Lineáris és absztrakt algebra, normál

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
Konzultáció: ewwkiss@gmail.com

https://algebra.elte.hu/nyitolap/oktatas-szakdolgozat/linearis-es-absztrakt-algebra/

12. előadás

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre,

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó:

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha műveletartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha műveletartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

(3) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha műveletartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

(3) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).

(4) $G = D_n$, $H = \mathbb{Z}_2^+$, $\varphi(x) = 0$ ha x forgatás, 1 ha teng. tükr.

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

(3) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).

(4) $G = D_n$, $H = \mathbb{Z}_2^+$, $\varphi(x) = 0$ ha x forgatás, 1 ha teng. tükr.

(5) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).

Homomorfizmus csoportokra

4.3.1. Definíció (ismétlés)

Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre.
A $\psi : G \to H$ leképezés csoporthomomorfizmus,
ha művelettartó: $\psi(a * b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re.
Ha ψ kölcsönösen egyértelmű, akkor ψ izomorfizmus.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ maradéka mod n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

(3) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).

(4) $G = D_n$, $H = \mathbb{Z}_2^+$, $\varphi(x) = 0$ ha x forgatás, 1 ha teng. tükr.

(5) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).

(6) $G = \mathbb{R}[x]^+$, $H = \mathbb{C}^+$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ izomorfizmus.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ izomorfizmus.

Példák

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ izomorfizmus.

Példák

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ izomorfizmus.

Példák

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

Homomorfizmus gyűrűkben

Definíció

Legyenek R és S gyűrűk.
Az R összeadása $+_R$, szorzása $*_R$.
Az S összeadása $+_S$, szorzása $*_S$.
A $\psi : R \to S$ leképezés gyűrűhomomorfizmus, ha az összeadást és a szorzást is tartja:
$\psi(a +_R b) = \psi(a) +_S \psi(b)$ minden $a, b \in R$-re,
$\psi(a *_R b) = \psi(a) *_S \psi(b)$ minden $a, b \in R$-re.
Ha ψ kölcsönösen egyértelmű is, akkor ψ izomorfizmus.

Példák

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

(3) $R = \mathbb{R}$, $S = \mathbb{C}$, $\varphi(r) = r + 0i$ az $\mathbb{R}$ beágyazása $\mathbb{C}$-be.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi,

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$$\varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G).$$

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva)

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.
Az inverzre vonatkozó állítás bizonyítása HF.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.
Az inverzre vonatkozó állítás bizonyítása HF.

4.3.15, 4.3.16. Gyakorlat

Legyen $\varphi : G \to H$ csoporthomomorfizmus és $g \in G$.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.
Az inverzre vonatkozó állítás bizonyítása HF.

4.3.15, 4.3.16. Gyakorlat

Legyen $\varphi : G \to H$ csoporthomomorfizmus és $g \in G$.
Ekkor $\varphi(g)$ rendje osztója g rendjének.

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.
Az inverzre vonatkozó állítás bizonyítása HF.

4.3.15, 4.3.16. Gyakorlat

Legyen $\varphi : G \to H$ csoporthomomorfizmus és $g \in G$.
Ekkor $\varphi(g)$ rendje osztója g rendjének.
Oka: φ tartja az egész kitevőjű hatványozást:

Elemi tulajdonságok csoportokra

2.2.44. Feladat

Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor
φ az egységelemet az egységelembe viszi, és inverz képe
a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás

$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$.
Az inverzre vonatkozó állítás bizonyítása HF.

4.3.15, 4.3.16. Gyakorlat

Legyen $\varphi : G \to H$ csoporthomomorfizmus és $g \in G$.
Ekkor $\varphi(g)$ rendje osztója g rendjének.
Oka: φ tartja az egész kitevőjű hatványozást: $\varphi(g^k) = \varphi(g)^k$.

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi,

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$,

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Példa (5.1.20. Gyakorlat)

$\varphi : \mathbb{R} \to \mathbb{R}^{2\times 2}$, $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ gyűrűhomomorfizmus,

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Példa (5.1.20. Gyakorlat)

$\varphi : \mathbb{R} \to \mathbb{R}^{2\times 2}$, $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ gyűrűhomomorfizmus, de $\mathbb{R}$ egységelemét nem viszi $\mathbb{R}^{2\times 2}$ egységelemébe.

Elemi tulajdonságok gyűrűkre

Minden gyűrűhomomorfizmus az additív csoportok közötti csoporthomomorfizmus is egyúttal.

Következmény

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor R nullelemét S nullelemébe viszi, azaz $\varphi(0) = 0$, továbbá $\varphi(-r) = -\varphi(r)$.

Példa (5.1.20. Gyakorlat)

$\varphi : \mathbb{R} \to \mathbb{R}^{2\times 2}$, $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ gyűrűhomomorfizmus, de $\mathbb{R}$ egységelemét nem viszi $\mathbb{R}^{2\times 2}$ egységelemébe.

Az izomorfizmus azért hasznos, mert az egyformán viselkedő struktúrák közül csak egyet kell megértenünk.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus, sokszor egy bonyolult struktúrát képez egy egyszerűbbe.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni. Az előjelképzés
(homomorfizmus!) segít,

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni. Az előjelképzés
(homomorfizmus!) segít, mert ± 1-gyel könnyű számolni.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni. Az előjelképzés
(homomorfizmus!) segít, mert ± 1-gyel könnyű számolni.

Megoldható-e az $x^2 - 4y^2 = 999999$ diofantikus egyenlet?

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni. Az előjelképzés
(homomorfizmus!) segít, mert ± 1-gyel könnyű számolni.

Megoldható-e az $x^2 - 4y^2 = 999999$ diofantikus egyenlet?
Nem: Vegyük a mod 4 maradékképzés homomorfizmusát $\mathbb{Z} \to \mathbb{Z}_4$.

Az izomorfizmus és a homomorfizmus haszna

Egy olyan homomorfizmus, amely nem izomorfizmus,
sokszor egy bonyolult struktúrát képez egy egyszerűbbe.
Az egyszerűbb struktúrában már tudunk dolgozni,
és ezzel információt nyerünk a bonyolultabbról is.
Ezt tesszük az életben is, folyamatok modellezésekor.
A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés

Előáll-e az (12) transzpozíció hármasciklusok szorzataként?
Az összes szorzatot nem tudjuk áttekinteni. Az előjelképzés
(homomorfizmus!) segít, mert ± 1-gyel könnyű számolni.

Megoldható-e az $x^2 - 4y^2 = 999999$ diofantikus egyenlet?
Nem: Vegyük a mod 4 maradékképzés homomorfizmusát $\mathbb{Z} \to \mathbb{Z}_4$.
$x^2 = 3$ nem oldható meg $\mathbb{Z}_4$-ben, csak négy elemet kell kipróbálni.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).

Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).

Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),

és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.
Ekkor $\mathrm{Im}(\varphi)$ a tisztán képzetes számok részcsoportja.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.
Ekkor $\mathrm{Im}(\varphi)$ a tisztán képzetes számok részcsoportja.

(3) G csoport, $G \leq H$, $\varphi(g) = g$.

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.
Ekkor $\mathrm{Im}(\varphi)$ a tisztán képzetes számok részcsoportja.

(3) G csoport, $G \leq H$, $\varphi(g) = g$. Ekkor $\mathrm{Im}(\varphi) = G$,

Csoporthomomorfizmus képe

4.7.2. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ képe (vagyis a φ függvény értékkészlete).
Nyilván $\mathrm{Im}(\varphi)$ részcsoport H-ban (4.5.23. Gyakorlat),
és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a pozitív valós számok részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.
Ekkor $\mathrm{Im}(\varphi)$ a tisztán képzetes számok részcsoportja.

(3) G csoport, $G \leq H$, $\varphi(g) = g$. Ekkor $\mathrm{Im}(\varphi) = G$, és így minden részcsoport egy alkalmas homomorfizmus képe.

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására.

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül).

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest,

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest, ha minden nem nulla elemének a T-beli inverzét is tartalmazza (HF, vö. 2.2.26. Feladat)

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest, ha minden nem nulla elemének a T-beli inverzét is tartalmazza (HF, vö. 2.2.26. Feladat)

5.1.3. Definíció

Ha $\varphi : R \to S$ egy gyűrűhomomorfizmus, akkor legyen $\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R\} \subseteq S$ a φ képe

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest, ha minden nem nulla elemének a T-beli inverzét is tartalmazza (HF, vö. 2.2.26. Feladat)

5.1.3. Definíció

Ha $\varphi : R \to S$ egy gyűrűhomomorfizmus, akkor legyen $\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R\} \subseteq S$ a φ képe (vagyis a φ értékkészlete).

Gyűrűhomomorfizmus képe

2.2.25. Definíció

Ha R gyűrű, akkor $S \subseteq R$ részgyűrű, ha S gyűrű R műveleteire, és résztest, ha maga is test R műveleteire nézve.

S pontosan akkor részgyűrű, ha nem üres, és zárt R összeadására, szorzására és kivonására. Ilyenkor S és R nulleleme megegyezik (az egységelem, ha van is, nem feltétlenül). Ha T test, akkor az $S \leq T$ részgyűrű akkor résztest, ha minden nem nulla elemének a T-beli inverzét is tartalmazza (HF, vö. 2.2.26. Feladat)

5.1.3. Definíció

Ha $\varphi : R \to S$ egy gyűrűhomomorfizmus, akkor legyen $\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R\} \subseteq S$ a φ képe (vagyis a φ értékkészlete). Nyilván $\mathrm{Im}(\varphi)$ részgyűrű S-ben.

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).

Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).

Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,

és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n alternáló csoport.

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n alternáló csoport.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n alternáló csoport.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.
$\mathrm{Ker}(\varphi)$ a speciális lineáris csoport, jele $\mathrm{SL}(n, T)$.

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n alternáló csoport.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.
$\mathrm{Ker}(\varphi)$ a speciális lineáris csoport, jele $\mathrm{SL}(n, T)$.

(3) $G = \mathbb{R}[x]^+$, $H = \mathbb{C}^+$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

Csoporthomomorfizmus magja

4.7.4. Definíció

Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ magja (itt 1_H a H csoport egységeleme).
Nyilván $\mathrm{Ker}(\varphi)$ részcsoport G-ben,
és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n alternáló csoport.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.
$\mathrm{Ker}(\varphi)$ a speciális lineáris csoport, jele $\mathrm{SL}(n, T)$.

(3) $G = \mathbb{R}[x]^+$, $H = \mathbb{C}^+$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
$\mathrm{Ker}(\varphi)$ az $x^2 + 1$ többszöröseiből áll (HF).

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi)$

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra)$

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a)$

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0$

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Azaz $a \pm b, ra \in I$,

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Azaz $a \pm b, ra \in I$,
és hasonlóan $ar \in I$.

Gyűrűhomomorfizmus magja

5.1.3, 5.1.4. Definíció

Minden gyűrűhomomorfizmus csoporthomomorfizmus az additív csoportok között, így lehet magról beszélni, ami nyilván részgyűrű.

5.1.5. Tétel

Az R gyűrű egy I részhalmaza pontosan akkor magja egy R-en értelmezett homomorfizmusnak, ha részcsoport R^+-ban, és minden $a \in I$ és $r \in R$ esetén $ar, ra \in I$.

Legyen $\varphi : R \to S$ és $I = \mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\}$.
Ha $a, b \in I = \mathrm{Ker}(\varphi)$ és $r \in R$, akkor $\varphi(a) = \varphi(b) = 0$.
Ezért $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0$, továbbá
$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Azaz $a \pm b, ra \in I$,
és hasonlóan $ar \in I$.
A megfordítást faktorgyűrű segítségével bizonyítjuk.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros, azaz részcsoport;

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros, azaz részcsoport;
továbbá páros szám minden egész számszorosa is páros.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros, azaz részcsoport;
továbbá páros szám minden egész számszorosa is páros.
Általában: Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros, azaz részcsoport;
továbbá páros szám minden egész számszorosa is páros.
Általában: Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Ennek magja az n-nel osztható számokból álló főideál,

Bal- és jobbideálok

5.1.6. Definíció

Egy R gyűrű egy I részhalmaza balideál, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$.
Az I jobbideál, ha részcsoport, és minden $a \in I$, $r \in R$-re $ar \in I$.
Az I (kétoldali) ideál, ha bal- és jobbideál is. Jele: $I \triangleleft R$.
Ha R kommutatív, egységelemes, akkor az $r \in R$ többszöröseinek a halmaza, $(r) = \{rs : s \in R\}$ az r által generált főideál.

Példa: A páros számok a $(2) = (-2)$ főideált alkotják $\mathbb{Z}$-ben.
Mert páros számok összege is páros, a nulla is páros,
és páros szám ellentettje is páros, azaz részcsoport;
továbbá páros szám minden egész számszorosa is páros.
Általában: Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Ennek magja az n-nel osztható számokból álló főideál, vagyis (n).

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy,

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet,

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, mod n maradékosztálya legyen.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály,

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály, akkor $P + P = P$ (mert pl. $2 + 4$ páros szám),

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály, akkor $P + P = P$ (mert pl. $2 + 4$ páros szám), $P + Q = Q$ (mert pl. $4 + 7$ páratlan szám),

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály, akkor $P + P = P$ (mert pl. $2 + 4$ páros szám), $P + Q = Q$ (mert pl. $4 + 7$ páratlan szám), és hasonlóan $Q + P = Q$,

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály, akkor $P + P = P$ (mert pl. $2 + 4$ páros szám), $P + Q = Q$ (mert pl. $4 + 7$ páratlan szám), és hasonlóan $Q + P = Q$, végül $Q + Q = P$.

Műveletek maradékosztályok között

Legyen $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n. Ennek magja, vagyis a 0-ba menő számok éppen az n-nel oszthatóak.
A $b \in \mathbb{Z}_n$-be pontosan az $mn + b$ alakú számok képződnek, ahol $m \in \mathbb{Z}$. Ez épp egy n szerinti maradékosztály.

Freud-Gyarmati: Számelmélet, 2.8. szakasz

Legyenek B és C mod n maradékosztályok. Ezek összegét és szorzatát értelmezzük úgy, hogy kiveszünk egy-egy $b \in B$, illetve $c \in C$ elemet, és $B + C$ a $b + c$ szám, BC pedig a bc szám mod n maradékosztálya legyen.

Például ha $n = 2$, és P a páros, Q a páratlan számokból álló maradékosztály, akkor $P + P = P$ (mert pl. $2 + 4$ páros szám), $P + Q = Q$ (mert pl. $4 + 7$ páratlan szám), és hasonlóan $Q + P = Q$, végül $Q + Q = P$. Mi ezzel a definícióval a baj?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké:

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit,

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk,

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk,

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$,

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$, és ugyanígy $n \mid c - c'$.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$, és ugyanígy $n \mid c - c'$. De akkor $bc - b'c' = bc - bc' + bc' - b'c'$

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$, és ugyanígy $n \mid c - c'$. De akkor $bc - b'c' = bc - bc' + bc' - b'c' = b(c - c') + (b - b')c'$,

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$, és ugyanígy $n \mid c - c'$. De akkor $bc - b'c' = bc - bc' + bc' - b'c' = b(c - c') + (b - b')c'$, ami n-nel osztható.

A jóldefiniáltság problémája

Mit jelent a „narancsszín”? Egy narancsnak a színe.
Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín”? Semmit, rosszul definiált fogalom.
Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Azaz ha másik, $b' \in B$, illetve $c' \in C$ számokat veszünk, akkor $b'c'$ maradékosztálya ugyanaz lesz-e, mint bc maradékosztálya?
Mert ha nem, akkor a kettő közül melyik legyen BC?
Vagyis ha a maradékosztályokat máshogy reprezentáljuk, ugyanaz lesz-e a művelet eredménye?

Tudjuk: $n \mid b - b'$, hiszen $b, b' \in B$, és ugyanígy $n \mid c - c'$. De akkor $bc - b'c' = bc - bc' + bc' - b'c' = b(c - c') + (b - b')c'$, ami n-nel osztható. Ezért a maradékosztályok szorzása jóldefiniált.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0$

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt,

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$,

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$, ekkor $r_1 - r_1' \in I$ és $r_2 - r_2' \in I$.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$, ekkor $r_1 - r_1' \in I$ és $r_2 - r_2' \in I$. Ezért $r_1 + r_2 - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$,

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$, ekkor $r_1 - r_1' \in I$ és $r_2 - r_2' \in I$. Ezért $r_1 + r_2 - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$, hiszen I zárt az összeadásra.

Ideál szerinti maradékosztályok

Legyen a $\varphi : R \to S$ gyűrűhomomorfizmus magja I. Ha $s \in S$, akkor az s-re képződő elemek egy I szerinti mellékosztályt alkotnak az R^+ csoportban. Ha $\varphi(r) = s$, akkor ez a halmaz $r + I$.

Valóban, $\varphi(x) = s = \varphi(r) \iff \varphi(x - r) = 0 \iff x \in r + I$.
Az I szerinti mellékosztályokat maradékosztályoknak is nevezzük.

Ha I ideál R-ben, akkor az $r_1 + I$ és $r_2 + I$ mellékosztályok összegén az $(r_1 + r_2) + I$ mellékosztályt, szorzatán pedig az $r_1 r_2 + I$ mellékosztályt értjük. Ezek a műveletek jóldefiniáltak.

Bizonyítás (lásd az 5.2. szakasz elején)

Tegyük föl, hogy $r_1 + I = r_1' + I$ és $r_2 + I = r_2' + I$, ekkor $r_1 - r_1' \in I$ és $r_2 - r_2' \in I$. Ezért $r_1 + r_2 - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$, hiszen I zárt az összeadásra. Ezért az összeadás jóldefiniált.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.
Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.
Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.
Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$.
Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I. Neve természetes homomorfizmus.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I. Neve természetes homomorfizmus.

HF: Igazoljuk, hogy a gyűrűaxiómák öröklődnek R-ről R/I-re,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I. Neve természetes homomorfizmus.

HF: Igazoljuk, hogy a gyűrűaxiómák öröklődnek R-ről R/I-re, a természetes homomorfizmus összeg- és szorzattartó,

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I. Neve természetes homomorfizmus.

HF: Igazoljuk, hogy a gyűrűaxiómák öröklődnek R-ről R/I-re, a természetes homomorfizmus összeg- és szorzattartó, és a magja I.

Faktorgyűrű

Továbbá $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$, hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, ugyanígy $(r_1 - r_1')r_2' \in I$. Ezért a szorzás is jóldefiniált.

Állítás (5.2. szakasz)

Ha I ideál R-ben, akkor az I szerinti maradékosztályok a most definiált összeadásra és szorzásra gyűrűt alkotnak.
Neve faktorgyűrű vagy maradékosztálygyűrű, jele R/I.
Az a $\varphi : R \to R/I$ leképezés, melyre $\varphi(r) = r + I$, egy gyűrűhomomorfizmus, magja I. Neve természetes homomorfizmus.

HF: Igazoljuk, hogy a gyűrűaxiómák öröklődnek R-ről R/I-re, a természetes homomorfizmus összeg- és szorzattartó, és a magja I. Ezért minden ideál homomorfizmus-mag.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n)$

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b$

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban,
ha n-nel osztva ugyanazt a maradékot adják.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n)$

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big)$

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big) = k_1 k_2 + (n)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big) = k_1 k_2 + (n)$.
Azaz $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$.

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big) = k_1 k_2 + (n)$.
Azaz $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$. Összegtartás hasonló, HF. □

Számolás a faktorgyűrűben

Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Bizonyítás

$a+(n) = b+(n) \iff a-b \in (n) \iff n \mid a-b \iff a \equiv b\,(n)$.
Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n-nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0+(n), 1+(n), \ldots, n-1+(n)$.
Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \to \mathbb{Z}/(n)$.
Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n.
Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.
Másrészt $\psi(k_1)\psi(k_2) = \big(k_1+(n)\big)\big(k_2+(n)\big) = k_1 k_2 + (n)$.
Azaz $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$. Összegtartás hasonló, HF. □

$0, 1, \ldots, n-1$ egy reprezentánsrendszer az (n) ideál szerint.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a + bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a + bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek).

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a + bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a + bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a + bi \iff 3 \mid a$ és $3 \mid b$.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a + bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a + bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a + bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a} + \overline{b}i$,

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$,

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van,

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel,

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel, hasonlóan ahhoz, ahogy $\mathbb{R}$-et bővítettük a komplex számok bevezetésekor.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel, hasonlóan ahhoz, ahogy $\mathbb{R}$-et bővítettük a komplex számok bevezetésekor. Az alapműveletek képlete ugyanaz,

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel, hasonlóan ahhoz, ahogy $\mathbb{R}$-et bővítettük a komplex számok bevezetésekor. Az alapműveletek képlete ugyanaz, osztásnál be kell látni, hogy $a^2+b^2=0 \implies a=b=0$.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel, hasonlóan ahhoz, ahogy $\mathbb{R}$-et bővítettük a komplex számok bevezetésekor. Az alapműveletek képlete ugyanaz, osztásnál be kell látni, hogy $a^2+b^2=0 \implies a=b=0$. Ez igaz, mert $a^2, b^2 \equiv 0$ vagy $1 \bmod 3$.

Számolás a faktorgyűrűben

Állítás

Legyen $\mathbb{G}$ az $a+bi$ alakú komplex számok gyűrűje, ahol $a, b \in \mathbb{Z}$ (Gauss-egészek). Ekkor $\mathbb{G}/(3)$ egy kilenc elemű test.

Bizonyítás: Nyilván $3 \mid a+bi \iff 3 \mid a$ és $3 \mid b$. Ezért $a+bi$ ugyanabban a maradékosztályban van (3) szerint, mint $\overline{a}+\overline{b}i$, ahol $\overline{a}$ és $\overline{b}$ az a-nak és b-nek a 3-mal való osztási maradéka. Azok az $a+bi$ számok viszont, melyekre $0 \leq a < 2$ és $0 \leq b < 2$, páronként különböző maradékosztályban vannak. Ezért a faktorgyűrűnek $3 \cdot 3 = 9$ eleme van, és úgy is felfoghatjuk, hogy a $\mathbb{Z}_3$ gyűrűt bővítjük i-vel, hasonlóan ahhoz, ahogy $\mathbb{R}$-et bővítettük a komplex számok bevezetésekor. Az alapműveletek képlete ugyanaz, osztásnál be kell látni, hogy $a^2+b^2=0 \implies a=b=0$. Ez igaz, mert $a^2, b^2 \equiv 0$ vagy $1 \bmod 3$. Ezért ez a faktorgyűrű test is.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$,

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I) = x^2+I$

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I) = x^2 + I = -1 + ((x^2+1)+I)$

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I) = x^2 + I = -1 + ((x^2+1)+I) = -1 + I$.
HF: $((a+bx)+I) + ((c+dx)+I) = ((a+c)+(b+d)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I = (x^2+1)$, akkor $f + I = g + I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b \in \mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I) = x^2 + I = -1 + ((x^2+1)+I) = -1 + I$.
HF: $((a+bx)+I) + ((c+dx)+I) = ((a+c)+(b+d)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.
Azaz $a+bi\mapsto(a+bx)+I$ izomorfizmus $\mathbb{C}\to\mathbb{R}[x]/(x^2+1)$.

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.
Azaz $a+bi\mapsto(a+bx)+I$ izomorfizmus $\mathbb{C}\to\mathbb{R}[x]/(x^2+1)$.

Igazoljuk, hogy $\mathbb{Z}_3[x]/(x^2+1)$ kilenc elemű test,

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki" az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.
Azaz $a+bi\mapsto(a+bx)+I$ izomorfizmus $\mathbb{C}\to\mathbb{R}[x]/(x^2+1)$.

Igazoljuk, hogy $\mathbb{Z}_3[x]/(x^2+1)$ kilenc elemű test, ami $\mathbb{G}/(3)$-mal izomorf,

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.
Azaz $a+bi\mapsto(a+bx)+I$ izomorfizmus $\mathbb{C}\to\mathbb{R}[x]/(x^2+1)$.

Igazoljuk, hogy $\mathbb{Z}_3[x]/(x^2+1)$ kilenc elemű test, ami $\mathbb{G}/(3)$-mal izomorf, de $\mathbb{Z}_5[x]/(x^2+1)$ nem test,

Példa polinomgyűrű faktorára

5.2.6. Állítás: „Számítsuk ki” az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűt.

Ha $I=(x^2+1)$, akkor $f+I=g+I \iff x^2+1 \mid f-g$.
Vagyis két polinom akkor van ugyanabban a maradékosztályban, ha x^2+1-gyel osztva ugyanazt a maradékot adják.
A lehetséges maradékok a legfeljebb elsőfokú polinomok.
Így az összes különböző mellékosztály: $(a+bx)+I$ $(a,b\in\mathbb{R})$.
Példa: Mi lesz $x+I$ négyzete?
$(x+I)(x+I)=x^2+I=-1+((x^2+1)+I)=-1+I$.
HF: $((a+bx)+I)+((c+dx)+I)=((a+c)+(b+d)x)+I$.
HF: $((a+bx)+I)((c+dx)+I)=((ac-bd)+(ad+bc)x)+I$.
Azaz $a+bi\mapsto(a+bx)+I$ izomorfizmus $\mathbb{C}\to\mathbb{R}[x]/(x^2+1)$.

Igazoljuk, hogy $\mathbb{Z}_3[x]/(x^2+1)$ kilenc elemű test, ami $\mathbb{G}/(3)$-mal izomorf, de $\mathbb{Z}_5[x]/(x^2+1)$ nem test, sőt nem is nullosztómentes.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni,

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$,

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$,

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$,

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz,

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne. Mivel $\mathbb{Z}_2$ fölött vagyunk, a gyűrűnek csak négy eleme lesz:

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne. Mivel $\mathbb{Z}_2$ fölött vagyunk, a gyűrűnek csak négy eleme lesz: 0, 1, ε és $\varepsilon + 1$.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne. Mivel $\mathbb{Z}_2$ fölött vagyunk, a gyűrűnek csak négy eleme lesz: 0, 1, ε és $\varepsilon + 1$. Testet kapunk, mert ε és $\varepsilon + 1$ egymás inverzei:

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne”. Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne. Mivel $\mathbb{Z}_2$ fölött vagyunk, a gyűrűnek csak négy eleme lesz: 0, 1, ε és $\varepsilon + 1$. Testet kapunk, mert ε és $\varepsilon + 1$ egymás inverzei: $\varepsilon(\varepsilon + 1) = \varepsilon^2 + \varepsilon = -1 = 1$.

Nulla a nevezőben

Az R/I faktorgyűrűre úgy érdemes gondolni, hogy az I elemeit nullává akarjuk tenni, és megnézzük, mik a következmények.

(1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ha $n = 0$, akkor $n + 2 = 2$, $(n + 2)(n + 3) = 6$, ténylegesen mod n számolunk.

(2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Ha $x^2 + 1 = 0$, akkor $x^2 = -1$, és ezért x „olyan, mint ha i lenne". Az $f(x)$ polinomból az $f(i)$ komplex szám lesz, a komplex számtestet kapjuk.

(3) $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Ha $x^2 + x + 1 = 0$, akkor x olyan, mint ha egy ε primitív harmadik egységgyök lenne. Mivel $\mathbb{Z}_2$ fölött vagyunk, a gyűrűnek csak négy eleme lesz: 0, 1, ε és $\varepsilon + 1$. Testet kapunk, mert ε és $\varepsilon + 1$ egymás inverzei: $\varepsilon(\varepsilon + 1) = \varepsilon^2 + \varepsilon = -1 = 1$.
Ezt a példát később részletesen kidolgozzuk.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\operatorname{Im}(\varphi) \cong R/\operatorname{Ker}(\varphi)$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált,

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$,

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$,

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Megjegyzés: Ez csak akkor működik, ha $\mathbb{C}$ már ismert!

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Megjegyzés: Ez csak akkor működik, ha $\mathbb{C}$ már ismert!
Ha meg akarjuk konstruálni $\mathbb{C}$-t

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Megjegyzés: Ez csak akkor működik, ha $\mathbb{C}$ már ismert!
Ha meg akarjuk konstruálni $\mathbb{C}$-t (vagy más testeket),

A homomorfizmustétel

5.2.5 Homomorfizmustétel

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Legyen $I = \mathrm{Ker}(\varphi)$. Ekkor az $r + I \leftrightarrow \varphi(r)$ megfeleltetés jóldefiniált, művelettartó és kölcsönösen egyértelmű.

Két alkalmazás

(1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n.
Itt $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ és $\mathrm{Ker}(\varphi) = (n)$, ezért $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(2) $R = \mathbb{R}[x]$, $S = \mathbb{C}$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
Itt $\mathrm{Im}(\varphi) = \mathbb{C}$ és $\mathrm{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Megjegyzés: Ez csak akkor működik, ha $\mathbb{C}$ már ismert!
Ha meg akarjuk konstruálni $\mathbb{C}$-t (vagy más testeket), akkor érdemes a faktorgyűrűt használni.

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I = (x^2+x+1)$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I = (x^2+x+1)$, $O = 0+I$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I = (x^2+x+1)$, $O = 0+I$, $E = 1+I$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I = (x^2+x+1)$, $O = 0+I$, $E = 1+I$, $A = x+I$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I = (x^2+x+1)$, $O = 0+I$, $E = 1+I$, $A = x+I$, $B = (x+1)+I$.

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)$

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I$

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I$

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$
(azaz x^2+x-nek az x^2+x+1-gyel való osztási maradéka 1).

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$
(azaz x^2+x-nek az x^2+x+1-gyel való osztási maradéka 1).
Test, mert a táblázat szerint $A^{-1}=B$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$
(azaz x^2+x-nek az x^2+x+1-gyel való osztási maradéka 1).
Test, mert a táblázat szerint $A^{-1}=B$, $B^{-1}=A$,

Négyelemű test

5.2.10 Gyakorlat

A $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrű négyelemű test.

Az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú.
$I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa: $AB=(x+I)(x+1+I)=(x^2+x)+I=1+I=E$,
mert $x^2+x=1+(x^2+x+1)$ és $x^2+x+1\in I$
(azaz x^2+x-nek az x^2+x+1-gyel való osztási maradéka 1).
Test, mert a táblázat szerint $A^{-1}=B$, $B^{-1}=A$, $E^{-1}=E$.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $\big(g + (f)\big)\big(h + (f)\big)$ nulla,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla. Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $(g + (f))(h + (f))$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.
Ezért $fp + gq = 1$ alkalmas $p, q \in T[x]$ polinomokra.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $\big(g + (f)\big)\big(h + (f)\big)$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.
Ezért $fp + gq = 1$ alkalmas $p, q \in T[x]$ polinomokra.
Innen $\big(g + (f)\big)\big(q + (f)\big) = 1 - fp + (f) = 1 + (f)$,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $\big(g + (f)\big)\big(h + (f)\big)$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.
Ezért $fp + gq = 1$ alkalmas $p, q \in T[x]$ polinomokra.
Innen $\big(g + (f)\big)\big(q + (f)\big) = 1 - fp + (f) = 1 + (f)$,
hiszen $f \mid fp$ miatt $-fp + (f)$ nulla.

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $\big(g + (f)\big)\big(h + (f)\big)$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.
Ezért $fp + gq = 1$ alkalmas $p, q \in T[x]$ polinomokra.
Innen $\big(g + (f)\big)\big(q + (f)\big) = 1 - fp + (f) = 1 + (f)$,
hiszen $f \mid fp$ miatt $-fp + (f)$ nulla.
Beláttuk tehát, hogy $q + (f)$ inverze $g + (f)$-nek,

A faktorgyűrű mikor test

5.2.9. Állítás

Ha T test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.

Bizonyítás

Ha $f = gh$ nemtriviális felbontás, akkor $\big(g + (f)\big)\big(h + (f)\big)$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha f irreducibilis, akkor legyen $g \in T[x]$, ahol $g + (f)$ nem nulla.
Azaz f nem osztója g-nek, és mivel f irreducibilis, $(f, g) = 1$.
Ezért $fp + gq = 1$ alkalmas $p, q \in T[x]$ polinomokra.
Innen $\big(g + (f)\big)\big(q + (f)\big) = 1 - fp + (f) = 1 + (f)$,
hiszen $f \mid fp$ miatt $-fp + (f)$ nulla.
Beláttuk tehát, hogy $q + (f)$ inverze $g + (f)$-nek,
hiszen $1 + (f)$ a $T[x]/(f)$ faktorgyűrű egységeleme. □

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$,

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot,

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot, az E, I, J, K szorzását elvégezzük úgy, ahogy a kvaterniócsoportban tanultuk,

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot, az E, I, J, K szorzását elvégezzük úgy, ahogy a kvaterniócsoportban tanultuk, majd összevonunk.

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot, az E, I, J, K szorzását elvégezzük úgy, ahogy a kvaterniócsoportban tanultuk, majd összevonunk.

Ezentúl E, I, J, K helyett rendre $1, i, j, k$-t fogunk írni.

A kvaterniók ferdeteste

5.11.1. Gyakorlat (HF)

A $\mathbb{C}^{2\times 2}$ gyűrű $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú elemei egy $\mathbb{K}$ részgyűrűt alkotnak.

Ennek minden nem nulla eleme invertálható (mátrix).

Legyen $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Ha $z = p + qi$ és $w = r + si$, akkor

$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = pE + qI + rJ + sK$ (itt E az egységmátrix).

Két ilyet úgy szorozhatunk össze, hogy a disztributív szabály alapján kibontjuk a szorzatot, az E, I, J, K szorzását elvégezzük úgy, ahogy a kvaterniócsoportban tanultuk, majd összevonunk.

Ezentúl E, I, J, K helyett rendre $1, i, j, k$-t fogunk írni.

A kapott $p + qi + rj + sk$ elemek a kvaterniók ($p, q, r, s \in \mathbb{R}$).

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$,

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$,
normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese,

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert
$(MN)^* = N^*M^*$

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert $(MN)^* = N^*M^*$ és $\det(MN) = \det(M)\det(N)$.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert $(MN)^* = N^*M^*$ és $\det(MN) = \det(M)\det(N)$.

Tehát ha $\alpha \neq 0$, akkor α inverze $\left(1/N(\alpha)\right)\overline{\alpha}$.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert $(MN)^* = N^*M^*$ és $\det(MN) = \det(M)\det(N)$.

Tehát ha $\alpha \neq 0$, akkor α inverze $\left(1/N(\alpha)\right)\overline{\alpha}$. Így $\mathbb{K}$ ferdetest.

Kvaternió konjugáltja és normája

5.1.2. Definíció, 5.11.3. Gyakorlat

Az $\alpha = p + qi + rj + sk$ kvaternió konjugáltja $\overline{\alpha} = p - qi - rj - sk$, normája $N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2$.
Továbbá $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$ és $N(\alpha\beta) = N(\alpha)N(\beta)$ minden $\alpha\beta \in \mathbb{K}$-ra.

Ha M az α-nak megfelelő mátrix, akkor $\overline{\alpha}$-nak M adjungáltja (transzponált konjugáltja), azaz M^* felel meg.

MM^* az egységmátrix $\det(M)$-szerese, azaz $\left(1/\sqrt{N(\alpha)}\right)M$ unitér.

A Gyakorlat utolsó két állítása azért teljesül, mert $(MN)^* = N^*M^*$ és $\det(MN) = \det(M)\det(N)$.

Tehát ha $\alpha \neq 0$, akkor α inverze $\left(1/N(\alpha)\right)\overline{\alpha}$. Így $\mathbb{K}$ ferdetest.

Mivel $ij = k \neq -k = ji$, ezért $\mathbb{K}$ nem kommutatív, azaz nem test.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus,

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag,

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű,

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál,

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű,

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

Tételek

A maradékosztályok közötti műveletek jóldefiniáltak.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

Tételek

A maradékosztályok közötti műveletek jóldefiniáltak.
Az ideálok épp a gyűrűhomomorfizmusok magjai.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

Tételek

A maradékosztályok közötti műveletek jóldefiniáltak.
Az ideálok épp a gyűrűhomomorfizmusok magjai.
Homomorfizmus-tétel.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

Tételek

A maradékosztályok közötti műveletek jóldefiniáltak.
Az ideálok épp a gyűrűhomomorfizmusok magjai.
Homomorfizmus-tétel.
Négy- és kilencelemű test konstrukciója.

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport- és gyűrűhomomorfizmus, mag, kép.
Részgyűrű, ideál, generált főideál.
Maradékosztály, faktorgyűrű, természetes homomorfizmus.
A kvaterniók ferdeteste, konjugált, norma.

Tételek

A maradékosztályok közötti műveletek jóldefiniáltak.
Az ideálok épp a gyűrűhomomorfizmusok magjai.
Homomorfizmus-tétel.
Négy- és kilencelemű test konstrukciója.
A $T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T fölött.