$. Tada vrijedi

$$\det(AB) = \det(A) \det(B).$$

Teorem

Neka je R komutativni prsten s jedinicom. Onda je $A \in M(n, R)$ invertibilna matrica ako i samo ako $\det(A)$ ima inverz u R .

Binet-Caucheyev teorem

Neka je R komutativni prsten s jedinicom i neka su $A, B \in M(n, R)$. Tada vrijedi

$$\det(AB) = \det(A) \det(B).$$

Teorem

Neka je R komutativni prsten s jedinicom. Onda je $A \in M(n, R)$ invertibilna matrica ako i samo ako $\det(A)$ ima inverz u R .

Prsten grupe

Neka je R prsten s jedinicom $1 \in R$ i neka je $G = \{g_1, g_2, \dots, g_n\}$ konačna grupa (označimo $g_1 = e$).

Definirajmo skup konačnih formalnih suma

$$RG = \left\{ \sum_{i=1}^n a_i g_i \mid n \geq 1, a \in R, g_i \in G \right\}.$$

Kraće pišemo

$$ae = a, \quad a \in R, \quad 1g = g, \quad g \in G \quad (1)$$

Na RG možemo uvesti strukturu prstena na sljedeći način:

Zbrajanje u RG definiramo sa

$$\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i.$$

Prsten grupe

Neka je R prsten s jedinicom $1 \in R$ i neka je $G = \{g_1, g_2, \dots, g_n\}$ konačna grupa (označimo $g_1 = e$).

Definirajmo skup konačnih formalnih suma

$$RG = \left\{ \sum_{i=1}^n a_i g_i \mid n \geq 1, a \in R, g_i \in G \right\}.$$

Kraće pišemo

$$ae = a, \quad a \in R, \quad 1g = g, \quad g \in G \quad (1)$$

Na RG možemo uvesti strukturu prstena na sljedeći način:

Zbrajanje u RG definiramo sa

$$\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i.$$

Prsten grupe

Neka je R prsten s jedinicom $1 \in R$ i neka je $G = \{g_1, g_2, \dots, g_n\}$ konačna grupa (označimo $g_1 = e$).

Definirajmo skup konačnih formalnih suma

$$RG = \left\{ \sum_{i=1}^n a_i g_i \mid n \geq 1, a \in R, g_i \in G \right\}.$$

Kraće pišemo

$$ae = a, \quad a \in R, \quad 1g = g, \quad g \in G \quad (1)$$

Na RG možemo uvesti strukturu prstena na sljedeći način:

Zbrajanje u RG definiramo sa

$$\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i.$$

Množenje definiramo sa

$$(ag_i)(bg_j) = (ab)g_k, \quad \text{gdje je } g_k = g_i g_j,$$

i linearno proširimo na formalne sume,

$$\left(\sum_{i=1}^n a_i g_i \right) \left(\sum_{j=1}^n b_j g_j \right) = \sum_{k=1}^n c_k g_k,$$

gdje je

$$c_k = \sum_{g_i g_j = g_k} a_i b_j.$$

Za svaku grupu G , $|G| > 1$, prsten RG ima djelitelje nule $e - g$, $g \neq e$.

Množenje definiramo sa

$$(ag_i)(bg_j) = (ab)g_k, \quad \text{gdje je } g_k = g_i g_j,$$

i linearno proširimo na formalne sume,

$$\left(\sum_{i=1}^n a_i g_i \right) \left(\sum_{j=1}^n b_j g_j \right) = \sum_{k=1}^n c_k g_k,$$

gdje je

$$c_k = \sum_{g_i g_j = g_k} a_i b_j.$$

Za svaku grupu G , $|G| > 1$, prsten RG ima djelitelje nule $e - g$, $g \neq e$.

Definicija

Neka je R prsten i neka je I aditivna pogrupa od R .

- 1 I je lijevi ideal od R ako je $ra \in I$ za sve $a \in I, r \in R$.
- 2 I je desni ideal od R ako je $ar \in I$ za sve $a \in I, r \in R$.

Kažemo da je $I \subseteq R$ dvostrani ideal ako je I lijevi i desni ideal.

Teorem

Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Propozicija

Neka je $\{I_k\}_{k \in J}$ familija ideala u prstenu R . Onda je $\bigcap_{k \in J} I_k$ ideal u prstenu R .

Definicija

Neka je R prsten i neka je I aditivna pogrupa od R .

- 1 I je lijevi ideal od R ako je $ra \in I$ za sve $a \in I, r \in R$.
- 2 I je desni ideal od R ako je $ar \in I$ za sve $a \in I, r \in R$.

Kažemo da je $I \subseteq R$ dvostrani ideal ako je I lijevi i desni ideal.

Teorem

Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Propozicija

Neka je $\{I_k\}_{k \in J}$ familija ideala u prstenu R . Onda je $\bigcap_{k \in J} I_k$ ideal u prstenu R .

Definicija

Neka je R prsten i neka je I aditivna pogrupa od R .

1 I je lijevi ideal od R ako je $ra \in I$ za sve $a \in I, r \in R$.

2 I je desni ideal od R ako je $ar \in I$ za sve $a \in I, r \in R$.

Kažemo da je $I \subseteq R$ dvostrani ideal ako je I lijevi i desni ideal.

Teorem

Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Propozicija

Neka je $\{I_k\}_{k \in J}$ familija ideala u prstenu R . Onda je $\bigcap_{k \in J} I_k$ ideal u prstenu R .

Definicija

Neka je R prsten i neka je I aditivna pogrupa od R .

1 I je lijevi ideal od R ako je $ra \in I$ za sve $a \in I, r \in R$.

2 I je desni ideal od R ako je $ar \in I$ za sve $a \in I, r \in R$.

Kažemo da je $I \subseteq R$ dvostrani ideal ako je I lijevi i desni ideal.

Teorem

Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Propozicija

Neka je $\{I_k\}_{k \in J}$ familija ideala u prstenu R . Onda je $\bigcap_{k \in J} I_k$ ideal u prstenu R .

Definicija

Neka je R prsten i neka je I aditivna pogrupa od R .

1 I je lijevi ideal od R ako je $ra \in I$ za sve $a \in I, r \in R$.

2 I je desni ideal od R ako je $ar \in I$ za sve $a \in I, r \in R$.

Kažemo da je $I \subseteq R$ dvostrani ideal ako je I lijevi i desni ideal.

Teorem

Neka su A i B ideali u prstenu R . Tada je skup

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

ideal u prstenu R .

Propozicija

Neka je $\{I_k\}_{k \in J}$ familija ideala u prstenu R . Onda je $\bigcap_{k \in J} I_k$ ideal u prstenu R .

Ideali generirani podskupom S prstena R

- $(S)_L$ najmanji lijevi ideal u R koji sadrži skup S
- $(S)_R$ najmanji desni ideal u R koji sadrži skup S
- (S) najmanji (dvostrani) ideal u R koji sadrži skup S

Ideal (S) možemo dobiti kao presjek

$$(S) = \bigcap_{I \in \mathcal{F}} I, \quad \mathcal{F} = \{I \subseteq R \mid I \text{ ideal u } R, S \subseteq I\}$$

Definicija

- 1 Ako je S konačan podskup prstena R , onda kažemo da je ideal (S) konačno generiran.
- 2 Ideal generiran elementom $a \in R$ nazivamo glavni ideal i označavamo sa (a) .

Ideali generirani podskupom S prstena R

$(S)_L$ najmanji lijevi ideal u R koji sadrži skup S

$(S)_R$ najmanji desni ideal u R koji sadrži skup S

(S) najmanji (dvostrani) ideal u R koji sadrži skup S

Ideal (S) možemo dobiti kao presjek

$$(S) = \bigcap_{I \in \mathcal{F}} I, \quad \mathcal{F} = \{I \subseteq R \mid I \text{ ideal u } R, S \subseteq I\}$$

Definicija

- 1 Ako je S konačan podskup prstena R , onda kažemo da je ideal (S) konačno generiran.
- 2 Ideal generiran elementom $a \in R$ nazivamo glavni ideal i označavamo sa (a) .

Ideali generirani podskupom S prstena R

$(S)_L$ najmanji lijevi ideal u R koji sadrži skup S

$(S)_R$ najmanji desni ideal u R koji sadrži skup S

(S) najmanji (dvostrani) ideal u R koji sadrži skup S

Ideal (S) možemo dobiti kao presjek

$$(S) = \bigcap_{I \in \mathcal{F}} I, \quad \mathcal{F} = \{I \subseteq R \mid I \text{ ideal u } R, S \subseteq I\}$$

Definicija

- 1 Ako je S konačan podskup prstena R , onda kažemo da je ideal (S) konačno generiran.
- 2 Ideal generiran elementom $a \in R$ nazivamo glavni ideal i označavamo sa (a) .

Konstrukcije nekih ideala

Neka je R prsten s jedinicom i neka je $a \in R$. Onda je

$$(a)_L = \{ra \mid r \in R\} \equiv Ra$$

$$(a)_R = \{ar \mid r \in R\} \equiv aR$$

$$(a) = \left\{ \sum_i r_i a s_i \mid r_i, s_i \in R \right\} \equiv RaR$$

Neka je I ideal u prstenu R . Na skupu susjednih klasa

$$R/I = \{a + I \mid a \in R\}$$

možemo definirati strukturu prstena uvodeći zbrajanja i množenje sa

$$(a + I) + (b + I) = (a + b) + I, \tag{2}$$

$$(a + I)(b + I) = ab + I, \quad a, b \in R. \tag{3}$$

Definicija

Neka je I ideal u prstenu R . Skup R/I s binarnim operacijama (2) i (3) se naziva kvocijenti prsten.

Neka je I ideal u prstenu R . Na skupu susjednih klasa

$$R/I = \{a + I \mid a \in R\}$$

možemo definirati strukturu prstena uvodeći zbrajanja i množenje sa

$$(a + I) + (b + I) = (a + b) + I, \tag{2}$$

$$(a + I)(b + I) = ab + I, \quad a, b \in R. \tag{3}$$

Definicija

Neka je I ideal u prstenu R . Skup R/I s binarnim operacijama (2) i (3) se naziva kvocijentni prsten.

Homomorfizmi prstena

Definicija

Neka su R i S prsteni. Preslikavanje $f: R \rightarrow S$ koje zadovoljava

$$\text{1} \quad f(a + b) = f(a) + f(b),$$

$$\text{2} \quad f(ab) = f(a)f(b),$$

za sve $a, b \in R$ naziva se homomorfizam prstena.

Ako je $f: R \rightarrow S$ bijekcija, onda kažemo da je f izomorfizam prstena i pišemo $R \simeq S$.

Definicija

Neka je $f: R \rightarrow S$ homomorfizam prstena. Jezgra homomorfizma je skup

$$\ker(f) = \{a \in R \mid f(a) = 0\}.$$

Homomorfizmi prstena

Definicija

Neka su R i S prsteni. Preslikavanje $f: R \rightarrow S$ koje zadovoljava

1 $f(a + b) = f(a) + f(b),$

2 $f(ab) = f(a)f(b),$

za sve $a, b \in R$ naziva se homomorfizam prstena.

Ako je $f: R \rightarrow S$ bijekcija, onda kažemo da je f izomorfizam prstena i pišemo $R \simeq S$.

Definicija

Neka je $f: R \rightarrow S$ homomorfizam prstena. Jezgra homomorfizma je skup

$$\ker(f) = \{a \in R \mid f(a) = 0\}.$$

Homomorfizmi prstena

Definicija

Neka su R i S prsteni. Preslikavanje $f: R \rightarrow S$ koje zadovoljava

$$\mathbf{1} \quad f(a + b) = f(a) + f(b),$$

$$\mathbf{2} \quad f(ab) = f(a)f(b),$$

za sve $a, b \in R$ naziva se homomorfizam prstena.

Ako je $f: R \rightarrow S$ bijekcija, onda kažemo da je f izomorfizam prstena i pišemo $R \simeq S$.

Definicija

Neka je $f: R \rightarrow S$ homomorfizam prstena. Jezgra homomorfizma je skup

$$\ker(f) = \{a \in R \mid f(a) = 0\}.$$

Teorem

Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Tada vrijedi:

- 1 $f(0_R) = 0_S$ gdje su 0_R i 0_S nule u prstenu R i S , redom,
- 2 $f(-a) = -f(a)$ za svaki $a \in R$,
- 3 f je injektivni homomorfizam ako i samo ako je $\ker(f) = \{0_R\}$.

Teorem

Neka su R i S prsteni i neka je $f: R \rightarrow S$ homomorfizam.

- 1 Jezgra $\ker(f)$ je ideal u R .
- 2 Slika $\text{Im}(f)$ je podprsten od S .
- 3 Ako je R komutativan, onda je $\text{Im}(f)$ komutativni podprsten od S .
- 4 Ako R ima jedinicu 1 , onda je $f(1)$ jedinica u $\text{Im}(f)$.

Teorem

Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Tada vrijedi:

- 1 $f(0_R) = 0_S$ gdje su 0_R i 0_S nule u prstenu R i S , redom,
- 2 $f(-a) = -f(a)$ za svaki $a \in R$,
- 3 f je injektivni homomorfizam ako i samo ako je $\ker(f) = \{0_R\}$.

Teorem

Neka su R i S prsteni i neka je $f: R \rightarrow S$ homomorfizam.

- 1 Jezgra $\ker(f)$ je ideal u R .
- 2 Slika $\text{Im}(f)$ je podprsten od S .
- 3 Ako je R komutativan, onda je $\text{Im}(f)$ komutativni podprsten od S .
- 4 Ako R ima jedinicu 1 , onda je $f(1)$ jedinica u $\text{Im}(f)$.

Fundamentalni teorem o homomorfizmu

Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Onda je

$$R/\ker(f) \simeq \operatorname{Im}(f).$$

Teorem

Neka je I ideal u prstenu R . Tada je svaki ideal u R/I oblika A/I gdje je $A \subseteq R$ ideal koji sadrži I .

Fundamentalni teorem o homomorfizmu

Neka je $f: R \rightarrow S$ homomorfizam iz prstena R u prsten S . Onda je

$$R/\ker(f) \simeq \operatorname{Im}(f).$$

Teorem

Neka je I ideal u prstenu R . Tada je svaki ideal u R/I oblika A/I gdje je $A \subseteq R$ ideal koji sadrži I .

Definicija

Neka je R prsten. Svaka funkcija $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ sa svojstvom $\phi(0) = 0$ i $\phi(a) > 0$ za $a \neq 0$ naziva se norma na prstenu R .

Prsteni u kojima možemo generalizirati dijeljenje s ostatkom nazivamo euklidske domene.

Definicija

Neka je R komutativna integralna domena s jedinicom. Kažemo da je R euklidska domena ako postoji norma $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ takva da za sve $a, b \in R$, $b \neq 0$, postoje $q, r \in R$ takvi da je

$$a = bq + r \quad \text{gdje je} \quad \phi(r) < \phi(b). \quad (4)$$

Rastav (4) nazivamo **algoritam dijeljenja**.

Definicija

Neka je R prsten. Svaka funkcija $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ sa svojstvom $\phi(0) = 0$ i $\phi(a) > 0$ za $a \neq 0$ naziva se norma na prstenu R .

Prsteni u kojima možemo generalizirati dijeljenje s ostatkom nazivamo euklidske domene.

Definicija

Neka je R komutativna integralna domena s jedinicom. Kažemo da je R euklidska domena ako postoji norma $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ takva da za sve $a, b \in R$, $b \neq 0$, postoje $q, r \in R$ takvi da je

$$a = bq + r \quad \text{gdje je} \quad \phi(r) < \phi(b). \quad (4)$$

Rastav (4) nazivamo **algoritam dijeljenja**.

Definicija

Neka je R prsten. Svaka funkcija $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ sa svojstvom $\phi(0) = 0$ i $\phi(a) > 0$ za $a \neq 0$ naziva se norma na prstenu R .

Prsteni u kojima možemo generalizirati dijeljenje s ostatkom nazivamo euklidske domene.

Definicija

Neka je R komutativna integralna domena s jedinicom. Kažemo da je R euklidska domena ako postoji norma $\phi: R \rightarrow \mathbb{N} \cup \{0\}$ takva da za sve $a, b \in R$, $b \neq 0$, postoje $q, r \in R$ takvi da je

$$a = bq + r \quad \text{gdje je} \quad \phi(r) < \phi(b). \quad (4)$$

Rastav (4) nazivamo **algoritam dijeljenja**.

Definicija

- Prsten u kojem je svaki ideal glavni naziva se prsten glavnih ideala.
- Komutativna integralna domena s jedinicom u kojoj je svaki ideal glavni naziva se domena glavnih ideala.

Teorem

Svaka euklidska domena je domena glavnih ideala.

Definicija

- Prsten u kojem je svaki ideal glavni naziva se prsten glavnih ideala.
- Komutativna integralna domena s jedinicom u kojoj je svaki ideal glavni naziva se domena glavnih ideala.

Teorem

Svaka euklidska domena je domena glavnih ideala.

Prsten polinoma

Neka je R komutativni prsten s jedinicom. Polinom u varijabli x nad prstenom R je formalna suma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0, \quad a_k \in R.$$

a_n vodeći koeficijent, a_nx^n vodeći član

- Polinom $f(x) = a_0$ se naziva konstantni polinom.
- Skup svih polinoma nad prstenom R označavamo sa $R[x]$.

Zbrajanje i množenje polinoma definiramo na standardni način.

$$f(x) = \sum_{k=0}^n a_k x^k, \quad g(x) = \sum_{k=0}^m b_k x^k$$

■ Zbrajanje

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$$

Prsten polinoma

Neka je R komutativni prsten s jedinicom. Polinom u varijabli x nad prstenom R je formalna suma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0, \quad a_k \in R.$$

a_n vodeći koeficijent, a_nx^n vodeći član

- Polinom $f(x) = a_0$ se naziva konstantni polinom.
- Skup svih polinoma nad prstenom R označavamo sa $R[x]$.

Zbrajanje i množenje polinoma definiramo na standardni način.

$$f(x) = \sum_{k=0}^n a_k x^k, \quad g(x) = \sum_{k=0}^m b_k x^k$$

■ Zbrajanje

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$$

Prsten polinoma

Neka je R komutativni prsten s jedinicom. Polinom u varijabli x nad prstenom R je formalna suma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0, \quad a_k \in R.$$

a_n vodeći koeficijent, a_nx^n vodeći član

- Polinom $f(x) = a_0$ se naziva konstantni polinom.
- Skup svih polinoma nad prstenom R označavamo sa $R[x]$.

Zbrajanje i množenje polinoma definiramo na standardni način.

$$f(x) = \sum_{k=0}^n a_k x^k, \quad g(x) = \sum_{k=0}^m b_k x^k$$

1 Zbrajanje

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$$

2 Množenje

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$$

Definicija

Skup $R[x]$ s operacijama zbrajanja i množenja polinoma nazivamo prsten polinoma nad R .

- Nula u $R[x]$ je nul-polinom $f(x) = 0$
- Jedinica u $R[x]$ je konstantni polinom $f(x) = 1$

Stupanj polinoma

Neka je

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0.$$

$$\deg(f(x)) = n$$

$$\deg(0) = -\infty \quad \text{ako je } f(x) = 0 \text{ nul-polinom}$$

Simbol $-\infty$ zadovoljava uobičajenu konvenciju:

$$-\infty < n, \quad -\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty \quad \forall n \geq 0.$$

2 Množenje

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$$

Definicija

Skup $R[x]$ s operacijama zbrajanja i množenja polinoma nazivamo prsten polinoma nad R .

- Nula u $R[x]$ je nul-polinom $f(x) = 0$
- Jedinica u $R[x]$ je konstantni polinom $f(x) = 1$

Stupanj polinoma

Neka je

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0.$$

$$\deg(f(x)) = n$$

$$\deg(0) = -\infty \quad \text{ako je } f(x) = 0 \text{ nul-polinom}$$

Simbol $-\infty$ zadovoljava uobičajenu konvenciju:

$$-\infty < n, \quad -\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty \quad \forall n \geq 0.$$

2 Množenje

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$$

Definicija

Skup $R[x]$ s operacijama zbrajanja i množenja polinoma nazivamo prsten polinoma nad R .

- Nula u $R[x]$ je nul-polinom $f(x) = 0$
- Jedinica u $R[x]$ je konstantni polinom $f(x) = 1$

Stupanj polinoma

Neka je

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0.$$

$$\deg(f(x)) = n$$

$$\deg(0) = -\infty \quad \text{ako je } f(x) = 0 \text{ nul-polinom}$$

Simbol $-\infty$ zadovoljava uobičajenu konvenciju:

$$-\infty < n, \quad -\infty + (-\infty) = -\infty, \quad -\infty + n = -\infty \quad \forall n \geq 0.$$

Za stupanj polinoma vrijedi

$$\begin{aligned}\deg(f(x) + g(x)) &\leq \max(\deg(f(x)), \deg(g(x))), \\ \deg(f(x)g(x)) &\leq \deg(f(x)) + \deg(g(x)),\end{aligned}$$

Primjedba

Prsten R promatramo kao podprsten konstantnih polinoma u $R[x]$ i pišemo $R \subset R[x]$.

Propozicija

Neka je R integralna domena. Onda je

- 1 $R[x]$ integralna domena,
- 2 $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

Za stupanj polinoma vrijedi

$$\begin{aligned}\deg(f(x) + g(x)) &\leq \max(\deg(f(x)), \deg(g(x))), \\ \deg(f(x)g(x)) &\leq \deg(f(x)) + \deg(g(x)),\end{aligned}$$

Primjedba

Prsten R promatramo kao podprsten konstantnih polinoma u $R[x]$ i pišemo $R \subset R[x]$.

Propozicija

Neka je R integralna domena. Onda je

- 1 $R[x]$ integralna domena,
- 2 $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

Euklidov algoritam

Neka je R komutativni prsten s jedinicom, i neka su $f(x), g(x) \in R[x]$ gdje je $g(x) \neq 0$. Ako vodeći koeficijent od $g(x)$ ima inverz u R , onda postoje jedinstveni polinomi $q(x), r(x) \in R[x]$ takvi da je

$$f(x) = q(x)g(x) + r(x), \quad \deg(r(x)) < \deg(g(x)).$$

Teorem

Ako je F polje, onda je $F[x]$ domena glavnih ideala.

Euklidov algoritam

Neka je R komutativni prsten s jedinicom, i neka su $f(x), g(x) \in R[x]$ gdje je $g(x) \neq 0$. Ako vodeći koeficijent od $g(x)$ ima inverz u R , onda postoje jedinstveni polinomi $q(x), r(x) \in R[x]$ takvi da je

$$f(x) = q(x)g(x) + r(x), \quad \deg(r(x)) < \deg(g(x)).$$

Teorem

Ako je F polje, onda je $F[x]$ domena glavnih ideala.

Ireducibilnost polinoma

Definicija

Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je

1 $\deg(f(x)) \geq 1$ i ako

2 $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x] \Rightarrow g(x) \in F$ ili $h(x) \in F$.

Definicija

Neka je R podprsten komutativnog prstena S , i neka je $f(x) \in R[x]$. Kažemo da je $\alpha \in S$ korijen polinoma $f(x)$ u prstenu S ako je $f(\alpha) = 0$.

Teorem

Neka je F polje i neka je $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$.

1 $\alpha \in F$ je korijen polinoma $f(x)$ ako i samo ako $x - \alpha$ dijeli $f(x)$.

2 $f(x)$ ima najviše n korijena u polju F .

Ireducibilnost polinoma

Definicija

Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je

1 $\deg(f(x)) \geq 1$ i ako

2 $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x] \Rightarrow g(x) \in F$ ili $h(x) \in F$.

Definicija

Neka je R podprsten komutativnog prstena S , i neka je $f(x) \in R[x]$. Kažemo da je $\alpha \in S$ korijen polinoma $f(x)$ u prstenu S ako je $f(\alpha) = 0$.

Teorem

Neka je F polje i neka je $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$.

1 $\alpha \in F$ je korijen polinoma $f(x)$ ako i samo ako $x - \alpha$ dijeli $f(x)$.

2 $f(x)$ ima najviše n korijena u polju F .

Ireducibilnost polinoma

Definicija

Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je

1 $\deg(f(x)) \geq 1$ i ako

2 $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x] \Rightarrow g(x) \in F$ ili $h(x) \in F$.

Definicija

Neka je R podprsten komutativnog prstena S , i neka je $f(x) \in R[x]$. Kažemo da je $\alpha \in S$ korijen polinoma $f(x)$ u prstenu S ako je $f(\alpha) = 0$.

Teorem

Neka je F polje i neka je $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$.

1 $\alpha \in F$ je korijen polinoma $f(x)$ ako i samo ako $x - \alpha$ dijeli $f(x)$.

2 $f(x)$ ima najviše n korijena u polju F .

Ireducibilnost polinoma

Definicija

Neka je F polje. Kažemo da je polinom $f(x) \in F[x]$ ireducibilan nad poljem F ako je

1 $\deg(f(x)) \geq 1$ i ako

2 $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x] \Rightarrow g(x) \in F$ ili $h(x) \in F$.

Definicija

Neka je R podprsten komutativnog prstena S , i neka je $f(x) \in R[x]$. Kažemo da je $\alpha \in S$ korijen polinoma $f(x)$ u prstenu S ako je $f(\alpha) = 0$.

Teorem

Neka je F polje i neka je $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$.

1 $\alpha \in F$ je korijen polinoma $f(x)$ ako i samo ako $x - \alpha$ dijeli $f(x)$.

2 $f(x)$ ima najviše n korijena u polju F .

Eisensteinov kriterij

Neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Ako postoji prosti broj p takav da

1 $p \mid a_k$ za $k = 0, 1, \dots, n-1$,

2 $p \nmid a_n$

3 i $p^2 \nmid a_0$,

onda je $f(x)$ ireducibilan nad poljem $\mathbb{Q}$.

Primjer

Neka je $p(x) = 3x^2 + 15x + 10 \in \mathbb{Z}[x]$. Odredite može li se $p(x)$ faktorizirati u prstenu $\mathbb{Q}[x]$.

Eisensteinov kriterij

Neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Ako postoji prosti broj p takav da

1 $p \mid a_k$ za $k = 0, 1, \dots, n-1$,

2 $p \nmid a_n$

3 i $p^2 \nmid a_0$,

onda je $f(x)$ ireducibilan nad poljem $\mathbb{Q}$.

Primjer

Neka je $p(x) = 3x^2 + 15x + 10 \in \mathbb{Z}[x]$. Odredite može li se $p(x)$ faktorizirati u prstenu $\mathbb{Q}[x]$.

Maksimalni ideali

Definicija

Kažemo da je R prosti prsten ako R nema netrivialnih ideala.

Primijetimo:

- Prosti prsten R ima samo trivijalne ideale $\{0\}$ i R .
- Svako polje je prosti prsten.

Definicija

Neka je R prsten. Kažemo da je A maksimalni ideal u R ako vrijedi:

- 1 $A \neq R$,
- 2 ako je B ideal u R i $B \supseteq A$, onda je $B = A$ ili $B = R$.

Primjer: $\{0\}$ je maksimalni ideal u polju F .

Definicija

Kažemo da je R prosti prsten ako R nema netrivialnih ideala.

Primijetimo:

- Prosti prsten R ima samo trivijalne ideale $\{0\}$ i R .
- Svako polje je prosti prsten.

Definicija

Neka je R prsten. Kažemo da je A maksimalni ideal u R ako vrijedi:

- 1 $A \neq R$,
- 2 ako je B ideal u R i $B \supseteq A$, onda je $B = A$ ili $B = R$.

Primjer: $\{0\}$ je maksimalni ideal u polju F .

Maksimalni ideali

Definicija

Kažemo da je R prosti prsten ako R nema netrivialnih ideala.

Primijetimo:

- Prosti prsten R ima samo trivijalne ideale $\{0\}$ i R .
- Svako polje je prosti prsten.

Definicija

Neka je R prsten. Kažemo da je A maksimalni ideal u R ako vrijedi:

- 1 $A \neq R$,
- 2 ako je B ideal u R i $B \supseteq A$, onda je $B = A$ ili $B = R$.

Primjer: $\{0\}$ je maksimalni ideal u polju F .

Maksimalni ideali

Definicija

Kažemo da je R prosti prsten ako R nema netrivialnih ideala.

Primijetimo:

- Prosti prsten R ima samo trivijalne ideale $\{0\}$ i R .
- Svako polje je prosti prsten.

Definicija

Neka je R prsten. Kažemo da je A maksimalni ideal u R ako vrijedi:

- 1 $A \neq R$,
- 2 ako je B ideal u R i $B \supseteq A$, onda je $B = A$ ili $B = R$.

Primjer: $\{0\}$ je maksimalni ideal u polju F .

Veza između prostih prstena i maksimalnih ideala je dana sljedećim teoremom.

Teorem

Neka je R prsten, i neka je $A \neq R$ ideal u R . Onda je A maksimalni ideal u R ako i samo ako je R/A prosti prsten.

Ako je R komutativni prsten s jedinicom, onda vrijedi sljedeći rezultat.

Teorem

Neka je R komutativni prsten s jedinicom. Ideal $M \subset R$ je maksimalan ako i samo ako je R/M polje.

Veza između prostih prstena i maksimalnih ideala je dana sljedećim teoremom.

Teorem

Neka je R prsten, i neka je $A \neq R$ ideal u R . Onda je A maksimalni ideal u R ako i samo ako je R/A prosti prsten.

Ako je R komutativni prsten s jedinicom, onda vrijedi sljedeći rezultat.

Teorem

Neka je R komutativni prsten s jedinicom. Ideal $M \subset R$ je maksimalan ako i samo ako je R/M polje.

U prstenu polinoma $F[x]$, maksimalni ideali su generirani ireducibilnim polinomima.

Teorem

Neka je F polje. Onda je $M \subseteq F[x]$ maksimalni ideal u $F[x]$ ako i samo ako je $M = (p(x))$ gdje je $p(x)$ ireducibilni polinom u $F[x]$.