

Algebra3, elemző szakirány

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

2. előadás

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$,

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás

Ha I és J ideálok az R gyűrűben,

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás

Ha I és J ideálok az R gyűrűben, a csoportelméleti $I + J$ komplexusösszeg az egész R ,

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás

Ha I és J ideálok az R gyűrűben,
a csoportelméleti $I + J$ komplexusösszeg az egész R ,
továbbá $I \cap J = 0$,

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás

Ha I és J ideálok az R gyűrűben, a csoportelméleti $I + J$ komplexusösszeg az egész R , továbbá $I \cap J = 0$, akkor $R \cong I \times J$.

Direkt szorzat

5.1.17. Definíció

Az R és S gyűrűk **direkt szorzatának** alaphalmaza $R \times S$, ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

HF: Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

5.1.18. Állítás

Ha I és J ideálok az R gyűrűben, a csoportelméleti $I + J$ komplexusösszeg az egész R , továbbá $I \cap J = 0$, akkor $R \cong I \times J$.

A bizonyítás ötlete: Ha $I \cap J = 0$, $a \in I$, $b \in J$, akkor $ab = 0$.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoport G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoport** elemei az N szerinti mellékosztályok

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoporth** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoport** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoport G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoport** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

A G/N csoport **egységeleme** az $N = 0 + N$ mellékosztály,

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoporth** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

A G/N csoport **egységeleme** az $N = 0 + N$ mellékosztály, a $g + N$ **inverze** $(-g) + N$.

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoporth** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

A G/N csoport **egységeleme** az $N = 0 + N$ mellékosztály, a $g + N$ **inverze** $(-g) + N$.

A $\psi : g \mapsto (g + N)$ leképezés a **természetes homomorfizmus** G -ből G/N -re.

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoporth** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

A G/N csoport **egységeleme** az $N = 0 + N$ mellékosztály, a $g + N$ **inverze** $(-g) + N$.

A $\psi : g \mapsto (g + N)$ leképezés a **természetes homomorfizmus** G -ből G/N -re. Ennek **képe** az egész G/N ,

Faktorcsoporth

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

Ha N részcsoporth G -ben, akkor tehát normálosztó is.

A G/N **faktorcsoporth** elemei az N szerinti mellékosztályok (ezek a $g + N$ halmazok, ahol g befutja G -t).

Az összeadás: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

A G/N csoport **egységeleme** az $N = 0 + N$ mellékosztály, a $g + N$ **inverze** $(-g) + N$.

A $\psi : g \mapsto (g + N)$ leképezés a **természetes homomorfizmus** G -ből G/N -re. Ennek **képe** az egész G/N , **magja** N .

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen.

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$,

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**. Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2$

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$,

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, hiszen
 $r_2 - r'_2 \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r'_2) \in I$,

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, 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

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
 Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
 De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, hiszen
 $r_2 - r'_2 \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r'_2) \in I$, ugyanígy $(r_1 - r'_1)r'_2 \in I$.
HF: Igazak erre a szorzásra a gyűrűaxiómák

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, hiszen
 $r_2 - r'_2 \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r'_2) \in I$, ugyanígy $(r_1 - r'_1)r'_2 \in I$.
HF: Igazak erre a szorzásra a gyűrűaxiómák
(szorzás asszociativitása,

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**.
 Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
 De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, hiszen
 $r_2 - r'_2 \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r'_2) \in I$, ugyanígy $(r_1 - r'_1)r'_2 \in I$.
HF: Igazak erre a szorzásra a gyűrűaxiómák
 (szorzás asszociativitása, mindkét oldali disztributivitás);

Faktorgyűrű

Állítás

Ha I ideál R -ben, akkor az R^+ / I^+ faktorcsoporton értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az R/I **faktorgyűrűt** kapjuk.

Bizonyítás (lásd az 5.2. szakasz elején)

Legyen $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Be kell látni, hogy **jóldefiniált**. Azaz ha $r_1 + I = r'_1 + I$ és $r_2 + I = r'_2 + I$, akkor $r_1 r_2 + I = r'_1 r'_2 + I$.
 $r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$ és $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$.
 De akkor $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$, hiszen $r_2 - r'_2 \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r'_2) \in I$, ugyanígy $(r_1 - r'_1)r'_2 \in I$.
HF: Igazak erre a szorzásra a gyűrűaxiómák (szorzás asszociativitása, mindkét oldali disztributivitás); az $r \mapsto r + I$ természetes homomorfizmus szorzattartó is. \square

Az egész számok faktorgyűrűi

Állítás

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

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

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

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

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

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

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

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Az egész számok faktorgyűrűi

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: $0+(n), 1+(n), \dots, n-1+(n)$.

Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z}/(n)$.

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n .

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n .

Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n)$

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n .

Vagyis $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$.

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

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 $\psi(k_1)\psi(k_2) = (k_1 + (n))(k_2 + (n))$

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

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 $\psi(k_1)\psi(k_2) = (k_1 + (n))(k_2 + (n)) = k_1 k_2 + (n)$.

Az egész számok faktorgyűrűi

Állítás

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

Bizonyítás

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha n -nel osztva ugyanazt a maradékot adják. Ezért az összes különböző mellékosztály: $0 + (n), 1 + (n), \dots, n - 1 + (n)$.

Állítás: A $\psi : k \mapsto k + (n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z} / (n)$.

Szorzattartás: $k_1 *_n k_2$ a $k_1 k_2$ maradéka modulo n .

$$\text{Vagyis } \psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n).$$

$$\text{Másképpen } \psi(k_1)\psi(k_2) = (k_1 + (n))(k_2 + (n)) = k_1 k_2 + (n).$$

$$\text{Azaz } \psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2).$$

Az egész számok faktorgyűrűi

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: $0+(n), 1+(n), \dots, n-1+(n)$.

Állítás: A $\psi : k \mapsto k+(n)$ bijekció izomorfizmus $\mathbb{Z}_n \rightarrow \mathbb{Z}/(n)$.

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 $\psi(k_1)\psi(k_2) = (k_1+(n))(k_2+(n)) = k_1 k_2 + (n)$.

Azaz $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$. **Összegeztartás** hasonló, **HF**. □

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I$$

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, ha $x^2 + 1$ -gyel osztva ugyanazt a maradékot adják.

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, ha $x^2 + 1$ -gyel osztva ugyanazt a maradékot adják.

A lehetséges maradékok a legfeljebb elsőfokú polinomok.

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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 a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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 a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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 a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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 a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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?

$$(x + I)(x + I) = x^2 + I = -1 + ((x^2 + 1) + I) = -1 + I.$$

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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?

$$(x + I)(x + I) = x^2 + I = -1 + ((x^2 + 1) + I) = -1 + I.$$

$$\text{HF: } ((a + bx) + I)((c + dx) + I) = ((ac - bd) + (ad + bc)x) + I.$$

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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?

$$(x + I)(x + I) = x^2 + I = -1 + ((x^2 + 1) + I) = -1 + I.$$

$$\text{HF: } ((a + bx) + I)((c + dx) + I) = ((ac - bd) + (ad + bc)x) + I.$$

$$\text{HF: } ((a + bx) + I) + ((c + dx) + I) = ((a + c) + (b + d)x) + I.$$

Példa a polinomgyűrűben

Példa (5.2.6. Állítás)

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

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, 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?

$$(x + I)(x + I) = x^2 + I = -1 + ((x^2 + 1) + I) = -1 + I.$$

$$\text{HF: } ((a + bx) + I)((c + dx) + I) = ((ac - bd) + (ad + bc)x) + I.$$

$$\text{HF: } ((a + bx) + I) + ((c + dx) + I) = ((a + c) + (b + d)x) + I.$$

Azaz $a + bi \mapsto (a + bx) + I$ izomorfizmus $\mathbb{C} \rightarrow \mathbb{R}[x]/(x^2 + 1)$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$,

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, ezért $\mathbb{Z} / (n) \cong \mathbb{Z}_n$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\varphi : R \rightarrow S$ gyűrűhomomorfizmus, akkor $\text{Im}(\varphi) \cong R / \text{Ker}(\varphi)$.

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

- (1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n .
Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$,

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$, ezért $\mathbb{R}[x] / (x^2 + 1) \cong \mathbb{C}$.

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

- (1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n .
Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$, 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 $\varphi : R \rightarrow S$ gyűrűhomomorfizmus, akkor $\text{Im}(\varphi) \cong R / \text{Ker}(\varphi)$.

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

- (1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n .
Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$, 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 $\varphi : R \rightarrow S$ gyűrűhomomorfizmus, akkor $\text{Im}(\varphi) \cong R / \text{Ker}(\varphi)$.

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

- (1) $R = \mathbb{Z}$, $S = \mathbb{Z}_n$, $\varphi(k) = k$ maradéka mod n .
Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$, 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 $\varphi : R \rightarrow S$ gyűrűhomomorfizmus, akkor $\text{Im}(\varphi) \cong R / \text{Ker}(\varphi)$.

Bizonyítás: Nyilván $\text{Im}(\varphi)^+$ és $R^+ / \text{Ker}(\varphi)^+$ izomorf **csoportok**.
Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (**HF**).

Két alkalmazás

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

Itt $\text{Im}(\varphi) = \mathbb{Z}_n$ és $\text{Ker}(\varphi) = (n)$, 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 $\text{Im}(\varphi) = \mathbb{C}$ és $\text{Ker}(\varphi) = (x^2 + 1)$, 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.

$$I = (x^2 + x + 1), \quad 0 = 0 + I,$$

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.

$$I = (x^2 + x + 1), \quad O = 0 + I, \quad E = 1 + I,$$

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.

$$I = (x^2 + x + 1), \quad O = 0 + I, \quad E = 1 + I, \quad A = x + I,$$

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 $A^{-1} = B$, $B^{-1} = A$, $E^{-1} = E$.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben,

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű**

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$,

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$,

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $|n|$ minimális volt,

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $|n|$ minimális volt, így r csak nulla lehet.

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $|n|$ minimális volt, így r csak nulla lehet.

Tehát $k \in (n)$,

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $|n|$ minimális volt, így r csak nulla lehet.

Tehát $k \in (n)$, azaz $I \subseteq (n)$. □

Ideálok az egészek között

Ha n rögzített egész, akkor (n) az n többszöröseiből álló ideál.

Állítás: A \mathbb{Z} gyűrűben nincs más ideál.

Bizonyítás

Legyen I nem nulla ideál \mathbb{Z} -ben, és n a legkisebb **abszolút értékű nem nulla** eleme. Belátjuk, hogy $I = (n)$.

Nyilván $(n) \subseteq I$, hiszen I tartalmazza n többszöröseit.

Legyen $k \in I$, ekkor $k = nq + r$, ahol $0 \leq r < |n|$.

De $r = k - nq \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $|n|$ minimális volt, így r csak nulla lehet.

Tehát $k \in (n)$, azaz $I \subseteq (n)$. □

HF: Hasonlítsuk össze ezt annak bizonyításával, hogy ciklikus csoport részcsoportja is ciklikus (4.3.26. Lemma).

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített.
Ekkor (s) az s összes többszöröseiből áll (főideál).

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített.
Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített.
Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben,

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített.
Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú**

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$,

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$,

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt,

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt, így r csak nulla lehet.

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$,

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Nyilvánvaló a hasonlóság a \mathbb{Z} -beli bizonyítással:

Ideálok a polinomok között

Legyen R **kommutatív, egységelemes** gyűrű és $s \in R$ rögzített. Ekkor (s) az s összes többszöröseiből áll (főideál).

Állítás: Ha T test, akkor $T[x]$ minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál $T[x]$ -ben, és g a legkisebb **fokú nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\text{gr}(r) < \text{gr}(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\text{gr}(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Nyilvánvaló a hasonlóság a \mathbb{Z} -beli bizonyítással: **maradékos osztásra** van szükség.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi,

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$,

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R, b \neq 0$

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$,

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi:

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

$T[x]$ euklideszi, ha T test:

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

$T[x]$ euklideszi, ha T test: $\varphi(f) = \text{gr}(f)$.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

$T[x]$ euklideszi, ha T test: $\varphi(f) = \text{gr}(f)$.

Gauss-egészek: $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

$T[x]$ euklideszi, ha T test: $\varphi(f) = \text{gr}(f)$.

Gauss-egészek: $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ez is euklideszi gyűrű: $\varphi(a + bi) = a^2 + b^2$.

Euklideszi gyűrű

5.5.1. Definíció

Euklideszi gyűrű: „elvégezhető benne a maradékos osztás.”
Az R szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény úgy, hogy minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$, és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Példák

\mathbb{Z} euklideszi: $\varphi(k) = |k|$.

$T[x]$ euklideszi, ha T test: $\varphi(f) = \text{gr}(f)$.

Gauss-egészek: $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ez is euklideszi gyűrű: $\varphi(a + bi) = a^2 + b^2$.

Bizonyítás, alkalmazás és további példák legközelebb.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben,

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$,

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$,

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt,

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$,

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Főideálgyűrű: szokásos gyűrű, melynek minden ideálja főideál.

Főideálgyűrű

5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

Bizonyítás

Legyen I nem nulla ideál R -ben, és g a legkisebb φ -értékű **nem nulla** eleme. Belátjuk, hogy $I = (g)$.

Nyilván $(g) \subseteq I$, hiszen I tartalmazza g többszöröseit.

Legyen $f \in I$, ekkor $f = qg + r$, ahol $\varphi(r) < \varphi(g)$ vagy $r = 0$.

De $r = f - qg \in I$, mert I zárt a többszörözésre és a kivonásra.

Mivel $\varphi(g)$ minimális volt, így r csak nulla lehet.

Tehát $f \in (g)$, azaz $I \subseteq (g)$. □

Főideálgyűrű: szokásos gyűrű, melynek minden ideálja főideál.
Ezekben érvényes a **számelmélet alaptétele** (legközelebb).