

# Egész számok definiálása HIT-kkel koherencia szabállyal és Kommutatív gyűrű tulajdonság formalizálása

Balázs Zoltán

Eötvös Loránd Tudományegyetem

2025. január 22.

# Egész szám definíciók

- Normálforma (zero, suc, pred - Agda-ban pos, negsuc):  $\text{pred}(\text{succ } z) = ?$
- HIT
  - Bi-Invertible (zero, suc, predr, suc-pred, predl, predl-suc)  
 $\text{predl} \equiv \text{predr}$  kell!
  - Koherencia szabállyal (zero, suc, pred, suc-pred, pred-suc, coh)

# Egész szám definíciók

- Normálforma (zero, suc, pred - Agda-ban pos, negsuc):  $\text{pred}(\text{succ } z) = ?$
- HIT
  - Bi-Invertible (zero, suc, predr, suc-predr, predl, predl-suc)  
 $\text{predl} \equiv \text{predr}$  kell!
  - Koherencia szabállyal (zero, suc, pred, suc-pred, pred-suc, coh)

# Egész szám definíciók

- Normálforma (zero, suc, pred - Agda-ban pos, negsuc):  $\text{pred}(\text{succ } z) = ?$
- HIT
  - Bi-Invertible (zero, suc, predr, suc-predr, predl, predl-suc)  
 $\text{predl} \equiv \text{predr}$  kell!
  - Koherencia szabállyal (zero, suc, pred, suc-pred, pred-suc, coh)

# Egész szám definíciók

- Normálforma (zero, suc, pred - Agda-ban pos, negsuc):  $\text{pred}(\text{succ } z) = ?$
- HIT
  - Bi-Invertible (zero, suc, predr, suc-predr, predl, predl-suc)  
 $\text{predl} \equiv \text{predr}$  kell!
  - Koherencia szabállyal (zero, suc, pred, suc-pred, pred-suc, coh)

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív



# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív

# Kommutatív gyűrű

- Az egész számok, összeadás és szorzás gyűrűt alkotnak
  - Az egész számok és összeadás Abel-csoportot alkotnak
    - Összeadás egységeleme létezik
    - Összeadás inverz eleme létezik
    - Összeadás asszociatív
    - Összeadás kommutatív
  - Az egész számok és szorzás egységelemes félcsoportot alkotnak
    - Szorzás egységeleme létezik
    - Szorzás asszociatív
  - A szorzás disztributív az összeadás felett
- Szorzás kommutatív



# Implementáció menete

- Egész számok definiálása

---

```
data  $\mathbb{Z}_h$  : Set where
  zero :  $\mathbb{Z}_h$ 
  succ :  $\mathbb{Z}_h \rightarrow \mathbb{Z}_h$ 
  pred :  $\mathbb{Z}_h \rightarrow \mathbb{Z}_h$ 
  sec  : (z :  $\mathbb{Z}_h$ )  $\rightarrow$  pred (succ z)  $\equiv$  z
  ret  : (z :  $\mathbb{Z}_h$ )  $\rightarrow$  succ (pred z)  $\equiv$  z
  coh  : (z :  $\mathbb{Z}_h$ )  $\rightarrow$  congS succ (sec z)  $\equiv$  ret (succ z)
```

---

- Izomorfizmus a normálforma definícióval
- Iterátor (+eliminátor) és induktív tulajdonság
- Műveletek definiálása
- Tulajdonságok formalizálása

# Implementáció menete

- Egész számok definiálása
- Izomorfizmus a normálforma definícióval

---

$\mathbb{Z}$ -iso : Iso  $\mathbb{Z}$   $\mathbb{Z}_h$

$\mathbb{Z}$ -iso .Iso.fun =  $\mathbb{Z} \rightarrow \mathbb{Z}_h$

$\mathbb{Z}$ -iso .Iso.inv =  $\mathbb{Z}_h \rightarrow \mathbb{Z}$

$\mathbb{Z}$ -iso .Iso.rightInv =  $\mathbb{Z}_h \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}_h$

$\mathbb{Z}$ -iso .Iso.leftInv =  $\mathbb{Z} \rightarrow \mathbb{Z}_h \rightarrow \mathbb{Z}$

---

- Iterátor (+eliminátor) és induktív tulajdonság
- Műveletek definiálása
- Tulajdonságok formalizálása

# Implementáció menete

- Egész számok definiálása
- Izomorfizmus a normálforma definícióval
- Iterátor (+eliminátor) és induktív tulajdonság
- Műveletek definiálása
- Tulajdonságok formalizálása

# Implementáció menete

- Egész számok definiálása
- Izomorfizmus a normálforma definícióval
- Iterátor (+eliminátor) és induktív tulajdonság
- Műveletek definiálása
- Tulajdonságok formalizálása

# Implementáció menete

- Egész számok definiálása
- Izomorfizmus a normálforma definícióval
- Iterátor (+eliminátor) és induktív tulajdonság
- Műveletek definiálása
- Tulajdonságok formalizálása

# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)

# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)

# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)



# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)

# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)

# Ez miért új? Mi a haszna?

- Az egész számok tényleg kommutatív gyűrűt alkotnak
- Egyszerűbb bebizonyítani tulajdonságokat mint a normálforma definícióval
- Kézenfoghatóbb HIT definíció mint a Bi-Invertible
- Automatikus levezetés összeadást, negálást (kivonást) és szorzást használó egyenlőségekre
- Eddig csak elméleti síkon volt belátva
- Eliminálhatunk magasabb univerzumba (típusok, Girard paradox, Russel paradox, System U)

Köszönöm a figyelmet!