Algebra3, alkalmazott matematikus

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
http://ewkiss.web.elte.hu/wp/wordpress
ewwkiss@gmail.com

6/11. előadás

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll. Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$,

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll. Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. □

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. □

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. □

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

5.3.1. Definíció

Az R egyszerű gyűrű, ha pontosan két ideálja van: 0 és R.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. □

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

5.3.1. Definíció

Az R egyszerű gyűrű, ha pontosan két ideálja van: 0 és R.

Főpélda (5.3.3): (Ferde)test fölötti teljes mátrixgyűrű egyszerű.

Testek ideáljai

5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak: $\{0\}$ és önmaga.

Bizonyítás

Legyen T test és I ideálja T-nek, amely nem csak a nullából áll.
Ha $0 \neq s \in I$, akkor $1 = ss^{-1} \in I$, hiszen I ideál.
Tehát minden $r \in T$-re $r = 1r \in I$. Ezért $I = T$. □

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

5.3.1. Definíció

Az R egyszerű gyűrű, ha pontosan két ideálja van: 0 és R.

Főpélda (5.3.3): (Ferde)test fölötti teljes mátrixgyűrű egyszerű.
8.7.10, 8.7.12: A teljes mátrixgyűrű balideáljainak leírása.

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0),

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$. Ezért $1 \in (s)$,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$. Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható, és így R test. □

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható, és így R test. □

Általánosítás (5.3.8. Tétel, NB)

Legyen R gyűrű, amelynek csak a két triviális balideálja van.

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható, és így R test. □

Általánosítás (5.3.8. Tétel, NB)

Legyen R gyűrű, amelynek csak a két triviális balideálja van.
Ekkor R vagy ferdetest,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható, és így R test. □

Általánosítás (5.3.8. Tétel, NB)

Legyen R gyűrű, amelynek csak a két triviális balideálja van.
Ekkor R vagy ferdetest, vagy olyan prímelemű gyűrű,

Kommutatív egyszerű gyűrűk

Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

Bizonyítás

Ha R kommutatív, egységelemes, egyszerű gyűrű és $0 \neq s \in R$, akkor $s = 1s \in (s)$ miatt az (s) ideál nem (0), és így $(s) = R$.
Ezért $1 \in (s)$, vagyis van olyan $r \in R$, hogy $sr = 1$.
Tehát az s elem invertálható, és így R test. □

Általánosítás (5.3.8. Tétel, NB)

Legyen R gyűrű, amelynek csak a két triviális balideálja van.
Ekkor R vagy ferdetest, vagy olyan prímelemű gyűrű, amelyben bármely két elem szorzata nulla.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, nullosztó.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$,

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$,

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r$

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r = s(xr)$

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r = s(xr) = s0 = 0$. □

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r = s(xr) = s0 = 0$. □

Elnevezés: Ez az r elem bal oldali annullátora.

Ideálok és nullosztók

Emlékeztető (2.2.27. Definíció)

Ha R gyűrű, $r, s \in R$ egyik sem nulla, de $rs = 0$,
akkor r baloldali, s jobboldali nullosztó.

5.3.7. Lemma

Legyen $r \in R$ rögzített. Ekkor $\{x \in R : xr = 0\}$ balideál,
pontatlanul: az „r-hez tartozó" bal nullosztók balideált alkotnak.

Bizonyítás

Ha $xr = 0$ és $yr = 0$, akkor nyilván $(x \pm y)r = 0$.
Ha $xr = 0$ és $s \in R$, akkor pedig $(sx)r = s(xr) = s0 = 0$. □

Elnevezés: Ez az r elem bal oldali annullátora.
Fontos szerepet játszik a balideálmentes gyűrűk leírásában.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.

leképezés a természetes homomorfizmus G-ből G/N-re.

Faktorcsoport

Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

Ismétlés

Legyen G kommutatív csoport a $+$ műveletre.
Ha N részcsoport G-ben, akkor tehát normálosztó is.

leképezés a természetes homomorfizmus

G-ből G/N-re.

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

leképezés a természetes homomorfizmus

G-ből G/N-re.

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).

leképezés a természetes homomorfizmus
G-ből G/N-re.

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

leképezés a természetes homomorfizmus
G-ből G/N-re.

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,

leképezés a természetes homomorfizmus
G-ből G/N-re.

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,
a $g + N$ inverze $(-g) + N$.

leképezés a természetes homomorfizmus
G-ből G/N-re.

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

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, 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,

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, 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. □

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.

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

Példa polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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 polinomgyűrű faktorára

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

$f + I = g + I \iff f - g \in I \iff x^2+1 \mid f-g$.
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?
$(x+I)(x+I) = x^2 + I = -1 + ((x^2+1)+I) = -1 + I$.
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. $\quad I := (x^2+1)$.

$f + I = g + I \iff f - g \in I \iff x^2+1 \mid f-g$.
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?
$(x+I)(x+I) = x^2 + I = -1 + ((x^2+1)+I) = -1 + I$.
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 $\mathbb{C} \to \mathbb{R}[x]/(x^2+1)$.

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

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

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

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

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

Két alkalmazás

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\varphi : R \to S$ gyűrűhomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong R/\mathrm{Ker}(\varphi)$.

Bizonyítás: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$

A homomorfizmustétel

5.2.5 Homomorfizmustétel

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

Bizonyítás: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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: Nyilván $\mathrm{Im}(\varphi)^+$ és $R^+/\mathrm{Ker}(\varphi)^+$ 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 $\mathrm{Im}(\varphi) = \mathbb{Z}_n$ 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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.

Elemi 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 faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$,

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$, lesz a nullelem R-ben.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben,

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.
Nyilván $(f) \subseteq J$,

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \lhd R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.
Nyilván $(f) \subseteq J$, ezért $h \mid f$.

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.
Nyilván $(f) \subseteq J$, ezért $h \mid f$. Mivel (f) irreducibilis, vagy h egység,
így $I = R$,

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.
Nyilván $(f) \subseteq J$, ezért $h \mid f$. Mivel (f) irreducibilis, vagy h egység,
így $I = R$, vagy az f-nek egységszerese, és I az R nulla ideálja. $\square$

A faktorgyűrű mikor egyszerű

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy f irreducibilis, és legyen $T = T[x]/(f)$.
Elég belátni, hogy R egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test.
Nyilván $1 + (f)$ egységelem.
Ha $\big(g + (f)\big)\big(h + (f)\big)$ nulla R-ben, akkor $gh \in (f)$, azaz $f \mid gh$.
Mivel $T[x]$ alaptételes, minden irreducibilis eleme prím.
Ezért vagy $f \mid g$ vagy $f \mid h$. Az első esetben $g + (f)$,
a másodikban $h + (f)$ lesz a nullelem R-ben.
Ha $I \triangleleft R$, akkor álljon J azokból a $g \in T[x]$ polinomokból,
melyekre $g + (f) \in I$. Ez ideál $T[x]$-ben, ezért főideál: $J = (h)$.
Nyilván $(f) \subseteq J$, ezért $h \mid f$. Mivel (f) irreducibilis, vagy h egység,
így $I = R$, vagy az f-nek egységszerese, és I az R nulla ideálja. □

(J az I teljes inverz képe a természetes homomorfizmusnál.)

Polinomok „nemlétező” gyökei

Példa

A $z^2 + 1$-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.

Polinomok „nemlétező” gyökei

Példa

A $z^2 + 1$-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni. Ezért bevezettük $\mathbb{C}$-t,

Polinomok „nemlétező” gyökei

Példa

A $z^2 + 1$-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni. Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.

Polinomok „nemlétező” gyökei

Példa

A $z^2 + 1$-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

Polinomok „nemlétező” gyökei

Példa

A $z^2 + 1$-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2 + 1)$ izomorf $\mathbb{C}$-vel,

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg.

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak,

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek,

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) Azonosítsuk $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel,

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) Azonosítsuk $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel, és mutassuk meg, hogy ezek az elemek $\mathbb{R}$-rel izomorf résztestet alkotnak.

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) Azonosítsuk $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel, és mutassuk meg, hogy ezek az elemek $\mathbb{R}$-rel izomorf résztestet alkotnak.

(4) Definiáljuk i-t $x+(x^2+1)$-nek,

Polinomok „nemlétező” gyökei

Példa

A z^2+1-nek nincs gyöke $\mathbb{R}$-ben, de i-vel kényelmes számolni.
Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy testbővítését.
A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az i-nek megfelelő elem $x+(x^2+1)$.

(2) Definiáljuk $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) Azonosítsuk $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel, és mutassuk meg, hogy ezek az elemek $\mathbb{R}$-rel izomorf résztestet alkotnak.

(4) Definiáljuk i-t $x+(x^2+1)$-nek, és lássuk be, hogy ez gyöke a z^2+1 polinomnak.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$,

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván művelettartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben. Végezzük el a $k = k + (s)$ azonosítást

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben. Végezzük el a $k = k + (s)$ azonosítást
(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben. Végezzük el a $k = k + (s)$ azonosítást
(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).
Legyen $\alpha = x + (s) \in L$.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben. Végezzük el a $k = k + (s)$ azonosítást
(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).
Legyen $\alpha = x + (s) \in L$. Be kell látni, hogy α gyöke s-nek.

Testbővítés konstrukciója

6.4.3. Tétel

Ha K test, és s egy K fölött irreducibilis polinom,
akkor létezik olyan L test, amelyben K résztest,
és amelyben az s polinomnak már van gyöke.

Bizonyítás

Legyen $L = K[x]/(s)$, ez test, mert s irreducibilis.
A $k \mapsto k + (s)$ megfeleltetés nyilván műveletartó és injektív.
Ezért a $k + (s)$ elemek ($k \in K$) a K-val izomorf résztestet
alkotnak L-ben. Végezzük el a $k = k + (s)$ azonosítást
(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).
Legyen $\alpha = x + (s) \in L$. Be kell látni, hogy α gyöke s-nek.
Ezzel a bizonyítást be is fejezzük majd.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt $s(\alpha) =$

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt $s(\alpha) =$

$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt $s(\alpha) =$

$$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$$
$$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s),$$

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk. Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt $s(\alpha) =$

$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$

$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,

vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. $\square$

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

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

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$,

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$,
$0 = (x^2 + x + 1)$,

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$,

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.
Azonosítás: $O \leftrightarrow 0$,

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.
Azonosítás: $O \leftrightarrow 0$, $E \leftrightarrow 1$,

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.
Azonosítás: $O \leftrightarrow 0$, $E \leftrightarrow 1$, $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$.

Gyök a bővítésben

Bizonyítás (folytatás)

Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az s-et $L[z]$-beli polinomnak képzeljük, hogy α-t helyettesíthessünk.
Ezért s együtthatói a (k_j-vel azonosított) $k_j + (s)$ elemek.
Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$,
vagyis a $K[x]/(s)$ faktorgyűrű nulleleme.
Ezért α tényleg gyöke az s polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.
Azonosítás: $O \leftrightarrow 0$, $E \leftrightarrow 1$, $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$.
Az $\alpha = A$ elem tényleg gyöke $Ez^2 + Ez + E$-nek.

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám,

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás”

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű.

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re,

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re, ekkor R karakterisztikája p,

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re, ekkor R karakterisztikája p, vagy

(2) tetszőleges $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$ esetén $nr \neq 0$,

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re, ekkor R karakterisztikája p, vagy

(2) tetszőleges $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$ esetén $nr \neq 0$, ekkor R karakterisztikája 0.

Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha R gyűrű, $r \in R$ és $n \geq 0$ egész szám, akkor nr azt jelenti, hogy r-nek n példányát összeadjuk.
Ha $n < 0$, akkor nr a $(-n)r$ ellentettje (ami $(-n)(-r)$ is).

Ez R additív csoportjában a „hatványozás” (többszörös).

5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy

(1) van olyan $p \in \mathbb{Z}$ prímszám, hogy $pr = 0$ minden $r \in R$-re, ekkor R karakterisztikája p, vagy

(2) tetszőleges $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$ esetén $nr \neq 0$, ekkor R karakterisztikája 0.

Valójában R^+ elemeinek rendjeit írjuk le.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$,

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (jó együtthatója) r-nek,

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (jó együtthatója) r-nek, és így $m = o(r) \mid n$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s$

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$,

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r$$

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben
$m = o(r) \mid a$,

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben $m = o(r) \mid a$, vagyis $a \mid m$ miatt $a = m$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben $m = o(r) \mid a$, vagyis $a \mid m$ miatt $a = m$. A második esetben ugyanígy kapjuk, hogy $b = m$.

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additív csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője" (jó együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Ha $s \in R$, akkor $0 = (mr)s = r(ms)$.
Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik.
Tehát $o(s)$ véges, és osztója $m = o(r)$-nek.
Az r és s szerepét kicserélve $s \neq 0$ esetén $o(s) = o(r) = m$.
Az (1)-hez már csak azt kell megmutatni, hogy m prímszám.
Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben $m = o(r) \mid a$, vagyis $a \mid m$ miatt $a = m$. A második esetben ugyanígy kapjuk, hogy $b = m$. Ezért m tényleg prímszám. □

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

ψ szorzattartása nyilvánvaló, mert R kommutatív.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

ψ szorzattartása nyilvánvaló, mert R kommutatív.
Az összegtartás a binomiális tételből következik.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

ψ szorzattartása nyilvánvaló, mert R kommutatív.
Az összegtartás a binomiális tételből következik.
Elemi számelmélet: $\binom{p}{j}$ osztható p-vel, ha $0 < j < p$.

A Frobenius-endomorfizmus

5.8.4. Tétel

Legyen R kommutatív, p karakterisztikájú gyűrű, ahol p prím.
Ekkor R-ben tagonként lehet p-edik hatványra emelni:

$$(r+s)^p = r^p + s^p \qquad (r, s \in R).$$

Ezért a $\psi(r) = r^p$ leképezés gyűrűhomomorfizmus R-ből R-be.
Neve: Frobenius-endomorfizmus.
Ugyanez az állítás érvényes p hatványaira is.

Endomorfizmus: önmagába képző homomorfizmus.

ψ szorzattartása nyilvánvaló, mert R kommutatív.
Az összegtartás a binomiális tételből következik.
Elemi számelmélet: $\binom{p}{j}$ osztható p-vel, ha $0 < j < p$.
A p^k-ra emelés ψ^k (k tényezős kompozíció). □

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test,

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest,

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem. Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem. Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem. Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem. Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.
Legszűkebb: Legyen $K \leq T$ résztest.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.
Legszűkebb: Legyen $K \leq T$ résztest.
Ekkor $K \neq \{0\}$, és így $K^\times$ részcsoportja $T^\times$-nek.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.
Legszűkebb: Legyen $K \leq T$ résztest.
Ekkor $K \neq \{0\}$, és így $K^\times$ részcsoportja $T^\times$-nek.
Ezért T egységeleme, $e \in K$.

Prímtest p karakterisztikában

5.8.7. Tétel

Legyen T egy $p > 0$ karakterisztikájú test, e az egységelem.
Ekkor $P = \{0, e, 2e, 3e, \ldots, (p-1)e\}$ $\mathbb{Z}_p$-vel izomorf résztest, amely T minden résztestének része (legszűkebb résztest).

A legszűkebb résztest neve: P a T prímteste.

Bizonyítás

Mivel $e \neq 0$ de $pe = 0$, az e elem rendje p.
Ezért P részcsoport és $m \mapsto me$ izomorfizmus $\mathbb{Z}_p^+$ és P^+ között.
Ez tartja a szorzást is: $(me)(ne) = (mn)e^2 = (mn)e$.
Legszűkebb: Legyen $K \leq T$ résztest.
Ekkor $K \neq \{0\}$, és így $K^\times$ részcsoportja $T^\times$-nek.
Ezért T egységeleme, $e \in K$. Így $P \subseteq K$. □

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test,

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest,

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált,

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált,
és izomorfizmus $\mathbb{Q}$ és P között.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált,
és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált,
és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván. Injektív: elég, hogy $\mathrm{Ker}(\psi) = \{0\}$.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván. Injektív: elég, hogy $\mathrm{Ker}(\psi) = \{0\}$.
Ha $(me)/(ne) = 0$ akkor $me = 0$,

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván. Injektív: elég, hogy $\mathrm{Ker}(\psi) = \{0\}$.
Ha $(me)/(ne) = 0$ akkor $me = 0$, ezért $m = 0$ mert $o(e) = \infty$.

Prímtest 0 karakterisztikában

5.8.7. Tétel

Legyen T egy 0 karakterisztikájú test, e az egységelem.
Ekkor $P = \{(me)/(ne) : m, n \in \mathbb{Z},\ n \neq 0\}$ egy $\mathbb{Q}$-val izomorf résztest, amely T minden résztestének része (prímtest).

Bizonyítás

Mivel $e \neq 0$ és a karakterisztika 0, az e elem rendje végtelen.
Ellenőrizni kell, hogy $\psi : m/n \mapsto (me)/(ne)$ jóldefiniált, és izomorfizmus $\mathbb{Q}$ és P között. Művelettartó: nyilván.
Jóldefiniált: $m/n = u/v \implies (me)/(ne) = (ue)(ve)$ HF.
Továbbá $ne \neq 0$ ha $n \neq 0$, mert e rendje végtelen.
Szürjektív: nyilván. Injektív: elég, hogy $\mathrm{Ker}(\psi) = \{0\}$.
Ha $(me)/(ne) = 0$ akkor $me = 0$, ezért $m = 0$ mert $o(e) = \infty$.
Legszűkebb: mint a p karakterisztikájú esetben. □