Csoportok, gyűrűk, testek

Azokat a nem üres halmazokat, amelyekben értelmezve van egy művelet, és ez a művelet asszociatív, létezik benne egységelem, és minden elemnek létezik benne inverze, csoportnak nevezzük.

Megnézem a kapcsolódó epizódot

A kommutatív csoportokat Abel-csoportnak nevezzük.

Megnézem a kapcsolódó epizódot

Azt az elemet, amely a művelet elvégzése során mindenkit változatlanul hagy, egységelemnek nevezzük.

Megnézem a kapcsolódó epizódot

Egy elem akkor lesz inverz, ha azt tudja, hogy a művelet elvégzése során az eredeti elemből egységelemet csinál.

Például ha vesszük az 5-öt és a szorzás műveletet, akkor az 5-nek a szorzás műveletre vett inverze az $\frac{1}{5}$, mert $5 \cdot \frac{1}{5} = 1$, vagy ha vesszük a 2-öt és az összeadás műveletet, akkor a 2-nek az összeadás műveletre vett inverze a -2, mert $2 + (-2) = 0$.

Megnézem a kapcsolódó epizódot

Ha egy csoportban az elemeknek nincs inverze, és nincs egységelem sem, akkor félcsoportnak nevezzük.

Megnézem a kapcsolódó epizódot

Egy csoportot ciklikus csoportnak nevezünk, ha előáll egyetlen elemének egész kitevős hatványaiból.

Megnézem a kapcsolódó epizódot

Egy elem rendje azt a legkisebb pozitív egész kitevőt jelenti, amelyre emelve az egységelemeket kapjuk.

A rend jele: σ (ordó)

Megnézem a kapcsolódó epizódot

Egy nem üres halmazt gyűrűnek nevezünk, ha értelmezve van benne egy összeadás és egy szorzás művelet.

Az összeadásnak azt kell tudnia, hogy asszociatív és kommutatív.

$(a+b)+c=a+(b+c)$

$a+b=b+a$

Van egységelem. Az összeadás egységelemét nullelemnek hívjuk.

Minden elemnek van inverze, amit ellentettnek hívunk.

A szorzásnak pedig mindössze annyit kell tudnia, hogy asszociatív.

$(ab)c=a(bc)$

A két művelet pedig egymásra nézve disztributív:

$a(b+c)=ab+ac$

$(a+b)c=ac+bc$

Példák gyűrűre: egész számok, $(n \times n)$-es mátrixok, $\bmod m$ maradékosztályok

Megnézem a kapcsolódó epizódot

A kommutatív nullosztómentes gyűrűket nevezzük integritási tartománynak.

Megnézem a kapcsolódó epizódot

Az R gyűrűben az I részhalmazt ideálnak nevezzük, ha I részgyűrű R-ben és minden $r \in R$ és $i \in I$ elemre $r \cdot i \in I$

És mivel a szorzás nem feltétlenül kommutatív, léteznek bal és jobb ideálok.

Bal ideál:

Az R gyűrűben az I részhalmaz bal ideál, ha I részgyűrű R-ben és $\forall r \in R$ és $i \in I$ elemre $r \cdot i \in I$

Jobb ideál:

Az R gyűrűben az I részhalmaz jobb ideál, ha I részgyűrű R-ben és $\forall r \in R$ és $i \in I$ elemre $i \cdot r \in I$

Megnézem a kapcsolódó epizódot

Az egy elem által generált ideált főideálnak nevezzük.

Megnézem a kapcsolódó epizódot

Azokat a gyűrűket, amelyben minden ideál főideál, úgy hívjuk, hogy főideálgyűrű.

Használatos rájuk a PIR rövidítés is (Principal Ideal Ring).

Megnézem a kapcsolódó epizódot

Azokat a komplex számokat, ahol a és b egész szám Gauss egésznek nevezzük.

$$z = a + b \cdot i$$

Megnézem a kapcsolódó epizódot

A komplex számok abszolútértékének mintájára bevezetünk egy fogalmat, amit normának hívunk:

$$N(z) = |\, z \,|^2 = a^2 + b^2$$

Ha z_1 és z_2 Gauss egészek, akkor

$$z_1 \mid z_2 \Rightarrow N(z_1) \mid N(z_2)$$

Az állítás megfordítása nem igaz:

$$N(z_1) \mid N(z_2) \not\Rightarrow z_1 \mid z_2$$

Megnézem a kapcsolódó epizódot

A Gauss egészek gyűrűt alkotnak az összedás és szorzás műveletekkel.

A Gauss egészek tudják az oszthatóságot is, egy Gauss egész akkor oszt egy másikat, ha az osztás eredménye is Gauss egész.

A Gauss egészek körében négy darab egység van: $1, -1, i, -i$

Megnézem a kapcsolódó epizódot

A Gauss egészek gyűrűjében prímek azok a p_1 és p_2 Gauss egészek, amelyek szorzata $4k+1$ alakú prím:

$$p_1 \cdot p_2 = p$$

Megnézem a kapcsolódó epizódot

Az n szám akkor és csak akkor áll elő két négyzetszám összegeként

$$n = x^2 + y^2$$

ha kanonikus alakjában

$$n = 2^\gamma \cdot p_1^{\alpha_1} p_2^{\alpha_2} \dots q_1^{\beta_1} q_2^{\beta_2} \dots \qquad p_i = 4k-1 \quad q_i = 4k+1$$

minden $4k-1$ alakú prím kitevője páros.

Megnézem a kapcsolódó epizódot

Azokat a gyűrűket, amikben működik az Euklideszi algoritmus úgy hívjuk, hogy Euklideszi gyűrű.

Minden Euklideszi gyűrű egyben főideálgyűrű.

Euklideszi gyűrű például az egész számok gyűrűje, vagy éppen a Gauss egészek gyűrűje.

Megnézem a kapcsolódó epizódot

Azokat a gyűrűket, melyeknek van additív inverze, és a 0-tól eltekintve minden elemének van multiplikatív inverze is, testnek nevezzük.

Megnézem a kapcsolódó epizódot

---

9 test-axióma van, ezek:

1. Az összeadás asszociatív

2. Az összeadás kommutatív

3. Létezik nullelem az összeadás műveletben

4. Minden elemnek van additív inverze

5. A szorzás asszociatív

6. A szorzás kommutatív

7. Létezik egységelem a szorzás műveletben

8. Minden elemnek van multiplikatív inverze, kivéve a nullelemet

9. Az összeadás és szorzás művelet disztributív

Megnézem a kapcsolódó epizódot

A rendezés reláció négy fontos tulajdonságát rendezési axiómának nevezzük.

1. Trichotómia: Bármely a és b valós számra, az $a < b$, az $a = b$ és az $a > b$ állítások közül pontosan egy igaz.

2. Tranzitivitás: Bármely a, b és c valós számra, ha $a < b$ és $b < c$ akkor $a < c$.

3. Bármely a, b és c valós számra ha $a < b$ akkor $a + c < b + c$.

4. Bármely a, b és $c > 0$ valós számra, ha $a < b$ akkor $ac < bc$.

Megnézem a kapcsolódó epizódot

Minden számnál van nagyobb természetes szám. Ezt az állítást Arkhimédészi-axiómaként szokás emlegetni.

$$\forall x \in R \quad \exists n \in N \quad n > x$$

Az Arkhimédészi-axióma átfogalmazható úgy is, hogy bármely a és b pozitív számokra létezik olyan n természetes szám, hogy $an > b$

Sőt, átfogalmazható így is:

Bármely a és b pozitív számokra létezik olyan n természetes szám, hogy $\frac{a}{b} > \frac{1}{n}$

Ez pedig azt jelenti, hogy bármely pozitív számra létezik olyan n természetes szám, hogy az $\frac{1}{n}$ kisebb ennél a számnál.

Megnézem a kapcsolódó epizódot

A Cantor-axióma azt mondja, hogy egymásba skatulyázott zárt intervallumok végtelen sorozatának metszete nem üres.

Ha $a_1 \leq a_2 \leq \cdots \leq a_n$ és $b_1 \geq b_2 \geq \cdots \geq b_n$ akkor $\exists x \in R$

$x \in \bigcap_{i=1}^{\infty} [a_i, b_i]$

Megnézem a kapcsolódó epizódot